



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

- CTE Agent AIX Integration Guides 3
 - Using CTE with Oracle 3
 - CTE on Oracle ACFS Overview 3
 - Creating an Oracle ASM Disk Group for Guarding 5
 - Oracle RAC ASM 11
 - Important ASM Commands and Concepts 11
 - Determining the Best Method for Encrypting Disks 13
 - General Prerequisites 14
 - Specific Prerequisites 15
 - About Oracle RAC ASM Raw Devices 16
 - Oracle RAC ASM Multi-Disk Online Method 16
 - Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore) 18
 - Surviving the Reboot and Failover Testing 19
 - Basic Troubleshooting Techniques 20
 - Using CTE with PowerTech Antivirus 22

CTE Agent AIX Integration Guides

This document covers the following information:

- Using CTE with Oracle
- Using CTE with PowerTech Antivirus

Using CTE with Oracle

This section describes how to install and configure CTE on Oracle RAC ASM, how to use an ASM Filter Driver as well as install and use CTE for AIX with Oracle Automated Storage Management (ASM™) Cluster File System (ACFS™) . It contains the following topics:

- CTE on Oracle ACFS Overview
- Oracle RAC ASM
- Creating an Oracle ASM Disk Group for Guarding
- About Oracle RAC ASM Raw Devices
- Oracle RAC ASM Multi-Disk Online Method
- Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)
- Surviving the Reboot and Failover Testing
- Basic Troubleshooting Techniques

CTE on Oracle ACFS Overview

CTE enables data protection of Oracle Automatic Storage Management Cluster File System (Oracle ACFS) on **secvm** volumes as part of the Oracle ASM stack. Oracle ACFS configured with **secvm** block devices is intended for use solely by the Oracle RAC application set to store related Oracle generated data such as:

- Oracle-generated related database files:
 - database datafile
 - control files
 - redo log files
 - archive log files
- Oracle-generated database backup files:

- hot/cold
- rman
- datapump exports
- Oracle-generated database TDE local wallet files

Note

CTE on ACFS only provides encryption. It does not provide access control.

For other files such as manually created shell scripts that require staging in a shared storage device, use other shared storage setups such as Veritas shared storage or share NFS mount.

Oracle RAC	Oracle RAC
Oracle ACFS (File System)	Oracle ADVM (Volume Manager)
Oracle ASM (Storage Manager)	SecVM

On Oracle, ACFS is layered on ASM disks, which in turn are built on **secvm** block devices. **secvm** is a proprietary device driver that supports GuardPoint protection to raw devices. **secvm** is inserted in between the device driver and the device itself.

Key Managers and SecVM

Server-side administrators must ensure that all **secvm** guards for an Oracle cluster use the same policies for encryption and access control.

Host Groups and Identical Keys and Policies

Thales recommends that you deploy host groups to ensure that identical policies and keys are applied on all nodes of the ACFS cluster. This is faster and less error-prone.

Restrictions and Caveats

- Thales does not support **secfs** layered on ACFS.
- Oracle ACFS encryption in conjunction with **secvm** encryption might impact performance.

Creating an Oracle ASM Disk Group for Guarding

Creating a new ASM Disk Group

Note

This document is for Oracle 19c on AIX 7.

1. List the available cluster shared disks, type:

```
xiv_devlist
```

Response

```
IBM storage devices
```

```
-----
Device          Size (GB)  Paths  Vol Name                                Vol ID
Storage ID      Storage Type Hyper-Scale Mobility
-----
/dev/hdisk2     51.6      2/2    sjaix81lpar069_sjaix81lpar079_vol_001  1053
7825664         XIV              Idle
-----
/dev/hdisk3     154.9     2/2    sjaix81lpar069_sjaix81lpar079_vol_002  1054
7825664         XIV              Idle
-----
/dev/hdisk4     154.9     2/2    sjaix81lpar069_sjaix81lpar079_vol_003  1055
7825664         XIV              Idle
-----
/dev/hdisk5     154.9     2/2    sjaix81lpar069_sjaix81lpar079_vol_004  1056
7825664         XIV              Idle
-----
/dev/hdisk6     51.6      2/2    sjaix81lpar069_sjaix81lpar079_vol_005  1075
7825664         XIV              Idle
-----
```

2. Ensure that the disks are available, type:

```
/usr/sbin/lssdev -Cc disk
```

Response

```
hdisk0 Available          Virtual SCSI Disk Drive
```

```

hdisk1 Available          Virtual SCSI Disk Drive
hdisk2 Available C5-T1-01 MPIO 2810 XIV Disk
hdisk3 Available C5-T1-01 MPIO 2810 XIV Disk
hdisk4 Available C5-T1-01 MPIO 2810 XIV Disk
hdisk5 Available C5-T1-01 MPIO 2810 XIV Disk
hdisk6 Available C5-T1-01 MPIO 2810 XIV Disk

```

3. To identify the device names for the physical disks that you want to use, type the following on any node:

```
/usr/sbin/lspv | grep -i none
```

Response

```

hdisk1          00fa0087e313f5c9          None
hdisk2          none                      None
hdisk3          none                      None
hdisk4          none                      None
hdisk6          none                      None

```

4. Select available candidate disks for a new ASM disk group. On the Oracle system, type:

```

SYS@+ASM2> COLUMN path format a20

SYS@+ASM2> SELECT name, header_status, path FROM V$ASM_DISK;

```

Response

```

NAME                                HEADER_STATUS PATH
-----
FORMER                               /dev/rhdisk1
FORMER                               /dev/rhdisk2
CANDIDATE                            /dev/rhdisk3
TDE1_0000                            MEMBER        /dev/rhdisk4
GRID_0000                            MEMBER        /dev/rhdisk6

```

5. Prepare the Targeted Disk for CTE and ASM Diskgroup creation:

```

chown grid:dba /dev/rhdisk3
chmod 660 /dev/rhdisk3
dd if=/dev/rhdisk3 of=zzz bs=4k count=1

```

Response

```
1+0 records in.
1+0 records out.
```

6. In CipherTrust Manager, create a key with the following characteristics:
 - Encryption mode: CBC
 - Algorithm: AES
 - Size: 128 or 256
7. Create a CipherTrust Transparent Encryption policy for Oracle on AIX.
 - a. Create a CBC key with CBC-AES128 or CBC-AES256.
 - b. Create a Security Rule:
 - **Action:** all_ops
 - **Effect:** Audit, Permit, Apply Key
 - c. Create a Key Selection Rule:
 - **Key:** cte_cbc_aes256_key
 - d. Guard your targeted RAC raw devices so that you can use the secvm disk to create a guarded Oracle RAC ASM or ASMLib disk group.

```
/dev/rhdisk3
```

- **Type** = Raw or Block Device (Auto or Manual Guard)

Once you guard your target, CipherTrust Transparent Encryption creates the following:

```
/dev/secvm/dev/rhdisk3
```

8. Install the same version of CipherTrust Transparent Encryption on all nodes in the cluster. To check the version, type:

```
vmd -v
```

Response

```
Version 7, Service Pack 3
7.3.0.35
2022-09-23 02:08:46 (PDT)
```

Copyright (c) 2009-2022, Thales Inc. All rights reserved.

9. Guard targeted disk on all cluster nodes.

a. Check the guard status of the disk on all cluster nodes, type:

```
secfsd -status guard
```

Response

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/dev/rhdisk3	encrypt_cbc_aes256_all	rawdevice	guarded	guarded	N/A

b. List the devices, type:

```
ls -l /dev/secvm/dev/rhdisk3

crw-rw----  1 grid  dba          43,  1 Sep 28 15:21 /dev/secvm/dev/rhdisk3
```

10. Add the following client settings for both RAC nodes that are set in the \$GRID_HOME & \$ORACLE_HOME variables.

```
echo $GRID_HOME
```

Response

```
/u01/app/19.0.0/grid
```

```
echo $ORACLE_HOME
```

Response

```
/u01/app/oracle/product/19.0.0/db_1
```

For each node in the cluster, in the client settings, type:

```
|authenticator_euid|/u01/app/19.0.0/grid/bin/grid
|authenticator_euid|/u01/app/19.0.0/grid/bin/orarootagent.bin
|authenticator_euid|/u01/app/oracle/product/19.0.0/db_1/oracle
```

```
|authenticator_euid|/u01/app/oracle/product/19.0.0/db_1/bin/oracle
```

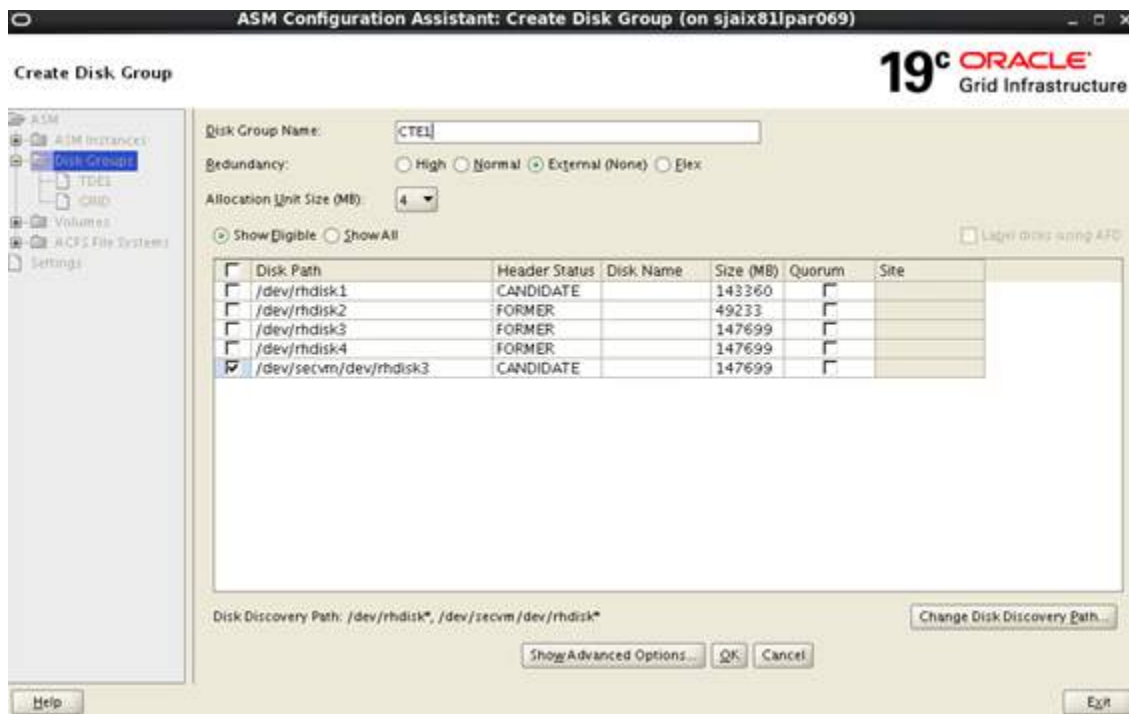
Note

This step is optional because it does not effect Oracle behavior. However, without these setting, CipherTrust Transparent Encryption can generate authentication error messages in the CTE log in `/var/log/vormetric`. These errors do not interfere with Oracle functions.

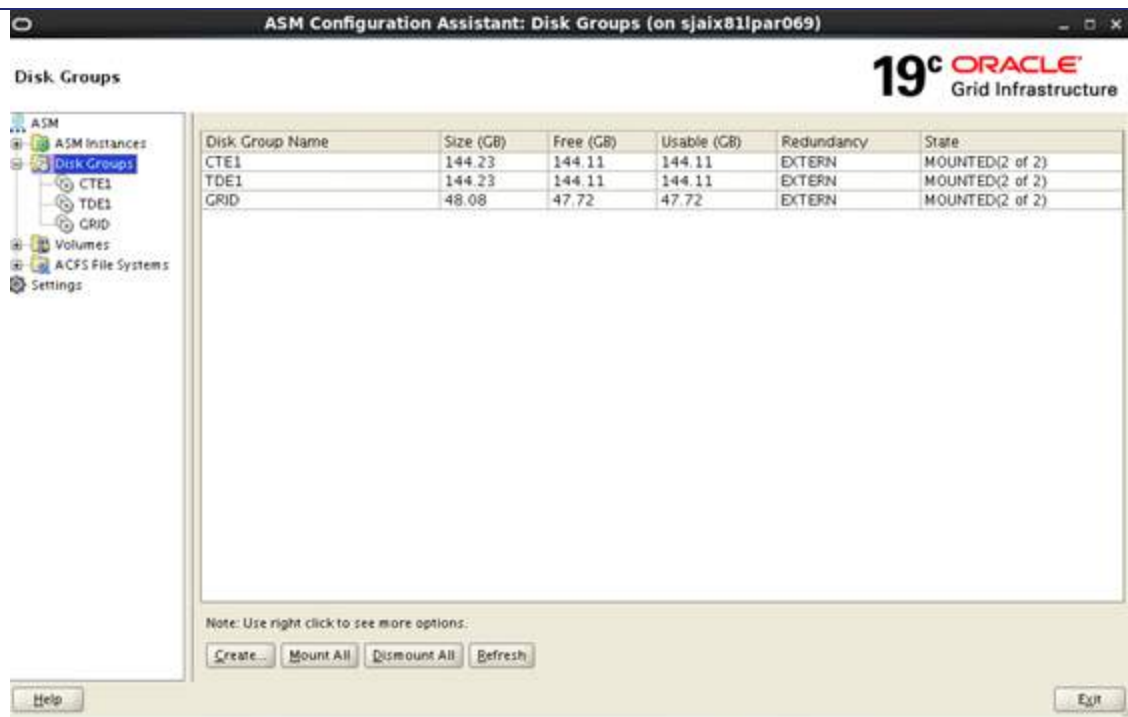
11. Launch the GUI for the GRID (`./asmca`) to create the new CipherTrust Transparent Encryption guarded ASM disk group:
12. Update the discovery path to the following in order for both the baseline and guarded disks to be found:

```
/dev/rhdisk*,/dev/secvm/dev/rhdisk*
```

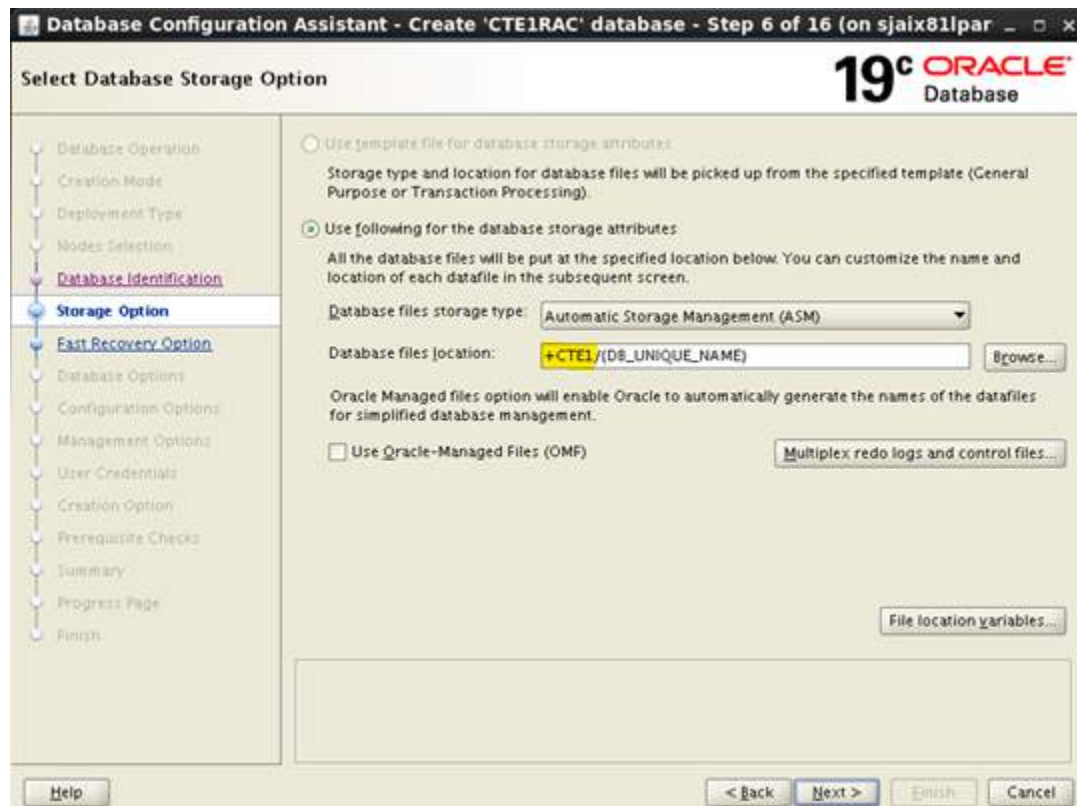
13. Select targeted `rhdisk3` disk with the guarded path of `secvm`.



14. The end result should show your new CTE guarded ASM disk group called CTE1.



15. When creating your RAC database, choose DB files to reside in the CTE guarded ASM disk group that you just created:



You can now use the secvm disk that you created to create a guarded Oracle RAC ASM or ASMLib disk group.

Oracle RAC ASM

This section describes how to install and configure CTE on an Oracle RAC ASM.

Using CTE with an Oracle RAC ASM

You can apply CTE when the Oracle DB is active or inactive. If you choose to use it while the Oracle DB is active, it eliminates any downtime. You can apply CTE during low volume traffic time frames. If you choose to use this option, then use the **rebalance** function of ASM. This allows you to:

1. Migrate data off of a disk so that it can be dropped/removed from a **Diskgroup**.
2. Apply CTE protection.
3. Add the disk back into the diskgroup.

Caution

If you drop a disk from an ASM diskgroup, then add it back to the diskgroup without cleanly wiping the disk, the ASM diskname will be corrupted. To avoid this problem, clear out the disk before you add it back to diskgroup. Example: `dd if=/dev/zero of=/dev/secvm/dev/mapper/asmdg-asm1v002 bs=32k`

- [Important ASM Commands and Concepts](#)
- [Determining the Best Method for Encrypting Disks](#)
- [General Prerequisites](#)
- [Specific Prerequisites](#)

Important ASM Commands and Concepts

Rebalancing Disks

When you drop/remove a disk from the diskgroup, it is important to apply the proper value for the power setting for rebalance and to use the **WAIT** command.

Example ASM Command:

```
SQL> ALTER DISKGROUP <DiskGroupName> DROP DISK <diskName> REBALANCE POWER 8 WAIT;
```

- The rebalance command moves the data off of the disk that you are removing from the diskgroup, distributing the data across the remaining DISKS.
- The power setting is a number from 1 to 11. It determines how much processing power is dedicated to the

rebalance, versus normal operations. Unless the encrypting occurs during heavy traffic volume, the minimum value you should use is 6. Otherwise, consult the customer's DBA for the proper setting. An appropriate value to start with is 8.

Mapping Raw Devices

You can map raw devices for this configuration using:

- **EMC PowerPath**

If using EMC PowerPath then the device names are similar to the following: `/dev/hdiskpowerXX`.

When browsing the CipherTrust Manager through the local host, you cannot find Power Path devices. You must manually input the paths. The guarded disk names are prepended with: `/dev/secvm`.

Checking Rebalance Status

The `wait` command is very important when ASM performs a rebalance. When you specify `wait`, the command prompt does not display until all of the data is rebalanced and migrated off of the disk. If you do not specify `wait`, the command prompt returns immediately, and you must issue the following ASM command to check the status of the rebalance:

```
SQL> select * from v$asm_operation;
```

This command returns information about the:

- State
- Current power level
- Current amount rebalanced
- Estimated work until completion
- Rate
- Estimated minutes
- Any error codes

Note

It is highly recommended that you always specify the `wait` command when performing a **Drop Disk** with Rebalance. If it is not specified, ASM may prematurely release the disk, thereby allowing CTE to place a GuardPoint on the disk before the rebalance completes. This action may corrupt the data.

Oracle cautions against this issue:

Caution

The **ALTER DISKGROUP . . . DROP DISK** statement returns before the drop and rebalance operations complete. Do not reuse, remove, or disconnect the dropped disk until the **HEADER_STATUS** column in the **V\$ASM_DISK** view for this disk changes to **FORMER**. You can query the **V\$ASM_OPERATION** view to determine the amount of time remaining for the drop/rebalance operation to complete. For more information, refer to the *Oracle Database SQL Language Reference and the Oracle Database Reference.

Determining the Best Method for Encrypting Disks

A diskgroup can contain one or multiple disks. You must determine if the diskgroup contains enough disks and free space for encryption. If the diskgroup contains only one disk, or multiple disks but not enough free space, then you must use the **Offline** (backup/restore) method for encryption.

If the diskgroup contains more than one, you can use the **Online** (rebalancing) method. During rebalancing, additional disks allow for migrating data from the original disk so that it can be encrypted, added back into the diskgroup, and then migrated back to the source disk. Therefore, if the customer does not want to permanently add extra disks, they can add disks temporarily, just for rebalancing.

In general, once you have completed the initial setup for the operating system with which you are working, for both ASM or ASMLib, the high-level process is the same for applying CTE protection to raw devices and using them.

Online Method (No Application / Database Downtime)

Typically, when using the online method, follow these steps:

1. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.
2. Apply CTE encryption to the disk.
3. Add each protected disk to the diskgroup.
4. Restart the nodes and the failover test.
5. Repeat the previous steps for each disk in the diskgroup.

Offline Method (Backup the DB)

Typically, when using the offline method, follow these steps:

1. Backup the database.
2. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.

3. Stop the Oracle database.
4. Delete the diskgroup.
5. Apply CTE encryption to the disk.
6. Recreate the diskgroup.
7. Add the protected disk to the diskgroup.
8. Restart the nodes and the failover test.
9. Repeat the previous steps for each disk in the diskgroup.

General Prerequisites

Setup

- Verify that you have a current backup of the database
- Install and register CTE agents on all RAC node Hosts
- Create a **Host Group** and add all RAC node hosts as members
- Create an encryption key for the Oracle RAC Database / Application
- Create an Oracle policy using the proper encryption key

Note

If the raw device mappings for the disk(s) are **not** identical across all nodes in the RAC, then you cannot use a Host Group for managing the GuardPoint within the CipherTrust Manager. You **must** apply the GuardPoint to each Host individually. This is typically not optimal, as a Host Group is the most effective and consistent way to manage GuardPoints for Oracle RAC environments.

Altering ASM_DISKSTRING on ASM

ASM uses the `asm_diskstring` setting to identify the path where ASM will attempt to locate available disks to use. If you are using device names when adding the disk, you must modify the string to include the path to SecVM.

1. To retrieve the `ASM_DISKSTRING` setting, type:

```
SQL> SHOW PARAMETER ASM_DISKSTRING
```

2. To modify the setting, type:

```
SQL> ALTER SYSTEM SET ASM_DISKSTRING='/dev/*', '/dev/secvm/dev/*';
```

Where the path added is the path to SecVM.

Specific Prerequisites

Establishing a Starting Point

In many production environments, you may find that it has been a very long time since the RAC nodes have had the services restarted or have been completely rebooted. This can result in a lack of understanding of the actual state of the RAC cluster and its ability to survive a reboot on its own, prior to installing CTE.

Restarts can uncover issues in the RAC environment that are unrelated to CTE. To avoid issues after a CTE installation, Thales recommends that you restart each RAC node **AFTER** CTE is installed and **PRIOR** to establishing any GuardPoints. This may not be feasible in a single node configuration. However, by doing so, CTE is installed but inactive, and you can ensure that the platform is in a workable state prior to getting started.

The Importance of Device Mapping

It is important to use device naming and mapping in a multi-node RAC configuration. Verify the device names to ensure that the disks are mapped to the same disks on each RAC node before applying any GuardPoints. Thales recommends that RAC nodes use the same device names across all nodes. If they do not match, then problems can occur.

If the RAC nodes use the same device names, use a Host Group to create GuardPoints. If they do not match, do not use a Host Group to create GuardPoints. Set them up independently on each Host.

Important Note about Raw Devices on AIX

In general, raw devices are created as either character or block mode devices. Any I/O performed on character devices is non-buffered, while I/O on block devices is buffered and performed in defined block sizes (that is, 4K bytes).

While the Oracle documentation for using ASM with raw devices indicates that you can use either character or block devices, **CTE REQUIRES a block device for guarding.**

Note

- Attempting to apply a GuardPoint on a character device that does not have a corresponding block device may result in a GuardPoint that never encrypts data. The status of the GuardPoint never shows as guarded.
- The WebUI does not support browsing for the character devices. You would need to manually paste the name into the WebUI.

Once guarded, CTE creates both a character and block mode version of the guarded device. Oracle ASM can use either device.

About Oracle RAC ASM Raw Devices

Standard Devices

In many cases the ASM configuration may be using plain device names, like the following:

`/dev/hdisk1`

Note

If you use standard device names in the ASM configuration to add a disk, you must modify the `ASM_DISKSTRING` parameter to include the `/dev/Secvm/dev/*` path.

Consistent Naming of Devices across RAC Nodes

As previously stated, if the raw device mappings for the disk(s) are **NOT** identical across all nodes in the RAC, then you **CANNOT** use a Host Group and you **MUST** apply the GuardPoints to each Host individually. This is typically NOT optimal, as a Host Group is the most effective way to manage an Oracle RAC environment.

Oracle RAC ASM Multi-Disk Online Method

Performing encryption with the online rebalancing method requires sufficient free space to allow the drop of the largest ASM disk.

Checking for Space

In the Oracle system, use the following commands to check for available disk space:

1. Check total free space in the disk group:

```
SQL> SELECT name, free_mb, total_mb, free_mb/total_mb*100 as percentage FROM
v$asm_diskgroup;
```

NAME	FREE_MB	TOTAL_MB	PERCENTAGE
DATA	7	2109	.331910858

2. Check individual ASM disk size and usage:

```
SQL> select a.name DiskGroup, b.disk_number Disk#, b.name DiskName, b.total_m
b, b.free_mb, b.path, b.header_status FROM v$asm_disk b, v$asm_diskgroup a whe
re a.group_number (+) =b.group_number order by b.group_number, b.disk_number,
b.name
```

DISKGROUP	DISK#	DISKNAME	TOTAL_MB	FREE_MB	PATH
HEADER_STATUS					
-----	-----	-----	-----	-----	
DATA	0	DATA_0000	1874	1273	/dev/oracleasm/disks/D
ATA3	MEMBER				
DATA	1	DATA_0001	1992	608	/dev/oracleasm/disks/D
ATA4	MEMBER				
DATA	3	DATA_0003	117	0	/dev/oracleasm/disks/D
ATA2	MEMBER				
	0	DATA_ENC_0000	109	28	/dev/oracleasm/disks/D
ATA1_ENC	MEMBER				

Adding a Disk to the Diskgroup

Using the Online Method assumes that there is enough free space in the diskgroup so that you can drop/remove a disk, protect it with CTE, and then add it back into the diskgroup.

To add the disk to the diskgroup:

1. Open a terminal session on both RAC Nodes.
2. On **RAC Node 1**, on the ASM, remove the disk from the disk group, type.

```
SQL> ALTER DISKGROUP <diskGroupName> DROP DISK <diskName> REBALANCE POWER 11 WAIT;
```

3. On both **RAC Node 1** and **2** type:

```
chown oracle:oinstall /dev/<rawDevice1Name>
chmod 660 /dev/<rawDevice1Name>
```

4. On the CipherTrust Manager, in the Host Group, apply a GuardPoint to the Raw Device: `<rawDevice1Name>`.
5. From **RAC Node 1**, to display the status of the guarded disks, type:

```
secfsd -status guard
```

6. On both **RAC Node 1** and **2** type:

```
chown oracle:oinstall /dev/secvm/dev/<rawDevice1Name>
```

```
chmod 660 /dev/secvm/dev/<rawDevice1Name>
```

7. From **RAC Node, on the ASM**, add the protected disk to the disk group:

```
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/dev/<rawDevice1Name>
NAME <disk1Name>;
```

The disk is now added to the diskgroup and ready for use.

8. The system is now ready for a reboot and failover test. For details, see [Surviving the Reboot and Failover Testing](#).

Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)

Using the Offline Method assumes that there is not enough free space in the diskgroup.

1. Open a terminal session on both RAC Nodes.
2. On RAC Node 1, on the ASM, type the following to remove the disk group.

```
SQL> DROP DISKGROUP <diskGroupName> FORCE INCLUDING CONTENTS;
```

Note

Make sure that the disk is removed before guarding the raw devices.

3. On both **RAC Node 1** and **2** type:

```
chown oracle:oinstall /dev/<rawDevice1Name>
chmod 660 /dev/<rawDevice1Name>
chown oracle:oinstall /dev/<rawDevice2Name>
chmod 660 /dev/<rawDevice2Name>
chown oracle:oinstall /dev/<rawDevice3Name>
chmod 660 /dev/<rawDevice3Name>
```

4. On the CipherTrust Manager, in the Host Group, apply GuardPoints to the three raw devices:

```
<rawDeviceName1>
<rawDeviceName2>
<rawDeviceName3>
```

- On **RAC Node 1**, to display the status of the guarded disks, type:

```
secfsd -status guard
```

- On both **RAC Node 1** and **2**, type:

```
chown oracle:oinstall /dev/secvm/dev/<rawDeviceName1>
chmod 660 /dev/secvm/dev/<rawDeviceName1>
chown oracle:oinstall /dev/secvm/dev/<rawDeviceName2>
chmod 660 /dev/secvm/dev/<rawDeviceName2>
chown oracle:oinstall /dev/secvm/dev/<rawDeviceName3>
chmod 660 /dev/secvm/dev/<rawDeviceName3>
```

- From **RAC Node 1**, on the **ASM**, add the protected disk to the disk group, type:

```
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/dev/<rawDeviceName1>
NAME <diskName1>;
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/dev/<rawDeviceName2>
NAME <diskName2>;
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/dev/<rawDeviceName3>
NAME <diskName3>;
```

The disks are now added to the diskgroup and ready for use.

- On **RAC Node 1**, restore the database.
- The system is now ready for a reboot and failover test. Go to the [Surviving the Reboot and Failover Testing](#).

Surviving the Reboot and Failover Testing

Failover Testing

Confirm that everything is functional:

- Ensure that the GuardPoints are all operational.
- Ensure that you receive valid results when you query the database.
- Verify that the load order ensures that CTE starts before ASM.

Once verified, you can start the failover testing for each RAC Node.

- Reboot the RAC Node 1 and monitor the startup.
- Once the restart is clean, reboot RAC Node 2 and monitor the startup.

Basic Troubleshooting Techniques

The following are some of the most common configuration issues that prevent the Oracle ASM configuration from working properly.

If you encounter errors similar to:

- ORA-15075: disk(s) are not visible cluster-wide
- ORA-15032: not all alterations performed

This could be the result of improper settings for the I/O layer, meaning that your disks are not properly configured.

Perform the following tasks to verify that the settings are correct:

1. On the CipherTrust Manager, in the Host Group that was created for the RAC cluster, verify that the host group for this configuration does **NOT** have the Cluster Group option set (this option is only for GPFS, which is not supported with CTE).
2. Ensure that the GuardPoints for the block devices are set at the Host Group level. This ensures that each node receives identical GuardPoints.
3. Verify that the GuardPoints are active on all nodes. When the GuardPoints are set, go to each node and verify that they are set and guarded, using the WebUI or the `secfsd -status guard` command. If they do not guard correctly, make sure the device names are the same across all nodes.
4. From ASM, make sure that the `asm_diskstring` parameter is modified to include the CTE devices and that the proper pathname is used, see [Altering ASM_DISKSTRING on ASM](#).

Verifying Database Encryption

Option 1

The best way to verify the state of the data, without impacting anything in the existing environment, is to use the Oracle `kfed` command. You can run this command against the native path of the existing GuardPoints and make sure it returns with valid header information. If it returns valid information with the GuardPoint in place, then this confirms that the data is properly encrypted. If it returns with invalid header information, then that indicates that the data is either clear, double encrypted, or not in the expected encrypted state. The syntax for running this command would look similar to the following but will vary based on your environment.

```
/app/oracle/grid/product/19.0.0/grid/bin/kfed read /dev/<diskName>
```

If the location is properly encrypted, following is an example of the viewable output:

```
/app/oracle/grid/product/19.0.0/grid/bin/kfed read /dev/<diskName>
```

System Response:

```
kfbh.endian: 1 ; 0x000: 0x01
```



```

kfbh.hard:                242 ; 0x001: 0xf2
kfbh.type:                124 ; 0x002: *** Unknown Enum ***
kfbh.datfmt:              66 ; 0x003: 0x42
kfbh.block.blk:          1088904227 ; 0x004: blk=1088904227
kfbh.block.obj:          1558192170 ; 0x008: file=8234
kfbh.check:              3321251423 ; 0x00c: 0xc5f6465f
kfbh.fcn.base:           932956641 ; 0x010: 0x379bc9e1
kfbh.fcn.wrap:           3040493590 ; 0x014: 0xb53a4016
kfbh.spare1:             3806015223 ; 0x018: 0xe2db2ef7
kfbh.spare2:             3794962182 ; 0x01c: 0xe2328706
60000000000D8000 01F27C42 40E75C23 5CE0202A C5F6465F
[...|B@.\#\..*..F_]
60000000000D8010 379BC9E1 B53A4016 E2DB2EF7 E2328706 [7.....:@.....2..]
60000000000D8020 CA2F30AD 522B4D21 99292639 004EBB34 [./0.R+M!.)&9.N.4]
60000000000D8030 A3896BE8 BD839D23 2204E19E 946C575C [...k....#"....lW\]
60000000000D8040 4CE2218F 35E1B101 AF751A70 780E6D6E [L!.5....u.px.mn]
60000000000D8050 5E7E6A38 C600ED5F 929047C4 DF372A8E [^~j8..._.G..7*.]
60000000000D8060 E103152D BA87CC03 11A7D963 9D72FCE1
[...-.....c.r..]
60000000000D8070 1EC6B48B 03EE869F 61D651F9 E7614957 [.....a.Q...aIW]
60000000000D8080 810E0353 9C461F49 69569733 501D19EF [...S.F.IiV.3P...]
60000000000D8090 B268002B 4F9457B6 BDB04AC5 D3D07446 [.h.+0.W...J...tF]
60000000000D80A0 FD9EE5E0 9B46CB66 30D10B22 F63AB77E [.....F.f0..."..~]
60000000000D80B0 6FF79075 4BBD1FAD 8F226188 7774300D [o..uK...."a.wt0.]
60000000000D80C0 A809B6FB E1F1C80B B5760E68 9747D97D [.....v.h.G.}]
KFED-00322: Invalid content encountered during block traversal: [kfbtTraverseBlock][Invalid OSM block type][124]

```

Option 2

The second option to verify the state of the data is to use the `dd` command. This requires you to specify some blocks and write it out to a file. After this completes, read the file using the `strings` command. You can do this while the device is in use. In the example below some sectors are skipped and it only dumps 10000 counts.

For example:

```
dd if=/dev/asm_data2p1 of=/tmp/dd2.out skip=1047 count=10000
```

Option 3

The third option to verify the state of the data without impacting the existing environment is to use the `strings` command.

Note

The `strings` command cannot read a busy or large device.

You can run this command against the native path (`/dev/<deviceName>`) of the existing GuardPoints (`/dev/secvm/dev/<deviceName>`). By executing the `strings` command against the native path `strings /dev/devicename | more`, this does not go through the SecVM device and therefore is not be decrypted. If it is encrypted the output should contain illegible text.

Using CTE with PowerTech Antivirus

When Powertech Antivirus is configured to use **on-access scanning**, CipherTrust Transparent Encryption Data Transformation may find files within the Data Transformation GuardPoint that are busy. These files are not processed by Data Transformation and are left unencrypted.

Note

This problem only occurs if Powertech is configured to use **on-access scanning**. This problem **does not** occur when using **on-demand scanning**.

Issue

When Powertech uses **on-access scanning**, it opens a file and keeps it open. Before the Data Transformation program encrypts a file, it checks to see if the file is in use by another process. If the file is in use, Data Transformation does not encrypt the file but rather appends the path to the file in the **dataxform_status_error-<guardpoint>** file located in **/var/log/vormetric/**. This prevents any retry of Data Transformation from succeeding.

Resolving PowerTech/Data Transformation "in-use" Errors

For the following scenario, Powertech is configured with **on_access scanning** and both Powertech and the Thales CTE agent have been installed at default locations. The example assumes the Data Transformation GuardPoint is **/test-dataxform**.

Running Data Transformation with Powertech Antivirus code deactivated

1. Type the following to prevent the Powertech package from starting on system boot.

```
/opt/sgav/avsvcctl disable
```

2. Reboot the system.
3. After the system restarts, verify that Powertech is not running, type:

```
/opt/sgav/avsvcctl status
```

Response

```
The following output indicates Powertech is not running:  
Subsystem Group PID Status  
avsvc powertech inoperative  
Device driver is not loaded
```

4. Perform a Data Transformation conversion on the Data Transformation GuardPoints.

Example

```
dataxform --rekey --gp /test-dataxform
```

5. Enable Powertech to start after system boot, type:

```
/opt/sgav/avsvcctl enable
```

6. Start Powertech, type:

```
/opt/sgav/avsvcctl start
```

Response

There is a delay before Powertech is completely loaded and active. The Powertech status may be found by the following command.

7. Verify the status, type:

```
/opt/sgav/avsvcctl status
```

Response

```
The Powertech avsvc subsystem should be `active' and the device driver loaded:  
Subsystem Group PID Status  
avsvc powertech 5964286 active  
Device driver is loaded  
The avsvc subsystem is configured to run at boot
```

Recovering from Data Transformation/Powertech Antivirus code errors

A Data Transformation rekey performed while Powertech is active can result in failed file conversion due to "busy" faults. The following section describes how to recover from this type of error.

Note

There are many reasons that a data transformation may fail. This topic only considers the failure due to the

interaction of Powertech with CTE. For other error recovery procedures, refer to the [Data Transformation guide](#)

The following section illustrates the process using an example data transformation and describes the steps needed to recover. The Data Transformation GuardPoint `/test-dataxform`.

1. Run Data Transformation.

```
dataxform --rekey --gp /test-dataxform
```

Response

```
Checking if /test-dataxform is a guardpoint with a rekey policy applied
/test-dataxform is a guardpoint with a rekey policy applied
About to perform the requested data transform operation
- Be sure to back up your data
- Please do not attempt to terminate the application
Do you wish to continue (y/n)?y
Scan found 19 files (14 MB) in 1 directories for guardpoint /test-dataxform
File /test-dataxform/xab is busy
File /test-dataxform/xaa is busy
Transformed 17 files (13 MB) of 19 files (14 MB) for guardpoint /test-dataxform
Data transform got errors on some files
File /test-dataxform/xab is busy
File /test-dataxform/xaa is busy
Number of files in error due to file being busy: 2
The data transform operation took 0 hours, 0 minutes and 3 seconds
The data transform program ran from Thu Feb 16 10:58:12 2023 until Thu Feb 16 10:58:15 2023
Data transform for guardpoint /test-dataxform finished but 2 files were not processed due to errors
```

2. Inspect the error file (`dataxform_status_error-_test-dataxform`) for `/test-dataxform`. The file is located in `/var/log/vormetric`. The contents for the file contain the error messages generated by Data Transformation.

Example

```
Skipped, file is busy : /test-dataxform/xab
Skipped, file is busy : /test-dataxform/xaa
```

Note

Other Data Transformation errors may be present besides those caused by the Powertech antivirus code.

3. Create a "todo" file. Using Data Transformation, extract the names of the files that need to be retried for conversion.

```
dataxform --recovery --file_list my-output --gp /test-dataxform
```

This generates two files in the local directory

```
my-output_done  
my-output_todo
```

The `my-output_todo` file contains the list of files to retry applying Data Transformation:

```
/test-dataxform/xaa  
/test-dataxform/xab
```

Note

The `my-output_todo` file may need to be edited to remove entries not caused by the `Skipped, file is busy` error.

4. Turn off Powertech on boot, type:

```
/opt/sgav/avsvcctl disable
```

5. Reboot the system.
6. Verify the status.

```
/opt/sgav/avsvcctl status
```

Response

```
Subsystem Group PID Status
avsvc powertech inoperative
Device driver is not loaded
```

7. Re-issue Data Transformation to transform files listed in the `my-output_todo` file.

```
dataxform --rekey_list --gp /test-dataxform --file_list ./my-output_todo
```

Response

```
Checking if /test-dataxform is a GuardPoint with a rekey policy applied
/test-dataxform is a GuardPoint with a rekey policy applied
Previous status information does not relate to a --rekey_file operation.
Number of files previously in error due to file being busy: 2
About to perform the requested data transform operation
- Be sure to back up your data
- Please do not attempt to terminate the application
Do you wish to continue (y/n)?y
Starting data transform of /test-dataxform for files listed in ./my-output_todo
0
The data transform operation took 0 hours, 0 minutes and 2 seconds
The data transform program ran from Thu Feb 16 12:33:47 2023 until Thu Feb 16
12:33:49 2023
```

8. Re-enable Powertech on boot.

```
/opt/sgav/avsvcctl enable
```

9. Start Powertech.

```
/opt/sgav/avsvcctl start
```

There is a delay before Powertech is completely loaded and active. The Powertech status may be found by the following command:

```
/opt/sgav/avsvcctl status
```

The Powertech avsvc subsystem should be `active' and the device driver loaded:

Response

```
Subsystem Group PID Status
```

```
avsvc powertech 5964286 active  
Device driver is loaded  
The avsvc subsystem is configured to run at boot
```



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

CTE Agent AIX User and Configuration Guide	4
Overview	4
Getting Started with CTE for AIX	8
Installation Workflow	9
AIX Package Installation	12
Installing CTE with No Key Manager Registration	12
Configuring CTE for AIX with CipherTrust Manager	13
Installation and Registration Options	14
Installation Prerequisites	15
Interactive Installation on AIX	15
Validating CM and CTE with a Local CA Certificate	19
Using external certificates for communication between CTE Agent and CipherTrust Manager ...	20
Silent Installation on AIX	23
Guarding a Device with CTE and CipherTrust Manager	26
Special Cases for CTE Policies	33
Re-Enabling Automatic Signing for Host Settings	33
Restricting Access Overrides from Unauthorized Identities	34
Backing up DB2 Databases after Encryption	35
Blocking ptrace system calls to prevent process injection attacks	36
Logs	37
Setting CTE Agent Logging Preferences	38
Audit Logs	39
Analyzing Audit log entries	39
File System Audit Log Effects Codes	40
Concise Logging	41
Enhanced Encryption Mode	42
Compatibility	43
Disk Space	44
Encryption Migration	44
File Systems Compatibility	45
Using the AES-CBC-CS1 Encryption Mode in CM	45
Exceptions and Caveats	45
Utilities for CTE Management	46
Agent Health Utility	46
agentinfo Utility (Java version)	50
Backup Utility	50
check_host Utility	52
Displaying Information for Nested File Systems with the DF tool	53
Protecting Files with Client Settings	53
Restricting Access Overrides with Client Settings	53
register_host Utility	55
secfsd Utility	55

secfsd Examples	56
secfsd and Raw Devices	61
Using Client Settings with Shell Scripts	61
vmsec Utility	62
vmsec Examples	62
Configuring Dynamic Host Settings for AIX	66
vmutil	67
vmd utility	68
Upgrading CTE on AIX	69
Uninstalling CTE from AIX	71

CTE Agent AIX User and Configuration Guide

This document covers the following information:

- Overview
- Getting Started with CTE for AIX
- Special Cases for CTE Policies
- Logs
- Enhanced Encryption Mode
- Utilities for CTE Management
- Upgrading CTE on AIX
- Uninstalling CTE from AIX

Overview

This document describes the installation and advanced configuration options for CTE for AIX, as well as detailed information about how to integrate CTE with Oracle.

CTE Terminology

The CTE documentation set uses the following terminology:

The guide uses the following terminology:

Term	Description	OS Applies to
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. Notes • This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". • For example, the default installation directory is <code>/opt/vormetric/DataSecurityExpert/agent/</code> for Linux and AIX, and <code>C:\Program Files\Vormetric\DataSecurityExpert\agent\</code> for Windows.	Windows/Linux/AIX

Term	Description	OS Applies to
	Windows.	
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.	Windows/Linux/AIX
CTE Capabilities	CipherTrust Transparent Encryption agent version-specific features like Multi-Factor Authentication.	Linux
CTE-K8s	CipherTrust Transparent Encryption for Kubernetes. Policy-based encryption of data stored on persistent volumes	Linux
CTE-RWP or RWP	CipherTrust Transparent Encryption with Ransomware Protection. Ransomware protection for volume-level (Windows)/GuardPoint (Linux) data storage through process behavior monitoring and analytics.	Windows/Linux
CTE UserSpace (CTE-U)	CipherTrust Transparent Encryption (formerly known as ProtectFile FUSE). File system level encryption and access control solution for Linux servers.	Linux
Data Transformation	Encrypting or decrypting data.	Windows/Linux/AIX
Domain Sharing	This allows Clients in one domain to get cross-domain resources, specifically GPs.	Windows/Linux/AIX
GuardPath	A directory to which a CTE Kubernetes data protection and encryption policy has been applied. CTEK8s will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.	Linux
GuardPoint	A device, or directory, to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.	Windows/Linux/AIX
Host /Client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is	Windows/Linux/AIX

Term	Description	OS Applies to
	installed.	
In-place Data transformation	Encryption mechanism for block devices.	Linux
Key Manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers CipherTrust Manager, a key manager for use with CTE.	Windows/Linux/AIX
LDT (Live Data Transformation)	After initial GuardPoint enablement, LDT performs initial encryption, or rekeying, in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block applications and user access to data during encryption or rekey operations, which can inconvenience users and affect operational efficiency.	Windows/Linux
LDT Communication (Comm) Group	A group of LDT clients who communicate with each other, and are responsible for, initial data transformation and future key rotation of CIFS/NFS GuardPoints.	Windows/Linux
LDT GuardPoint Group	An LDT GuardPoint Group contains a collection of LDT-enabled CTE clients that are all on the same network, managed by one CipherTrust Manager, guarding a common NFS/CIFS share and can communicate with each other over that network. An LDT GuardPoint Group enables the primary host of an LDT GuardPoint Group to communicate with the secondary hosts that are members of that LDT GuardPoint Group.	Windows/Linux
LDT Primary node	The LDT GuardPoint Group node that performs LDT rekeying of data.	Windows/Linux
LDT Secondary node	All of the other clients in the LDT GuardPoint Group are assigned as secondary nodes. Note: Secondary nodes do not participate in rekeying data, however, they can be promoted to primary nodes if a primary node fails.	Windows/Linux
LDT Subordinate nodes	The subordinate nodes are the remaining nodes in the LDT Communication Group.	Windows/Linux

Term	Description	OS Applies to
LDT Triad nodes	The triad nodes are the first three servers in the LDT Communication Group.	
Learn Mode	Logging mode for audit logs to help generate security policies. Learn Mode allows access to guarded paths while logging access details. Users can analyze the content users and processes are accessing, the data used, and define GuardPoint policies accordingly.	Windows/Linux
MFA	Multifactor authorization ensures that the access credentials presented belong to the actual person. After logging in to the system, when a user tries to access a CipherTrust Transparent Encryption GuardPoint, it triggers a second factor authorization to verify the user with a second form of authentication, like sending a passcode to the users's registered cell phone, that they then have to input into the application.	Windows/Linux
Profile	Shared configuration resource for Client logging, Quality of Service, Multi-Factor Authentication, Ransomware Protection and key manager communication settings.	Windows/Linux/AIX
Signature	The hash of an entity. Where Entity can be the process or the docker image.	Windows/Linux/AIX
Versioned key and Key versions	Keys whose name remains the same but keybytes are different for each different version.	Windows/Linux/AIX

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.

After the CTE Agent has encrypted a device on a host, that device is called a *GuardPoint*. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.

- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you

can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Note

For a list of CTE versions and supported operating systems, see the [CTE Compatibility Portal](#).

CTE Compliance with AIX Lock Semantics

CTE is compliant with AIX lock semantics. In the following cases, CTE deviates from AIX lock semantics:

- For a guarded file, an `fcntl(2)` system call will block if the current process file location and specified `fcntl` number of bytes overlaps an existing file lock.
- For a non-guarded file, the `fcntl(2)` system call blocks only if the `fcntl` number of bytes falls within the range limits of a specified file lock.

How to Protect Data with CTE

CTE uses policies created in the associated key manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your protected hosts. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of GuardPoints.

Policies specify:

- Whether or not the resting files are encrypted.
- Who can access decrypted files and when.
- What level of file access auditing is applied when generating fine-grained audit trails.

A Security Administrator accesses the key manager through a web browser. You must have administrator privileges to create policies using either key manager. The CTE Agent then implements the policies once they are pushed to the protected host.

CTE can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

Getting Started with CTE for AIX

This section describes how to install CTE for AIX, register it with your selected key manager, and then create a simple GuardPoint on the protected host. It contains the following topics:

- [Installation Workflow](#)
- [AIX Package Installation](#)

- [Installing CTE with No Key Manager Registration](#)
- [Configuring CTE for AIX with CipherTrust Manager](#)

Installation Workflow

In order to install and configure CTE, you need to perform the following high-level tasks:

1. If you want to include the CTE Agent software with the AIX distribution files, see [AIX Package Installation](#).
2. If you want to install the CTE Agent without registering with a key manager, see [Installing CTE with No Key Manager Registration](#). However, you cannot protect any data on the host until it has been registered. See [Configuring CTE for AIX with CipherTrust Manager](#).
3. Create your policies, encryption keys, and GuardPoints using the selected key manager. For details, see: [Guarding a Device with CipherTrust Manager](#).

Additional Considerations

The following sections describe some of the things to keep in mind when configuring CTE.

Port Selection

The following port information applies to both Windows and Linux systems.

Communication through a Firewall

If a protected client must communicate with CipherTrust Manager through a firewall, see the CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

Communication with CipherTrust Manager

The default port for http communication between CipherTrust Manager and the CTE Agent is **443**. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

Communication for LDT over CIFS/NFS

All nodes that intend to use **LDT over CIFS/NFS** GuardPoint must have the following ports open:

- 7024
- 7025

Note

When you are registering a CipherTrust Transparent Encryption client with CipherTrust Manager, you can

manually include a destination port number, (Default: 443). If you enter a port value, using the syntax `<hostname or IP address>:<port number>` then CipherTrust Transparent Encryption **does not** perform a port scan. CipherTrust Transparent Encryption uses the port number provided to verify the target server type using a TLS operation.

If you do not enter a port number, CipherTrust Transparent Encryption performs a port scan to check which ports are listening, including port 443.

Tracking and Preventing Local User Creation

CTE audits any attempts to change user authentication files. It also allows you to prevent any change to user authentication files using the host settings **protect**. This includes, but is not limited to user creation, modification, and deletion, or to deny users.

- The **audit** setting is set to on by default. It logs access to the system credential files but does not prevent account modifications.
- The **protect** setting both audits and prevents local user account modifications. You must manually enable the **protect** setting for tracking and prevention of local user account creation.

The **protect** tag will prevent changes to the files mentioned below. In the absence of the **protect** tag in host/client settings, operations on these files are permitted. When a log entry is generated, it is tagged with an **[audit]** tag.

- `/etc/passwd`
- `/etc/group`
- `/etc/ssh/sshd_config`
- `/etc/ssh/sshrc`

Note

The first time you use the **protect** host setting, you must restart CTE. Subsequent files tagged with the **protect** setting do not require a restart.

Restricted Mode

Caution

If you install or upgrade in restricted mode, you cannot revert to unrestricted mode without

uninstalling CTE.

You can install CTE in restricted mode. This mode prevents any user other than `root` from accessing the following directories:

- `/var/log/vormetric`
- `/opt/vormetric/DataSecurityExpert`

Restricted Mode also prevents non-root users from running the following utilities:

- `agenthealth`
- `agentinfo`
- `check_host`
- `register_host`
- `secfsd`
- `vmd`
- `vmsec`
- `voradmin`

Key Agents and Restricted Mode

- On systems where CTE is installed in restricted mode, you cannot install a key agent (pkcs11) or CipherTrust TDE Key Management.
- On systems where a key agent (pkcs11) or CipherTrust TDE are already installed, you cannot install CTE in restricted mode.

Restricted Mode Installation

To install in restricted mode, use the `-r` option.

```
./vee-fs-<release>-<build>-<system>.bin -r
```

For example:

```
./vee-fs-7.8.0.75-aix71.bin -r
```

Upgrade in Restricted Mode

The upgrade mode is the same as the installation mode.

AIX Package Installation

This section describes how to install AIX packages directly so that the CTE Agent installation integrates with AIX distribution software. The CTE installation `bin` files contain the native packages and are extracted by running the `bin` file with the `-e` flag.

To extract and run the `.bff` file on AIX:

1. Log on to the host system as root and copy or mount the installation file onto the host system.
2. Extract the package files.

```
./vee-fs-7.8.0.75-aix71.bin -e
Contents extracted.
# ls *bff
vee-fs-7.8.0.75-aix71.bff
```

3. Run `installp` and then follow the prompts.

```
installp -aX -d vee-fs-7.8.0.75-aix71.bff vee.fs
```

- If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for AIX with CipherTrust Manager](#).

Installing CTE with No Key Manager Registration

The following procedure installs the CTE Agent on the host but does not register it with a key manager. You cannot protect any data on the host until the CTE Agent is registered with one of the supported key managers. For a comparison of the available key managers, see [CTE Components](#).

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
./vee-fs-7.8.0.75-aix71.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
./vee-fs-7.8.0.75-aix71.bin -d /home/my-cte-dir/
```

Note

If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
./vee-fs-7.8.0.75-aix71.bin -h
```

4. The Thales License Agreement displays. When prompted, type `Y` and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

Welcome to the CipherTrust Transparent Encryption File System Agent Registration Program.

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>
```

```
In order to register with a CipherTrust Manager you need a valid registration token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Type `N` and press Enter to end the installation procedure without registering the CTE Agent with either key manager.

When you are ready to register the CTE Agent with a key manager, see [Configuring CTE for AIX with CipherTrust Manager](#).

Configuring CTE for AIX with CipherTrust Manager

This section describes how to install and configure CTE on AIX systems that you plan to register with a CipherTrust Manager.

The installation and configuration process when you are using CTE with a CipherTrust Manager consists of three basic steps:

1. Installation Prerequisites

Gather the information needed for the installation and set up your network.

2. Interactive Installation and Registration AIX

Install CTE interactively on a protected host and register the protected host with CipherTrust Manager.

Silent Installation on AIX

Install CTE silently (non-interactive) on a protected host and register the protected host with CipherTrust Manager.

3. External Certificates

Use for communication between CTE and CM. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

4. Validating CipherTrust Manager and CipherTrust Transparent Encryption with a Local CA Certificate

Ensure that registration by the CTE agent is serviced only by the expected key manager by providing a copy of the CA certificate that will be used to authenticate the TLS communications with the key manager.

5. Guarding a Device with CipherTrust Manager

Create as many standard GuardPoints on the client as you need

Installation and Registration Options

CTE provides the following installation and registration options. The options you choose determine the information you need to supply during the actual install procedure.

Installation Method Options

There are two methods for installing CTE on AIX platforms:

- **Typical:** Most common and recommended type of installation. Use this method for installing the CTE Agent on one host at a time. See [Interactive Installation on AIX](#).
- **Silent:** Create pre-packaged installations by providing information and answers to a set of installation questions. Use silent installations when installing on a large number of hosts. See [Silent Installation on AIX](#).

Hardware Association (Cloning Prevention) Option

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware clients.

You can enable hardware association during CTE registration process. You can disable hardware association by re-running the registration program.

Installation Prerequisites

This section lists the tasks you must complete, and the information you must obtain, before installing CTE.

Recommendations and Considerations

- Thales recommends that you install CTE in the default location.
- Make the installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.

For example:

```
./vee-fs-7.8.0.75-aix71.bin -d /home/hello/
```

- Ensure read/write permission is granted to other users accessing your shared resource.
- P8 Hardware Encryption is supported, but there is a required fix from IBM. If the required fix is not found, the installation defaults to Software Encryption for P8.
 - AIX 7.1 requires TL level 7100-04-04 or later.
 - AIX 7.2 requires TL level 7200-01-02 or later.

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the AIX system on which you plan to install CTE to the CipherTrust Manager. After the AIX system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.
- It must also allow for connectivity of the CipherTrust Manager to all clients where you install CTE.
- If the system is a virtual machine, the VM must be deployed and running.

Communication with CipherTrust Manager

The default port for http communication between CipherTrust Manager and the CTE Agent is **443**. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

Interactive Installation on AIX

The AIX typical install is an interactive script that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see [Silent Installation on AIX](#)).

After you install CTE, you are prompted to register it immediately with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

Note

Do not install CTE on network-mounted volumes like NFS.

Before You Begin

The following prerequisites must be met for CTE/CTE-U to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on to the host where you will install the CTE Agent as **root**. You cannot install the CTE Agent without root access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the **chmod** command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
./vee-fs-7.8.0.75-aix71.bin
```

To install the CTE Agent in a custom directory, use the **-d <custom-dir>** option. For example:

```
./vee-fs-7.8.0.75-aix71.bin -d /home/my-cte-dir/
```

Note

If possible, Thales recommends that you use the default directory **/opt/vormetric**.

To view all installer options, use the `-h` parameter. For example:

```
./vee-fs-7.8.0.75-aix71.bin -h
```

4. The Thales License Agreement displays. When prompted, type Y and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

Welcome to the CipherTrust Transparent Encryption File System Agent Registration Program.

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>

In order to register with a CipherTrust Manager you need a valid registration token from the CM.

Do you want to continue with agent registration?(Y/N) [Y]:
```

5. Enter Y to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE.

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: `<hostName>:<port#>`

For example:

```
Do you want to continue with agent registration? (Y/N) [Y]: Y

Please enter the primary key manager host name: 10.3.200.141:8445

You entered the host name 10.3.200.141
Is this host name correct? (Y/N) [Y]: Y
```

6. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the following list.

[1] sys31186.qa.com
[2] 10.3.31.186

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 2
You selected "10.3.31.186".
```


7. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```

Please enter the registration token: 12345
Please enter the profile name for this host: My-Profile
Please enter the host group name for this host, if any:
Please enter a description for this host: West Coast Datacenter server 5

Token           : 12345
Profile name     : My-Profile
Host Group       : (none)
Host description : West Coast Datacenter server 5
Are the above values correct? (Y/N) [Y]: Y

```

8. At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloned machines from accessing the key manager (for details, see [Hardware Association \(Cloning Prevention\) Option](#)). The default is Y (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again. Do you want to enable this functionality? (Y/N) [Y]: Y

Warning

The registration token, profile name, client group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

9. CTE finishes the installation and registration process.

```

Generating key pair for the kernel component...done.
Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption File System Agent with the
CipherTrust Manager on 10.3.200.141.

Installation success.

```

10. If you are using CipherTrust Manager version 2.2 or later, you can now use CipherTrust Manager to administer CTE on the client.

If you are using CipherTrust Manager version 2.1 or earlier, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Validating CM and CTE with a Local CA Certificate

To ensure that registration by the CTE agent is serviced only by the expected key manager, you can provide a copy of the root CA certificate that will be used to authenticate the TLS communications with the key manager, during the registration process.

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Note

You can only download the CA certificate when you are a root user in the root domain. You cannot download the certificate from a subdomain. It will not work.

Prerequisite

Make sure that you have previously [created the client](#) in CipherTrust Manager.

Using a Local CA Certificate

1. Extract the root CA certificate from the CipherTrust Manager.
 - a. Log on to CipherTrust Manager as an administrator.
 - b. In the left navigation pane, click **CA > Local**. The list of available CAs displays.
 - c. Click the ellipsis icon corresponding to the CA.
 - d. Click **Download** to download the CA.
 - e. Copy the certificate to a directory on the agent system.
2. Present the root certificate data to CTE in one of two ways:

a. Use a file:

When written to a file, it must be in PEM file format, starting and ending with:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

b. Use a string parameter:

If you are providing the information in a single string, it must contain the same data as in the preceding case, except that all new lines are replaced by `\n` escape sequences. For example:

```
CA_CERT=-----BEGIN CERTIFICATE-----\n -----END CERTIFICATE-----\n
```

3. To install the root certificate into the CTE client:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host.exe -s <Path-to-install-file> AGENT_HOST_NAME=<Hostname-or-IP-of-agent> REG_TOKEN=<CM registration token> CA_FILE=<Path-to-root-ca-cert>
```

Example

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host.exe -s /opt/silent/vte_reg_log.txt AGENT_HOST_NAME=ani-vm-217-35190.sjcicd.com REG_TOKEN=mMEz3Y60b9D4L7QuvK5S0mhulRm8DYI8odV5j30dVuHqk6LhZqE0FeIZHILYtMDiE9 CA_FILE=/cert_files/Austin175.pem
```

4. Confirm in CipherTrust Manager that the client is registered and healthy.

Using external certificates for communication between CTE Agent and CipherTrust Manager

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Overview

Use for communication between CTE and CipherTrust Manager. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

Prerequisites

The external certificate must be:

- On the file system
- In PEM format

A key pair must already exist for the client:

- Must have Encryption type of either:
 - sha256WithRSAEncryption
 - ecdsa-with-SHA384
- Must be Encrypted with a pass phrase

Initial setup

1. Obtain your external CA certificate.
2. Create a certificate using the external CA certificate and key.

CipherTrust Manager Setup

To setup CipherTrust Manager to communicate through an external certificate:

1. Import the CA certificate into the CipherTrust Manager, click **CA > External > Add External CA**.

Note

In the Add External CA dialog, copy and paste the `<ca_certificate_name>.pem` file content from the UI page and provide a user-friendly name.

For more information, see [Using an Externally Generated Server Certificate for an Interface](#)

2. Add the CA certificate to the list of trusted sources for the web interface, click **Admin Settings > Interfaces > web > Edit > External Trusted CAs**.
3. Restart the web server, click **Admin Settings > Services > web > Restart**.
4. [Create a Registration Token](#) for the CTE agent.

CTE Agent setup

1. Create a directory on the system to hold the required files, for example:

- `/root/cert_files` (**Linux/AIX**)
- `c:\temp\cert_files` (**Windows**)

2. Copy or create the following files in this directory:

- `client_cert.pem`
- `client_key.pem`
- `passphrase` - this is currently expected as plain text

3. For **Linux/AIX** systems, to add the directory path to the environment, type:

```
$ export EXTERNAL_CERT_DIR=/root/cert_files
```

4. For **Windows** system, invoke `registerhost.exe` from the command line and add this argument:

```
c:\> register_host.exe -extcertdir=c:\temp\cert_files
```

5. Register the CTE client with the CM server as normal. If this is being done as part of an installation, then the above steps should be done before the installation, or, on windows, added to the registration parameters passed to the installer.

Post Registration

During registration, the certificate file is uploaded to the CipherTrust Manager, and the certificate and key files are imported into the CTE pem store. The key is decoded using the provided passphrase, then re-encoded using a random key using the normal CTE key security mechanisms for TLS keys. There is no need to keep the input files after registration is successful, so for security reasons they should be removed / shredded.

Certificate Renewal

The location of the external certificate files (i.e. the `EXTERNAL_CERT_DIR` or `-extcertdir` parameters) will be recorded in the CTE agent configuration file, `agent.conf`. When the current certificate is approaching expiration date (i.e. approx. 60 days prior to expiration) the CTE agent will look in this directory for an updated set of files.

If a new certificate file is present, then the file will be read and pushed to the CM, and if accepted, then the certificate and key will be imported into the CTE pem store, and the VMD process restarted to use the new certificate.

If no new certificate is present, a **WARNING** level message will be written to the logs and/or uploaded to the CM as per the logging settings, and the CTE agent will check again after 24 hours.

If the user wishes to change the directory path to store the new certificates, then the entry in the `agent.conf`

file should be updated and the vmd service restarted. Alternatively, the user can update the external certificate set using the following command (this will not update the saved path):

```
# vmutil -a vmd -d <ext_cert_Dir> updatecerts
```

If the user fails to update the certificate set prior to expiration then communication with the CM may be blocked, and re-registration will be required.

Note

Any renewed certificates must have exactly the same common name field as the original certificate, or the CipherTrust Manager will reject the update.

Silent Installation on AIX

This section describes how to perform a silent (unattended) installation of the CTE on a single host. The silent installation automates the installation process by storing the answers to installation and registration questions in a separate file that you create. You can also use the silent installation to install CTE on multiple hosts simultaneously.

The silent install method installs CTE on the host, and registers the host with the CipherTrust Manager you specify in the silent installation file.

Prerequisites

The following prerequisites must be met for CTE/CTE-U to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on as an administrator to the host where you will install CTE.
2. Create a parameter file and store it on your system, or copy an existing file from another location. The file can contain any of the following parameters:

Parameter	Description
AGENT_HOST_NAME	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

Parameter	Description
AGENT_HOST_PORT	Specifies the port number for this CTE Agent to use.
AGENT_USEIP	Use the IP address of the protected host instead of host name. Used when hostname is not supplied.
CA_CERT	Set to provide CA certificate data to CipherTrust Manager.
CA_FILE	Set to provide a CA certificate file to CipherTrust Manager.
CERT_FIELD_PARAM	Installer option. Default behavior is to use hard-coded values for Root Certificate fields. Uses the same <code><Certificate Parameters></code> string format as is used in the voradmin command <code>voradmin cos ca_cert create <Certificate Parameters></code>
ENABLE_CLOUD	Set to enable cloud in the Key Manager.
ENABLE_HOST_CHECKS	When using CipherTrust Data Security Platform Services (CDSPaaS), set this value to 1 to enable SSL certificate host name checks. Set to 0 to disable. Default: 0 . This also forces CTE to enable the verify peer feature during registration. Use only when the CDSPaaS web server certificates contain the target DNS name or IP address.
ENABLE_LDT	Set this value to 1 to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.
HOST_DESC	Specifies a description for the host. This description is displayed in the CipherTrust Manager. If an entry for this host already exists, and the host already has a description, CipherTrust Manager
HOST_GROUP	Specifies the optional host/client group with which this host/client will be associated.
HOST_PROFILE	Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.
LDTGROUP_NAME	Set the LDT Communication Group for LDT over NFS/CIFS.
REG_TOKEN	The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.
ENABLE_RWP	Enable Ransomware Protection.
SERVER_HOSTNAME	Required if you want to register CTE with a CipherTrust Manager.
SERVER_IP	Alternative for hostname when registering.
TMPDIR	Specifies a custom temporary directory that the

Parameter	Description
	installer can use during the installation process. If this value is omitted, the installer uses the default temporary directory.
USEHWSIG	Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.

Example 1: Registering with CipherTrust Manager

The following example contains just the required information for registration with CipherTrust Manager. In this case, the client will be registered with the CipherTrust Manager using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
AGENT_HOST_NAME=10.192.80.86
```

Example 2: Registering with CipherTrust Manager

The following example specifies the required registration information, adds a host name and description, and enables hardware association. In this case, the client will be registered with the CipherTrust Manager using its host name instead of the IP address:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
AGENT_HOST_NAME=myagent.example.com
HOST_DESC="West Coast Server 12"
USEHWSIG=1
CERT_FIELD_PARAM="/C=US/ST=California/L=San Jose/O=Thales eSecurity/OU=Vormetric/CN=localhost/emailAddress=admin@thalesgroup.com"
SUBJECT_ALT_NAME_PARAM="DNS:www.thalesgroup.com,email:admin@thalesgroup.com"
```

1. Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.
2. Run the installer using the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin [-d <custom-dir>] -s <install-file>
```

where:

- `-d <custom-dir>` is an optional parameter that specifies the installation directory for CTE. If you omit this parameter, CTE is installed in `/opt/vormetric/DataSecurityExpert/agent/`.
- `-s <install-file>` indicates that you want to install silently using the installation options file `<install-file>`

For example, if the installation options file is called `/tmp/unattended.txt`, you would enter:


```
./vee-fs-7.8.0.75-aix71.bin -s /tmp/unattended.txt
```

3. Verify the installation by checking CTE processes on the host:
 - Run `vmd -v` to check the version of CTE matches that just installed.
 - Run `vmsec status` to display CTE kernel status.
 - Look at the log files in `/var/log/vormetric`, especially `install.fs.log.<date>` and `vorvmd_root.log`.
4. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Guarding a Device with CTE and CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many standard GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device or directory.
3. Identify or create a policy for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. Assign a GuardPoint to the device or directory.

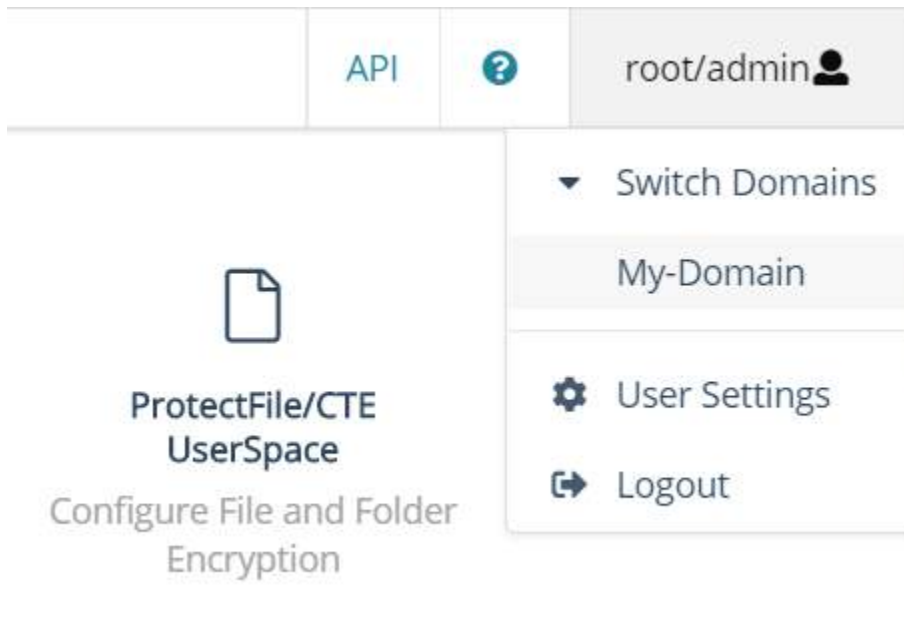
The following example creates a simple policy and uses it to guard a directory on a registered client. For all of the following procedures, you must be logged into the CipherTrust Manager Console as a CipherTrust Manager Administrator, and you must be in the domain with which the client is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the CipherTrust Manager documentation.

Access the CipherTrust Manager Domain

1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to [Create an Encryption Key](#). If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the user name **root/admin** on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.

- c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

Note

The following procedure is based on CipherTrust Manager version 2.2. If you are using a different version, see the CipherTrust Manager documentation for the version that you are using.

1. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.

Tip

To navigate to the Products page from anywhere in the CipherTrust Manager Console, click the App Switcher icon in the top left corner.

2. Above the Key table, click **Create a New Key**.
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
4. In the **Key Usage** section, make sure **Encrypt** and **Decrypt** are selected.
5. Click **Create**. CipherTrust Manager displays the properties for the new key.
6. In the general options area, enable the **Exportable** option.

You can also enable the **Deletable** option in this section if you want a CipherTrust Manager Administrator to be able to delete the key.

ID	2e58c582...61136313	Owner	Global	Object Type	Symmetric Key
UUID	e3ad9c3e...7f047711	Created	05 Mar 2021, 05:13	Algorithm	AES
MUID	e3ad9c3e...f6333c9f	Last Modified	05 Mar 2021, 05:13	Size	256
KeyID	N/A	Exportable	☒	Deletable	☐

7. In the **Key Access** section, do the following:

a. In the Search Groups box, type "cte".

If no groups are displayed, make sure the **Added Only** option is *disabled*.

b. Click the **All** check box for both the CTE Admins and CTE Clients groups.

KEY ACCESS

Key Owner

Search:

2 Results | 2 group

☐ Added Only

Group	Read	Use	Decrypt	Encrypt	Sign	Sign/Verify	Export	All
CTE Admins	☒	☒	☒	☒	☒	☒	☒	☒
CTE Clients	☒	☒	☒	☒	☒	☒	☒	☒

c. When you are done, click **Update**.

8. Click the **CTE** tab and set the following properties:

- **CTE Versioned:** Specify whether the key is versioned. By default, the key is set as versioned.

For a standard policy, you should clear this check box. If you do not, the key will *not* appear in the keys list when you add the key rule to the standard policy.

- **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.

When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.

When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.

- **Encryption Mode:** Encryption mode of the key. The options are:
 - CBC

- CBC-CS1
- XTS

Encryption using the XTS and CBC-CS1 keys is known as enhanced encryption. For details, see the *CTE Agent for AIX Installation and Configuration Guide*.

When you are done, click **Update**.

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **Transparent Encryption** application.
2. In the sidebar on the Clients page, click **Policies**.
3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
4. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a Standard policy.
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints.
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption.

Field	Description
	Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.
Data Transformation	If you select Standard as the policy type, also select the Data Transformation option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

When you are done, click **Next**.

- On the Security Rules page, define the security rules that you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of **key_op** and the effects **Permit** and **Apply Key**. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version.

To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

When you are done, click **Next**.

- On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one. If the data has not yet been encrypted, select clear_key. Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select clear_key.
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to

Field	Description
	encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

When you are done, click **Next**.

- On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click Select to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in Create an Encryption Key.

When you are done, click **Next**.

- Click **Next**.
- On the confirmation page, review the information for the policy and click **Save**.

Create Policy



- 1 General Info 2 Security Rules 3 Key Rules 4 Data Transformation 5 Confirmation

Review the provided policy details.

1 General Info

Name: Simple-Policy

Policy Type: Standard

Description: Standard policy for new GuardPoints

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*			key_op	permit:applykey	Yes
*					Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	Simple-Key

[Back](#)

Save

Create a GuardPoint

1. Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
2. In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
3. In the Clients table, click on the name of the client you want to protect.
4. Above the GuardPoints table, click **Create GuardPoint**.
5. In the Create GuardPoint page:
 - a. In the **Policy** field, select the policy you created earlier.
 - b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a explorer window.

If you want to enter multiple paths, put each path on its own line. For example:

- d. Click **Create**.
- e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**. For this example, click No.

The CTE clients pull the GuardPoint configuration information from the CipherTrust Manager.

6. Type the following to transform the data:

```
dataxform --rekey --print_stat --preserve_modified_time --gp <pathToGP>
```

When the data transformation has finished, applications can resume accessing the now-protected data. (See the “*CTE Data Transformation Guide*” for more information.)

Special Cases for CTE Policies

This section describes CTE-specific configuration tasks related to configuring policies in the key manager. It contains the following topics:

- Re-Enabling Automatic Signing for Host Settings
- Restricting Access Overrides from Unauthorized Identities
- Backing up DB2 Databases after Encryption
- Blocking ptrace system calls to prevent process injection attacks

Re-Enabling Automatic Signing for Host Settings

Starting with VTE for AIX release 5.2.6, VTE blocks automatic re-signing of the host settings. Some users may have established procedures for updating system software that are based on the assumption that restarting the **vmd** will generate new signatures when signed software is updated. This is no longer true. However, you can re-enable automatic re-signing if your environment requires it.

Caution

Re-enabling the automatic regeneration of signatures exposes a potential security vulnerability for CTE Agents. When enabled, host setting binaries are re-signed when CTE receives a push from the associated key manager. If an attacker were to replace a binary with a Trojan, and then force a push from the key manager by, for example, restarting the CTE Agent, CTE could generate a signature for the malicious binary and pass it.

To re-enable automatic re-signing for host settings:

1. Change to the directory where the `agent.conf` file resides. For example, type:


```
cd /opt/vormetric/DataSecurityExpert/agent/vmd/etc/
```

2. Edit the `agent.conf` file.
3. Change or add the following line:

```
AUTO_RESIGN_HOST_SETTINGS=TRUE
```

Note

Previously this setting was known as `RE_SIGN_HOST_SETTINGS`. Starting with VTE for AIX 5.3.0, the attribute name is `AUTO_RESIGN_HOST_SETTINGS` as shown above.

4. Save your changes and exit the file.
5. Restart the `vmd` to set the changes. Type:

```
/etc/rc.d/init.d/secfs restart
```

6. Type the following command to verify that the host settings is set to true:

```
vmsec vmdconfig
```

Restricting Access Overrides from Unauthorized Identities

CipherTrust Transparent Encryption host/client settings are the means by which an administrator configures user authorization. Users with root privileges, on Linux or AIX systems, have the unfettered ability to override all file access and execution permissions imposed by the system.

CipherTrust Transparent Encryption access control allows you to restrict privileges of users, groups, application processes and binaries, including root users and setuid programs. By default, CipherTrust Transparent Encryption agent **DOES NOT** trust any process as authenticated. Any attempt to access a resource, by any process, will therefore be flagged with a "User Not Authenticated" notification. The CipherTrust Transparent Encryption agent must be instructed to trust the authenticator process progeny. For example, `/usr/sbin/sshd` is a process that can be trusted to authenticate the user to the system and to CipherTrust Transparent Encryption.

In some setups, when editing a host, system administrators can use the **host settings > |authenticator|** feature with **su** to change identities and gain access to restricted data. You can instruct CipherTrust Transparent Encryption to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CipherTrust Transparent Encryption can block from authenticating other processes.

Any executable path that is marked with a **|path_no_trust|** host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

CipherTrust Transparent Encryption prevents overrides from other host settings authenticators, using the `|path_no_trust|` status. If a user runs the `su` command from a non-trusted shell, that new shell is still marked as `|path_no_trust|`, even if `|authenticator|/usr/bin/su` is specified in the host-settings. The `|path_no_trust|` feature overrides any and all authenticators under host settings.

Note

Using `|trust|*` before a `|path_no_trust|` host setting no longer disables the `|path_no_trust|` host setting.

For example, the following host setting denies authentication for users accessing through `sshd`:

```
|trust|*
|path_no_trust|/usr/sbin/sshd
```

To restrict access overrides:

1. In the CipherTrust Manager products page, click **Transparent Encryption > Clients**.
2. Click on an existing Client name to edit the host.
3. Click **Client Settings** tab.
4. Add the following to the settings:

```
|path_no_trust|<path of the binary>
```

Example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **Apply**.

Backing up DB2 Databases after Encryption

After encrypting a DB2 database running on AIX, CipherTrust Transparent Encryption cannot make a backup of the database. Both scheduled and manual backup fail. The problem was the user's policy. An AIX policy used in this scenario must follow a few rules.

With a `CBC_CS1` key, a guarded file is modified to have a 4096 byte header holding key information. When an **Apply Key** effect is specified, the CipherTrust Transparent Encryption code adjusts the length and file offset for this header. Without an **Apply Key** effect, the size and access of the offset include the `CBC_CS1` header.

Thales recommends that you modify the first rule of your policy. Remove the action entry for `f_rd_att` from the first rule and add a new rule before it:

```
**action**: f_rd_att
**effect**: Permit, Apply Key
```

Policy processing starts with the first rule and continues until a matching rule is found. The effect for the matching rule is then applied.

For the `f_rd_att` action, this results in the secfs code including the CBC_CS1 key header and adjusts the file size value. Without the Apply Key effect, the file size includes the CBC_CS1 header size and the file appears as 4096 bytes larger than its real size.

Blocking ptrace system calls to prevent process injection attacks

To prevent a process injection attack, which could lead to access to encrypted data by a tampered process, Thales implemented a global blocking for the ptrace system call. The purpose of this feature is to provide configurable options for disabling the ptrace system call based on user need. CTE provides toggle options on CipherTrust Manager based on the dynamic parameter which allows a security administrator to select which binaries are protected from ptrace attachment.

Note

This change can be very invasive and block legitimate uses of the ptrace system call.

Options

There are three new options:

Enabled_For_Authenticators

The CTE binaries and the binaries specified in the authenticator list are protected from the ptrace attachment. Other binaries are not protected from the ptrace attachment. (Default behavior)

Enabled_For_All

All of the installed binaries are protected from ptrace attachment. This protects from a tampered processes causing process injection attacks through the ptrace attach call.

Disabled_For_All

The CTE binaries are protected from ptrace attachment but the binaries specified in the authenticator list are allowed to attach to a ptrace system call. This solves the problem of a user trying to attach a ptrace system call to one of the binaries specified in the authenticator list for other use cases. Other binaries are not protected from the ptrace attachment.

Note

If you select Disabled for All, make sure that you set the log level on CipherTrust Manager to WARN or higher. If it is set to the default log level of ERROR, there will not be any messages related to ptrace logged

in the vmd.log file.

Configuration

To configure blocking the ptrace system call:

1. Log on to CipherTrust Manager.
2. Click **Transparent Encryption**.
3. Click on the desired client name to open it.
4. In the **Advanced Security Configuration**, click **View/Edit Settings** link.

Advanced Security Configuration [X]

This screen lists the security configuration parameters that can be updated after CTE client registration. Every parameter has the fixed set of values, as given below.

PTRACE_PROTECTION Enable/Disable ptrace capability for installed binaries	☒ Enabled_For_Authenticators ☐ Enabled_For_All ☐ Disabled_For_All

[Cancel](#)

5. Select the appropriate option and click **save**.

Logs

This section contains the following sections:

- [Setting CTE Agent Logging Preferences](#)
- [Audit Logs](#)
- [Analyzing Audit log entries](#)
- [File System Audit Log Effects Codes](#)
- [Concise Logging](#)

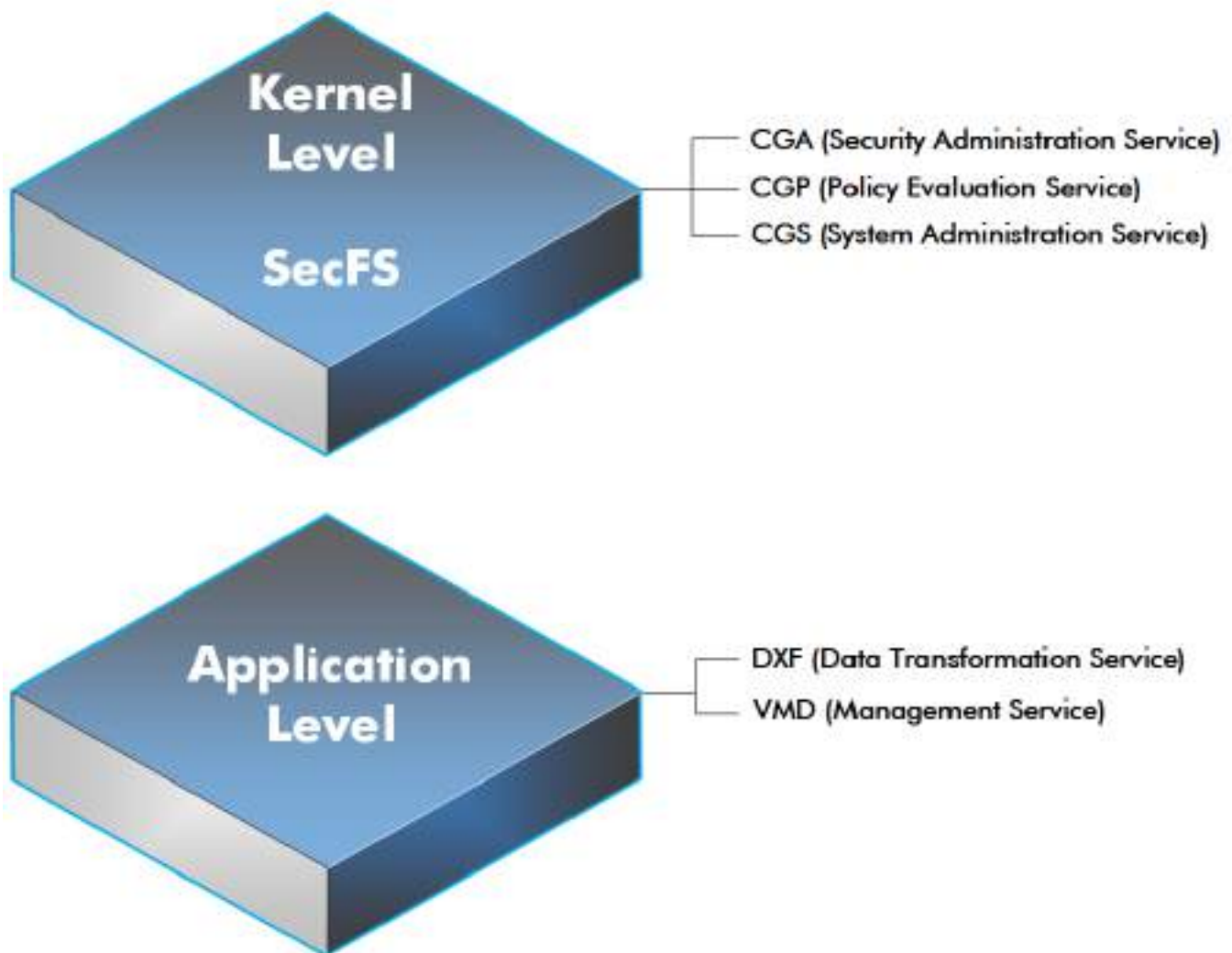
Setting CTE Agent Logging Preferences

You can configure the Agent process information that is entered into the Message Log. You can configure the process information globally, in which all the Agents that are added after the configuration change inherit the log attributes, while all current file system configurations remain intact. Alternatively, you can configure log attributes for individual Agent installations.

Always monitor log generation on new server and agent installations, and after changing logging preferences and options.

A variety of logging services are available and configured in the Log tab.

Logging Services



CTE log data may be sent to various different files such as:

- Sys log files, such as:

```
/var/log/messages
```

```
/var/log/syslog
```

Event log on

Note

The CM domain name can include spaces. However, Syslog does not allow spaces in header fields. Therefore, for Syslog purposes, the CTE client replaces the spaces with an underscore. For example: My_Domain instead of My Domain.

- CTE log files local to the agent, such as:

```
/var/log/vormetric/vorvmd_root.log
```

```
C:\ProgramData\Vormetric\DataSecurityExpert\agent\log\vorvmd.log (Windows)
```

- Uploaded to the Key Manager
- Uploaded to a Syslog server

Data Transformation log files are sent to:

```
/var/log/vormetric/vordxf_path_usr.log
```

Audit Logs

```
Example audit log:
CGP2601I: [SecFS, 0] [AUDIT] Policy[allowAllOps_fs] User[root,uid=0,gid=0\root,bin,daemon,sys,adm,disk,wheel\] Process[/bin/cat] Action[write_app] Res[/opt/apps/app1/doc/file2.txt] Key[aes128] Effect[PERMIT Code (1U,2U,3R,4M)]
```

Analyzing Audit log entries

The format of a File System Audit log entry is:

```
CGP2602I: [SecFS, 0] Level: Policy[policyName?] User[userID?] Process[command?] Access[whatIsItDoing?] Res[whatIsItDoingItTo?] Effect[allowOrDeny? Code (whatMatched?)]
```

Parameter	Description
Identifier	The TLA for the error message.
SECFS	Indicates that the message was generated by an Agent. You can enter secfs in the Search Message field in the Logs window to display the Agent policy evaluation and GuardPoint activity for all configured hosts.
Level	Indicates the importance of the message. For example, AUDIT indicates an informational message, whereas ALARM indicates a critical failure that you should not ignore.
Policy	Indicates the name of the policy that is being used to evaluate the access attempt.
User	Identifies the system user attempting to access data in the GuardPoint. It typically displays the user name, user ID, and group ID.
Process	Indicates the command, script, or utility being executed.
Access	Indicates what access is being attempted. Access may be read_dir, remove_file, write_file_attr, write_app, create_file, etc. These correspond to the Access methods that you configure in the policy. Read_dir corresponds to d_rd. Remove_file corresponds to f_rm, etc.
Res	Indicates the object/resource being accessed by the Process[].
Effect	Indicates the rule that matched and, based upon that rule, whether or not the CipherTrust Manager grants access. Access states may be either PERMIT or DENIED.

File System Audit Log Effects Codes

Codes are provided in the audit logs that identify actions by the policy enforcement engine. The code follows the number of the rule being processed.

Code	Definition
A	The Action component of a security rule failed to match.
M	All security rule components match and, unless overridden, the Effect for that security rule is applied.
P	The Process component of a security rule failed to match.
R	The Resource component of a security rule failed to match.
T	The time specified in the When component of a

Code	Definition
	security rule failed to match.
U	The User component of a security rule failed to match.

Refer to the audit log example above:

- The first and second Security Rules fail because of a mismatch in the User component (1U, 2U).
- The third Security Rule fails because of a Resource component (3R) mismatch.
- All of the rules in the fourth Security Rule match (4M), and the actions defined in the policy, such as use an encryption key, are applied.

Concise Logging

Thales' standard operational logging sends audit messages for each file system operation each time a file is opened, read, updated, or written. Thales's standard logging can generate high volumes of log data. Most of these messages might not be useful or required by security administrators to monitor file system activity on the system.

Agent log data can be stored on the local host, sent to a syslog server, or uploaded to the Management Console. On an agent system, log entries can flood the local messages file or Event Log. Extreme logging can also affect network performance.

Concise Logging eliminates the following types of messages:

- Duplicate audit messages for each and every block read by the user or application. With Concise Logging, CTE only sends an audit message the *first* time a user or application performs a read/write activity. Subsequent read/write activity by that user or application is not logged.
- Audit messages that read the attributes, read the basic information of file-set attributes, and other event-based messages.
- Audit messages for directory open, read directory attributes, and directory close.

Configuring Concise Logging for CTE Clients or Client Groups with CipherTrust Manager

In **CipherTrust Manager > CipherTrust Transparent Encryption > Settings > Profiles**, when you create a Client Profile, you can select to Enable Concise Logging. Then, you can apply that Client Profile to a specific client, or to all clients in a Client Group.

- Concise Logging changes the set of log messages that are sent to Security Information and Event Management (SIEM) software systems. If this results in loss of data required for customer reports, then disable Concise Logging.
- Concise Logging is only supported by CTE `secfs`.
- Enable and disable Concise Logging on the client, in the Client Profile. CTE applies it for all users of that Client Profile. There is no finer-grained control, such as per GuardPoint, user, or message type.
- Do not use Learn mode with Concise Logging.

This section describes the enhanced AES-CBC-CS1 encryption mode for keys. It contains the following topics:

- The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

Note

AES-CBC-CS1 encryption does not require any additional license.

Security Improvements

	AES-CBC	AES-CBC-CS1
Unique IV per-file	No	Yes
IV predictability	Yes	No

File System Support

	AES-CBC	AES-CBC-CS1
Local FS (AIX)	JFS2	JFS2
Remote FS (AIX)	NFS3/NFS4	NFS3/NFS4
Block Device Support (secvm)	Fully supported	No. When a policy contains a key with CBC-CS1 encryption mode, the guarding fails on the CipherTrust Manager, and an error message displays.

Compatibility

- Starting with VTE for AIX version 5.3, CTE is backward compatible with, and fully supports, the existing AES-CBC mode for both new and existing datasets.
- Starting with VTE for AIX version 5.3, CTE fully supports AES-CBC-CS1 encryption for offline data transformation on CTE AIX environments.

Versions of VTE prior to version 5.3 are not backwards compatible with AES-CBC-CS1 encryption. On these earlier versions, attempting to guard a device using a policy containing an AES-CBC-CS1 key will fail.

- Protected hosts supporting AES-CBC-CS1 encryption can be added to host groups.

Difference between AES-CBC and AES-CBC-CS1

The two encryption modes are completely different from a file format standpoint.

- AES-CBC-CS1 encryption only applies to file system directories; AES-CBC encryption applies to both files and block devices.

Note

- If you attempt to use an AES-CBC-CS1 key to guard a block device or partition, the guarding fails with an error reported on the CipherTrust Manager, similar to: Raw or Block Device (Manual and Auto Guard) GuardPoints are incompatible with Policy "policy-xxx" that contains a key that uses the CBC-CS1 encryption mode."
- AES-CBC-CS1 encryption is supported in AIX environments; as long as it is a local JFS2 or remote file system using NFS, the file formats will be compatible. It is possible that an encrypted file created with a specific AES-CBC-CS1 key on AIX cannot be read on a Linux or Windows local file system, even if that specific key were to be used, and vice versa.

- AES-CBC-CS1 uses cipher-text stealing to encrypt the last partial block of a file whose size is not aligned with 16 bytes.
- Each file encrypted with an AES-CBC-CS1 key is associated with a unique and random base IV.
- AES-CBC-CS1 implements a secure algorithm to tweak the IV used for each segment (512 bytes) of a file.

Disk Space

Files encrypted with AES-CBC-CS1 keys consume additional disk space in contrast to files encrypted with AES-CBC keys. This is because AES-CBC-CS1 encryption requires file IVs to be created and persistently stored in contrast to AES-CBC encryption which does not consume any additional disk storage.

Therefore, administrators need to plan and provision additional disk capacity prior to deploying AES-CBC-CS1 encryption.

	AES-CBC	AES-CBC-CS1
Local AIX FS	No change to file size. No extended attribute allocation	Extra 4KB allocation in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.
Remote AIX FS	No change to file size. No extended attribute allocation	Extra 4KB allocation in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.

Encryption Migration

You can use offline dataxform to:

- Transform data encrypted by AES-CBC to AES-CBC-CS1 and vice versa.
- Transform AES-CBC-CS1 encrypted data to clear contents and vice versa.

File Systems Compatibility

On AIX, you can use AES-CBC-CS1 keys to guard currently supported file systems.

AES-CBC-CS1 encrypted files on AIX local file systems can result in additional space consumption.

AES-CBC-CS1 files on AIX local or remote file systems such as JFS2 embed the IV in a 4K-byte header within the file. When these files are guarded, CTE masks the file header to applications and system utilities. The expanded file is only apparent when CTE guarding is disabled.

Note

The file system must have enough extra space to store the extra 4K bytes of the embedded header.

On AIX, with AES-CBC-CS1 encryption, encrypted files on all file systems, both remote or local, have the same file format.

Storing Metadata

AES-CBC-CS1 encrypted files on AIX store the base IV of a file in the embedded header of the file.

To get the value of the base IV, type:

```
voradmin secfs iv get <file-name>
```

Note

The base IV of a file is protected. It cannot be set/modified/removed by commands and applications. However, if a GuardPoint is unguarded, the files in the GuardPoint are no longer protected. An adversary can then corrupt the content of the files, as well as the IVs.

Using the AES-CBC-CS1 Encryption Mode in CM

When you create a key in CTE, you enable Encryption Mode by selecting CTE Key Properties. See *Creating a New Key* in the [Managing Policies](#) chapter in the [CTE Administrator Guide](#).

Best Practices for AES-CBC-CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC-CS1 keys unless all hosts are running VTE for AIX version 5.3 or CTE version 7.0.0 or later.

Exceptions and Caveats

Note the following when using AES-CBC-CS1 keys.

Guarding Existing Files Without Data Transformation

You must convert an existing file with clear text through offline data transformation. If you do not transform the file, then after you guard using an AES-CBC key, the file displays garbled characters.

If you use an AES-CBC-CS1 key, access to the file is blocked with an I/O error.

Utilities for CTE Management

Thales provides a variety of utilities that augment the standard AIX utilities. This combination of tools helps administrators manage CTE. The following utilities are described in this section:

- [Agent Health Return Codes](#)
- [Agentinfo \(Java version\)](#)
- [Backup](#)
- [Check_host](#)
- [Displaying Information for Nested File Systems with the DF tool](#)
- [Protecting Files with Client Settings](#)
- [Restricting Access Overrides with Client Settings](#)
- [Register_host](#)
- [SecFSD](#)
- [Using Client Settings with Shell Scripts](#)
- [Vmutil](#)
- [VMsec](#)
- [VMD](#)

Agent Health Utility

The `agenthealth` utility validates:

- Super-user privilege
- CTE Agent installation
- CTE registration to CipherTrust Manager Server
- CTE processes/ modules that are running

- Available disk resources
- Current GuardPoints
- Tests if the agent can reach the GuardPoints
- CTE log directory resource status
- This directory contains pending CTE log files for upload. This utility reports the size and number of pending files for upload. These text files are logs that contain vmd/SecFS information. They are regenerated whenever secfs restarts. If the number of files is unexpectedly large, this can indicate a problem.

The Agent Health check script

By default, the `agenthealth` script is installed in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`.

To run the `agenthealth` check script, type:

```
./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
```

System Response

```
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
dsm4209.sjinternal.com is resolvable ..... OK
dsm4209.sjinternal.com port 8446 is reachable .... OK
dsm4209.sjinternal.com port 8447 is reachable .... OK
Can communicate to at least one server ..... OK
VMD is listening on port 7024 ..... OK
Time of last update from server ..... 2021-07-07 15:47:08.290
Checking available disk space ..... OK
Checking logging space ..... OK
    Log directory is "/var/log/vormetric"
    File system for log data is "/", 48G free (5% full)
    Log directory contains 9 of maximum 200 files (4% full)
    Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to /media ..... OK
Testing access to /usr/data/sub1 ..... OK
[root@agt4206 bin]#
```

Agent Health Return Codes

Previously, the agent health return codes were only available in `/var/log/vormetric/agenthealth.log`. Now, the following options are also available through the help pages:

Help

This agent health script checks various facets of the CipherTrust agent to make sure that everything is functioning properly. Results are also logged to `/var/log/vormetric/agenthealth.log`.

Syntax

```
./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --help
```

Return Codes

Use the return code option to get a list of the return codes and what they mean. The codes are returned if the Agent is not running.

Syntax

```
./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --return_codes
```

Response

Return Code	Definition
EPERM	User is not root.
ENOENT	One of the programs used in this script does not exist. See <code>/var/log/vormetric/agenthealth.log</code> for which program is missing.
ENOPKG	Agent software is not properly installed. Agent configuration directory is missing or corrupt. See <code>/var/log/vormetric/agenthealth.log</code> for more details.
EPROTO	Agent is not registered to a key manager. Register the agent to a key manager and try again. Try the wait option if the agent has never started correctly after registration. See <code>/var/log/vormetric/agenthealth.log</code> for more details.
EIO	Kernel modules are not loaded. To load a kernel module, type: <code>/etc/vormetric/secfs start</code>
ESRCH	VMD is not running. To start vmd manually, type: <code>/usr/bin/vmd</code>
SECFSD	Secfsd is not running. To start the secfsd manually, type <code>/usr/bin/secfsd</code>
EHOSTUNREACH	Unable to reach the Key Manager. Check network connectivity.
ECONNREFUSED	VMD is not listening. VMD did not finish initialization. See <code>/var/log/vormetric/vmd.log</code>
EWOULDBLOCK	VMD is attempting to connect to the Key Manager but has exceeded the designated wait time. Check <code>/var/</code>

Return Code	Definition
	log/vormetric/vmd.log to fix any issues and retry.

Wait Time

Use --w to set a maximum wait time in seconds. The minimum is 10 seconds to test for the VMD to Key Manager initial contact. The default setting is 0, which means that there is no wait. Maximum is 1200 seconds.

Syntax

```
[root@agt4206 bin]# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
--w <value>
```

Example

```
[root@agt4206 bin]# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin//agenthealth
--w 60
```

Response

```
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
dsm148.i.vormetric.com is resolvable ..... OK
dsm148.i.vormetric.com port 8446 is reachable .... OK
dsm148.i.vormetric.com port 8447 is reachable .... OK
Can communicate to at least one server ..... OK
VMD is listening on port 7024 ..... OK
Time of last update from server ..... 2021-08-18 10:34:56.665
Checking available disk space ..... OK
Checking logging space ..... OK
Log directory is "/var/log/vormetric"
File system for log data is "/", 29G free (23% full)
Log directory contains 1 of maximum 200 files (0% full)
Log directory contains 0 of maximum 100 Mbytes used (0% full)
```

If the customer did not use the wait time options, the output would look similar to the following:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
Can communicate to at least one server ..... FAILED
```


For more information consult the log file `/var/log/vormetric/agenthealth.log`

agentinfo Utility (Java version)

The `agentinfo` utility collects system and CTE configuration data. The `agentinfo` utility is used to take a configuration snapshot of the system that you will send to Thales Customer Support to debug an issue, (This section describes the Java version.)

The `agentinfo` utility is a Java Script file. You can open it in a text editor to see specific functions.

The `agentinfo` utility displays status information on the screen and outputs the results to a compressed tar file. The compressed tar file name format is `ai.<os_name_ver>.qa.com.tar.gz` and it is located in the current working directory.

To create an `agentinfo` file, type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/agentinfo
```

Backup Utility

When a backup is performed, certain files and directories may be protected against access. Therefore, those files and directories are not written to the backup repository. These include files located in Data Transformation GuardPoints or files in GuardPoints with appropriate policies. Additionally, the following files are locked by default by CTE agent:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/.access
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/etc/*
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem/*
```

The following describes how to bypass the issue for multiple scenarios:

Agent is installed in the default location

1. Stop SecFS, type:

```
/etc/vormetric/secfs stop           //Linux

/etc/rc.d/rc2.d/S99secfs stop       //AIX
```

2. Run the backup application with the desired arguments.
3. Restart SecFS, type:

```
/etc/vormetric/ start
```

Using a backup image to install to other agents or restore to a different system

Note

When the image is used to reinstall the system, the agent will automatically start at system boot and will attempt to connect to the key manager to which it was originally registered.

To prevent multiple systems with the same agent ID, you must uninstall CTE from the system before running the backup application. The restore/install from the backup will not have an agent running.

1. Uninstall the agent, type

```
/opt/vormetric/DataSecurityExpert/agent/secfs/bin/uninstallsfs
```

2. Run the backup application with the desired arguments.
3. Re-install CTE agent.

Performing a backup while the agent is running

Before running the backup application, add the files that are protected by the agent to the exclusion rules to exclude them from the backup:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/.access  
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/etc/*  
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem/*
```

The GuardPoint policy may implement access restrictions which would also cause the backup application to generate error messages. These GuardPoint/directories will also need to be added to the exclusion rule method to exclude them from the backup. Alternatively, you can temporarily unguard them while the backup application is running.

If the CTE agent reports a status of incomplete in the backup application and does not start properly, or partially starts but generates error messages at system boot time, then uninstall and reinstall the agent. The restore/clone image contains everything needed to uninstall the agent. Use the following command to perform this operation:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/bin/uninstallsfs
```

Backing up Databases after Encryption

After encrypting a database, CipherTrust Transparent Encryption cannot make a backup of the database. Both scheduled and manual backup fail. The problem was the user's policy. A policy used in this scenario must follow a few rules.

With a CBC_CS1 key, a guarded file is modified to have a 4096 byte header holding key information. When an

Apply Key effect is specified, the CipherTrust Transparent Encryption code adjusts the length and file offset for this header. Without an **Apply Key** effect, the size and access of the offset include the CBC_CS1 header.

Thales recommends that you modify the first rule of your policy. Remove the action entry for `f_rd_att` from the first rule and add a new rule before it:

```
**action**: f_rd_att

**effect**: Permit, Apply Key
```

Policy processing starts with the first rule and continues until a matching rule is found. The effect for the matching rule is then applied.

For the `f_rd_att` action, this results in the secfs code including the CBC_CS1 key header and adjusts the file size value. Without the Apply Key effect, the file size includes the CBC_CS1 header size and the file appears as 4096 bytes larger than its real size.

check_host Utility

If a CTE software installation fails during the certificate generation and exchange stage, use the `check_host` utility to list the network addresses for the host. The utility checks network interfaces, `/etc/hosts`, DNS, and so on, to compare, test, and evaluate possible addresses for the host, and weights them based upon their network efficiency. FQDNs are the most preferred and stand-alone IP addresses are the least preferred. Some applications, such as silent-mode installation, use `check_host` to determine the best host address to submit to the CipherTrust Manager during registration.

Run the `check_host` utility on a system that is hosting CTE to display available network host names, FQDNs, and IP numbers for the host.

Type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/check_host
```

check_host Syntax

```
check_host [[-h | -i | -a ] [-s name]] |
-l name:port[,name:port] | -r name
```

Syntax	Description
-h	Print the best host name for this machine
-i	Print the best IP address
-a	Print all the host names and IP addresses
-s	The name of the server (optional hint)
-r	The name of the server for name resolution checks
-l	The name and port of the server for listening checks

Displaying Information for Nested File Systems with the DF tool

When a file system mounts on top of another file system, the command `df -a` does not display the attributes for the covered file system.

On Linux environments, this is the expected behavior for any file system that is overlayed by another file system.

The secfs driver properly handles the call, which is made by the `statfs` system call, which is issued by the `df` tool. When the system call returns, its structures are correctly populated with the details of the nested file system. On examining the source of the `df` tool, it is found that when the `-a` switch is on, it nullifies the stats which are received for overlayed mounts. When the `-a` option is not enforced, the stats are maintained.

Issue the `df` command for a specific mount point, for example `df /xfs/nested-xfs` (where `/xfs` is a secfs GuardPoint). It works correctly.

Protecting Files with Client Settings

When any file is now marked as protected (`|protect|`) in the client settings, that file is protected from being modified or deleted, (even from a root process).

Note

The file is not guarded and it can be external to a GuardPoint.

Previously, the only files that were protected were the following:

```
/etc/passwd
/etc/group
/etc/security/passwd
/etc/ssh/sshd_config
/etc/ssh/sshrd
/opt/testfile
```

If the file marked as `|protect|` does not exist, then CipherTrust Transparent Encryption creates a 0-length file in its place. This provides an efficient means to identify and implement file protection. When the agent is stopped or uninstalled, these 0-length files are deleted and then re-created if the agent is restarted. Additionally, an audit record is generated when a file operation is denied.

The `|protect|` status is displayed using `secfsd -status auth`.

Restricting Access Overrides with Client Settings

CipherTrust Transparent Encryption host/client settings are the means by which an administrator configures user authorization. Users with root privileges, on Linux or AIX systems, have the unfettered ability to override all file access and execution permissions imposed by the system.

CipherTrust Transparent Encryption access control allows you to restrict privileges of users, groups, application processes and binaries, including root users and setuid programs. By default, CipherTrust Transparent Encryption agent **DOES NOT** trust any process as authenticated. Any attempt to access a resource, by any process, will therefore be flagged with a "User Not Authenticated" notification. The CipherTrust Transparent Encryption agent

must be instructed to trust the authenticator process progeny. For example, `/usr/sbin/sshd` is a process that can be trusted to authenticate the user to the system and to CipherTrust Transparent Encryption.

In some setups, when editing a host, system administrators can use the **host settings** > **|authenticator|** feature with **su** to change identities and gain access to restricted data. You can instruct CipherTrust Transparent Encryption to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CipherTrust Transparent Encryption can block from authenticating other processes.

Any executable path that is marked with a **|path_no_trust|** host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

CipherTrust Transparent Encryption prevents overrides from other host settings authenticators, using the **|path_no_trust|** status. If a user runs the **su** command from a non-trusted shell, that new shell is still marked as **|path_no_trust|**, even if **|authenticator|/usr/bin/su** is specified in the host-settings. The **|path_no_trust|** feature overrides any and all authenticators under host settings.

Note

Using **|trust|*** before a **|path_no_trust|** host setting no longer disables the **|path_no_trust|** host setting.

For example, the following host setting denies authentication for users accessing through `sshd`:

```
|trust|*
|path_no_trust|/usr/sbin/sshd
```

To restrict access overrides:

1. In the CipherTrust Manager products page, click **Transparent Encryption > Clients**.
2. Click on an existing Client name to edit the host.
3. Click **Client Settings** tab.
4. Add the following to the settings:

```
|path_no_trust|<path of the binary>
```

Example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **Apply**.

register_host Utility

Use the `register_host` utility to create certificate requests, exchange certificates between the CipherTrust Manager and the host, and to register CTE on the CipherTrust Manager. After the host is registered, you can configure CTE, apply GuardPoints, or perform database backups. Run the `register_host` utility in text mode on a terminal window.

Caution

The default host registration timeout is 10 minutes. If the host is unable to reach the CipherTrust Manager within the allotted period because of an extremely slow network connection, set the **REGISTER_HOST_TIMEOUT** environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

secfsd Utility

The `secfsd` utility displays the following attributes of CTE:

- GuardPoints defined in the *GuardPoints* tab
- Authentication parameters defined in the *Host Settings* tab
- Lock status set by enabling **FS Agent Locked** and **System Locked**
- Web destination and SSL certificate for uploading log entries
- Policies applied in the **GuardPoints** tab
- Status of required processes (`secfsd` and `vmd`)
- Version of `secfs`

The `secfs` utility is also used to mount GuardPoints for **Directory (Manual Guard)**. Normally, CTE automatically mounts the `secfs` file system when you apply a GuardPoint to a directory. On AIX, the `secfsd` utility is located in `<install_dir>/secfs/.sec/bin` and a symbolic link to this file is placed in `/usr/bin/secfsd`.

secfsd syntax

Command	Description
<code>-help</code>	display <code>secfsd</code> options

Status Options

Command	Description
<code>-status guard [-v -tree]</code>	list all GuardPoints

Command	Description
<code>-status keys</code>	show current encryption key state
<code>-status auth</code>	list authentication settings
<code>-status lockstat</code>	show CTE lock status
<code>-status logger</code>	list logging details
<code>-status policy</code>	list configured policies
<code>-status pslist</code>	list protected processes
<code>-status devmap</code>	list guarded devices

Manual GuardPoint options

Command	Description
<code>-guard path [container ID]</code>	manually guard path
<code>-unguard path [container ID]</code>	manually unguard path

Version option

Command	Description
<code>-version</code>	list version of kernel module <code>secfs2</code>

Encryption Mode option information

Command	Description
<code>crypto</code>	Displays the encryption modes that are supported.

Configuration Mode option information

Command	Description
<code>config <config_param> <value></code>	Displays the encryption modes that are supported.

secfsd Examples

Display GuardPoint Information

To display the GuardPoint paths, applied policies, policy type, and guard status, use the `secfsd -status guard` command. For example:

```
secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/opt/apl/lib	allow AllOps_fs	local	guarded	guarded	N/A
/dev/sdb	watchaccess_rd	rawdevice	guarded	guarded	N/A

/dev/sdc	watchaccess_rd	manualrawdevice	guarded	guarded	N/A
/dev/sdd	watchaccess_rd	manualrawdevice	unguarded	not guarded	Inactiv
/opt/apl/tmp	MSSQL00123	manual	unguarded	not guarded	Inactiv

Column	Description
GuardPoint	Full path of the GuardPoint.
Policy	Name of the policy applied to the GuardPoint.
Type	Can be local, automount, manual, raw device, or manual raw device. Configured in the GuardPoints tab.
ConfigState	Guard status of the GuardPoint, as recognized by the key manager. It can be guarded or unguarded.
Status	Current guard status, as recognized by CTE. State can vary.
Reason	Additional information about the status, if any.

Note

- Config State and Status can vary. As an example, if you apply a GuardPoint and someone is currently working in the GuardPoint, the policy cannot be applied at that time. In this case, the ConfigState is guarded and the Status is not guarded.
- When the user removes an auto-mounted GuardPoint from CipherTrust Manager, the CTE Agent is only deleted after the configured `autofs` timeout expires. This timeout does not start until the GuardPoint is free.

Display GuardPoint Information in a Different Format

To display the same information in a block format, use the `secfsd -status guard -v` command. For example:

```
secfsd -status guard -v

GuardPoint: 1
  Policy:      allowAllOps_fs
  Directory:   /opt/apps/apps1/tmp
  Type:        local
  ConfigState: guarded
  Status:      guarded
  Reason:      N/A
GuardPoint: 2
  Policy:      allowAllRootUsers_fs
  Directory:   /opt/apps/apps1/lib
```



```
Type:          local
ConfigState:   guarded
Status:        guarded
Reason:        N/A
```

Display Host Settings

To display the SHA2 hash signature for each protected host setting, use the `secfsd -status auth` command. For example:

```
secfsd -status auth

|authenticator|/bin/su 3E765375897E04C39AB17D4C755F50A35195535B6747DBA28DF9BD4AA6
72DFF9
|authenticator|/usr/sbin/sshd 98FC599D459EDEA52A60AB394B394803B5DAB96B53148DC6087
32DDA6777FA1A
|authenticator|/usr/sbin/in.rlogind 5C9A0EDD8BF54AE513F039476D21B3032507CF957AA0C
B28C368EB8AB6E684FB
|authenticator|/bin/login 0D2EE0B995A30AE382B4B1CA5104715FC8902F457D283BDABAAD857
B09259956
|authenticator|/usr/bin/gdm-binary 363780522E3CCF9ABF559F059E437743F9F97BBBB0EE85
769007A464AD696BD1
|authenticator|/usr/bin/kdm BAD41BBCDD2787C7A33B5144F12ACF7ABC8AAA15DA9FDC09ECF93
53BFCE614B5
```

Display Key Status

To display the status of CTE keys, use the `secfsd -status keys` command. For example:

```
secfsd -status keys
Encryption keys are available
```

Display Lock Status

To display the status of CTE locks, use the `secfsd -status lockstat` command. For example:

```
secfsd -status lockstat
FS Agent Lock: false
System Lock: false
```

The value is **true** if the lock is applied. The value is **false** if the lock is not applied. **System Lock** corresponds to **System Locked** in the *Host* window. **FS Agent Lock** corresponds to **FS Agent Locked** in the *Host* window.

Note

Before you upgrade, remove CTE software, or change operating system files, the status of FS Agent Lock and System Lock must be false.

Agent Security Configuration Protection

The Agent lock directory, `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec` contains secfs secret files, configuration files, host setting signatures, etc. Thales recommends protecting the directory whenever secfs is online.

Applying improved directory protection ensures that only CTE applications (`vmd`, `secfsd`, `voradmin`, etc.) can modify the `.sec` directory and the files in it. All users, including root, are denied read/write access to the files. They also do not have permissions to modify `conf` and `bin` directories, using other tools.

A new command has been created to protect the directory: `voradmin secfs config`

Syntax

```
voradmin secfs config <configuration_parameter> <value>
```

Example

```
voradmin secfs config pagecache_writeback 1
```

Previously, you would have had to use the following command to achieve the same results as the example above:

```
echo 1 > /opt/vormetric/DataSecurityExpert/agent/secfs/.sec/conf/pagecache_writeback
```

Note

When CTE is upgraded to v7.2.0 from the previous release, it may display 'Permission Denied' warnings which display when files are removed from subdirectories of the `.sec` directory. You can ignore these warnings. They are harmless.

Display CTE Log Status

To display the status of CTE log service, use the `secfsd -status logger` command. For example:

```
secfsd -status logger

Upload URL: https://vmSSA06:8444/upload/logupload,https://vmSSA07:8444/upload/logupload, \
https://vmSSA05:8444/upload/logupload
Logger Certificate directory: /opt/vormetric/DataSecurityExpert/agent/vmd/pem
```

This command sequence returns the URL to which the log service sends log data. It also returns the directory that contains the CTE certificate. CTE uses the certificate to authenticate CTE when it uploads the log data to the CipherTrust Manager.

Display Applied Policies

To display the policies that are applied to CTE, use the `secfsd -status policy` command. For example:

```
secfsd -status policy

Policy: enc-audit
Type: ONLINE
```

Display CTE Process Information

To display CTE processes, use the `secfsd -status pslist` command. This command shows the process number associated with each CTE process. To show the details about a specific CTE process, use the `ps -fp <process #>` command, where `<process #>` is the process number from the `secfsd -status pslist` command.

For example:

```
secfsd -status pslist
Protected pid list:      739    731

ps -fp 739
UID      PID    PPID   C   STIME      TTY   TIME   CMD
root     739     1      0   11:04:56   -    0:00 /opt/vormetric/ \
        DataSecurityExpert/agent/vmd/bin/vmd
```

Display CTE Version Information

To display CTE version information, use the `secfsd -version` command. For example:

```
secfsd -version
version: <Release.build-number>
```

Manually Enable a GuardPoint in CipherTrust Manager

To manually enable a GuardPoint on an AIX host:

1. Click **CTE > Clients > <clientName> GuardPoints**
2. Click **Create GuardPoint**.
3. In the Policy field, select a policy.
4. Set Type to **Manual Directory**.
5. Click **Browse** and enter the GuardPoint path.
6. Click **Create**.
7. Log onto the system hosting CTE as the root user.

8. To manually enable the GuardPoint, use the `secfsd -guard <path>` command. For example:

```
secfsd -guard /opt/apps/etcsecfsd: Path is Guarded
```

9. To verify the change, use the `secfsd -status guard` command. For example:

```
secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/opt/apps/etc	allowAllOps_fs	manual	guarded	guarded	N/A

secfsd and Raw Devices

CTE only creates block devices. To display them, use the `ls -l /dev/secvm/dev` command. For example:

```
ls -l /dev/secvm/dev
```

```
brw----- 1 root    system    38,  1 Jan 29 16:37 hdisk1
brw----- 1 root    system    38,  2 Jan 29 16:37 hdisk2
crw----- 1 root    system    38,  3 Jan 29 16:37 rhdisk1
crw----- 1 root    system    38,  4 Jan 29 16:37 rhdisk2
```

Using Client Settings with Shell Scripts

Client settings on a shell script do not work as expected in AIX. This is because a shell script is not executed as a binary by a shell, rather, it is interpreted by the shell as a sequence of commands.

This limitation may be overcome by running the shell script in the context of a binary. A program is constructed to issue an `exec1(2)` of a shell with the desired script as its argument.

The client settings are then applied to the binary. When it executes, the client setting is applied to it by the agent code. Therefore, when it runs the shell, the client setting is inherited by the shell and is subsequently applied to all of the commands run as the script executes.

Following is an example program for implementing Client Settings:

```
cc testcode.c -o testcode
-----

#include <unistd.h>
#include <errno.h>
#include <stdlib.h>

int
main(int argc, char *argv)
{
    int rv;
```

```

    rv = execl("/usr/bin/ksh", "ksh", "./testdata", NULL);
    if (rv < 0) {
        printf("execl errno %d\n", errno);
        exit(1);
    }

    exit(0);
}

```

- The file, testdata, contains the shell script text.
- For test purposes, use a shell script that contains:

```
/usr/bin/cat
```

- The client setting is applied to the testcode binary. When it runs, the client settings are applied to the components of the script, testdata.

vmsec Utility

The vmsec utility allows you to manage security aspects of CTE on the host. On AIX hosts, the **vmsec** utility is located in:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/vmsec
```

vmsec Syntax

Syntax	Description
checkinstall	Show vmd kernel status
challenge	Enter the dynamic host password
vmdconfig	Display the vmd configuration
check_hwenc	Display kernel configuration
hwok	Report status of hardware signature
passwd [-p <password>]	Enter the static host password
version	Display CTE version

vmsec Examples

- Display CTE Challenge String
- Display CTE Status
- Entering a Password

- Display Kernel Status
- Display CTE Build Information
- Display Contents of Conf files

Display CTE Challenge String

To display a CTE password challenge string and enter the response string when the CipherTrust Manager is not network accessible, use the `vmsec challenge` command. This command displays a challenge string that you can send to your key manager administrator, who will then send you back the correct response information.

For example:

```
vmsec challenge
Contact a Security Server administrator for a response.
Your hostname is host120.my.domain.com
Your challenge is: F5TL-42HU-5H6Y-EJCK
Response (part 1) -> 6B2T-Q3DV-5EK3-Q0FD
Response (part 2) -> XBP5-LQXB-TDWA-SILG
Response (part 3) -> XSEA-CQB5-S6U5-3YWV
Response (part 4) -> KXRS-QYXB-BP74-C4RN
Success!
```

Contact your key manager administrator and give them the challenge string. The administrator will give you four response strings. Enter the first response string in the **Response (part 1)** field and press **Enter**, then enter the second, third, and fourth response strings in the same way. You have 15 minutes to enter the first response string.

Tip

If you are using CipherTrust Manager, the ability to change the contact string will be added in a future release. For CipherTrust Manager, the contact string says "Contact your CM administrator".

Display CTE Status

This utility shows you if CTE is configured and running. If it is not running, you might need to start it manually. To display CTE status, use the `vmsec checkinstall` command. For example:

```
vmsec checkinstall
The kernel component is installed and running.
```

Entering a Password

To enter the CTE static host password, use the `vmsec passwd` command. For example:

```
vmsec passwd
Please enter password:
```

```
OK passwd
```

To enter CTE static host password on the command line so you can specify it in a batch script, specify the password using the `-p` option. For example:

```
vmsec passwd -p myPass123
OK passwd
```

Display Kernel Status

To display the kernel status, use the `vmsec status` command. For example:

```
vmsec status
FILE_FORMAT=2
FILE_GENERATED=08/27/2019 18:54:10
SA_QOS_STATUS=0
SA_HOST_CPU_UTIL=0
GP_1_Policy=27
GP_1_Dir=/gp
GP_1_lock=1
GP_1_type=1
GP_1_gtype=manual
GP_1_opt=gtype=2,policy=27,lock=1,type=1,dir=/gp/
GP_1_config_state=unguarded
GP_1_status=not guarded
GP_1_statuschk_tm=0-00-00 00:00:00
GP_1_config_op_retry_cnt=0
GP_1_config_op_attempt_tm=0-00-00 00:00:00
GP_1_flags=0
GP_1_reason=Inactive
GP_1_usage=free
TOTAL_GP=1
KEYS_AVAILABLE=TRUE
sdk_version=<Release.build-number>
sdk_builddate=2019-08-19 15:16:46 (PDT)
coreguard_locked=false
system_locked=false
logger_upload_url=https://thl602-2114.qa.com:8447/upload/logupload,https://thl602-2116.qa.com:8447/upload/logupload
logger_cert_dir=/opt/vormetric/DataSecurityExpert/agent/vmd/pem
hostname_for_logging=vmd
QOS_PAUSED=false
vmd_STRONG_ENTROPY=false
vmd_URL=https://thl602-2114.qa.com:8446
vmd_SRV_URLS=https://thl602-2114.qa.com:8446, https://thl602-2116.qa.com:8446
vmd_PRIMARY_URL=https://thl602-2114.qa.com:8446
vmd_SUPPORTS_F8P=TRUE
vmd_SUPPORTS_CR256=TRUE
vmd_RANDHP=TRUE
learn_mode=false
concise_logging=false
vmd_listening_port=7024
vmd_initialization_time=2019-07-25 12:07:14.514
vmd_last_server_update_time=2019-07-25 12:12:04.747 policy_name_27=aes256
policy_version_27=0
```

```

policy_keyvers_27=0
policy_type_27=ONLINE
policies=27
logger_suppression_VMD=SUPPRESS
logger_intervaltime_VMD=600
logger_repeat_max_VMD=5
logger_suppression_POL=SUPPRESS
logger_intervaltime_POL=600
logger_repeat_max_POL=5
CONFIG_SA_1=27
TOTAL_CONFIG_SA=1
SA_1_NAME=27
SA_1_ALIAS=aes256
SA_1_TYPE=0
SA_1_REF=1
SA_1_HIP_REG_TIME=0
SA_1_FLAGS=1
TOTAL_SA=1
TOTAL_AUTH=0
AUTHBIN_1=|authenticator|/usr/sbin/sshd B92A3D7EEF67B82230F7F76097D65159FCF5722A4
154A249EFD C22C20F1B572C
AUTHBIN_2=|authenticator|/bin/login 4F210D1B83ACD79B006BCF7DB247ED002A45FC892C427
20390BFA6AE21AEA8DC
TOTAL_AUTHBIN=2

```

Display CTE Build Information

To see the CTE build version, use the `vmsec version` command. For example:

```

vmsec version
version 7
2020-07-31 10:03:59 (PDT)
Copyright (c) 2009-2022, Thales. All rights reserved.

```

Display Contents of Conf files

To display the contents of the `agent.conf` and `.agent.conf.defaults` files, use the `vmsec vmdconfig` command. For example:

```

vmsec vmdconfig
appender_syslogdest_Syslog_Appender_0=127.0.0.1
VMSDK_AGENT_CONFIG_FILE=/opt/vormetric/DataSecurityExpert/agent/vmd/etc/agent.conf
appender_layout_Syslog_Appender_0=Syslog_Layout
VMSDK_AGENT_VERSION=7.2.0.128
VMSDK_AGENT_BUILD_ID=28
PREV_URLS=https://srv.my.thales.com:8443
syslog_appender_myhost name=dev.my.thales.com
VMD_PORT=7024
...
...
appenders=Upload_Appender, File_Appender, Syslog_Appender_0
layouts=Upload_Layout, File_Layout, Syslog_Layout, Simple

```



```
CONNECT_TIMEOUT=180000
URL=https://srv.my.thales.com:8443
STRONG_ENTROPY=false
```

Configuring Dynamic Host Settings for AIX

Previously, when host settings were changed, currently executing processes for the specified images were not modified. Only when a new process started would the changed host settings take effect. To make an already running process use the new host setting values, you had to terminate the process and restart it. The Dynamic Host Setting feature now permits the modified host settings take effect when the new entries are pushed from the CipherTrust Manager to the agent.

If the Dynamic Host Setting feature is enabled, then when a host setting is altered, all running processes with that signature are affected and their existing security attributes are modified to the new host settings parameters. Future actions by a process will contain authorization(s) derived from the new attributes. It is important to note that all descendent processes are affected by a process's host setting change. If an existing host setting entry is modified, the same situation occurs.

If an existing process did not have a host setting and one is applied, then all processes with that signature are updated with the new values. All of the existing descendent processes are affected by the changes. New child processes inherit the host setting parameters and authorizations.

In v7.2 of CTE, three new `vmadmin` commands are provided to enable, disable, and report the status of the Dynamic Host Settings:

- To turn on dynamic host settings, type:

```
voradmin secfs config dhs_on 1
```

Note

You must restart the agent for this to setting to take effect.

- To turn off dynamic host settings, type:

```
voradmin secfs config dhs_on 0
```

Note

You must restart the agent for this to setting to take effect.

- To report the state of the dynamic host settings, type:

```
voradmin secfs config dhs_state
```

Note

State information is added to the secfs.log file.

- To immediately enable dynamic host settings without restarting the agent, type:

```
voradmin cmd dhs_enable
```

Note

You must restart the agent for this to setting to take effect. Perform this command after turning on DHS.

- To immediately disable dynamic host settings without restarting the agent, type::

```
voradmin cmd dhs_enable
```

Note

Restarting the agent will enable it unless you turn the dynamic host settings off first.

vmutil

Usage

```
vmutil <options> <operations>
```

Options

Option	Function	Description
-a	--agent <name>	Specify agent type (vmd or pkcs11)
-d	--extdir <string>	Specify location of external certificate and key set

Option	Function	Description
-e	--error <string>	Specify one or more errors for state report
-h	--help	Display help and exit
-l	--loglevel <level>	Specify log output level (debug, info, warn, error or fatal)
-f	--force enabled	Force option for delete host operation
-v	--version	Display program version and exit

Operations

Operation	Description
certexpiry	Report the certificate expiration date for this agent
deletehost	Delete this client from the server
renewcerts	Renew certificate set for this agent
reportstate	Report agent state and error conditions to server
unregister	Unregister this agent/client from the server
updatecerts	Update external certificate and key set for this agent/client

vmd utility

The **vmd** utility displays CTE software version information.

The **vmd** utility is located in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin` and a symbolic link to this file is placed in `/usr/bin/vmd`.

Syntax

vmd [OPTIONS...]

-h show utility syntax

-v display CTE version

-f runs **vmd** in the foreground

Display the Installed Version

To display the installed CTE version, type:

```
vmd -v
```

```
Version 7  
<Release.build-number>  
2022-02-04  
Copyright (c) 2009-2022, Thales.. All rights reserved.
```

Upgrading CTE on AIX

This chapter describes how to upgrade an existing VTE for AIX host to CipherTrust Transparent Encryption (CTE) for AIX.

Scheduling a CTE Agent Upgrade

You can schedule an upgrade of the CTE Agent to occur the next time the server on which a CTE Agent is installed reboots normally. Scheduling an upgrade can minimize CTE service interruptions and reduce coordination issues in organizations where the security roles are separated.

Note

Scheduled upgrade on reboot is available in VTE for AIX version 5.3.0 GA and onwards. You cannot schedule an upgrade from an earlier version of VTE to version 5.3.0 GA or to CTE version .

Before You Begin

Keep in mind the following prerequisites for using scheduled upgrade, usage notes, and how scheduled upgrade behaves when errors occur:

- If a crash/power failure occurs before a user-initiated reboot, the scheduled upgrade runs when the system comes up after the crash/power failure.
- CipherTrust Manager connectivity is required during the scheduled upgrade process.
- All databases must be configured to automatically stop before CTE services stop during reboot/shutdown.
- Stopping and restarting the CTE Agent does not trigger a scheduled upgrade.
- The installation binary used to run the scheduled upgrade is stored in `/var/tmp` until the scheduled upgrade runs. Ensure that no scheduled maintenance jobs periodically delete files in `/var/tmp`. All temporary files used by scheduled upgrade are removed following a successful scheduled upgrade.

Using the Scheduled Upgrade Feature

Note

If a scheduled upgrade has been enabled but has not run because the system wasn't rebooted, you can override the existing scheduled upgrade with a newer CTE version by using the procedure described here with the newer installation binary.

1. Verify that the version of CTE you currently have installed is eligible for scheduled upgrade:

```
vmd -v
```

The version listed must be version 5.3.0 or later.

2. Log in as root, change to the directory containing the installation binary, and run the binary with the `-u` scheduled upgrade option. For example:

```
./vee-fs-7.8.0.75-aix71.bin -u
```

The following upgrade confirmation is displayed:

```
upgrade on reboot configured
```

Note

If syslog is properly configured, appropriate logs will be logged in syslog.

3. When you are ready, reboot the server.

```
shutdown -Fr
```

When the system restarts, the scheduled upgrade runs without any intervention needed.

4. After the system is up and running, log in and run `vmd -v` to verify that the new version has been installed.

Performing an Upgrade Manually When an Upgrade is Already Scheduled

If you want to upgrade without waiting for the system to reboot, follow these steps to perform an upgrade manually when a scheduled upgrade is already enabled:

1. Log in as root, change to the directory containing the installation binary, and run the binary without the `-u` scheduled upgrade option. For example:

```
./vee-fs-7.8.0.75-aix71.bin
```

The following upgrade confirmation is displayed:

```
upgrade on reboot pending
do you wish to continue [y/n]: y
```

2. Enter “Y” to cancel the scheduled upgrade and proceed with an immediate installation. If you enter “N”, the scheduled upgrade remains enabled and occurs on the next reboot.

If you enter “Y”, the binary runs and displays the license agreement.

3. When prompted, enter “Y” to accept the license agreement or “N” to exit.

After accepting the license agreement, the normal upgrade proceeds, the scheduled upgrade is canceled, and temporary files used by the scheduled upgrade are removed.

Uninstalling CTE from AIX

Considerations

- The CTE Agent must be removed from the AIX host before the host is removed from the key manager with which it is registered.
- Database applications like DB2 and Oracle can lock the user space while they run. If the uninstall fails because a GuardPoint is in use, determine which applications are using the files in the GuardPoint and stop them. Then run the uninstall again.
- Commands like `fuser` and `lsof` might not reveal an active GuardPoint because they detect active usage, not locked states. Although it may appear that a GuardPoint is inactive, it may be in a locked state. Under this condition, software removal may fail with an error similar to the following:

```
/home: device is busy.
```

Procedure

1. Stop any application from accessing files in the GuardPoint.
2. In the key manager with which this host is registered, do the following:
 - Decrypt any data you want to use after uninstall. After the CTE Agent software is removed, access to data

is no longer controlled. If data was encrypted, it will remain encrypted. If decrypted or copied out of the GuardPoint, the data is visible as clear text.

This decryption must be done on every GuardPoint on the host if you want to access all existing data on the host.

- Make sure the Agent and System locks have been disabled for the host.
- Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.

Do not remove the host from the key manager yet.

3. Log on to the host as **root**.
4. Change the directory to an unguarded location (for example, /.).

Caution

Do not change (cd) into the /opt/vormetric directory or into any directory below /opt/vormetric. If you run the uninstaller from /opt/vormetric or any of its subdirectories, the package removal utility may fail and return the following message:

You are not allowed to uninstall from the /opt/vormetric directory or any of its sub-directories.
Agent uninstallation was unsuccessful.

5. Start the uninstall. Type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/uninstall
would you like to uninstall the vee-fs package? (Y/N) [Y]: Y
.....
Success!
```

6. Remove the host record from the key manager.



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

CTE Agent Linux Advanced Configuration Guide	5
Overview of CTE.	5
Getting Started with CTE for Linux.	10
Additional Considerations	10
CTE Agent Installation with UEFI Secure Boot.	13
Linux Package Installation for Linux Distributions.	16
Linux Package Installation for RHEL	16
Linux Package Installation for SLES	23
Linux Package Installation for Ubuntu	27
Verifying Kernel Compatibility	31
Installing CTE with No Key Manager Registration	32
Configuring CTE for Linux with CipherTrust Manager.	34
Installation Prerequisites	34
Interactive Installation on Linux	36
Silent Installation for CTE or CTE-U on Linux	41
Validating CM and CTE with a Local CA Certificate	45
Using external certificates for communication between CTE Agent and CipherTrust Manager ...	46
Installation and Registration Options	49
Guarding a Device with CipherTrust Manager.	49
Ransomware Protection	58
Ransomware Protection Overview	58
Creating GuardPoints for Ransomware Protection	61
Multifactor Authentication for CTE GuardPoints	63
Introduction to Multifactor Authentication.	63
Using Keycloak for Multifactor Authentication for CTE GuardPoints	66
Exempting some users from authentication with a Whitelist	68
Setting up Multifactor Authentication with a One-Time-Password	69
Setting up Multifactor Authentication with a Time Out	71
Administrator Tasks for Multifactor Authentication	71
Troubleshooting Multifactor Authentication	74
Special Cases for CTE Policies	74
Re-Enabling Automatic Signing for Host Settings.	74
Restricting Access Overrides from Unauthorized Identities	75
Blocking ptrace system calls to prevent process injection attacks	77
Logging.	78
Setting CTE Agent Logging Preferences	78
Audit Logs	80
Concise Logging	82
Enhanced Encryption Mode	83
Compatibility	84
Disk Space	85
Encryption Migration	85

File Systems Compatibility	85
Container Compatibility	87
Using the AES-CBC-CS1 Encryption Mode in CM	87
Exceptions and Caveats	88
Best Practices for AES-CBC-CS1 Keys and Host Groups	88
CTE and systemd	88
Overview of CTE and systemd	88
CTE Agent Control Changes on systemd	89
CTE Configuration Changes Required on systemd	89
About systemd Dependency Changes for Unit Configuration Files	90
Location of Application Unit Configuration Files	91
Adding Dependencies to systemd Unit Configuration Files	91
Adding Applications to the secfs-fs-barrier.service File	92
Drop-in Files for systemd	93
Adding Dependencies to the `saslauthd.service` File	93
SystemD Protection	94
Manually Stopping Application or Service	95
Utilities for CTE Management	96
Agent Health Utility	97
agentinfo Utility (Java version)	100
Backup Utility	100
check_host Utility	102
Displaying Information for Nested File Systems with the DF tool	103
fsfreeze and xfs_freeze	103
Protecting Files with Client Settings	105
Restricting Access Overrides with Client Settings	105
register_host Utility	106
secfsd Utility	107
secfsd Examples	108
Secfsd Raw and Block Devices	113
Using Advanced Encryption Set New Instructions (AES-NI)	113
User Cache Lookup Improvements	114
vmutil	115
vmd utility	116
vmsec Utility	116
CipherTrust in-Place Data Transformation for Linux	120
Introduction to in-Place Data Transformation (IDT)	121
Requirements for IDT-Capable GuardPoints	121
The CTE Private Region and IDT Device Header	122
IDT-Capable GuardPoint Encryption Keys	123
Guarding an IDT-Capable Device on Linux	125
Initializing an IDT-Capable Device	125
Guard the Linux Device with an IDT-Capable GuardPoint	129
Example of Creating an IDT-Capable GuardPoint on an Existing Linux Device	131
Changing the Encryption Key on Linux IDT-Capable Devices	133

Guarding an IDT-Capable Device with Multiple IO Paths on Linux	136
Linux System and IDT-Capable GuardPoint Administration	137
Resizing Guarded IDT Devices	140
Resizing Guarded IDT Devices	140
Alerts and Errors on Linux	142
Upgrading CTE on Linux	146
Uninstalling CTE from Linux	151
Migrating Agents from CTE-U to CTE	152

CTE Agent Linux Advanced Configuration Guide

This document covers the following information:

- Overview of CTE
- Getting Started with CTE for Linux
- Special Cases for CTE Policies
- Logging
- Enhanced Encryption Mode
- CTE and systemd
- Utilities for CTE Management
- CipherTrust in-Place Data Transformation for Linux
- Upgrading CTE on Linux
- Uninstalling CTE from Linux
- Migrating CTE-U Agents to CTE

Overview of CTE

For very large data sets, initial encryption deployments can affect data availability, require unacceptable maintenance windows or require cloning and synchronizing data. Encrypting millions of files can span hours or even days, which can delay encryption, or require extra disk space and data synchronization, which can be labor-intensive. Rekeying large data sets can demand significant processing time and lengthy maintenance windows. Security and IT teams face tough tradeoffs, having to choose between security and availability.

CipherTrust Transparent Encryption operates with minimal disruption, effort, and cost. Its transparent approach enables security organizations to implement encryption without changing application, networking, or storage architectures. CipherTrust Live Data Transformation builds on these advantages, offering patented capabilities that deliver breakthroughs in availability, resiliency and efficiency.

CTE includes several unique utilities to help you encrypt and manage your data. It also integrates with several third-party platforms such as Oracle, Teradata Database Appliances, and Amazon S3.

This document describes the installation and advanced configuration options for CTE, as well as detailed information about how to integrate CTE with the supported third-party products.

CTE Terminology

The guide uses the following terminology:

Term	Description	OS Applies to
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. Notes • This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". • For example, the default installation directory is /opt/vormetric/DataSecurityExpert/agent/ for Linux and AIX, and C:\Program Files\Vormetric\DataSecurityExpert\agent\ for Windows.	Windows/Linux/AIX
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.	Windows/Linux/AIX
CTE Capabilities	CipherTrust Transparent Encryption agent version-specific features like Multi-Factor Authentication.	Linux
CTE-K8s	CipherTrust Transparent Encryption for Kubernetes. Policy-based encryption of data stored on persistent volumes	Linux
CTE-RWP or RWP	CipherTrust Transparent Encryption with Ransomware Protection. Ransomware protection for volume-level (Windows)/GuardPoint (Linux) data storage through process behavior monitoring and analytics.	Windows/Linux
CTE UserSpace (CTE-U)	CipherTrust Transparent Encryption (formerly known as ProtectFile FUSE). File system level encryption and access control solution for Linux servers.	Linux
Data Transformation	Encrypting or decrypting data.	Windows/Linux/AIX
Domain Sharing	This allows Clients in one domain to get cross-domain resources, specifically GPs.	Windows/Linux/AIX
GuardPath	A directory to which a CTE Kubernetes data protection and	Linux

Term	Description	OS Applies to
	encryption policy has been applied. CTEK8s will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.	
GuardPoint	A device, or directory, to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.	Windows/Linux/AIX
Host /Client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.	Windows/Linux/AIX
In-place Data transformation	Encryption mechanism for block devices.	Linux
Key Manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers CipherTrust Manager, a key manager for use with CTE.	Windows/Linux/AIX
LDT (Live Data Transformation)	After initial GuardPoint enablement, LDT performs initial encryption, or rekeying, in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block applications and user access to data during encryption or rekey operations, which can inconvenience users and affect operational efficiency.	Windows/Linux
LDT Communication (Comm) Group	A group of LDT clients who communicate with each other, and are responsible for, initial data transformation and future key rotation of CIFS/NFS GuardPoints.	Windows/Linux
LDT GuardPoint Group	An LDT GuardPoint Group contains a collection of LDT-enabled CTE clients that are all on the same network, managed by one CipherTrust Manager, guarding a common NFS/CIFS share and can communicate with each other over that network. An LDT GuardPoint Group enables the primary host of an LDT GuardPoint Group to	Windows/Linux

Term	Description	OS Applies to
	communicate with the secondary hosts that are members of that LDT GuardPoint Group.	
LDT Primary node	The LDT GuardPoint Group node that performs LDT rekeying of data.	Windows/Linux
LDT Secondary node	All of the other clients in the LDT GuardPoint Group are assigned as secondary nodes. Note: Secondary nodes do not participate in rekeying data, however, they can be promoted to primary nodes if a primary node fails.	Windows/Linux
LDT Subordinate nodes	The subordinate nodes are the remaining nodes in the LDT Communication Group.	Windows/Linux
LDT Triad nodes	The triad nodes are the first three servers in the LDT Communication Group.	
Learn Mode	Logging mode for audit logs to help generate security policies. Learn Mode allows access to guarded paths while logging access details. Users can analyze the content users and processes are accessing, the data used, and define GuardPoint policies accordingly.	Windows/Linux
MFA	Multifactor authorization ensures that the access credentials presented belong to the actual person. After logging in to the system, when a user tries to access a CipherTrust Transparent Encryption GuardPoint, it triggers a second factor authorization to verify the user with a second form of authentication, like sending a passcode to the users's registered cell phone, that they then have to input into the application.	Windows/Linux
Profile	Shared configuration resource for Client logging, Quality of Service, Multi-Factor Authentication, Ransomware Protection and key manager communication settings.	Windows/Linux/AIX
Signature	The hash of an entity. Where Entity can be the process or the docker image.	Windows/Linux/AIX
Versioned key and Key versions	Keys whose name remains the same but keybytes are different for	Windows/Linux/AIX

Term	Description	OS Applies to
	each different version.	

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.

After the CTE Agent has encrypted a device on a host, that device is called a GuardPoint. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.

- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Note

For a list of CTE versions and supported operating systems, see the [CTE Compatibility Portal](#).

How to Protect Data with CTE

CTE uses policies created in the associated key manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your protected hosts. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of GuardPoints.

Policies specify:

- Whether or not the resting files are encrypted.
- Who can access decrypted files.
- What level of file access auditing is applied when generating fine-grained audit trails.

A Security Administrator accesses key manager through a web browser. You must have administrator privileges to create policies using key Manager. The CTE Agent then implements the policies once they are pushed to the protected host.

CTE can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

Getting Started with CTE for Linux

This section describes how to install CTE for Linux, register it with your selected key manager, and then create a simple GuardPoint on the protected host. It contains the following topics:

- [Additional Considerations](#)
- [CTE Agent Installation with UEFI Secure Boot](#)
- [Linux Package Installation](#)
- [Verifying Kernel Compatibility](#)
- [Installing and Configuring CTE for Linux with CipherTrust Manager](#)
- [Multifactor Authentication for CTE GuardPoints](#)
- [Ransomware Protection](#)

Additional Considerations

The following sections describe some of the things to keep in mind when configuring CTE.

Tracking and Preventing Local User Creation

CTE audits any attempts to change user authentication files. It also allows you to prevent any change to user authentication files using the host settings **protect**. This includes, but is not limited to user creation, modification, and deletion, or to deny users.

- The **audit** setting is set to on by default. It logs access to the system credential files but does not prevent account modifications.
- The **protect** setting both audits and prevents local user account modifications. You must manually enable the **protect** setting for tracking and prevention of local user account creation.

The **protect** tag will prevent changes to the files mentioned below. In the absence of the **protect** tag in host/client settings, operations on these files are permitted. When a log entry is generated, it is tagged with an **[audit]** tag.

- `/etc/passwd`
- `/etc/group`
- `/etc/shadow`
- `/etc/gshadow`
- `/etc/ssh/sshd_config`
- `/etc/ssh/sshr`

Note

You do not have to restart CTE after applying or removing these host settings.

Restricted Directories

Linux does not allow you to guard the following directories:

- <secfs install root>/agent/secfs/
- /etc
- /tmp
- /usr
- /usr/lib
- /usr/lib/pam
- /var/log/vormetric

Linux does not allow you to guard the following directories and all of their subdirectories:

- <install root>/agent/secfs/bin
- <secfs install root>/agent/vmd
- /etc/vormetric
- /etc/pam.d
- /etc/security
- /usr/lib/security
- /etc/rc*

Restricted Mode

Caution

If you install or upgrade in restricted mode, you cannot revert to unrestricted mode without uninstalling CTE.

You can install CTE in restricted mode. This mode prevents any user other than `root` from accessing the following directories:

- `/var/log/vormetric`
- `/opt/vormetric/DataSecurityExpert`

Restricted Mode also prevents non-`root` users from running the following utilities:

- `agenthealth`
- `agentinfo`
- `check_host`
- `register_host`
- `secfsd`
- `vmd`
- `vmsec`
- `voradmin`

Key Agents and Restricted Mode

- On systems where CTE is installed in restricted mode, you cannot install a key agent (pkcs11) or CipherTrust TDE Key Management.
- On systems where a key agent (pkcs11) or CipherTrust TDE are already installed, you cannot install CTE in restricted mode.

Restricted Mode Installation

To install in restricted mode, use the `-r` option.

```
./vee-fs-<release>-<build>-<system>.bin -r
```

For example:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin -r
```

RPM Installation

If installing from an RPM directly, prior to installation, type:

```
export VOR_RESTRICTED_INSTALL_MODE=yes
```

Upgrade in Restricted Mode

The upgrade mode is the same as the installation mode.

CTE Agent Installation with UEFI Secure Boot

If you want to install the CTE Agent software on a Linux system that has UEFI Secure Boot enabled, you must first download the appropriate Thales public certificate for your version of CipherTrust Transparent Encryption, and add that certificate to the MOK (Machine Owner Key) list.

Note

- The Thales public certificate is valid for three years from the date of issuance. Six months before the current public certificate is set to expire, Thales will release an advisory, along with the new certificate, that will become valid after the six month grace period expires. All future builds of CipherTrust Transparent Encryption will be built with the new certificate.

Warning

- You can only use the new certificate if the CTE build has been signed with the new certificate. If you are using an older version of CipherTrust Transparent Encryption that was signed with a previous certificate, then you **must** use that certificate with CipherTrust Transparent Encryption.

Public Certificate Naming Convention

The Thales public certificate name is `CTE_Secure_Boot_Cert_MM-DD-YYYY.der`:

Example

```
CTE_Secure_Boot_Cert_05-15-2023.der
```

Getting the Current Public Certificate

There are two options for getting the certificate:

Option 1: Install the DER file

1. Download the CipherTrust Transparent Encryption binaries to your local system.
2. Use the `-e` option to extract the public certificate from the downloaded binary:

```
./<cte-binary-name>.bin -e
```

Example

```
./vee-fs-7.8.0.75-95-rh8-x86_64.bin -e
```

3. Add the certificate to the MOK list.

Option 2: Convert the PEM file to DER

1. Download the certificate from the Thales public directory [CTE_Secure_Boot Repository](#)

```
curl -O https://packages.vormetric.com/pub/CTE_Secure_Boot/<certificate_name>.pem
```

Example

```
curl -O https://packages.vormetric.com/pub/CTE_Secure_Boot/CTE_Secure_Boot_Cert_05-15-2023.pem
```

Note

You can also download it from the [Thales Customer Support Portal: KB0027431](#).

2. Convert the certificate from a PEM file to a DER file using the following command:

```
openssl x509 -inform PEM -outform DER -in <certificate_name>.pem -out <certificate_name>.der
```

Example

```
openssl x509 -inform PEM -outform DER -in CTE_Secure_Boot_Cert_05-15-2023.pem -out CTE_Secure_Boot_Cert_05-15-2023.der
```

3. Add the certificate to the MOK list.

Adding the Certificate to the MOK List

Note

During this procedure, you **must** reboot the Linux host and then respond to a system prompt as soon as the host restarts.

1. Log into the host as `root`.
2. Add the certificate to the MOK list:

```
mokutil --import <cert-name>
```

Example

```
mokutil --import CTE_Secure_Boot_Cert_05-15-2023.der
```

3. Enter and confirm a password for this request when prompted.
4. Reboot the host and follow the instructions on the console when the host is back online. You will need to enter the password you created in the previous step when prompted. For detailed information, refer to the specific instructions from each linux distribution.

Note

If you do not respond to the system prompt to update the MOK when the host restarts, the prompt will time out and you will need to run the `mokutil` command again.

5. When prompted, reboot the host again.
6. After the host has rebooted for the second time, verify that the certificate has been properly added to the MOK list:

```
mokutil --test-key <cert-name>
```

Example

```
mokutil --test-key CTE_Secure_Boot_Cert_05-15-2023.der
```

Response

```
CTE_Secure_Boot_Cert_05-15-2023.der is already enrolled.
```

Linux Package Installation for Linux Distributions

- [Linux Package Installation for RHEL](#)
- [Linux Package Installation for SLES](#)
- [Linux Package Installation for Ubuntu](#)

Linux Package Installation for RHEL

This section describes how to access the Linux RPM installation package so that the CTE Agent installation integrates with the distribution software. To access the Linux RPM file, you can:

- Extract the RPM file from the CTE Agent install bin file. This is the easiest method, but the files in the package are not signed and therefore cannot be verified. For details, see [Installing the Unsigned RPM Package](#).
- Download the package from the Yum repository. If you use Yum, the files in the package are signed and the signatures are automatically verified when the package is installed. For details, see [Installing the Signed RPM Package with Yum](#).
- Manually download the RPM package outside of Yum and manually verify the package signatures. For details, see [Installing the Signed RPM Package Manually](#).

Prerequisites

Note

Before you can download and install the package using the Yum repository, you must contact [Thales Support](#) to get the username and password for the package repository on which the package resides.

Installing the Unsigned RPM Package

The CTE installation `bin` files contain the unsigned native packages. Extract them by running the `bin` file with the `-e` flag.

1. Log on to the host system as root and copy, or mount, the installation file to the host system.
2. Extract the RPM file using the following command:

```
./vee-fs-<release>-<build>-<distro>-<architecture>.bin -e
```

Example

```
./vee-fs-7.8.0.75-rh9-x86_64.bin -e
```

Response

```
Contents extracted.
```

3. Verify that the package extracted correctly:

```
ls *rpm
```

Example Response

```
vee-fs-7.8.0.75-rh9-x86_64.rpm
```

4. To start the installation using the RPM file, use the following command:

```
rpm -ivh vee-fs-<release>-<build>-<distro>-<architecture>.rpm
```

5. Follow the prompts to install and register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

6. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing the Signed RPM Package with Yum

To install the latest released version with the `yum` command:

1. Create the repository file, `/etc/yum.repos.d/Vormetric-VTE.repo`, with the following content:

```
[vormetric-vte]
releasever=REL_VERSION
name=Vormetric VTE Packages $releasever - $basearch - Source
baseurl=https://USER:PASSWORD@packages.vormetric.com/vte/DIST_VERSION/Latest
gpgkey=https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
enabled=1
gpgcheck=1
```



```
repo_gpgcheck=1
sslverify=1
```

Where:

- **USER:PASSWORD:** Username/password obtained from Thales Support
- **DIST_VERSION:** RHEL release version directory name. Ex: RH8, RH9
- **REL_VERSION:** RHEL release version. Ex: rhel-8, rhel-9

2. Clean up the Yum cache directory:

```
yum clean all
```

3. List all available versions of CTE:

```
yum list --showduplicates vee-fs
```

4. Use Yum to install the CTE binary. For example:

If the CTE binary name is vee-fs-7.8.0.75-rh9-x86_64, type:

```
yum install vee-fs-7.8.0.75-rh9-x86_64
```

To install the latest version, type:

```
yum install vee-fs
```

Note

The first time you install CTE through Yum, you will be asked to import the GPG key. Make sure that you download this key or the installation will fail. For example:

```
vormetric-vte/7Server/signature | 198 B 00:00:00
Retrieving key from https://packages.vormetric.com/pub/PKG-GPG-KEY-
vormetric
Importing GPG key 0x628536B7:
Userid : "Vormetric (PKG-GPG-KEY) <support@vormetric.com>"
Fingerprint: 7cb5 4f55 40d4 1b63 bf91 c896 f00a 13b0 6285 36b7
From : https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
```

```
Is this ok [y/N]: y
```

5. Follow the prompts to install and register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

6. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing the Signed RPM Package Manually

If you want to manually verify the signed version of the CTE RPM package, you can download the public key from the Thales package repository and manually verify the rpm signature.

1. Download the `rpm` file for the latest release, type:

```
wget -c --user USER --password PASSWORD https://packages.vormetric.com/vte/DIST_VERSION/Latest/TARGET_RPM_NAME
```

Example

```
wget -c --user ctetest --password abcdef12345678ab https://packages.vormetric.com/vte/RH9/Latest/vee-fs-7.8.0.75-rh9-x86_64.rpm
```

Where:

- **DIST_VERSION:** RHEL release version directory name. Ex: RH8, RH9
- **USER/PASSWORD:** Username/password obtained from Thales Support
- **TARGET_RPM_NAME:** Target rpm filename to download. Ex: vee-fs-7.8.0.75-rh9-x86_64.rpm

2. Import the public key from the Thales package repository:

```
sudo rpm --import https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
sudo rpm -qa grep gpg-pub*
```

Response

```
gpg-pubkey-628536b7-56f9887b : Imported CTE GPG public key.
gpg-pubkey-fd431d51-4ae0493b
```

3. Verify the signature of the package.

```
sudo rpm -Kv vee-fs-<release>-<build>-<distro>-<architecture>.rpm
```

Example

```
sudo rpm -Kv vee-fs-7.8.0.75-rh9-x86_64.rpm
```

4. To start the installation using the RPM file, use the following command:

```
sudo rpm -ivh vee-fs-<release>-<distro>-x86_64.rpm
```

5. Follow the prompts to register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

6. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing a previous version

To install a previous version with the YUM command, use the following URL for the baseurl in the file, `/etc/yum.repos.d/Vormetric-VTE.repo`:

```
baseurl=https://USER:PASSWORD@packages.vormetric.com/vte/CTE_VERSION/rhel-$releasever/
```

To install an previous version manually, use the following URL for the download URL.

```
https://packages.vormetric.com/vte/CTE_VERSION/REL_VERSION/TARGET_RPM_NAME
```

Where:

- **USER/PASSWD**: contact Thales Support to obtain the credential
- **TARGET_RPM_NAME**: Target rpm filename to download. Ex: vee-fs-7.8.0.75-rh9-x86_64.rpm
- **CTE_VERSION**: CTE release version. Ex: 7.7.0
- **REL_VERSION**: Distribution version. Ex: rhel-8, rhel-9

Upgrading from RHEL 9.6 to RHEL 10

This section describes an In-place upgrade of an RHEL 9.6 system to RHEL 10 using the [RHEL Leapp utility](#), with the added objective of upgrading CTE in the process.

Note

This procedure **only** applies to when upgrading RHEL 9.6 to RHEL 10. IT does not apply for any other versions.

Leapp allows you to:

- Preserve the configuration of your system
- Reinstall RHEL
- Retain existing subscription data on the client as long as the system is subscribed to using subscription-manager

Note

The upgrade process may take several hours.

Prerequisites

- Requires an active RHEL subscription on the source system
- Backup your data using the recommendations in the upgrade guide

Installation with the Leapp Utility

1. Check the subscription status, type:

```
subscription-manager status
```

2. Set the subscription manager release, type:

```
subscription-manager release --set 9.6
```

3. Open the global configuration file, `/etc/dnf/dnf.conf`, in a text editor for editing.
4. Add an exception for updating CTE so that Leapp can ignore the CTE package. This lets you upgrade CTE with the CTE Upgrade on Reboot feature. Add the following line to the end of the file:

```
exclude=libns12, vee-fs
```

-
5. Install the Leapp tools, type:

```
yum install leapp leapp-repository leapp-upgrade
```

6. Update the software, type:

```
yum update
```

7. Reboot the system.

8. Enable **Upgrade on Reboot** using the attached `schedule.sh` file, type:

```
./schedule.sh <cte-binary>
```

Example

```
./schedule.sh vee-fs-7.8.0-100-rh10-x86_64.bin
```

Note

The Leapp utility installs the latest CVE kernel package on the target RHEL 10 system. Ensure that the CTE binary provided to the Upgrade on Request scheduler is certified for this kernel version.

9. Run the pre-upgrade tool, type:

```
leapp preupgrade
```

10. Examine the pre-upgrade details in `/var/log/leapp/leapp-report.txt`. Resolve any error or inhibitor conditions.
11. Rerun the tool after resolving the conditions to verify that they have been resolved.
12. Set the upgrade target, type:

```
leapp preupgrade --target 10.0
```

13. Examine the pre-upgrade details again, in `/var/log/leapp/leapp-report.txt`. Resolve any error or inhibitor conditions.
14. Rerun the tool after resolving the conditions to verify that they have been resolved.
-

15. Start the upgrade, type:

```
leapp upgrade --target 10.0
```

16. If a failure occurs due to a package or dependency, Leapp logs the error to the console. Fix the issues and then proceed.

If there are no error or inhibitor conditions displayed on the console, **reboot**.

17. Wait for the system to upgrade and return to the online state. Verify the CTE service status.

Linux Package Installation for SLES

This section describes how to access the Linux RPM installation package so that the CTE Agent installation integrates with the distribution software. To access the Linux RPM file, you can:

- Extract the RPM file from the CTE Agent install bin file. This is the easiest method, but the files in the package are not signed and therefore cannot be verified. For details, see [Installing the Unsigned RPM Package](#).
- Download the package from the RPM repository. If you use Zypper Package Manager, the files in the package are signed and the signatures are automatically verified when the package is installed. For details, see [Installing the Signed RPM Package with Zypper](#).
- Manually download the RPM package outside of Zypper and manually verify the package signatures. For details, see [Installing the Signed RPM Package Manually](#).

Prerequisites

Note

Before you can download and install the package using the Zypper repository, you must contact [Thales Support](#) to get the username and password for the package repository on which the package resides.

Installing the Unsigned RPM Package

The CTE installation **bin** files contain the unsigned native packages. Extract them by running the **bin** file with the **-e** flag.

1. Log on to the host system as root and copy or mount the installation file to the host system.
2. Extract the RPM file using the following command:

```
./vee-fs-<release>-<build>-<distro>-<architecture>.bin -e
```

Example

```
./vee-fs-7.8.0.75-sles15-x86_64.bin -e
```

Response

```
Contents extracted.
```

3. Verify that the package extracted correctly:

```
ls *rpm
```

Example Response

```
vee-fs-7.8.0.75-sles15-x86_64.rpm
```

4. To start the installation using the RPM file, use the following command:

```
sudo rpm -ivh vee-fs-<release>-<distro>-x86_64.rpm
```

5. Follow the prompts to install and register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

6. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing the Signed RPM Package with Zypper Package Manager

To install the latest released version:

1. Create the repository file `/etc/zypp/repos.d/Vormetric-VTE.repo`, with the following contents:

```
/etc/zypp/repos.d/Vormetric-VTE.repo
```

2. Add with the following contents:

```
[vormetric-vte]
name=Vormetric VTE Packages for SLES
enabled=1
autorefresh=0
baseurl=https://USER:PASSWORD@packages.vormetric.com/vte/DIST_VERSION/Latest
```

```
type=rpm-md
```

Where:

- **USER/PASSWD:** contact Thales Support to obtain the credential
- **DIST_VERSION:** SLES release version. Ex: SLES12, SLES15

3. Import public key from the repository:

```
sudo rpm --import https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
```

4. Clean up cached data:

```
$ sudo zypper clean
$ sudo zypper refresh
```

5. List available versions of the CTE.

```
$ zypper se --match-exact -t package -s vee-fs
```

6. Install CTE binary:

```
$ zypper in vee-fs                : download the latest
$ zypper in vee-fs=<CTE_VERSION> : download the specific version
```

7. Follow the prompts to install and register CTE. For details about the installation and registration process, see the appropriate installation procedure.
8. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing the Signed RPM Package Manually

If you want to manually verify the signed version of the CTE RPM package, you can download the public key from the Thales package repository and manually verify the rpm signature.

1. Download the `rpm` file for the latest release, type:

```
$ wget -c --user USER --password PASSWORD https://packages.vormetric.com/vt
e/DIST_VERSION/Latest/TARGET_RPM_NAME
```

Example


```
$ wget -c --user USER --password PASSWORD https://packages.vormetric.com/vte/SLES15/Latest/vee-fs-7.8.0.75-sles15-x86_64.rpm
```

Where:

- **DIST_VERSION:** SLES release version. Ex: SLES12, SLES15,
- **USER/PASSWORD:** Username/password obtained from Thales Support
- **TARGET_RPM_NAME:** Target rpm filename to download. Ex: vee-fs-7.8.0.75-sles15_64.rpm

2. Import the public key from the Thales package repository:

```
sudo rpm --import https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
sudo rpm -qa grep gpg-pub*
```

Response

```
gpg-pubkey-628536b7-56f9887b : Imported CTE GPG public key.
gpg-pubkey-fd431d51-4ae0493b
```

3. Verify the signature of the package using the `rpm -Kv` command.

```
sudo rpm -Kv vee-fs-<release>-<build>-<distro>-<architecture>.rpm
```

Example

```
sudo rpm -Kv vee-fs-7.8.0.75-sles15-x86_64.rpm
```

Response

```
Header V4 DSA/SHA1 Signature, key ID 628536b7: OK
Header SHA1 digest: OK (ed3d33dca580c66c70961cfee143e9877a09544c)
MD5 digest: OK (95273b36ef1c205a7cea444e14bef15f)
V4 DSA/SHA1 Signature, key ID 628536b7: OK
The output should show that the keys match is OK.
```

4. To start the installation using the RPM file, use the following command:

```
sudo rpm -ivh vee-fs-<release>-<build>-<distro>-<architecture>.rpm
```

5. Follow the prompts to register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

6. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing a previous version

To install a previous version with the `zypper` command, use the following URL for baseurl in file: `/etc/zypp/repos.d/Vormetric-VTE.repo`

```
baseurl=https://USER:PASSWORD@packages.vormetric.com/vte/CTE_VERSION/REL_VERSION
```

To install a previous version manually, use the following URL for the download URL.

```
https://packages.vormetric.com/vte/CTE_VERSION/REL_VERSION/TARGET_RPM_NAME
```

Where:

- **USER/PASSWD**: contact Thales Support to obtain the credential
- **REL_VERSION**: SLES release version. Ex: sles12, sles15
- **TARGET_RPM_NAME**: Target rpm filename to download. Ex: vee-fs-7.8.0.75-sles15-x86_64.rpm
- **CTE_VERSION**: CTE release version. Ex: 7.7.0

Linux Package Installation for Ubuntu

Prerequisites

Note

Before you can download and install the package using the Apt repository, you must contact [Thales Support](#) to get a username and password for the package repository on which the packages reside.

Installing the Unsigned DEB Package

The CTE installation `bin` files contain the unsigned native packages. Extract them by running the `bin` file with the `-e` flag.

1. Log on to the host system as root and copy or mount the installation file to the host system.
2. Extract the DEB file using the following command:

```
./vee-fs-<release>-<build>-<distro>-<architecture>.bin -e
```

Example

```
./vee-fs-7.7.0-87-ubuntu22-x86_64.bin -e
```

Response

```
Contents extracted.
```

3. Verify that the package extracted correctly:

```
ls *deb
```

Example Response

```
vee-fs-7.7.0-87-ubuntu22-x86_64.deb
```

4. To start the installation using the deb file, use the following command:

```
dpkg -i vee-fs-7.7.0-87-ubuntu22-x86_64.deb
```

5. Follow the prompts to install and register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

6. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing the Signed DEB Package with the latest version

To install the latest released version:

1. Create the source list file, `/etc/apt/sources.list.d/Vormetric-VTE.list`, with the following contents:
 - a. Add the following contents from the Vormetric Source repository.

```
deb https://packages.vormetric.com/vte/DIST_VERSION/Latest/
```

Where:

- **DIST_VERSION:** Ubuntu distribution release version. Ex: UBUNTU20, UBUNTU22

b. Create the login configuration file, type:

```
vi /etc/apt/auth.conf
```

c. Enter the login information, type:

```
machine packages.vormetric.com/vte/DIST_VERSION/Latest login USER password PAS  
SWD
```

Where:

- **USER:PASSWORD:** Username/password obtained from Thales Support

2. Import public key from the repository.

```
$ sudo curl -O https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric-ubuntu  
$ sudo gpg --import PKG-GPG-KEY-vormetric-ubuntu  
$ sudo apt-key add PKG-GPG-KEY-vormetric-ubuntu  
$ sudo apt-key update
```

3. Retrieve the new list of packages.

```
$ sudo apt-get update
```

4. List all versions of the CTE binary:

```
$ apt-cache madison vee-fs
```

5. Install CipherTrust Transparent Encryption.

```
$ sudo apt-get install vee-fs : installs the latest version of CTE  
$ sudo apt-get install vee-fs=<release>-<build> : installs the specific versio  
n of CTE
```

6. Follow the prompts to install and register CTE. For details about the installation and registration process, see the appropriate installation procedure.
7. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing the Signed DEB Package Manually with the latest version

If you want to manually verify the signed version of the CTE DEB package, you can download the public key from the Thales package repository and manually verify the DEB signature.

1. Download the `deb` file, type:

```
wget -c --user USER --password PASSWORD https://packages.vormetric.com/vte/DIST_VERSION/Latest/TARGET_PKG_NAME
```

Example

```
wget -c --user USER --password PASSWORD https://packages.vormetric.com/vte/UBUNTU22/Latest/vee-fs-7.7.0-87-ubuntu22-x86_64.deb
```

Where:

- **DIST_VERSION:** Ubuntu DISTRIBUTION release version. Ex: UBUNTU20, UBUNTU22
- **TARGET_PKG_NAME:** Target PKG filename to download. Ex: `vee-fs-7.7.0-87-ubuntu22-x86_64.rpm`

2. Import the public key from the Thales package repository:

```
$ sudo gpg --import PKG-GPG-KEY-vormetric-ubuntu  
$ sudo apt-key add PKG-GPG-KEY-vormetric-ubuntu  
$ sudo apt-key update
```

3. Verify the signature of the package.

```
sudo dpkg-sig --verify vee-fs-<release>-<build>-<distro>-<architecture>.deb
```

Example

```
sudo dpkg-sig --verify vee-fs-7.7.0-87-ubuntu22-x86_64.deb
```

Response

```
Processing vee-fs-7.7.0-119-ubuntu20-x86_64.deb...  
GOODSIG _gpgvormetric 7CB54F5540D41B63BF91C896F00A13B0628536B7 1698960263
```

4. To start the installation using the deb file, use the following command:

```
sudo dpkg -i vee-fs-7.7.0-87-ubuntu22-x86_64.deb
```

5. Follow the prompts to register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

6. If you are going to register the system with a CipherTrust Manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Installing a previous version

To download a previous deb package using `wget` on the command line, use the following URL:

```
https://packages.vormetric.com/vte/CTE_VERSION/REL_VERSION/TARGET_PKG_NAME
```

Where:

- **REL_VERSION**: Ubuntu distribution version. Ex: ubuntu20, ubuntu22
- **TARGET_PKG_NAME**: Target rpm filename to download. Ex: vee-fs-7.7.0-87-ubuntu22-x86_64.deb
- **CTE_VERSION**: CTE release version. Ex: 7.7.0.

To install a previous version of CTE with the `apt` command, use the following URL in `/etc/apt/sources.list.d/Vormetric-VTE.list`:

```
deb https://packages.vormetric.com/vte/CTE_VERSION/REL_VERSION /
```

Use the following URL in `/etc/apt/auth.conf`:

```
machine packages.vormetric.com/vte/CTE_VERSION/REL_VERSION login USER password PASSWD
```

Verifying Kernel Compatibility

Thales maintains a compatibility matrix in a JSON file that maps all CTE Agent releases to the Operating Systems and kernels that support those releases. The information in this file allows you to verify the compatibility between any Linux host and the version of the CTE Agent that you want to install on that host.

You can view the current compatibility information in CipherTrust Manager by downloading the most recent compatibility JSON file from Thales and then uploading it to CipherTrust Manager. After the JSON file has been uploaded, the CipherTrust Manager displays the compatibility of all Linux hosts registered with the CipherTrust Manager in the **Compatibility View** on the **Hosts** page.

For details about how to do this in CipherTrust Manager refer to: [Kernel Compatibility Matrix](#).

The following procedure describes how to download the compatibility JSON file and verify its authenticity.

1. Download the `cte_compatibility_matrix.tgz` file from <https://packages.vormetric.com/pub/> or from the [Thales Customer Support Portal](#).
2. Extract the files from the TGZ file. The resulting files are:
 - `CTE_Compatibility_Matrix_Cert_mm-dd-yyyy.pem` — The X.509 Public Key Certificate.
 - `cte_compatibility_matrix.json` — The compatibility JSON file.
 - `cte_compatibility_matrix.sign.sha256` — The SHA256 signature for the JSON file.

For example:

```
tar -xvzf cte_compatibility_matrix.tgz
```

`CTE_Compatibility_Matrix_Cert_12-17-2020.pem`

`cte_compatibility_matrix.json`

`cte_compatibility_matrix.sign.sha256`

3. Extract the Public Key from the X.509 Public Key Certificate. For example:

```
openssl x509 -in CTE_Compatibility_Matrix_Cert_12-17-2020.pem -pubkey \
-noout > cte_compatibility_matrix_public_key.pem
```

The Public Key is in PEM format in the file `cte_compatibility_matrix_public_key.pem`.

4. Verify the SHA signature using the Public Key. For example:

```
openssl dgst -sha256 -verify cte_compatibility_matrix_public_key.pem \
-signature cte_compatibility_matrix.sign.sha256 cte_compatibility_matrix.json
Verified OK
```

Installing CTE with No Key Manager Registration

The following procedure installs the CTE Agent on the host but does not register it with a key manager. You cannot protect any data on the host until the CTE Agent is registered with one of the supported key managers. For a comparison of the available key managers, see [CTE Components](#).

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.

3. Install the CTE Agent. A typical installation uses the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note

If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type **Y** and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

Welcome to the CipherTrust Transparent Encryption File System Agent Registration Program.

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>
```

```
In order to register with a CipherTrust Manager you need a valid registration token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Type **N** and press Enter to end the installation procedure without registering the CTE Agent with either key manager.

When you are ready to register the CTE Agent with a key manager, see [Configuring CTE for Linux with CipherTrust Manager](#).

Configuring CTE for Linux with CipherTrust Manager

This section describes how to install and configure CTE on Linux systems that you plan to register with a CipherTrust Manager.

Installation Overview

The installation and configuration process when you are using CTE with a CipherTrust Manager consists of the following steps:

1. Installation Prerequisites

Gather the information needed for the installation and set up your network.

2. Interactive Installation on Linux

Install CTE interactively on a protected host and register the protected host with CipherTrust Manager.

Silent Installation on Linux

Install CTE silently (non-interactive) on a protected host and register the protected host with CipherTrust Manager.

3. Installing CTE with No Key Manager Registration

Install CTE without registering to a CipherTrust Manager.

4. External Certificates

Use for communication between CTE and CM. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

5. Validating CipherTrust Manager and CipherTrust Transparent Encryption with a Local CA Certificate

Ensure that registration by the CTE agent is serviced only by the expected key manager by providing a copy of the CA certificate that will be used to authenticate the TLS communications with the key manager.

6. Registration

Register the protected host with CipherTrust Manager and make sure that CipherTrust Manager and CipherTrust Transparent Encryption can communicate with each other. This can be done as part of the initial installation or at any point after the CTE Agent has been installed.

7. Guard Devices

Create GuardPoint to protect sensitive data.

Installation Prerequisites

This section lists the tasks you must complete, and the information you must obtain, before installing CTE.

Recommendations and Considerations

- The host on which you want to install CTE *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE to release 7.0.0 or later will fail.
- Thales recommends that you install CTE in the default location.
- Make the Installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.

For example:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin -d /home/hello/
```

- Ensure read/write permission is granted to other users accessing your shared resource.

Network Setup Requirements

Recommendations and Considerations

- The host on which you want to install CTE *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE to release 7.0.0, or any subsequent version, will fail.
- Thales recommends that you install CTE in the default location.
- Do not install CTE on network-mounted volumes such as NFS.
- Make the Installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.

For example:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin -d /home/hello/
```

Port Configuration Requirements

The following port information applies to both Windows and Linux systems.

Communication through a Firewall

If a protected client must communicate with CipherTrust Manager through a firewall, see the CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

Communication with CipherTrust Manager

The default port for http communication between CipherTrust Manager and the CTE Agent is **443**. If this port is

already in use, you can set the port to a different number during the CTE Agent installation.

Communication for LDT over CIFS/NFS

All nodes that intend to use **LDT over CIFS/NFS** GuardPoint must have the following ports open:

- 7024
- 7025

Note

When you are registering a CipherTrust Transparent Encryption client with CipherTrust Manager, you can manually include a destination port number, (Default: 443). If you enter a port value, using the syntax `<hostname or IP address>:<port number>` then CipherTrust Transparent Encryption **does not** perform a port scan. CipherTrust Transparent Encryption uses the port number provided to verify the target server type using a TLS operation.

If you do not enter a port number, CipherTrust Transparent Encryption performs a port scan to check which ports are listening, including port 443.

Interactive Installation on Linux

The Linux typical install is an interactive script that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see [Silent Installation on Linux](#)).

After you install CTE, you are prompted to register it immediately with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

Note

Do not install CTE on network-mounted volumes like NFS.

Prerequisites

The following prerequisites must be met for CTE/CTE-U to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.

- CipherTrust Manager must contain an LDT Communication Group if you will use CTE to guard data over CIFS/ NFS shares using LDT policies. See [Managing LDT Communication Groups](#) for more information.

Procedure

1. Log on to the host where you will install the CTE Agent as **root**. You cannot install the CTE Agent without **root** access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the **chmod** command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the **-d <custom-dir>** option. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note

- If possible, Thales recommends that you use the default directory **/opt/vormetric**.
- Custom directories are **only available** for RHEL and SLES.
- Custom directories are **not available** for COS (Cloud Object Storage).

To view all installer options, use the **-h** parameter. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type **Y** and press Enter to accept.

The install script installs the CTE Agent software in either **/opt/vormetric** or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

Welcome to the CipherTrust Transparent Encryption File System Agent Registration Program.

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>
```

```
In order to register with a CipherTrust Manager you need a valid registration token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Type **N** and press Enter to end the installation procedure without registering the CTE Agent with a key manager.
6. Enter **Y** to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE. For example:

CTE for CipherTrust Manager

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Please enter the primary key manager host name: 10.3.200.141
```

```
You entered the host name 10.3.200.141
```

```
Is this host name correct? (Y/N) [Y]: Y
```

CTE for CDSPaaS

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Enter the primary key manager host name of the service:
```

```
You entered the host name us1.ciphertrust.dpondemand.io
```

```
Is this host name correct? (Y/N) [Y]: Y
```

Host names:

- **Europe:** ciphertrust.dpondemand.io
- **North America:** us1.ciphertrust.dpondemand.io

Note

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: <hostName>:<port#>. For example, 10.3.200.141:8445.

7. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the following list.

[1] sys31186.qa.com
[2] 10.3.31.186

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 2
You selected "10.3.31.186".
```

8. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
Please enter the profile name for this host: My-Profile
Please enter the host group name for this host, if any:
Please enter a description for this host: RHEL7 system West Coast Datacenter

Token           : 12345
Profile name     : My-Profile
Host Group      : (none)
Host description : RHEL7 system West Coast Datacenter
Are the above values correct? (Y/N) [Y]: Y
```

9. At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloning. The default is Y (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again. Do you want to enable this functionality? (Y/N) [Y]: Y

10. Type Y to support Filesystem encryption and to choose other features. Type N if you only want to support Ransomware Protection. If you type N, then LDT and COS are not supported.

```
Do you want this host to have Filesystem encryption support enabled on the server? (Y/N) [Y]:
```

11. At the LDT prompt, specify that you want this client to use CTE-LDT by typing **Y** and pressing Enter:

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]: Y
```

12. If you are planning to create GuardPoints on NFS shares, enter the name of the LDT Communication Group that this node will join.

```
Enter the LDT Communication Group name: LCG1
```

Warning

The registration token, profile name, client group name and LDT Communication Group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

13. The installation checks for Confidential Computing adapter types. If it finds one, it states:

```
The following confidential computing adapter types have been identified.
1. Intel Trust Domain Extensions (tdx)
Do you want this host to have confidential computing enabled? (Y/N) [N]:
```

Type **Y** to enable Confidential Computing.

14. At the Cloud Object Storage (COS) prompt, specify whether you want this client to use CTE COS.

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

15. Specify if you want to enable Ransomware Protection.

```
Do you want this host to have Ransomware Protection support enabled on the server? (Y/N) [N]:
```

16. CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.
```

```

Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption CTE Agent with
the CipherTrust Manager on 10.3.200.141.

Installation success.

```

- In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Silent Installation for CTE or CTE-U on Linux

This section describes how to perform a silent (unattended) installation on CTE or CTE-U on a single host. The silent installation automates the installation process by storing the answers to installation and registration questions in a separate file that you create. It installs CTE/CTE-U on the host, and registers the host with the CipherTrust Manager you specify in the silent installation file. You can also use the silent installation to install CTE/CTE-U, on multiple hosts simultaneously.

Prerequisites

The following prerequisites must be met for CTE/CTE-U to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.

Procedure

- Log on as an administrator to the host where you will install CTE/CTE-U.
- Create a parameter file and store it on your system, or copy an existing file from another location. The file can contain any of the following parameters:

Parameter	Description
AGENT_HOST_NAME	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
AGENT_HOST_PORT	Specifies the port number for this CTE Agent to use.
AGENT_USEIP	Use the IP address of the protected host instead of

Parameter	Description
	host name. Used when hostname is not supplied.
CA_CERT	Set to provide CA certificate data to CipherTrust Manager.
CA_FILE	Set to provide a CA certificate file to CipherTrust Manager.
CERT_FIELD_PARAM	Installer option. Default behavior is to use hard-coded values for Root Certificate fields. Uses the same <code><Certificate Parameters></code> string format as is used in the voradmin command <code>voradmin cos ca_cert create <Certificate Parameters></code>
ENABLE_CLOUD	Set to enable cloud in the Key Manager.
ENABLE_HOST_CHECKS	When using CipherTrust Data Security Platform Services (CDSPaaS), set this value to 1 to enable SSL certificate host name checks. Set to 0 to disable. Default: 0 . This also forces CTE to enable the verify peer feature during registration. Use only when the CDSPaaS web server certificates contain the target DNS name or IP address.
ENABLE_LDT	Set this value to 1 to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.
HOST_DESC	Specifies a description for the host. This description is displayed in the CipherTrust Manager. If an entry for this host already exists, and the host already has a description, CipherTrust Manager
HOST_GROUP	Specifies the optional host/client group with which this host/client will be associated.
HOST_PROFILE	Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.
LDTGROUP_NAME	Set the LDT Communication Group for LDT over NFS/ CIFS.
REG_TOKEN	The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.
ENABLE_RWP	Enable Ransomware Protection.
SERVER_HOSTNAME	Required if you want to register CTE with a CipherTrust Manager.
SERVER_IP	Alternative for hostname when registering.
TMPDIR	Specifies a custom temporary directory that the installer can use during the installation process. If this value is omitted, the installer uses the default temporary directory.

Parameter	Description
USEHWSIG	Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.

Example 1: Registering with CipherTrust Manager

The following example contains just the required information for registration with CipherTrust Manager. In this case, the client will be registered with the CipherTrust Manager using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
AGENT_HOST_NAME=10.192.80.86
```

Example 2: Registering with CipherTrust Manager

The following example specifies the required registration information, adds a host name and description, enables hardware association, and CTE-LDT. In this case, the client will be registered with the CipherTrust Manager using its host name instead of the IP address:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
AGENT_HOST_NAME=myagent.example.com
HOST_DESC="West Coast Server 12"
USEHWSIG=1
CERT_FIELD_PARAM="/C=US/ST=California/L=San Jose/O=Thales eSecurity/OU=Vormetric
s/CN=localhost/emailAddress=admin@thalesgroup.com"
SUBJECT_ALT_NAME_PARAM="DNS:www.thalesgroup.com,email:admin@thalesgroup.com"
```

1. Copy or mount the installation file to the host system. The installation file is in the format:

CTE

```
vee-fs-<release>-<build>-<system>.bin
```

CTE-U

```
cte-fuse_<version>.<build>_<processor>.rpm
```

2. Run the installer using the following syntax:

CTE

```
./vee-fs-<release>-<build>-<system>.bin [-d <custom-dir>] -s <install-file>
```

where:

- **-d <custom-dir>** is an optional parameter that specifies the installation directory for CTE. If you omit

this parameter, CTE is installed in: `/opt/vormetric/DataSecurityExpert/agent/`

- `-s <install-file>` indicates that you want to install CTE silently using the installation options file `<install-file>`

For example, if the installation options file is called `/tmp/unattended.txt`, you would enter:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin -s /tmp/unattended.txt
```

CTE-U

```
rpm -i cte-fuse_<version>.<build>_<processor>.rpm
```

- Invoke Registration for CTE-U:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host silent <silent_reg_file>
```

Note

You can also invoke registration by replacing 'register_host' with the following two options:

- `REG_HOST_CLEAN`: Register and remove certificates used for communication
- `REG_HOST_SILENT_<fileName>`: Use silent/non-interactive mode; get name=value input from

3. Verify the installation by checking the CTE/CTE-U processes on the host:
 - Run `vmd -v` to check that the version of CTE/CTE-U matches that just installed.
 - Run `vmsec status` to display CTE kernel status. (CTE only)
 - Look at the log files in `/var/log/vormetric`, especially `install.fs.log.<date>` and `vorvmd_root.log`.
4. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the [CipherTrust Manager documentation](#).

Validating CM and CTE with a Local CA Certificate

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

To ensure that registration by the CTE agent is serviced only by the expected key manager, you can provide a copy of the root CA certificate that will be used to authenticate the TLS communications with the key manager, during the registration process.

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Note

You can only download the CA certificate when you are a root user in the root domain. You cannot download the certificate from a subdomain. It will not work.

Prerequisite

Make sure that you have previously [created the client](#) in CipherTrust Manager.

Using a Local CA Certificate

1. Extract the root CA certificate from the CipherTrust Manager.
 - a. Log on to CipherTrust Manager as an administrator.
 - b. In the left navigation pane, click **CA > Local**. The list of available CAs displays.
 - c. Click the ellipsis icon corresponding to the CA.
 - d. Click **Download** to download the CA.
 - e. Copy the certificate to a directory on the agent system.
2. Present the root certificate data to CTE in one of two ways:
 - a. Use a file:

When written to a file, it must be in PEM file format, starting and ending with:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

- b. Use a a string parameter:

If you are providing the information in a single string, it must contain the same data as in the preceding case, except that all new lines are replaced by `\n` escape sequences. For example:

```
CA_CERT=-----BEGIN CERTIFICATE-----\n -----END CERTIFICATE-----\n
```

3. To install the root certificate into the CTE client:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host.exe -s <Path-to-install-file> AGENT_HOST_NAME=<Hostname-or-IP-of-agent> REG_TOKEN=<CM registration token> CA_FILE=<Path-to-root-ca-cert>
```

Example

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host.exe -s /opt/silent/vte_reg_log.txt AGENT_HOST_NAME=ani-vm-217-35190.sjcicd.com REG_TOKEN=mMEz3Y60b9D4L7QuvK5S0mhulRm8DYI8odV5j30dVuHqk6LhZqE0FeIZHILYtmDiE9 CA_FILE=/cert_files/Austin175.pem
```

4. Confirm in CipherTrust Manager that the client is registered and healthy.

Using external certificates for communication between CTE Agent and CipherTrust Manager

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Overview

Use for communication between CTE and CipherTrust Manager. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

Prerequisites

The external certificate must be:

- On the file system
- In PEM format

A key pair must already exist for the client:

- Must have Encryption type of either:
 - sha256WithRSAEncryption
 - ecdsa-with-SHA384
- Must be Encrypted with a pass phrase

Initial setup

1. Obtain your external CA certificate.
2. Create a certificate using the external CA certificate and key.

CipherTrust Manager Setup

To setup CipherTrust Manager to communicate through an external certificate:

1. Import the CA certificate into the CipherTrust Manager, click **CA > External > Add External CA**.

Note

In the Add External CA dialog, copy and paste the `<ca_certificate_name>.pem` file content from the UI page and provide a user-friendly name.

For more information, see [Using an Externally Generated Server Certificate for an Interface](#)

2. Add the CA certificate to the list of trusted sources for the web interface, click **Admin Settings > Interfaces > web > Edit > External Trusted CAs**.
3. Restart the web server, click **Admin Settings > Services > web > Restart**.
4. [Create a Registration Token](#) for the CTE agent.

CTE Agent setup

1. Create a directory on the system to hold the required files, for example:

- `/root/cert_files` (**Linux/AIX**)
- `c:\temp\cert_files` (**Windows**)

2. Copy or create the following files in this directory:

- `client_cert.pem`
- `client_key.pem`
- `passphrase` - this is currently expected as plain text

3. For **Linux/AIX** systems, to add the directory path to the environment, type:

```
$ export EXTERNAL_CERT_DIR=/root/cert_files
```

4. For **Windows** system, invoke `registerhost.exe` from the command line and add this argument:

```
c:\> register_host.exe -extcertdir=c:\temp\cert_files
```

5. Register the CTE client with the CM server as normal. If this is being done as part of an installation, then the above steps should be done before the installation, or, on windows, added to the registration parameters passed to the installer.

Post Registration

During registration, the certificate file is uploaded to the CipherTrust Manager, and the certificate and key files are imported into the CTE pem store. The key is decoded using the provided passphrase, then re-encoded using a random key using the normal CTE key security mechanisms for TLS keys. There is no need to keep the input files after registration is successful, so for security reasons they should be removed / shredded.

Certificate Renewal

The location of the external certificate files (i.e. the `EXTERNAL_CERT_DIR` or `-extcertdir` parameters) will be recorded in the CTE agent configuration file, `agent.conf`. When the current certificate is approaching expiration date (i.e. approx. 60 days prior to expiration) the CTE agent will look in this directory for an updated set of files.

If a new certificate file is present, then the file will be read and pushed to the CM, and if accepted, then the certificate and key will be imported into the CTE pem store, and the VMD process restarted to use the new certificate.

If no new certificate is present, a **WARNING** level message will be written to the logs and/or uploaded to the CM as per the logging settings, and the CTE agent will check again after 24 hours.

If the user wishes to change the directory path to store the new certificates, then the entry in the `agent.conf`

file should be updated and the vmd service restarted. Alternatively, the user can update the external certificate set using the following command (this will not update the saved path):

```
# vmutil -a vmd -d <ext_cert_Dir> updatecerts
```

If the user fails to update the certificate set prior to expiration then communication with the CM may be blocked, and re-registration will be required.

Note

Any renewed certificates must have exactly the same common name field as the original certificate, or the CipherTrust Manager will reject the update.

Installation and Registration Options

CTE provides the following installation and registration options. The options you choose determine the information you need to supply during the actual install procedure.

Installation Method Options

There are two methods for installing CTE on Linux platforms:

- **Typical:** Most common and recommended type of installation. Use this method for installing the CTE Agent on one host at a time. See [Interactive Installation on Linux](#).
- **Silent:** Create pre-packaged installations by providing information and answers to a set of installation questions. Use silent installations when installing on a large number of hosts. See [Silent Installation on Linux](#).

Hardware Association (Cloning Prevention) Option

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware clients.

You can enable hardware association during CTE registration process. You can disable hardware association by re-running the registration program.

To verify if hardware association (cloning prevention) is enabled on a Linux host, on the command line enter the following:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/access
```

If you see `usehw:true`, then hardware association is enabled. If you see `usehw:false`, it's disabled.

Guarding a Device with CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many standard GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

Note

For guarding using LDT on a local drive, or on a CIFS/Share drive, refer to [CTE-Live Data Transformation with CipherTrust Manager guide](#).

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

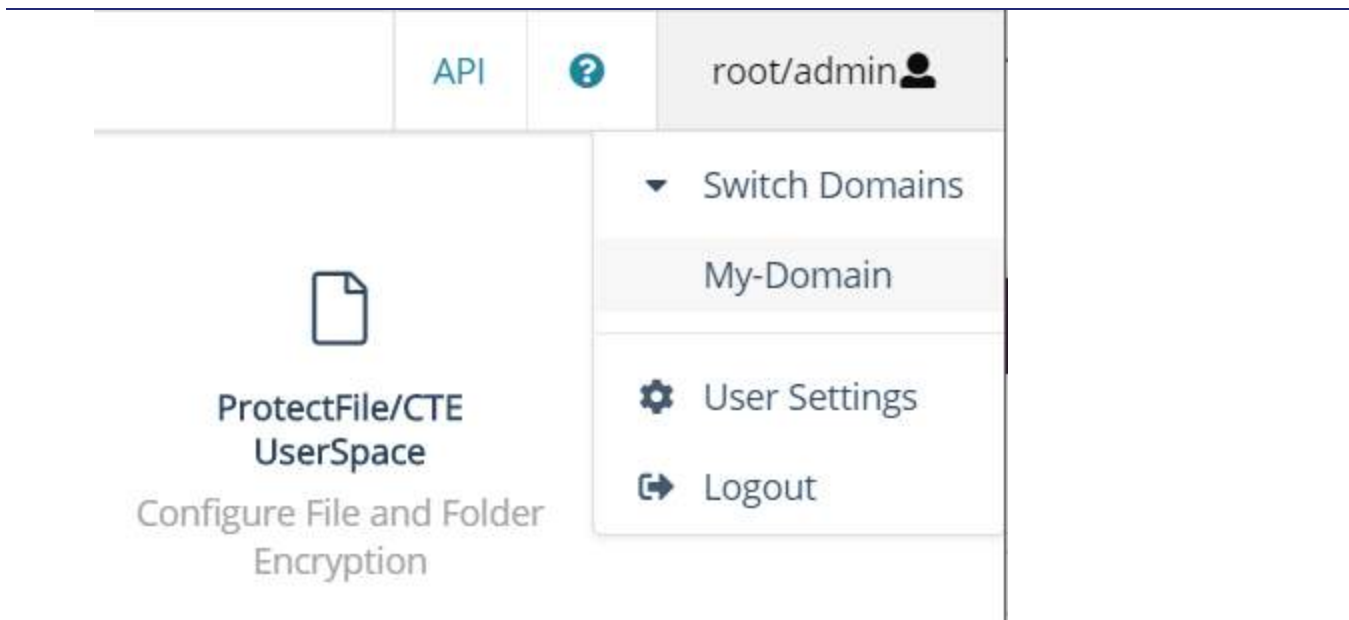
1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or [create an encryption key](#) that CTE will use to encrypt the data on the device or directory.
3. Identify or [create a policy](#) for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. [Assign a GuardPoint](#) to the device or directory.

The following example creates a simple policy and uses it to guard a directory on a registered client. For all of the following procedures, you must be logged into the CipherTrust Manager Console as a CipherTrust Manager Administrator, and you must be in the domain with which the client is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the CipherTrust Manager documentation.

Access the CipherTrust Manager Domain

1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to [Create an Encryption Key](#). If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the user name **root/admin** on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.
 - c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

Note

The following procedure is based on CipherTrust Manager version 2.2. If you are using a different version, see the CipherTrust Manager documentation for the version that you are using.

1. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.

Tip

To navigate to the Products page from anywhere in the CipherTrust Manager Console, click the App Switcher icon in the top left corner.

2. Above the Key table, click **Create a New Key**.
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
4. In the **Key Usage** section, make sure **Encrypt** and **Decrypt** are selected.
5. Click **Create**. CipherTrust Manager displays the properties for the new key.
6. In the general options area, enable the **Exportable** option.

You can also enable the **Deletable** option in this section if you want a CipherTrust Manager Administrator to

be able to delete the key.

ID	2e58c582...61136313	Owner	Global	Object Type	Symmetric Key
UUID	e3ad9c3e...7047711	Created	05 Mar 2021, 05:13	Algorithm	AES
MUID	e3ad9c3e...f6333c9f	Last Modified	05 Mar 2021, 05:13	Size	256
KeyID	N/A	Exportable	☒	Deletable	☐

7. In the **Key Access** section, do the following:

a. In the Search Groups box, type "cte".

If no groups are displayed, make sure the **Added Only** option is *disabled*.

b. Click the **All** check box for both the CTE Admins and CTE Clients groups.

KEY ACCESS

Key Owner

2 Results | 2 groups

☐ Added Only

Group	Read	Use	Decrypt	Encrypt	Sign	Sign/Verify	Export	All
CTE Admins	☒	☒	☒	☒	☒	☒	☒	☒
CTE Clients	☒	☒	☒	☒	☒	☒	☒	☒

c. When you are done, click **Update**.

8. Click the **CTE** tab and set the following properties:

- **CTE Versioned:** Specify whether the key is versioned. By default, the key is set as versioned.

For a standard policy, you should clear this check box. If you do not, the key will *not* appear in the keys list when you add the key rule to the standard policy.

- **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.

When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.

When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.

- **Encryption Mode:** Encryption mode of the key. The options are:

- CBC

- CBC-CS1
- XTS

Encryption using the XTS and CBC-CS1 keys is known as enhanced encryption.

When you are done, click **Update**.

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **Transparent Encryption** application.
2. In the sidebar on the Clients page, click **Policies**.
3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
4. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a Standard policy.
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints.
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a

Field	Description
	Deny rule unless the policy is in Learn Mode.
Data Transformation	If you select Standard as the policy type, also select the the Data Transformation option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

When you are done, click **Next**.

- On the Security Rules page, define the security rules that you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of **key_op** and the effects **Permit** and **Apply Key**. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version.

To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

When you are done, click **Next**.

- On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one. If the data has not yet been encrypted, select clear_key. Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select clear_key.
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is

Field	Description
	currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

When you are done, click **Next**.

- On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click Select to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in Create an Encryption Key.

When you are done, click **Next**.

- Click **Next**.
- On the confirmation page, review the information for the policy and click **Save**.

Create Policy ✕

1 General Info
2 Security Rules
3 Key Rules
4 Data Transformation
5 Confirmation

Review the provided policy details.

1 General Info

Name: Simple-Policy
Policy Type: Standard
Description: Standard policy for new GuardPoints

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*			key_op	permit:applykey	Yes
*					Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	Simple-Key

[Back](#)
[Save](#)

Create a GuardPoint

- Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key.
 - /dir/hr/files
 - /dir/accounting/files
 - /dir/shared/hr
 - /dir/shared/accounting

Tip

If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

- In the Applications page of the CipherTrust Manager Console, select the **CTE** application.

3. In the Clients table, click on the name of the client you want to protect.
4. Above the GuardPoints table, click **Create GuardPoint**.
5. In the Create GuardPoint page:
 - a. In the **Policy** field, select the policy you created earlier.
 - b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a explorer window.

If you want to enter multiple paths, put each path on its own line. For example:

- d. Click **Create**.
- e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**. For this example, click No.

The CTE clients pull the GuardPoint configuration information from the CipherTrust Manager.

6. Type the following to transform the data:

```
dataxform --rekey --print_stat --preserve_modified_time --gp <pathToGP>
```

When the data transformation has finished, applications can resume accessing the now-protected data. (See the [CTE Data Transformation Guide](#) for more information.)

Ransomware Protection

- [Ransomware Protection Overview](#)
- [Creating GuardPoints](#)
- [Use Cases for Ransomware Protection](#)

Ransomware Protection Overview

Compatibility

Operating System	CipherTrust Manager version
Ransomware Protection for Windows	v2.12 and subsequent versions
Ransomware Protection for Linux	v2.17 and subsequent versions

Overview

Ransomware is a type of malicious software that is designed to block access to a computer system until a sum of money is paid. CTE for supports detection of Ransomware and protection of sensitive data from Ransomware.

CTE Agent monitors volumes and looks for processes that perform suspicious behavior such as processes that try to encrypt files or open thousands of files. If a process displays suspicious behavior, then it is either audited, which means it is flagged in a log file, or it is blocked. The action taken is pre-configured by the user in the profile linked to the client.

Licensing

Ransomware Protection is supported with RWP-enabled CTE clients. A CTE for Ransomware Protection license must be activated on the CipherTrust Manager to register an RWP-enabled CTE client. Refer to [CTE Licensing Model](#) for details.

Protecting Non-Sensitive Data

Use the Ransomware Protection mode to protect systems that do not contain sensitive data, but have access to your network.

A use case of this scenario is when you have users with laptops who frequently use your network and access servers on it, but they do not have any sensitive data locally on their laptops. A system like this might belong to a salesperson who travels and frequently uses other networks to access the internet. When such users log on to your network, they access the sales network server and upload data to it. They could easily pick up a Ransomware from another network and accidentally upload it to your company's network. Using the Ransomware Protection mode would protect the data on the local volumes, mounted volumes, and the network servers from being infected with Ransomware.

Protecting Sensitive Data

The Ransomware Protection mode protects data on servers and endpoints from Ransomware attacks by auditing

and blocking malicious IPs. Users can strengthen the security posture with CTE access and encryption policies and Ransomware protection for complete control on their data.

To protect sensitive data against Ransomware:

1. Ensure that the CTE Ransomware Protection license is activated and available on the CipherTrust Manager. Refer to [CTE Licensing Model](#) for details.
2. Install the CTE Agent with the Ransomware Protection capability enabled. The Ransomware Protection support uses the same registration process as CTE clients. Refer to [Configuring CTE with CipherTrust Manager](#) for information on installing and configuring CTE Agents.
3. Configure the Ransomware Protection settings in the linked client profile. Refer to [Setting Ransomware Protection Configuration](#) for details.
4. Create a Ransomware Protection GuardPoint on a volume (Windows)|directory (Linux) and on the directory for Linux to be protected. Refer to the [Creating Ransomware GuardPoints](#) for details.

CTE Registration

During CTE registration with CipherTrust Manager, the following question displays:

```
Do you want this host to have Filesystem encryption support enabled on the server? (Y/N) [Y]:
Do you want this host to have Ransomware Protection support enabled on the server? (Y/N) [N]
```

CTE Ransomware Protection can support the following protection modes:

- **Filesystem protection (CTE)**

Allows you to protect and encrypt files with policies **without** Ransomware Protection. (Available if you answer Y to the first question.)

- **Ransomware Protection (RWP)**

CTE is deployed to monitor volumes (Windows)|GuardPoints (Linux), for suspicious behavior from processes, and supports auditing or blocking of the processes while file encryption and protection is not supported. (Available if you answer Y to the second question.)

- **Filesystem and Ransomware Protection (CTE-RWP)**

Protects GuardPoints from Ransomware and allows you to protect and encrypt CTE files with policies. Therefore, all types of GuardPoints are available. (Available if you answer Y to both questions.)

Use Ransomware Protection GuardPoints to monitor or block Ransomware access attempts to a protected GuardPoints on the CTE clients. Note that if the GuardPoint type is "Ransomware Protection Only", Ransomware Protection GuardPoint does not require any policy.

Locking the System after a Ransomware Attack

After enabling Ransomware Protection during installation, turn on the agent lock and the system lock in CipherTrust Manager. The Agent lock protects the CTE Agent files from modification and deletion. The System lock protects a system files from modification and deletion. Agent Lock automatically enables when System Lock enables. You can manually enable or disable the Agent Lock only when the System Lock is disabled.

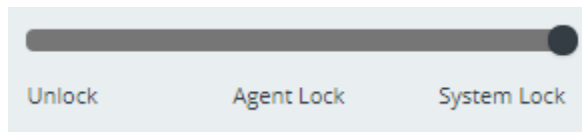
Make sure that no one is currently accessing the Agent installation directories while applying the locks.

To apply the locks:

1. In CipherTrust Manager, open the **Transparent Encryption** application.
2. Click on the **Client Name** or **Client Group Name**.
3. On the lock bar, click **Agent Lock**.



4. Click **System Lock**.



5. Click **Apply**.

Reference Information

- [Setting Client Locks](#)

Disabling Ransomware Protection

To disable Ransomware Protection for all GuardPoints on the clients linked with a profile.

1. In CipherTrust Manager, open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **RANSOMWARE PROTECTION CONFIGURATION**.
5. Select the **Operation** to **Disable**.
6. Click **Update**.

Creating GuardPoints for Ransomware Protection

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

To create a Ransomware Protection GuardPoint:

1. In CipherTrust Manager, open the **Transparent Encryption** application.
2. Select the client or client group on which you want to create a GuardPoint.
 - Click an Ransomware Protection-enabled client under the **Client Name** column (**Clients > Clients**). These are the clients with either Ransomware Protection, or CTE Ransomware Protection, protection mode.
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click **Create GuardPoint**:

Note

Once Ransomware Protection is enabled during CTE registration, Ransomware Protection is applied to all GuardPoints.

Ransomware Protection is supported in 2 Protection Modes:

- **RWP**: In CipherTrust Manager, when creating a GuardPoint, you cannot assign a policy and type is automatically set to Ransomware Protection Only.
- **CTE-RWP**: On clients with **CTE RWP** mode, you can create a Ransomware Protection GuardPoint set to Ransomware Protection Only, as well as other types of GuardPoints that use policies as shown below. In Linux, Ransomware Protection is also available for other GuardPoints if the GuardPoints are set on a directory.



Status	Policy Name	Protected Path	Type	Client Group	Enabled	LEP Progress	Multistep Authentication	
	Active	/usr/bin/cryptolib	Auto Cleaning		Yes	100%		
	Active	/usr/bin/cryptolib	Ransomware Protection Only		Yes	100%		

4. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:
 - **Enter/Browse Path**: Select this option, and enter the path by either typing or clicking the **Browse** button.

Note

- For **CTE Windows**, Ransomware Protection GuardPoints are applied at the volume level. Even if you specify the path of a folder or a file, the GuardPoint will be applied at the volume level.
- For **CTE Linux**, Ransomware Protection is applied at GuardPoint level.
- If you specify a network share, all of the network shares to be mounted subsequently will be protected.
- A CTE client administrator can configure protection of all existing GuardPoints, and those to be added to the client subsequently.
- A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

Browse Method

- a. Click **Browse** to select the path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths. Note that the client must be registered with CipherTrust Manager in order to browse its file system.
- b. In the **Enter Path** field, specify the path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.
- c. Click **Add**.

Manual Method

Alternatively, if you know the path, manually enter path in the given text box. Enter one path per line.

- **Upload CSV**: Select this option and click **Browse** to upload the CSV file containing the list of one or more paths. This is the recommended method to specify a large number of paths in one step.

Note

If a manually entered path does not yet exist, check that you entered the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.

5. Click **Create**. A message appears prompting to confirm the reuse of these GuardPoint settings on another path.
 - Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:

- a. In the **Enter Path** field, specify the path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.
- b. Click **Add Path**. The newly added path appears under the Paths list on the left. Similarly, add as many paths as required.
- c. Click **OK**.

- Click **No** if you do not want to use the same settings on another path.

6. Check the GuardPoint status, type:

```
secfsd -status guard
```

Multifactor Authentication for CTE GuardPoints

CipherTrust Transparent Encryption is supporting Multifactor Authentication through integration with an MFA provider. CipherTrust Transparent Encryption will continue to integrate with additional providers and release that information in the future.

Note

Multifactor Authentication for CipherTrust Transparent Encryption Linux is only supported with CipherTrust Manager v2.14 and subsequent versions.

- [Introduction to Multifactor Authentication](#)
- [Set up your account with KeyCloak](#)
- [Use Cases for Multifactor Authentication](#)
- [Exempting some users from authentication with a Whitelist](#)
- [Setting up Multifactor Authentication with a One-Time-Password](#)
- [Setting up Multifactor Authentication with a Time Out](#)
- [Administration for Multifactor Authentication](#)
- [Troubleshooting Multifactor Authentication](#)

Introduction to Multifactor Authentication

Why do companies need Multifactor Authentication

Every day, the threat of ransomware attacks increase in frequency, sophistication, and effectiveness. Victims of

ransomware attacks can be blocked from data, applications, and systems – making an organization unable to function.

Credential compromise is the leading cause of ransomware attacks, because credentials give hackers the access they need to hold your systems hostage. Unfortunately, credentials can be stolen, shared, bought or hacked. Once the hackers gain entry, the threat actors will often look to compromise privileged access credentials to further infiltrate your network and steal sensitive data.

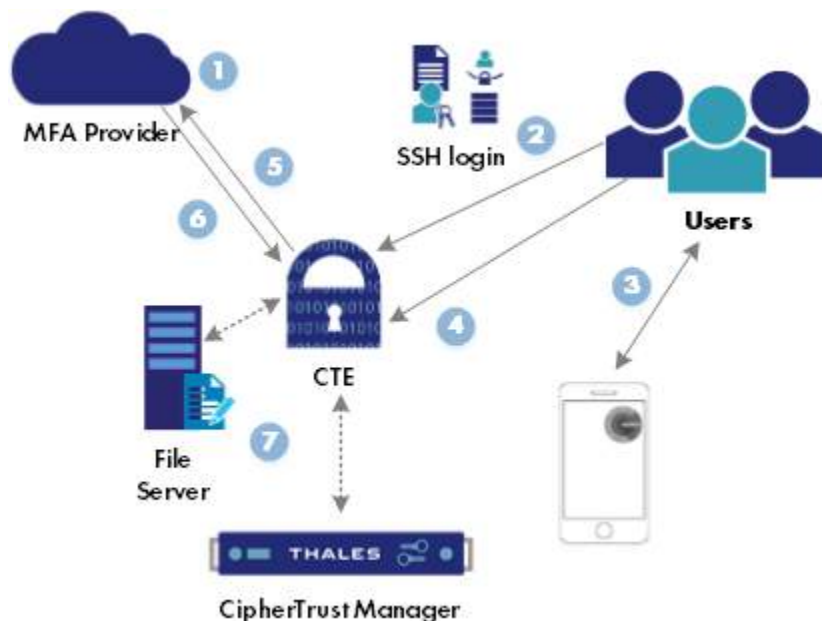
What is Multifactor Authentication

Multifactor authorization ensures that the access credentials presented belong to the actual person. After logging in to the system, when a user tries to access a CipherTrust Transparent Encryption GuardPoint, it triggers a second factor authorization to verify the user with a second form of authentication, like sending a passcode to the users's registered cell phone, that they then have to input into the application.

How does Multifactor Authentication work

The following diagram explains how Multifactor Authentication operates in a CipherTrust Transparent Encryption environment.

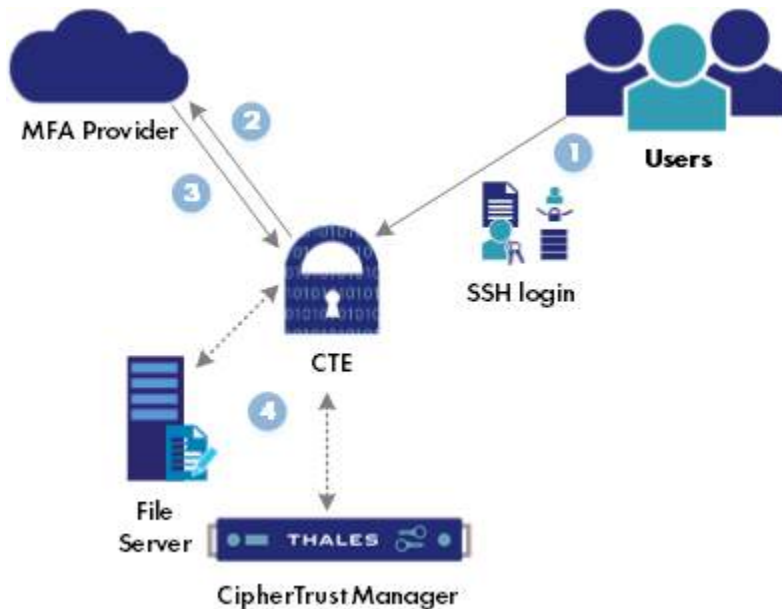
OTP (One-Time-Password)



Step	Description
1	A Multifactor Authentication administrator configures the MFA provider to use OTP (one-time password) for CTE multifactor authentication.
2	Multifactor Authentication is performed when either an SSH connection with MFA has already been enabled by a root user using the command <code>voradmin mfa ssh_enable</code> , and a user starts an SSH connection; or after an SSH connection is already established and a user uses the command: <code>voradmin mfa login</code> .

Step	Description
3	A CTE user who has previously registered the CTE site URL with an authenticator application (such as Google Authenticator), running on his/her registered mobile device, uses the authenticator to generate a one time password.
4	CTE user enters the OTP from their mobile phone into CTE.
5	CipherTrust Transparent Encryption sends a message to the Multifactor Authentication provider to verify the user.
6	Multifactor Authentication provider confirms/denies user access.
7	If authenticated using <code>voradmin mfa login</code> , the user's current shell, and all of the programs running inside that same shell, are authenticated. If authenticated during an ssh login, the entire ssh session is authenticated for the user.

Password



Step	Description
1	Multifactor Authentication is performed when either an SSH connection with MFA has already been enabled by a root user using the command <code>voradmin mfa ssh_enable</code> and a user starts an SSH connection, or after an SSH connection is already established and a user uses the command: <code>voradmin mfa login</code> and enters their Multifactor Authentication password.
2	CTE sends a verification request to the Multifactor Authentication.

Step	Description
3	Multifactor Authentication provider confirms/denies user access.
4	If authenticated using <code>voradmin voradmin mfa login</code> , the user's current shell, and all of the programs running inside that same shell, are authenticated. If authenticated during an ssh login, the entire ssh session is authenticated for the user.

Note

Multifactor Authentication is **NOT** supported on RHEL 7 or SLES 12.

For more information on Multifactor Authentication, see [Multifactor Authentication](#).

Using Keycloak for Multifactor Authentication for CTE GuardPoints

Integration with Keycloak requires creating an OIDC connection in CipherTrust Manager, after you create an OIDC template in Keycloak.

Prerequisites

- Have a CipherTrust Manager set up with:
 - Client Profile enabled for Multifactor Authentication
 - Registration token

On the Keycloak platform

The following is the minimum setup for a Keycloak platform. Refer to [Keycloak documentation](#) for more information.

1. Create an admin user.
2. Login to the realm and create one or more users.
3. Create a password for the user.
4. Create an OIDC client in realm with the following settings enabled:
 - **General Settings:**
 - **Client Type:** OpenID Connect
 - **Client ID:** Client name

- **Capability Config:**
 - **Client Authentication:** On
- **Authentication flow:**
 - **Select:** Standard flow and Direct access grants

5. Note three OIDC parameters:

- **OIDC Provider:** `https://<keycloak-name>:<keycloak-port>/realms/<realm-name>/well-known/openid-configuration`
- Client-ID as configured for the OIDC client
- Client-Secret as shown for the OIDC client

Create an OIDC connection on CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management > Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values for the configuration information.

Note

Refer to your Multifactor Authentication provider profile for the values:

- URL of OIDC provider:

Linux

- For KeyCloak, select the URL of the OIDC provider

Windows

- For Thales SafeNet Trusted Access, select **Well Known Configuration URL**
- For all other providers, select the URL of the OIDC provider
- Client-ID as configured for the OIDC client
- Client-Secret as shown for the OIDC client

7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

Exempting some users from authentication with a Whitelist

When you activate CTE Multifactor Authentication, all users attempting to log in to the CTE client must successfully pass through CTE Multifactor Authentication to gain entry to the MFA-enabled GuardPoints. However, there are specific exemptions to this rule. Users whose system services, or applications, initiate automatically during system boot-up cannot undergo authentication though CTE Multifactor Authentication, as Multifactor Authentication necessitates user interaction. To accommodate such cases, exempt these users from Multifactor Authentication enforcement within the Client Profile by including them in the user set exemption list. Typically, only system users responsible for running system services are included in this list. However, since many system applications operate under the root user, or even under normal application user accounts, you must also add these system administrator/application users to the list. These users form part of the user set, commonly referred to as a whitelist.

Caution

Be careful when adding a user to the whitelist. The exemption applies for the entire client. Users on this list can bypass Multifactor Authentication and access all MFA-enabled GuardPoints. If a system service, or application, accesses only one GuardPoint among multiple GuardPoints, Thales advises you to leave that specific GuardPoint without Multifactor Authentication enforcement.

Note

You **cannot** share the whitelist between Windows and Linux operating systems. Each client profile must contain a unique Multifactor Authentication whitelist. Therefore, the User Set contains different users in Windows and Linux platforms. A CTE Windows client and a CTE Linux client **cannot** share the same client profile when Multifactor Authentication is enabled.

Creating a User Set

See [Creating User Sets](#) for information on creating a User Set in a Policy Element.

Adding the User Set to the Client Profile

To add an Multifactor Authentication whitelist to the client profile:

1. Create your [Client Profile](#) if it is not already created.
2. Click on your client profile to open it.
3. Click **Multifactor Authentication**.
4. In the **Select OIDC connection** field, select the OIDC connection that you created.

5. In the **Select the MFA exempted User Set** field, select the User Set that contains the people/applications that are exempted from authorization.
6. Click **Update**.

Setting up Multifactor Authentication with a One-Time-Password

CipherTrust Transparent Encryption Multifactor Authentication supports KeyCloak OTP through direct grant flow. This topic explains how to configure OTP support in KeyCloak.

Prerequisites

- [Setup Keycloak](#)

Enabling OTP Authentication in KeyCloak

1. Log in to the KeyCloak Admin Console. See [KeyCloak documentation](#) for more information.
2. Select **Authentication** from the menu for your CTE realm, e.g. cte-linux. This is the area where you can configure the different credential types.
3. Select the Browser Flow:
 - a. Conditional OTP: **Required**
 - b. Condition: User configured: **Required**
 - c. OTP Form: **Required**
4. Modify, clone, or create a new Direct Grant flow:

Option 1:

Modify the built-in direct grant flow, or clone a direct grant flow, by clicking **Action > Duplicate**.

Update the flow as the follows:

- a. Username Validation: **Required**
- b. Password: **Disabled**
- c. Direct Grant: Conditional OTP: **Required**
- d. Condition: User configured: **Required**
- e. OTP: **Required**

Option 2:

Create a new direct grant flow:

- a. Select **Create Flow**
 - b. Fill out the Name and Description
 - c. Select flow type: **Basic Flow**
 - d. Select **Add step**
 - e. Select Username Validation: **Required**
 - f. Select **Add step**
 - g. Select OTP: **Required**
5. Bind the generated direct grant flow to the client defined for CTE Linux:
- a. Choose the client setup for CTE Linux, and select **Advanced**
 - b. Select Browser Flow: **Browser**
 - c. Select Direct Grant Flow: **<the new direct grant>**

Configuring OTP Policy

CTE Linux Multifactor Authentication only supports time-based OTP, which is the default KeyCloak OTP policy. To verify the policy configuration:

1. Navigate to the **CTE realm > Authentication**.
2. Select **Policies > OTP Policy**.
3. Ensure that Time-based is selected.

Note

Counter-based is **NOT** supported with CipherTrust Transparent Encryption.

4. Change other configurations as needed.

Note

Google authenticator only supports the algorithm: **SHA1**.

Setting Up User's OTP Authenticator

1. Add a user that has permissions to access CTE clients.
2. The user must install an authenticator that is able to provide an OTP token on their mobile phone.

Note

Thales recommends using Google Authenticator.

3. Instruct the user to login through a web browser to the CTE realm account. See [KeyCloak documentation](#) for more information.
4. Once authenticated, the OTP token form displays.
5. The user needs to finish the setup of OTP authentication in the OTP token form.

Conclusion

After a successful setup, the local users of the CTE Linux hosts can perform OTP authentication through `voradmin mfa login` or `SSH login`.

Setting up Multifactor Authentication with a Time Out

You can set Multifactor Authentication so that it times out after a specified period. The timeout value for an MFA session is set in minutes. The default is 0, meaning no timeout.

Note

MFA timeout only applies to new processes. Once a process, like Bash, for example, is MFA-authenticated, it does not time out. Additionally, when a timeout value changes, all MFA-authenticated processes remain authenticated. The timeout change does not affect them.

Administrator Tasks for Multifactor Authentication

Note

Root user privilege is required for all commands except for logging in.

Voradmin Commands

The Multifactor Authentication command group contains the following commands:

Syntax voradmin mfa [config | login | ssh_enable | ssh_disable | set_auth | set_timeout]

voradmin mfa config

Displays configuration information.

Syntax

```
voradmin mfa config
```

Response

```
Host Mfa Enable is not set.
MFA enabled guardpath(s) (Number of paths: 2):
    /home/work1/gp_mfa
    /home/work1/gp_mfa
MFA Exempt-List: (Number of entries: 1)
    uid:1001,      gid:1001,      user: "malfoy", group: "wizards", dom
ain(s): ""
OIDC configuration:
    client-id : cte-client-malfoy-1
    url : https://www.keycloak-sj1.org:8443/realms/cte-linux/.well-known/openid-configuration
ssh with MFA : enabled
```

voradmin mfa login

Enables Multifactor Authentication for the current shell, and commands and programs running in that shell, so that it can access MFA-enabled GuardPoints. You must provide a login name and password for Multifactor Authentication enablement.

Syntax

```
voradmin mfa login
```

Response

```
CTE MFA username: #####
CTE MFA password: #####
CTE MFA authentication successful
```

voradmin mfa ssh enable

Enables the option to use Multifactor Authentication once a user has established an ssh login to the current host. After running this command, user is asked if they want to use Multifactor Authentication. Once logged in successfully, user is asked if they want to enable Multifactor Authentication. Once you enable MFA successfully, CTE Agent can access Multifactor Authentication-enabled GuardPoints.

Syntax

```
voradmin mfa ssh_enable
```

voradmin mfa ssh_disable

Disables the option to use Multifactor Authentication once a user has established an ssh login to the current host.

Syntax

```
voradmin mfa ssh_disable
```

voradmin mfa set_auth

Set up the authentication method (either OTP or password) to use during CTE multi- factor authentication. If not setup, users have to choose a method during ssh login or voradmin mfa login.

Syntax

```
voradmin mfa set_auth
```

Response

```
Choose authentication method (type p for password, or o for OTP, default o):`<type p or o>`: o
```

```
MFA authentication method is set.
```

voradmin mfa set_timeout

You can set Multifactor Authentication so that it times out after a specified period. The timeout value for an MFA session is set in minutes. The default is 0, meaning no timeout.

Note

MFA timeout only applies to new processes. Once a process, like Bash, for example, is MFA-authenticated, it does not time out. Additionally, when a timeout value changes, all MFA-authenticated processes remain authenticated. The timeout change does not affect them.

Syntax

```
voradmin mfa set_timeout <minutes>
```

Example 1


```
voradmin mfa set_timeout 5
```

Response

```
MFA session will expire after 5 minute(s).
```

Example 2

```
voradmin mfa set_timeout 0
```

Response

```
Disabled MFA session timeout.
```

Troubleshooting Multifactor Authentication

Multifactor Authentication Client Profile Failed on CipherTrust Manager enrollment**

Switching existing Multifactor Authentication Client Profile using `register_host` failed on CipherTrust Manager enrollment.*

Work-around

- In CipherTrust Manager, change the existing Multifactor Authentication `Select MFA Exempted User Set` parameter to your new target user set

Special Cases for CTE Policies

This section describes some CTE-specific configuration tasks related to configuring policies in the key manager. It contains the following topics:

- [Re-Enabling Automatic Signing for Host Settings](#)
- [Restricting Access Overrides from Unauthorized Identities](#)
- [Blocking ptrace system calls to prevent process injection attacks](#)

Re-Enabling Automatic Signing for Host Settings

Starting with VTE for Linux release 6.0.2, VTE blocks automatic re-signing of the host settings. Some users may have established procedures for updating system software that are based on the assumption that restarting the vmd will generate new signatures when signed software is updated. This is no longer true. However, you can re-enable automatic re-signing if your environment requires it.

Caution

Re-enabling the automatic regeneration of signatures exposes a potential security vulnerability for CTE Agents. When enabled, host setting binaries are re-signed when CTE receives a push from the associated key manager. If an attacker were to replace a binary with a Trojan, and then force a push from the key manager by, for example, restarting the CTE Agent, CTE could generate a signature for the malicious binary and pass it.

To re-enable automatic re-signing for host settings:

1. Change to the directory where the `agent.conf` file resides. For example, type:

```
cd /opt/vormetric/DataSecurityExpert/agent/vmd/etc/
```

2. Edit the `agent.conf` file.
3. Change or add the following line:

```
AUTO_RESIGN_HOST_SETTINGS=TRUE
```

Note

Previously this setting was known as `RE_SIGN_HOST_SETTINGS`. Starting with VTE for Linux 6.1.3, the attribute name is `AUTO_RESIGN_HOST_SETTINGS` as shown above.

4. Save your changes and exit the file.
5. Restart the `vmd` to set the changes. Type:

```
/etc/vormetric/secfs restart
```

6. Type the following to verify that the host settings is set to true:

```
vmsec vmdconfig
```

Restricting Access Overrides from Unauthorized Identities

CipherTrust Transparent Encryption host/client settings are the means by which an administrator configures user authorization. Users with root privileges, on Linux or AIX systems, have the unfettered ability to override all file access and execution permissions imposed by the system.

CipherTrust Transparent Encryption access control allows you to restrict privileges of users, groups, application

processes and binaries, including root users and setuid programs. By default, CipherTrust Transparent Encryption agent **DOES NOT** trust any process as authenticated. Any attempt to access a resource, by any process, will therefore be flagged with a “User Not Authenticated” notification. The CipherTrust Transparent Encryption agent must be instructed to trust the authenticator process progeny. For example, `/usr/sbin/sshd` is a process that can be trusted to authenticate the user to the system and to CipherTrust Transparent Encryption.

In some setups, when editing a host, system administrators can use the **host settings > |authenticator|** feature with **su** to change identities and gain access to restricted data. You can instruct CipherTrust Transparent Encryption to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CipherTrust Transparent Encryption can block from authenticating other processes.

Any executable path that is marked with a `|path_no_trust|` host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as “User Not Authenticated” to prevent access on user-based policies.

CipherTrust Transparent Encryption prevents overrides from other host settings authenticators, using the `|path_no_trust|` status. If a user runs the **su** command from a non-trusted shell, that new shell is still marked as `|path_no_trust|`, even if `|authenticator| /usr/bin/su` is specified in the host-settings. The `|path_no_trust|` feature overrides any and all authenticators under host settings.

Note

Using `|trust| *` before a `|path_no_trust|` host setting no longer disables the `|path_no_trust|` host setting.

For example, the following host setting denies authentication for users accessing through `sshd`:

```
|trust|*
|path_no_trust|/usr/sbin/sshd
```

To restrict access overrides:

1. In the CipherTrust Manager products page, click **Transparent Encryption > Clients**.
2. Click on an existing Client name to edit the host.
3. Click **Client Settings** tab.
4. Add the following to the settings:

```
|path_no_trust|<path of the binary>
```

Example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **Apply**.

Blocking ptrace system calls to prevent process injection attacks

To prevent a process injection attack, which could lead to access to encrypted data by a tampered process, Thales implemented a global blocking for the ptrace system call. The purpose of this feature is to provide configurable options for disabling the ptrace system call based on user need. CTE provides toggle options on CipherTrust Manager based on the dynamic parameter which allows a security administrator to select which binaries are protected from ptrace attachment.

Note

This change can be very invasive and block legitimate uses of the ptrace system call.

Options

There are three new options:

Enabled_For_Authenticators

The CTE binaries and the binaries specified in the authenticator list are protected from the ptrace attachment. Other binaries are not protected from the ptrace attachment. (Default behavior)

Enabled_For_All

All of the installed binaries are protected from ptrace attachment. This protects from a tampered processes causing process injection attacks through the ptrace attach call.

Disabled_For_All

The CTE binaries are protected from ptrace attachment but the binaries specified in the authenticator list are allowed to attach to a ptrace system call. This solves the problem of a user trying to attach a ptrace system call to one of the binaries specified in the authenticator list for other use cases. Other binaries are not protected from the ptrace attachment.

Note

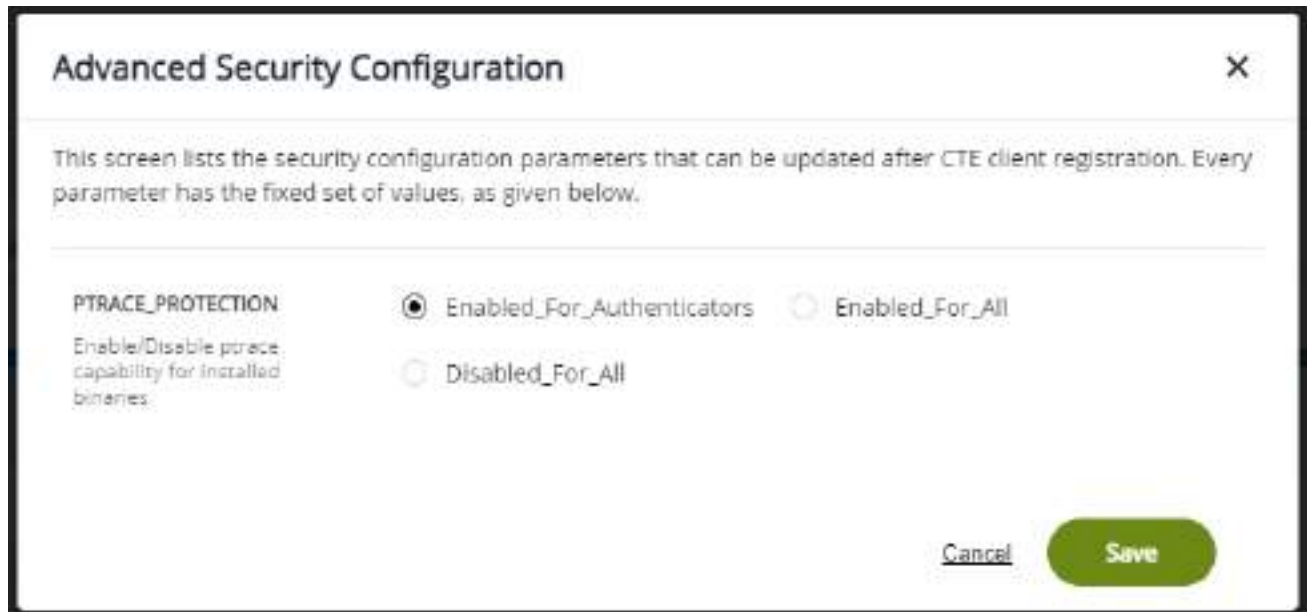
If you select Disabled for All, make sure that you set the log level on CipherTrust Manager to WARN or higher. If it is set to the default log level of ERROR, there will not be any messages related to ptrace logged in the vmd.log file.

Configuration

To configure blocking the ptrace system call:

1. Log on to CipherTrust Manager.

2. Click **Transparent Encryption**.
3. Click on the desired client name to open it.
4. In the **Advanced Security Configuration**, click **View/Edit Settings** link.



5. Select the appropriate option and click **save**.

Logging

This chapter contains the following sections:

- [Setting CTE Agent Logging Preferences](#)
- [Audit Logs](#)
- [Concise Logging](#)

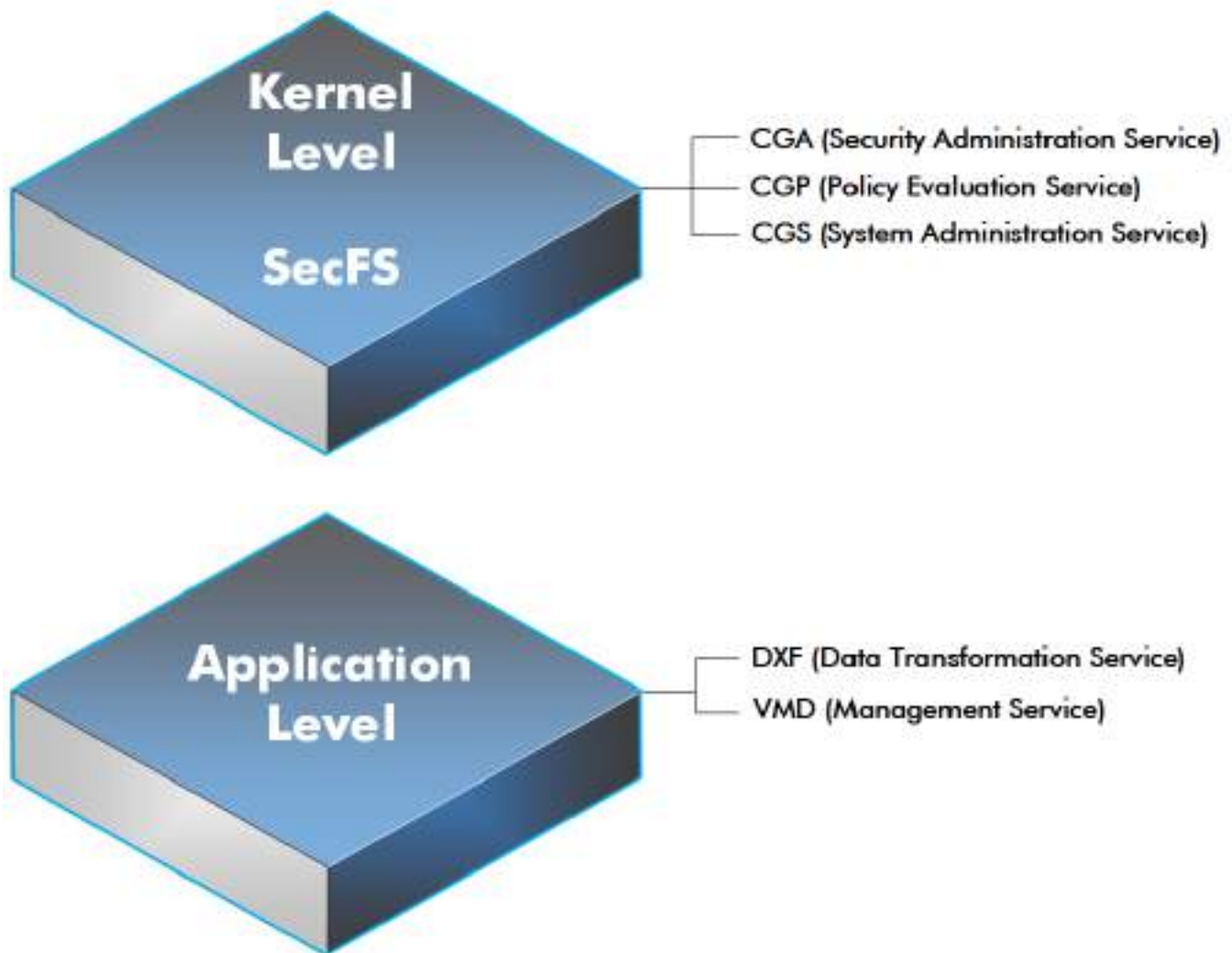
Setting CTE Agent Logging Preferences

You can configure the Agent process information that is entered into the Message Log. You can configure the process information globally, in which all the Agents that are added after the configuration change inherit the log attributes, while all current file system configurations remain intact. Alternatively, you can configure log attributes for individual Agent installations.

Always monitor log generation on new server and agent installations, and after changing logging preferences and options.

A variety of logging services are available and configured in the Log tab.

Logging Services



CTE log data may be sent to various different files such as:

- Sys log files, such as:

```
/var/log/messages
```

```
/var/log/syslog
```

Event log on

Note

The CM domain name can include spaces. However, Syslog does not allow spaces in header fields. Therefore, for Syslog purposes, the CTE client replaces the spaces with an underscore. For example: My_Domain instead of My Domain.

- CTE log files local to the agent, such as:

```
/var/log/vormetric/vorvmd_root.log
```

```
C:\ProgramData\Vormetric\DataSecurityExpert\agent\log\vorvmd.log (Windows)
```

- Uploaded to the Key Manager
- Uploaded to a Syslog server

Data Transformation log files are sent to:

```
/var/log/vormetric/vordxf_path_usr.log
```

Audit Logs

Example audit log:

```
CGP2601I: [SecFS, 0] [AUDIT] Policy[allowAllOps_fs] User[root,uid=0,gid=0\root,bin,daemon,sys,adm,disk,wheel\] Process[/bin/cat] Action[write_app] Res[/opt/apps/apps1/doc/file2.txt] Key[aes128] Effect[PERMIT Code (1U,2U,3R,4M)]
```

Analyzing Audit log entries

The format of a File System Audit log entry is:

```
CGP2602I: [SecFS, 0] Level: Policy[policyName?] User[userID?] Process[command?] Access[whatIsItDoing?] Res[whatIsItDoingItTo?] Effect[allowOrDeny? Code (whatMatched?)]
```

Parameter	Description
Identifier	The TLA for the error message.
SECFS	Indicates that the message was generated by an Agent. You can enter secfs in the Search Message field in the Logs window to display the Agent policy evaluation and GuardPoint activity for all configured hosts.

Parameter	Description
Level	Indicates the importance of the message. For example, AUDIT indicates an informational message, whereas ALARM indicates a critical failure that you should not ignore.
Policy	Indicates the name of the policy that is being used to evaluate the access attempt.
User	Identifies the system user attempting to access data in the GuardPoint. It typically displays the user name, user ID, and group ID.
Process	Indicates the command, script, or utility being executed.
Access	Indicates what access is being attempted. Access may be read_dir, remove_file, write_file_attr, write_app, create_file, etc. These correspond to the Access methods that you configure in the policy. Read_dir corresponds to d_rd. Remove_file corresponds to f_rm, etc.
Res	Indicates the object/resource being accessed by the Process[].
Effect	Indicates the rule that matched and, based upon that rule, whether or not the CipherTrust Manager grants access. Access states may be either PERMIT or DENIED.

File System Audit Log Effects Codes

Codes are provided in the audit logs that identify actions by the policy enforcement engine. The code follows the number of the rule being processed.

Code	Definition
A	The Action component of a security rule failed to match.
M	All security rule components match and, unless overridden, the Effect for that security rule is applied.
P	The Process component of a security rule failed to match.
R	The Resource component of a security rule failed to match.
T	The time specified in the When component of a security rule failed to match.
U	The User component of a security rule failed to match.

Refer to the audit log example above:

- The first and second Security Rules fail because of a mismatch in the User component (1U, 2U).

- The third Security Rule fails because of a Resource component (3R) mismatch.
- All of the rules in the fourth Security Rule match (4M), and the actions defined in the policy, such as use an encryption key, are applied.

Concise Logging

Thales' standard operational logging sends audit messages for each file system operation each time a file is opened, read, updated, or written. Thales's standard logging can generate high volumes of log data. Most of these messages might not be useful or required by security administrators to monitor file system activity on the system.

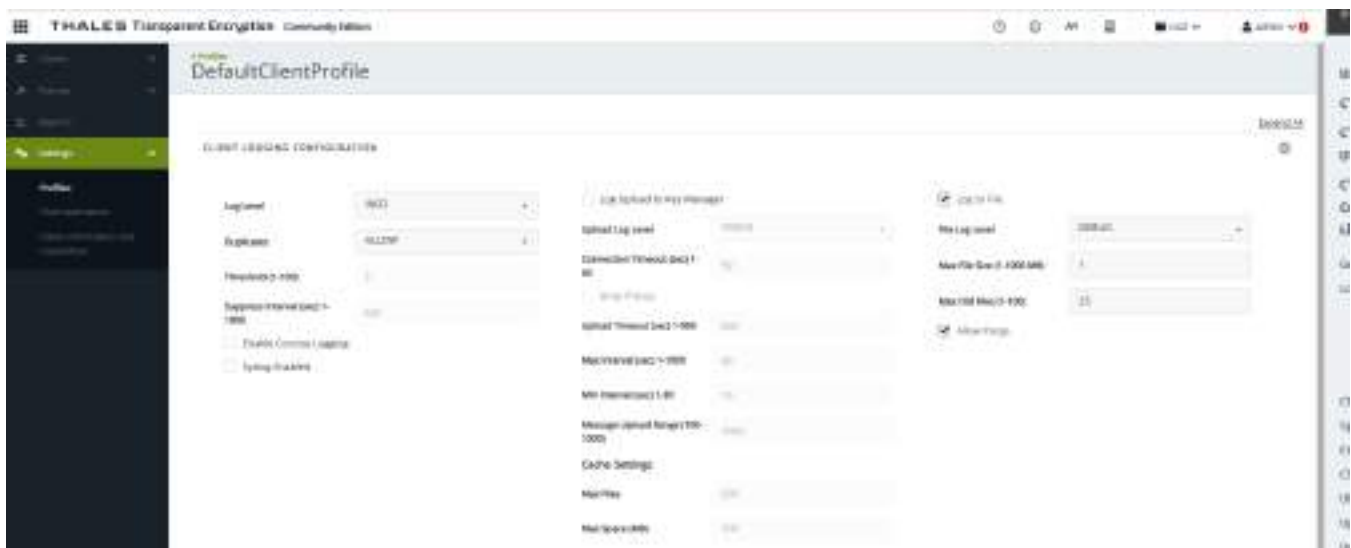
Agent log data can be stored on the local host, sent to a syslog server, or uploaded to the Management Console. On an agent system, log entries can flood the local messages file or Event Log. Extreme logging can also affect network performance.

Concise Logging eliminates the following types of messages:

- Duplicate audit messages for each and every block read by the user or application. With Concise Logging, CTE only sends an audit message the *first* time a user or application performs a read/write activity. Subsequent read/write activity by that user or application is not logged.
- Audit messages that read the attributes, read the basic information of file-set attributes, and other event-based messages.
- Audit messages for directory open, read directory attributes, and directory close.

Configuring Concise Logging for CTE Clients or Client Groups with CipherTrust Manager

In **CipherTrust Manager > CipherTrust Transparent Encryption > Settings > Profiles**, when you create a Client Profile, you can select to Enable Concise Logging. Then, you can apply that Client Profile to a specific client, or to all clients in a Client Group.



Considerations

- Concise Logging changes the set of log messages that are sent to Security Information and Event Management (SIEM) software systems. If this results in loss of data required for customer reports, then disable Concise Logging.
- Concise Logging is only supported by CTE `secfs`.
- Enable and disable Concise Logging on the client, in the Client Profile. CTE applies it for all users of that Client Profile. There is no finer-grained control, such as per GuardPoint, user, or message type.
- Do not use Learn mode with Concise Logging.

Enhanced Encryption Mode

This section describes the enhanced AES-CBC-CS1 encryption mode for keys. It contains the following topics:

- [Compatibility](#)
- [Disk Space](#)
- [Encryption Migration](#)
- [File Systems Compatibility](#)
- [Container Compatibility](#)
- [Using the AES-CBC-CS1 Encryption Mode in CM](#)
- [Exceptions and Caveats](#)
- [Best Practices for AES-CBC-CS1 Keys and Host Groups](#)

The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

Note

AES-CBC-CS1 encryption does not require any additional license.

Security Improvements

	AES-CBC	AES-CBC-CS1
Unique IV per-file	No	Yes
IV predictability	Yes	No

File System Support

	AES-CBC	AES-CBC-CS1
Local FS	EXT3/EXT4/XFS	EXT3/EXT4/XFS
Remote FS	NFS3/NFS4/CIFS	NFS3/NFS4
Block Device Support (secdm)	Fully supported	No. When a policy contains a key with CBC-CS1 encryption mode, the guarding fails on the CipherTrust Manager, and an error message displays.

Compatibility

- CTE is backward compatible with, and fully supports, the existing AES-CBC mode for both new and existing datasets.
- CTE fully supports AES-CBC-CS1 encryption for LDT and offline data transformation on CTE Linux environments.

Versions of VTE prior to version 6.1.0 are not backwards compatible with AES-CBC-CS1 encryption. On these earlier versions, attempting to guard a device using a policy containing an AES-CBC-CS1 key will fail.

- Protected hosts supporting AES-CBC-CS1 encryption can be added to host groups.

Difference between AES-CBC and AES-CBC-CS1

The two encryption modes are completely different from a file format standpoint.

- AES-CBC-CS1 encryption only applies to file system directories; AES-CBC encryption applies to both files and block devices.

Note

- If you attempt to use an AES-CBC-CS1 key to guard a block device or partition, the guarding fails with an error reported on the CipherTrust Manager, similar to: Raw or Block Device (Manual and Auto Guard) GuardPoints are incompatible with Policy "policy-xxx" that contains a key that uses the CBC-CS1 encryption mode."

- AES-CBC-CS1 uses cipher-text stealing to encrypt the last partial block of a file whose size is not aligned with 16 bytes.
- Each file encrypted with an AES-CBC-CS1 key is associated with a unique and random base IV.
- AES-CBC-CS1 implements a secure algorithm to tweak the IV used for each segment (512 bytes) of a file.

Disk Space

Files encrypted with AES-CBC-CS1 keys consume additional disk space in contrast to files encrypted with AES-CBC keys. This is because AES-CBC-CS1 encryption requires file IVs to be created and persistently stored in contrast to AES-CBC encryption which does not consume any additional disk storage.

Therefore, administrators need to plan and provision additional disk capacity prior to deploying AES-CBC-CS1 encryption.

	AES-CBC	AES-CBC-CS1
Local Linux (CTE)	No change to file size. No extended attribute allocation	Internal use of extended attribute per file. Extra 4KB increase in file size.
Local Linux (CTE-U)	Internal use of extended attribute per file. Extra 4KB increase in file size.	Internal use of extended attribute per file. Extra 4KB increase in file size.
Remote Linux (CTE)	No change to file size. No extended attribute allocation	Extra 4KB allocation in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.
Remote Linux (CTE-U)	Internal use of extended attribute per file. Extra 4KB increase in file size.	Internal use of extended attribute per file. Extra 4KB increase in file size.

Encryption Migration

You can use either LDT or offline dataxform to:

- Transform data encrypted by AES-CBC to AES-CBC-CS1 and vice versa.
- Transform AES-CBC-CS1 encrypted data to clear contents and vice versa.

File Systems Compatibility

On Linux, you can use AES-CBC-CS1 keys to guard currently supported file systems.

AES-CBC-CS1 encrypted files on Linux remote file systems like NFS and CIFS increase the file size compared to encrypted files on Linux local file systems which retain the original file size.

AES-CBC-CS1 encrypted files on Linux local file systems, in conjunction with LDT policies, can result in additional space consumption. Unlike the current AES-CBC encryption where encrypted files on all file systems, both remote or local, have the same file format, AES-CBC-CS1 encrypted file formats differ based on whether or not they were created on local or remote file systems.

AES-CBC-CS1 files on Linux remote file systems such as NFS and CIFS embed the IV in a 4K-byte header within the file. When these files are guarded, CTE masks the file header -- to applications and system utilities. The expanded file is only apparent when CTE guarding is disabled.

Note

The remote file system must have enough extra space to store the extra 4K bytes of the embedded header. You can run the following script in the GuardPoint to identify how much space to reserve before data transformation:

```
x=$(find . -type f | wc -l); y=$(echo "$x * 4 /1024" | bc); echo ${y}MB
```

File System Requirements

Unlike with AES-CBC encryption, files encrypted with AES-CBC-CS1 on remote file systems cannot be copied over to local file systems in the absence of CTE guarding. Similarly, AES-CBC-CS1 encrypted files on local file systems cannot be copied over to remote file systems in the absence of CTE guarding.

The fundamental reason for this incompatibility is the usage of extended attributes on local file systems to store the IV, in contrast to its storage as a part of the file metadata on remote file systems. This is why files cannot be transferred across these file system boundaries in the absence of CTE guarding.

Storing Metadata

AES-CBC-CS1 encrypted files on Linux store the base IV of a file in either the extended attributes or in the file metadata:

- On local FS (EXT3/EXT4/XFS), Linux saves it as an extended attribute associated with the file. The underlying file system requires that you mount it with the extended attribute mount option.
- On remote FS (NFS and CIFS), Linux saves it in the embedded header of the file.
- For CipherTrust Transparent Encryption UserSpace, all files have an embedded header.

To get the value of the base IV, type:

```
voradmin secfs iv get <file-name>
```

Note

The base IV of a file is protected. It cannot be set/modified/removed by commands and applications. However, if a GuardPoint is unguarded, the files in the GuardPoint are no longer protected. An adversary can then corrupt the content of the files, as well as the IVs.

AES-CBC-CS1 depends on the physical file system's support for extended attributes.

Missing IV file

If the IV for a file is missing, or CTE is unable to read the IV, then CTE denies access to the file. This access denied message may trigger an application to display an error message. This message may vary from application

to application.

HDFS

The AES-CBC-CS1 key is compatible with the current Hadoop File System support.

Backups

Backups and other data protection utilities should take into account the extended attributes present in each AES-CBC-CS1 encrypted file on a Linux local file system to ensure that they are safely backed up. An AES-CBC-CS1 encrypted file whose IV is corrupted, renders the files to be corrupted and therefore unreadable. Hence all data protection software must preserve the file's extended attributes.

CTE Linux can inspect a file's IV using the following command:

```
voradmin secfs iv get file
```

On Linux, the backup utility specified in the guarding policy should automatically backup/restore extended attributes as well. For example, you must use the options to preserve extended attributes when running `cp` or `rsync.normal`.

Due to the different file formats, the backup/restore process across the local and remote file systems are not allowed. If you want to backup a GuardPoint from a local directory, you must restore it to a local directory. If a GuardPoint is backed up on a remote file system, you must restore it to a remote file system.

Backup/Restore Process	AES-CBC	AES-CBC-CS1
General backup utility requirement (all platforms)	Backup utility defined in guarding policy with clear view	Backup utility defined in guarding policy with clear view
Special requirement for backup/restore local fs on Linux	No	Backup utility must be run with user extended attribute enabled
Special requirement for backup/restore remote fs on Linux	No	No
On Linux, backup local fs and restore to remote fs	Allowed	Not allowed, the restored files cannot be accessed with I/O error
On Linux, backup remote fs and restore to local fs	Allowed	Not allowed, the restored files cannot be accessed with I/O error

Container Compatibility

The CBC-CS1 key is compatible with current Docker and OpenShift support.

Using the AES-CBC-CS1 Encryption Mode in CM

When you create a key in CTE, you enable Encryption Mode by selecting CTE Key Properties. See *Creating a New Key* in the [Managing Policies](#) chapter in the [CTE Administrator Guide](#).

Exceptions and Caveats

Note the following when using AES-CBC-CS1 keys.

Ensure User Extended Attributes are Enabled on RHEL 6

On RHEL6, EXT3/EXT4 are not mounted with user extended attributes enabled, by default. If a GuardPoint is on EXT3/EXT4, then remount EXT3/EXT4 with `user_xattr` as an option. Otherwise, guarding fails with the error "Extended attribute not enabled for GuardPoint."

Guarding Existing Files Without Data Transformation

You must convert an existing file with clear text through offline data transformation or LDT. If you do not transform the file, then after you guard using an AES-CBC key, the file displays garbled characters.

If you use an AES-CBC-CS1 key, access to the file is blocked with an I/O error.

Best Practices for AES-CBC-CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC-CS1 keys unless all hosts are running VTE for Linux version 6.1.0 or CTE version 7.0.0 or later.

CTE and systemd

CipherTrust Transparent Encryption (CTE) for Linux is integrated with the `systemd` framework. To ensure that applications start after the CTE agent starts at startup, you must modify `systemd`. This is also true when the CTE agent is started and stopped manually.

This section contains the following topics:

- Overview of CTE and `systemd`
- CTE Agent Control Changes on `systemd`
- CTE Configuration Changes Required on `systemd`
- SystemD Protection
- Manually Stopping an Application or Service

Overview of CTE and systemd

You can use `systemd` to configure dependent applications to start up or shut down in the proper order when CTE starts up or shuts down on a live system. If applications start before CTE starts, those applications may not be guarded. This applies to cases when you manually start or stop the system, such as when you upgrade CTE.

`systemd` replaces `init` in Linux as a system and service manager. Linux inherited `init` from the UNIX System V `init`. `systemd` is a collection of daemons, libraries, and utilities to provide central management and configuration for certain Linux distributions (see [Linux Distributions that Support CTE and systemd](#)). In addition to

providing enhanced features and performance, **systemd** is backwards compatible with System V and Linux Standard Base **init** scripts.

Linux Distributions that Support CTE and systemd

The entries in the following table are Linux distributions that are compatible with CTE. The table shows which distributions implement **systemd**, and those that do not. See the *Compatibility Matrix for CTE Agent with CipherTrust Manager* or the *Compatibility Matrix for CTE Agent with Data Security Manager* for the Linux distributions and kernels supported with your CTE version and key manager.

Distributions that support systemd	**Distributions that do not support systemd
RHEL 8	SLES
SLES 12	
SLES 15	
Ubuntu 20	
Ubuntu 22	

CTE Agent Control Changes on systemd

The commands to start, stop, restart, and check CTE status on **systemd** are shown in the following table:

Command	Command syntax for distributions that support systemd
Start	<code>/etc/vormetric/secfs start</code>
Restart	<code>/etc/vormetric/secfs restart</code>
Stop	<code>/etc/vormetric/secfs stop</code>
Check status	<code>/etc/vormetric/secfs status</code>

The normal states of CTE services on a system with one or more active GuardPoints is the following:

- **secfs-fs**: active (exited) state

Example

To check the status of CTE, type:

```
/etc/vormetric/secfs status
```

Result secfs-fs service: active (running) since Tue 2022-09-27 09:51:04 CDT; 1h 3min ago

CTE Configuration Changes Required on systemd

The following table is a high-level overview of the required changes in **systemd** unit configuration files to control the applications that must be in sync with CTE during system startup and shutdown.

Typical applications that require `systemd` changes include `postgres`, `httpd`, `mongodb`, `mysqld` and `mariadb`. For example, `mongodb` requires that CTE to be running before `mongodb` starts.

Caution

Configuring the dependencies as recommended here mean that whenever you stop CTE or if CTE stops unexpectedly, the dependent applications will automatically stop shortly before CTE stops. Be sure you understand the implications of this behavior on your production environment.

Task	For more information
Compile a list of your applications that use GuardPoints.	See the application examples above.
Shut down the applications that use GuardPoints.	Adding Dependencies to systemd Unit Configuration Files
Add the following lines to the <code>[Unit]</code> section of the <code>systemd</code> unit configuration file for each application: <code>After=secfs-fs-barrier.service</code> <code>Bindsto=secfs-fs-barrier.service</code>	Adding Dependencies to systemd Unit Configuration Files
To the <code>Before=</code> line in the <code>[Unit]</code> section of the <code>secfs-fs-barrier.service</code> file, add the following: <code>saslauthd.service</code> An entry for each application you added to the <code>systemd</code> unit configuration file.	Adding Applications to the secfs-fs-barrier.service File
Add the following lines to the <code>[Unit]</code> section of the <code>saslauthd.service</code> configuration file: <code>Bindsto=secfs-fs-barrier.service</code> <code>After=secfs-fs-barrier.service</code>	Adding Dependencies to the saslauthd.service File
Force the system to read the changed <code>systemd</code> configuration files by typing <code>systemctl daemon-reload</code> .	Adding Dependencies to the saslauthd.service File
Restart the applications that you shut down to make these changes.	Adding Dependencies to the saslauthd.service File

About systemd Dependency Changes for Unit Configuration Files

The previous table describes the effect of the required unit configuration file changes that are described in the following sections. See the [systemd documentation](#) for more information about the `After=` and `Bindsto=` unit configuration options.

Caution

In some cases, the unit configuration file for an application other than CTE may be overwritten when the application is upgraded. After upgrading an application, verify that changes to that

application's unit configuration file are still in place. Changes to the `secfs-fs-barrier.service` file are retained after you upgrade CTE.

The `secfs-fs-barrier.service` service ensures that CTE services and dependent applications start after CTE services and stop before CTE services as needed during system startup, shutdown, and when starting and stopping services on a live system. This special service manages the dependencies between applications and the `secfs-fs`, `secfs-init`, `secfsd`, and `vmd` services that make up the CTE agent:

File and Change	Purpose
File: Application-specific unit configuration file Add this line to <code>[Unit]</code> section: <code>After=secfs-fs-barrier.service</code>	In conjunction with the <code>Bindsto=</code> option, this option ensures that the application starts after the CTE agent on system startup.
File: Application-specific unit configuration file Add this line to <code>[Unit]</code> section: <code>Bindsto=secfs-fs-barrier.service</code>	If the CTE agent shuts down, the application also shuts down.
File: <code>secfs-fs-barrier.service</code> Add each application to the existing <code>Before=</code> line in the <code>[Unit]</code> section. Add <code>saslauthd.service</code> to the existing <code>Before=</code> line in the <code>[Unit]</code> section.	Ensure that the <code>secfs-fs-barrier.service</code> starts before the application services mentioned in the <code>Before=</code>

Location of Application Unit Configuration Files

To configure the proper startup order of services, modify the unit configuration file for applications that require CTE to be running. You must also modify the `secfs-fs-barrier.service` file. The location of these files varies between Linux distributions as described in the following table.

Distribution	Location of systemd unit configuration files
RHEL 8 SLES 12 SLES 15	<code>/usr/lib/systemd/ system/<application_name>.service</code>
Ubuntu 20 Ubuntu 22	<code>/lib/systemd/ system/<application_name>.service</code>

Adding Dependencies to systemd Unit Configuration Files

If your system supports `systemd` (see [Linux Distributions that Support CTE and systemd](#)), before you can safely reboot your protected host or use the files in the GuardPoint, you must perform the following steps to set the proper CTE dependencies for your applications.

1. Compile a list of your applications that use GuardPoints.
2. Prepare users of those applications for the interruption in service required to make these changes.
3. Shut down each of the affected applications.

- For each application, log in as root and open the unit configuration file for that application using a text editor such as `vi`. See the table above to determine the location of the `systemd` unit file.

For example, the unit configuration file for a hypothetical `exampled` application would be located in `/usr/lib/systemd/system/exampled.service`.

- Locate the `[Unit]` area in the file and add the following two lines at the end of the `[Unit]` section:

```
After=secfs-fs-barrier.service
BindsTo=secfs-fs-barrier.service
```

For example, the `exampled` application unit configuration file might have the following existing `[Unit]` section:

```
[Unit]
Description=Example server
After=syslog.target
After=network.target
```

In this case, you would add the two new lines after `After=network.target`.

- Save and close the unit configuration file.
- Repeat steps 3–6 for each application.

Continue to [Adding Applications to the secfs-fs-barrier.service File](#) to make necessary changes to `secfs-fs-barrier.service`.

Adding Applications to the secfs-fs-barrier.service File

After editing the `systemd` unit configuration file for each dependent application, you must also add each application to the `secfs-fs-barrier.service` file that is installed as part of CTE. The `secfs-fs-barrier.service` file ensures that CTE starts before dependent applications during boot and CTE stops before dependent applications when the system is shut down.

- As a root user, open the `secfs-fs-barrier.service` file in a text editor such as `vi`.

For example, the `secfs-fs-barrier.service` file is located in `/usr/lib/systemd/system/secfs-fs-barrier.service`.

- Add `saslauthd.service` along with the names of the unit configuration files that you edited in the last section to the end of the `"Before="` clause.

For example, the `secfs-fs-barrier.service` file might contain the following before editing:

```
Before=postgresql.service httpd.service mongodb.service mongod.service
mysqld.service mariadb.service nails.service
```

To add an entry for `saslauthd.service` and two custom application services called

`example1.service` and `example2.service`, you would edit the `Before=` line to look like this:

```
Before=postgresql.service httpd.service mongodb.service mongod.service
mysqld.service mariadb.service nails.service saslauthd.service
example1.service example2.service
```

3. Save and close the `secfs-fs-barrier.service` file.

In the future, CTE will start before each application listed in the `Before=` line and those applications will stop before CTE stops.

Drop-in Files for systemd

As an alternative to adding applications to the barrier file, you can use drop-in files to configure the `secfs-fs-barrier.service` file for dependency management using `systemd`. This eliminates the need to modify the service file for configuring dependencies.

All drop-in directory files with the suffix `.conf` are merged in alphanumeric order and parsed after the main unit file has been parsed. Each drop-in file must contain appropriate section headers. `Systemd` reads the `.conf` files in the following order.

1. The instance `.d/` subdirectory
2. The template `.d/` subdirectory

The drop-in `.d/` directories for system services can be placed in the following directories:

- `/etc/systemd/system`
- `/usr/lib/systemd/system` (Ubuntu only)
- `/run/systemd/system`

Drop-in files in `/etc/` take precedence over those in the `/run/` directory which, in turn, take precedence over those in the `/usr/lib/` directory. Drop-in files in any of those directories take precedence over unit files wherever they are located. Multiple drop-in files with different names are applied in lexicographic order, regardless of which directories they reside in.

Following is an example of a drop-in file (`dependencies.conf`) for the `secfs-fs-barrier.service`:

```
cat /usr/lib/systemd/system/sec-fs-barrier.service.d/dependencies.conf
[Unit]
Before=mfetpd.service mfeespd.service
```

The above example displays a drop-in file which adds two McAfee related services in the `Before=` clause of the `secfs-fs-barrier.service` file without modifying the service file itself. Eventually, `systemd` detects the drop-in files and links them to the `secfs-fs-barrier.service` file.

Adding Dependencies to the ``saslauthd.service`` File

The `saslauthd` process handles plaintext authentication requests on behalf of the SASL library. It isolates all code

requiring superuser privileges into a single process, and it can be used to provide proxy authentication services to clients that do not understand SASL based authentication.

The `saslauthd` service must start after the `secfs-fs-barrier` service:

1. As a root user, open the `saslauthd.service` file in a text editor such as `vi`.

For example, the `saslauthd.service` file is located in `/usr/lib/systemd/system/saslauthd.service`.

2. Locate the `[Unit]` area in the file and add the following two lines at the end of the `[Unit]` section:

```
After=secfs-fs-barrier.service
Bindsto=secfs-fs-barrier.service
```

For example, the `saslauthd.service` file might have the following existing `[Unit]` section:

```
[Unit]
After=syslog.target
After=network.target
```

In this case, you would add the two new lines after `After=network.target`.

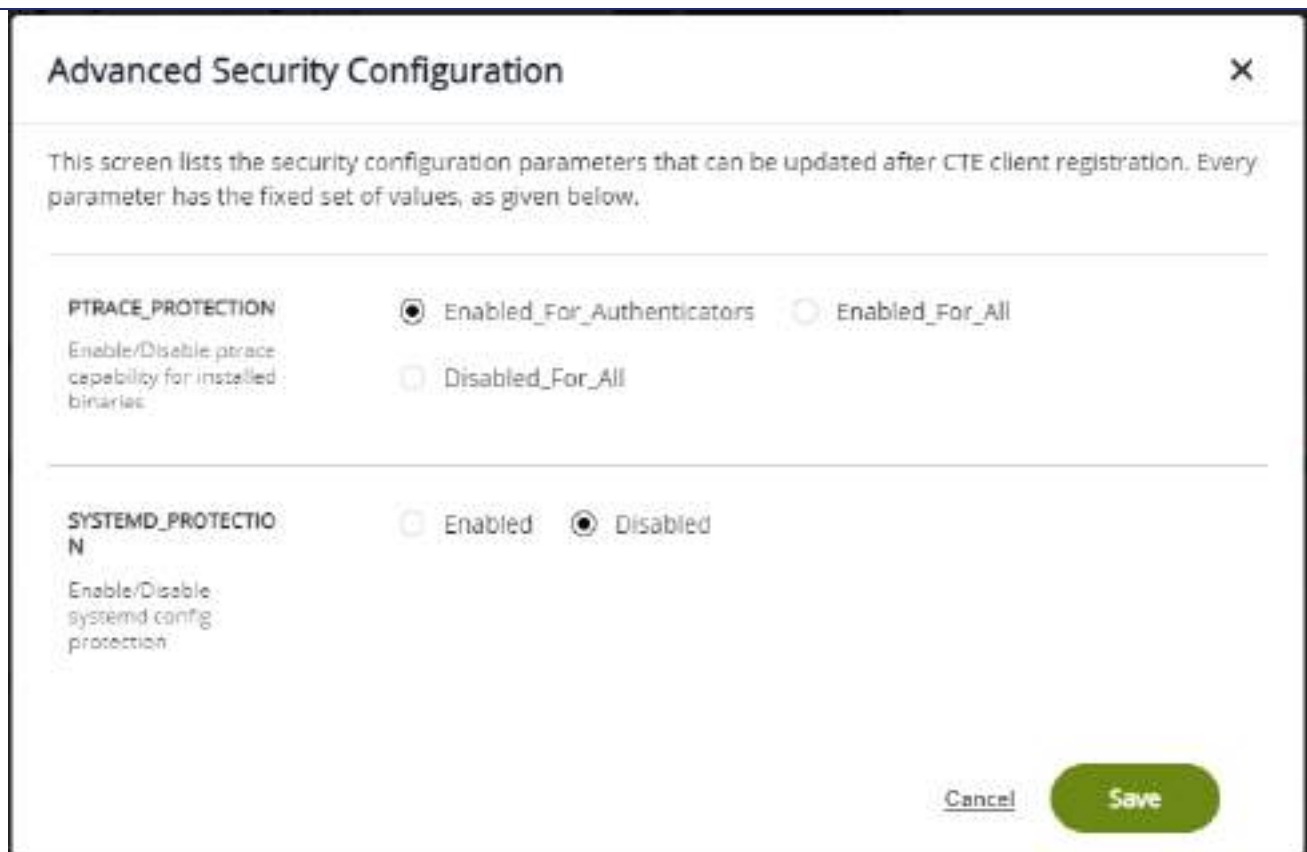
3. Save and close the `saslauthd.service` file.
4. To force the system to re-read the `systemd` configuration files that you changed in this section and the previous section, type `systemctl daemon-reload`.
5. Start each application that you shut down to make the configuration changes.

SystemD Protection

In RedHat 7 and subsequent versions, a lot of system functionality has been moved to `/etc/systemd/` which was previously not protected in CipherTrust Transparent Encryption. CipherTrust Transparent Encryption now gives you the option to protect it, meaning that no one can modify or delete files.

To protect the `systemD` directory:

1. Log on to CipherTrust Manager.
2. Click **Transparent Encryption**.
3. Click on the desired client name to open it.
4. In the **Advanced Security Configuration**, click **View/Edit Settings** link.



Advanced Security Configuration ✕

This screen lists the security configuration parameters that can be updated after CTE client registration. Every parameter has the fixed set of values, as given below.

PTRACE_PROTECTION ☒ Enabled_For_Authenticators ☐ Enabled_For_All
Enable/Disable ptrace capability for installed binaries. ☐ Disabled_For_All

SYSTEMD_PROTECTION ☐ Enabled ☒ Disabled
Enable/Disable systemd config protection.

Cancel Save

5. Select enabled or disabled and click **save**.
6. If you need to add a process to the directory:
 - a. Disable protection.
 - b. Add the file to the `/etc/systemd/` directory.
 - c. Re-enable protection.

Manually Stopping Application or Service

Manually Stop 3rd Party Applications on a Live System

The applications must already be configured as dependencies in the unit configuration files using the `BindsTo` clause (required). For more information, see [Adding Dependencies to systemd Unit Configuration Files](#).

Use the following commands to stop CTE on a live system with dependent applications running.

```
systemctl stop secfs-fs
/etc/vormetric/secfs stop
```

Response

```
Stopping the CipherTrust Transparent Encryption Agent.
Stopping Live Data Transform processes (if any).
WARNING: Following dependent services will be stopped in order to stop secfs serv
ices.
isecesp.service
isectpd.service
mysql.service
These services are required to start manually.
Successfully stopped the Encryption Expert CTE Agent.
```

Warning

- The 3rd party application services using the **BindsTo** clause that automatically stop must be restarted manually after an upgrade.
- Only GuardPoints that are busy due to 3rd party applications are freed using the new use case. Any GuardPoint due to other I/O operations must be stopped manually.

Utilities for CTE Management

Thales provides a variety of utilities that augment the standard Linux utilities. This combination of tools helps administrators manage CTE. The following utilities are described in this section:

- Agent Health Utility
- Agentinfo Utility (Java version)
- Backup Utility
- Check_host Utility
- Displaying Information for Nested File Systems with the DF tool
- Fsfreeze and xfs_freeze (CTE only)
- Protecting Files with Client Settings (CTE only)
- Restricting Access Overrides with Client Settings
- Register_host Utility
- Secfsd Utility
- Using Advanced Encryption Set New Instructions (AES-NI)
- User Cache Lookup Improvements

- Vmutils
- VMD
- Vmsec

Agent Health Utility

The `agenthealth` utility validates:

- Super-user privilege
- CTE Agent installation
- CTE registration to CipherTrust Manager Server
- CTE processes/ modules that are running
- Available disk resources
- Current GuardPoints
- Tests if the agent can reach the GuardPoints
- CTE log directory resource status
- This directory contains pending CTE log files for upload. This utility reports the size and number of pending files for upload. These text files are logs that contain vmd/SecFS information. They are regenerated whenever secfs restarts. If the number of files is unexpectedly large, this can indicate a problem.

The Agent Health check script

By default, the `agenthealth` script is installed in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`.

To run the `agenthealth` check script, type:

```
./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
```

System Response

```
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
dsm4209.sjinternal.com is resolvable ..... OK
dsm4209.sjinternal.com port 8446 is reachable .... OK
```



```

dsm4209.sjinternal.com port 8447 is reachable .... OK
Can communicate to at least one server ..... OK
VMD is listening on port 7024 ..... OK
Time of last update from server ..... 2021-07-07 15:47:08.290
Checking available disk space ..... OK
Checking logging space ..... OK
    Log directory is "/var/log/vormetric"
    File system for log data is "/", 48G free (5% full)
    Log directory contains 9 of maximum 200 files (4% full)
    Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to /media ..... OK
Testing access to /usr/data/sub1 ..... OK
[root@agt4206 bin]#

```

Agent Health Return Codes

Previously, the agent health return codes were only available in `/var/log/vormetric/agenthealth.log`. Now, the following options are also available through the help pages:

Help

This agent health script checks various facets of the CipherTrust agent to make sure that everything is functioning properly. Results are also logged to `/var/log/vormetric/agenthealth.log`.

Syntax

```
./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --help
```

Return Codes

Use the return code option to get a list of the return codes and what they mean. The codes are returned if the Agent is not running.

Syntax

```
./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --return_codes
```

Response

Return Code	Definition
EPERM	User is not root.
ENOENT	One of the programs used in this script does not exist. See <code>/var/log/vormetric/agenthealth.log</code> for which program is missing.
ENOPKG	Agent software is not properly installed. Agent configuration directory is missing or corrupt. See <code>/var/log/vormetric/agenthealth.log</code> for more details.
EPROTO	Agent is not registered to a key manager. Register the

Return Code	Definition
	agent to a key manager and try again. Try the wait option if the agent has never started correctly after registration. See <code>/var/log/vormetric/agenthealth.log</code> for more details.
EIO	Kernel modules are not loaded. To load a kernel module, type: <code>/etc/vormetric/secfs start</code>
ESRCH	VMD is not running. To start vmd manually, type: <code>/usr/bin/vmd</code>
SECFSD	Secfsd is not running. To start the secfsd manually, type <code>/usr/bin/secfsd</code>
EHOSTUNREACH	Unable to reach the Key Manager. Check network connectivity.
ECONNREFUSED	VMD is not listening. VMD did not finish initialization. See <code>/var/log/vormetric/vmd.log</code>
EWOULDBLOCK	VMD is attempting to connect to the Key Manager but has exceeded the designated wait time. Check <code>/var/log/vormetric/vmd.log</code> to fix any issues and retry.

Wait Time

Use `--w` to set a maximum wait time in seconds. The minimum is 10 seconds to test for the VMD to Key Manager initial contact. The default setting is 0, which means that there is no wait. Maximum is 1200 seconds.

Syntax

```
[root@agt4206 bin]# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
--w <value>
```

Example

```
[root@agt4206 bin]# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin//agenthealth
--w 60
```

Response

```
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
dsm148.i.vormetric.com is resolvable ..... OK
dsm148.i.vormetric.com port 8446 is reachable .... OK
dsm148.i.vormetric.com port 8447 is reachable .... OK
Can communicate to at least one server ..... OK
```

```
VMD is listening on port 7024 ..... OK
Time of last update from server ..... 2021-08-18 10:34:56.665
Checking available disk space ..... OK
Checking logging space ..... OK
Log directory is "/var/log/vormetric"
File system for log data is "/", 29G free (23% full)
Log directory contains 1 of maximum 200 files (0% full)
Log directory contains 0 of maximum 100 Mbytes used (0% full)
```

If the customer did not use the wait time options, the output would look similar to the following:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
Can communicate to at least one server ..... FAILED
For more information consult the log file /var/log/vormetric/agenthealth.log
```

agentinfo Utility (Java version)

The **agentinfo** utility collects system and CTE configuration data. The **agentinfo** utility is used to take a configuration snapshot of the system that you will send to Thales Customer Support to debug an issue, (This section describes the Java version.)

The **agentinfo** utility is a Java Script file. You can open it in a text editor to see specific functions.

The **agentinfo** utility displays status information on the screen and outputs the results to a compressed tar file. The compressed tar file name format is **ai.<os_name_ver>.qa.com.tar.gz** and it is located in the current working directory.

To create an **agentinfo** file, type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/agentinfo
```

Backup Utility

When a backup is performed, certain files and directories may be protected against access. Therefore, those files and directories are not written to the backup repository. These include files located in Data Transformation GuardPoints or files in GuardPoints with appropriate policies. Additionally, the following files are locked by default by CTE agent:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/.access
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/etc/*
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem/*
```

The following describes how to bypass the issue for multiple scenarios:

Agent is installed in the default location

1. Stop SecFS, type:

```
/etc/vormetric/secfs stop           //Linux  
  
/etc/rc.d/rc2.d/S99secfs stop      //AIX
```

2. Run the backup application with the desired arguments.
3. Restart SecFS, type:

```
/etc/vormetric/ start
```

Using a backup image to install to other agents or restore to a different system

Note

When the image is used to reinstall the system, the agent will automatically start at system boot and will attempt to connect to the key manager to which it was originally registered.

To prevent multiple systems with the same agent ID, you must uninstall CTE from the system before running the backup application. The restore/install from the backup will not have an agent running.

1. Uninstall the agent, type

```
/opt/vormetric/DataSecurityExpert/agent/secfs/bin/uninstallsfs
```

2. Run the backup application with the desired arguments.
3. Re-install CTE agent.

Performing a backup while the agent is running

Before running the backup application, add the files that are protected by the agent to the exclusion rules to exclude them from the backup:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/.access  
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/etc/*  
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem/*
```

The GuardPoint policy may implement access restrictions which would also cause the backup application to

generate error messages. These GuardPoint/directories will also need to be added to the exclusion rule method to exclude them from the backup. Alternatively, you can temporarily unguard them while the backup application is running.

If the CTE agent reports a status of incomplete in the backup application and does not start properly, or partially starts but generates error messages at system boot time, then uninstall and reinstall the agent. The restore/clone image contains everything needed to uninstall the agent. Use the following command to perform this operation:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/bin/uninstallsfs
```

Backing up Databases after Encryption

After encrypting a database, CipherTrust Transparent Encryption cannot make a backup of the database. Both scheduled and manual backup fail. The problem was the user's policy. A policy used in this scenario must follow a few rules.

With a CBC_CS1 key, a guarded file is modified to have a 4096 byte header holding key information. When an **Apply Key** effect is specified, the CipherTrust Transparent Encryption code adjusts the length and file offset for this header. Without an **Apply Key** effect, the size and access of the offset include the CBC_CS1 header.

Thales recommends that you modify the first rule of your policy. Remove the action entry for `f_rd_att` from the first rule and add a new rule before it:

```
**action**: f_rd_att

**effect**: Permit, Apply Key
```

Policy processing starts with the first rule and continues until a matching rule is found. The effect for the matching rule is then applied.

For the `f_rd_att` action, this results in the secfs code including the CBC_CS1 key header and adjusts the file size value. Without the Apply Key effect, the file size includes the CBC_CS1 header size and the file appears as 4096 bytes larger than its real size.

check_host Utility

If a CTE software installation fails during the certificate generation and exchange stage, use the `check_host` utility to list the network addresses for the host. The utility checks network interfaces, `/etc/hosts`, DNS, and so on, to compare, test, and evaluate possible addresses for the host, and weights them based upon their network efficiency. FQDNs are the most preferred and stand-alone IP addresses are the least preferred. Some applications, such as silent-mode installation, use `check_host` to determine the best host address to submit to the CipherTrust Manager during registration.

Run the `check_host` utility on a system that is hosting CTE to display available network host names, FQDNs, and IP numbers for the host.

Type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/check_host
```

check_host Syntax

```
check_host [[-h | -i | -a ] [-s name]] |
-l name:port[,name:port] | -r name
```

Syntax	Description
-h	Print the best host name for this machine
-i	Print the best IP address
-a	Print all the host names and IP addresses
-s	The name of the server (optional hint)
-r	The name of the server for name resolution checks
-l	The name and port of the server for listening checks

Displaying Information for Nested File Systems with the DF tool

When a file system mounts on top of another file system, the command `df -a` does not display the attributes for the covered file system.

On Linux environments, this is the expected behavior for any file system that is overlayed by another file system.

The secfs driver properly handles the call, which is made by the `statfs` system call, which is issued by the `df` tool. When the system call returns, its structures are correctly populated with the details of the nested file system. On examining the source of the `df` tool, it is found that when the `-a` switch is on, it nullifies the stats which are received for overlayed mounts. When the `-a` option is not enforced, the stats are maintained.

Issue the `df` command for a specific mount point, for example `df /xfs/nested-xfs` (where `/xfs` is a secfs GuardPoint). It works correctly.

fsfreeze and xfs_freeze

Users can freeze, snapshot, and unfreeze a file system with an SecFS GuardPoint using `fsfreeze|xfs_freeze` for both XFS and EXT3/4.

SecFS supports freezing with `fsfreeze|xfs_freeze` or by any other program issuing the same type of requests. Freezing SecFS results in freezing the underlying file system, as well as the primary file system.

Restrictions

There are restrictions for using `fsfreeze|xfs_freeze` support with CTE.

Platform Restrictions

The following platform restrictions occur with CTE and `fsfreeze|xfs_freeze`:

- CTE supports the `fsfreeze|xfs_freeze` utility for freezing SECFS GuardPoints on all Linux distributions for kernels ≥ 3.0 for Redhat, SLES, and Ubuntu platforms on EXT3/EXT4/XFS file systems. (Earlier Kernels

do not contain the proper freeze_super VFS code).

Target Restrictions

The expected target of the `fsfreeze|xfs_freeze` command is the path of the GuardPoint.

For example, if `/dev/sdb` is mounted as ext4 on `/data` and CTE contains the GuardPoint: `/data/protected`, then the target of `fsfreeze` must be `/data/protected`, not `/data`.

Valid:

```
fsfreeze -f /data/protected
```

Not valid:

```
fsfreeze -f /data
```

File System Restrictions

The following file system restrictions occur with CTE and `fsfreeze|xfs_freeze`:

- If multiple GuardPoints exist on the same file system, you only need to freeze one.

For example, if `/dev/sdb` is mounted as ext4 on `/data` and the CTE GuardPoints are `/data/protected1` and `/data/protected2`, then issuing:

```
fsfreeze -f /data/protected1
```

freezes `/data/protected1`, `/data/protected2` and the underlying ext4 file system.

Caution

Do not unguard a GuardPoint, or restart the CTE Agent, while the file system is frozen. The only action permitted on a frozen file system is taking a snapshot or backing up.

- If you try to freeze `/data/protected2` after freezing `/data/protected1`, it returns as busy
- If you are not permitted to freeze one GuardPoint, then you cannot freeze any GuardPoints

LDT Restrictions

- You cannot freeze a file system while it is undergoing an LDT rekey operation. If it detects a rekey, the freeze returns as busy
- You cannot start an LDT rekey on a frozen file system

Offline Data Transformation Restrictions

Do **NOT** use `fsfreeze` | `xfs_freeze` while an offline transform policy is in effect.

Protecting Files with Client Settings

When any file is now marked as protected (`|protect|`) in the client settings, that file is protected from being modified or deleted, (even from a root process).

Note

The file is not guarded and it can be external to a GuardPoint.

Previously, the only files that were protected were the following:

```
/etc/passwd
/etc/group
/etc/security/passwd
/etc/ssh/sshd_config
/etc/ssh/sshrd
/opt/testfile
```

If the file marked as `|protect|` does not exist, then CipherTrust Transparent Encryption creates a 0-length file in its place. This provides an efficient means to identify and implement file protection. When the agent is stopped or uninstalled, these 0-length files are deleted and then re-created if the agent is restarted. Additionally, an audit record is generated when a file operation is denied.

The `|protect|` status is displayed using `secfsd -status auth`.

Restricting Access Overrides with Client Settings

CipherTrust Transparent Encryption host/client settings are the means by which an administrator configures user authorization. Users with root privileges, on Linux or AIX systems, have the unfettered ability to override all file access and execution permissions imposed by the system.

CipherTrust Transparent Encryption access control allows you to restrict privileges of users, groups, application processes and binaries, including root users and setuid programs. By default, CipherTrust Transparent Encryption agent **DOES NOT** trust any process as authenticated. Any attempt to access a resource, by any process, will therefore be flagged with a "User Not Authenticated" notification. The CipherTrust Transparent Encryption agent must be instructed to trust the authenticator process progeny. For example, `/usr/sbin/sshd` is a process that can be trusted to authenticate the user to the system and to CipherTrust Transparent Encryption.

In some setups, when editing a host, system administrators can use the **host settings > |authenticator|** feature with **su** to change identities and gain access to restricted data. You can instruct CipherTrust Transparent Encryption to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CipherTrust Transparent Encryption can block from authenticating other processes.

Any executable path that is marked with a `|path_no_trust|` host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

CipherTrust Transparent Encryption prevents overrides from other host settings authenticators, using the `|path_no_trust|` status. If a user runs the `su` command from a non-trusted shell, that new shell is still marked as `|path_no_trust|`, even if `|authenticator|/usr/bin/su` is specified in the host-settings. The `|path_no_trust|` feature overrides any and all authenticators under host settings.

Note

Using `|trust|*` before a `|path_no_trust|` host setting no longer disables the `|path_no_trust|` host setting.

For example, the following host setting denies authentication for users accessing through `sshd`:

```
|trust|*
|path_no_trust|/usr/sbin/sshd
```

To restrict access overrides:

1. In the CipherTrust Manager products page, click **Transparent Encryption > Clients**.
2. Click on an existing Client name to edit the host.
3. Click **Client Settings** tab.
4. Add the following to the settings:

```
|path_no_trust|<path of the binary>
```

Example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the `kshell` executable will be authenticated.

5. Click **Apply**.

register_host Utility

Use the `register_host` utility to create certificate requests, exchange certificates between the CipherTrust Manager and the host, and to register CTE on the CipherTrust Manager. After the host is registered, you can configure CTE, apply GuardPoints, or perform database backups. Run the `register_host` utility in text mode on a terminal window.

Caution

The default host registration timeout is 10 minutes. If the host is unable to reach the CipherTrust Manager within the allotted period because of an extremely slow network connection, set the **REGISTER_HOST_TIMEOUT** environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

secfsd Utility

The **secfsd** utility displays the following attributes of CTE:

- GuardPoints defined in the **GuardPoints*
- Authentication parameters defined in the *Host Settings* tab
- Lock status set by enabling **FS Agent Locked** and **System Locked**
- Web destination and SSL certificate for uploading log entries
- Policies applied in the **GuardPoints** tab
- Status of required processes (**secfsd** and **vmd**)
- Version of **secfs**

The **secfsd** utility is also used to mount GuardPoints for **Directory (Manual Guard)**. Normally, CTE automatically mounts the **secfs** file system when you apply a GuardPoint to a directory. On Linux, the **secfsd** utility is located in `<install_dir>/secfs/.sec/bin` and a symbolic link to this file is placed in `/usr/bin/secfsd`.

secfsd syntax

Command	Description
<code>-help</code>	display secfsd options

Status Options

Command	Description
<code>-status guard [-v -tree]</code>	list all GuardPoints
<code>-status keys</code>	show current encryption key state
<code>-status auth</code>	list authentication settings
<code>-status lockstat</code>	show CTE lock status
<code>-status logger</code>	list logging details

Command	Description
<code>-status policy</code>	list configured policies
<code>-status pslist</code>	list protected processes
<code>-status devmap</code>	list guarded devices

Manual GuardPoint options

Command	Description
<code>-guard path [container ID]</code>	manually guard path
<code>-unguard path [container ID]</code>	manually unguard path

Version option

Command	Description
<code>-version</code>	list version of kernel module <code>secfs2</code>

** Encryption Mode option information**

Command	Description
<code>crypto</code>	Displays the encryption modes that are supported.

** Configuration Mode option information**

Command	Description
<code>config <config_param> <value></code>	Displays the encryption modes that are supported.

secfsd Examples

Display GuardPoint Information

To display the GuardPoint paths, applied policies, policy type, and guard status, use the `secfsd -status guard` command. For example:

```
secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/opt/apl/lib	allow AllOps_fs	local	guarded	guarded	N/A
/dev/sdb	watchaccess_rd	rawdevice	guarded	guarded	N/A
/dev/sdc	watchaccess_rd	manualrawdevice	guarded	guarded	N/A
/dev/sdd	watchaccess_rd	manualrawdevice	unguarded	not guarded	Inactiv
e					
/opt/apl/tmp	MSSQL00123	manual	unguarded	not guarded	Inactiv
e					

Column	Description
GuardPoint	Full path of the GuardPoint.
Policy	Name of the policy applied to the GuardPoint.
Type	Can be local, automount, manual, raw device, or manual raw device. Configured in the GuardPoints tab.
ConfigState	Guard status of the GuardPoint, as recognized by the key manager. It can be guarded or unguarded.
Status	Current guard status, as recognized by CTE. State can vary.
Reason	Additional information about the status, if any.

Note

- Config State and Status can vary. As an example, if you apply a GuardPoint and someone is currently working in the GuardPoint, the policy cannot be applied at that time. In this case, the ConfigState is guarded and the Status is not guarded.
- When the user removes an auto-mounted GuardPoint from CipherTrust Manager, the CTE Agent is only deleted after the configured `autoFs` timeout expires. This timeout does not start until the GuardPoint is free.
The timeout can be changed in the `auto.master` file on the host.

Display GuardPoint Information in a Different Format

To display the same information in a block format, use the `secfsd -status guard -v` command. For example:

```
secfsd -status guard -v

GuardPoint: 1
  Policy:      allowAllOps_fs
  Directory:   /opt/apps/apps1/tmp
  Type:        local
  ConfigState: guarded
  Status:      guarded
  Reason:      N/A
GuardPoint: 2
  Policy:      allowAllRootUsers_fs
  Directory:   /opt/apps/apps1/lib
  Type:        local
  ConfigState: guarded
  Status:      guarded
  Reason:      N/A
```

Display Host Settings

To display the SHA2 hash signature for each protected host setting, use the `secfsd -status auth`

command. For example:

```
secfsd -status auth

|authenticator|/bin/su 3E765375897E04C39AB17D4C755F50A35195535B6747DBA28DF9BD4AA6
72DFF9
|authenticator|/usr/sbin/sshd 98FC599D459EDEA52A60AB394B394803B5DAB96B53148DC6087
32DDA6777FA1A
|authenticator|/usr/sbin/in.rlogind 5C9A0EDD8BF54AE513F039476D21B3032507CF957AA0C
B28C368EB8AB6E684FB
|authenticator|/bin/login 0D2EE0B995A30AE382B4B1CA5104715FC8902F457D283BDABAAD857
B09259956
|authenticator|/usr/bin/gdm-binary 363780522E3CCF9ABF559F059E437743F9F97BBBB0EE85
769007A464AD696BD1
|authenticator|/usr/bin/kdm BAD41BBCDD2787C7A33B5144F12ACF7ABC8AAA15DA9FDC09ECF93
53BFCE614B5
```

Display Key Status

To display the status of CTE keys, use the `secfsd -status keys` command. For example:

```
secfsd -status keys
Encryption keys are available
```

Display Lock Status

To display the status of CTE locks, use the `secfsd -status lockstat` command. For example:

```
secfsd -status lockstat
FS Agent Lock: false
System Lock: false
```

The value is **true** if the lock is applied. The value is **false** if the lock is not applied. **System Lock** corresponds to **System Locked** in the *Host* window. **FS Agent Lock** corresponds to **FS Agent Locked** in the *Host* window.

Note

Before you upgrade, remove CTE software, or change operating system files, the status of FS Agent Lock and System Lock must be false.

Agent Security Configuration Protection

The Agent lock directory, `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec` contains secfs secret files, configuration files, host setting signatures, etc. Thales recommends protecting the directory whenever secfs is online.

Applying improved directory protection ensures that only CTE applications (`vmd`, `secfsd`, `voradmin`, etc.) can modify the `.sec` directory and the files in it. All users, including root, are denied read/write access to the files. They also do not have permissions to modify `conf` and `bin` directories, using other tools.

A new command has been created to protect the directory: `voradmin secfs config`

Syntax

```
voradmin secfs config <configuration_parameter> <value>
```

Example

```
voradmin secfs config pagecache_writeback 1
```

Previously, you would have had to use the following command to achieve the same results as the example above:

```
echo 1 > /opt/vormetric/DataSecurityExpert/agent/secfs/.sec/conf/pagecache_writeback
```

Note

When CTE is upgraded to v7.2.0 from the previous release, it may display 'Permission Denied' warnings which display when files are removed from subdirectories of the `.sec` directory. You can ignore these warnings. They are harmless.

Display CTE Log Status

To display the status of CTE log service, use the `secfsd -status logger` command. For example:

```
secfsd -status logger
```

Upload URL: `https://vmSSA06:8444/upload/logupload,https://vmSSA07:8444/upload/logupload, \`
`https://vmSSA05:8444/upload/logupload` Logger Certificate directory: `/opt/vormetric/DataSecurityExpert/agent/vmd/pem`

This command sequence returns the URL to which the log service sends log data. It also returns the directory that contains the CTE certificate. CTE uses the certificate to authenticate CTE when it uploads the log data to the CipherTrust Manager.

Display Applied Policies

To display the policies that are applied to CTE, use the `secfsd -status policy` command. For example:

```
secfsd -status policy
```

```
Policy: enc-audit  
Type: ONLINE
```

Display CTE Process Information

To display CTE processes, use the `secfsd -status pslist` command. This command shows the process number associated with each CTE process. To show the details about a specific CTE process, use the `ps -fp <process #>` command, where `<process #>` is the process number from the `secfsd -status pslist` command.

For example:

```
secfsd -status pslist
Protected pid list:      739    731

ps -fp 739
  UID      PID    PPID    C   STIME          TTY   TIME    CMD
  root      739     1      0   11:04:56      -    0:00 /opt/vormetric/ \
        DataSecurityExpert/agent/vmd/bin/vmd
```

Display CTE Version Information

To display CTE version information, use the `secfsd -version` command. For example:

```
secfsd -version
version: <Release.build-number>
```

Display CTE Crypto Information

To display CTE support information for encryption modes, use the `voradmin secfs crypto` command. For example:

```
voradmin secfs crypto
AES CBC, CBC_CS1, XTS modes are supported
Encryption key protection is supported
```

Manually Enable a GuardPoint in CipherTrust Manager

To manually enable a GuardPoint on an AIX host:

1. Click **CTE > Clients > <clientName> GuardPoints**
2. Click **Create GuardPoint**.
3. In the Policy field, select a policy.
4. Set Type to **Manual Directory**.
5. Click **Browse** and enter the GuardPoint path.
6. Click **Create**.
7. Log onto the system hosting CTE as the root user.

8. To manually enable the GuardPoint, use the `secfsd -guard <path>` command. For example:

```
secfsd -guard /opt/apps/etcsecfsd: Path is Guarded
```

9. To verify the change, use the `secfsd -status guard` command. For example:

```
secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/opt/apps/etc	allowAllOps_fs	manual	guarded	guarded	N/A

Secfsd Raw and Block Devices

CTE only creates block devices. To display them, use the `ls -l /dev/secvm/dev` command. For example:

```
ls -l /dev/secvm/dev
```

```
brw----- 1 root    system    38,  1 Jan 29 16:37 hdisk1
brw----- 1 root    system    38,  2 Jan 29 16:37 hdisk2
crw----- 1 root    system    38,  3 Jan 29 16:37 rhdisk1
crw----- 1 root    system    38,  4 Jan 29 16:37 rhdisk2
```

Note

- Access controls on SECVm devices are supported with **only** Direct IO.
- CipherTrust Transparent Encryption **does not** support access controls on SECVm devices when using buffered I/O.
- Buffered I/O on SECVm devices are only supported with a wide-open (applyKey/permit) policy.

Using Advanced Encryption Set New Instructions (AES-NI)

To verify AES-NI hardware support, type:

```
vmsec check_hwenc
```

Unlike the `-c algo` command above, CTE does not have to be running for this command to execute. This command displays one of the following messages to stdout:

```
"AES-NI hardware encryption is supported on this system."
"AES-NI hardware encryption is not supported on this system. "
```

User Cache Lookup Improvements

CTE has added a feature to improve the performance of the user cache lookup function, which contains information such as username and group name(s), plus timestamps and other supporting flags. It is mainly used during LDAP authentication. This feature improves lookup performance by allowing user-configurable values for lookup retries and user information refresh times. Performance can be impacted if authentication/ user lookups and timeout/ retries take a significant amount of time. Previously, these values were hard-coded. Now they are user-configurable.

The configuration options for this feature contain three new configuration parameters:

Initial cache miss

Initial check of access when no user information cache entry exists.

- **Default value:** 60 seconds
- **Default minimum:** 2 seconds
- **Default maximum:** 3600 seconds (1 hour)

To set this value, type:

```
voradmin secfs config usrinf_miss_timeout <seconds>
```

Cache expiration timeout

Used when user information cache entry has not been used for the duration needed to trigger a refresh.

- **Default value:** 300 seconds (5 minutes)
- **Default minimum:** 60 seconds
- **Default maximum:** 86400 seconds (1 day)

To set this value, type:

```
voradmin secfs config usrinf_expiry_timeout <seconds>
```

Cache stale timeout

When a cache entry has not been updated for the duration of the timeout, the entry will be considered inactive and removed.

- **Default value:** 300 seconds (5 minutes)
- **Default minimum:** 60 seconds
- **Default maximum:** 86400 seconds (1 day)

To set this value, type:

```
voradmin secfs config usrinf_stale_timeout <seconds>
```

Usage

CTE uses the default values initially. If network errors occur and LDAP failure is observed (in system logs, look for timeout errors), then you have two options:

- If the network errors can be corrected in a short time, then the timeout values can remain unchanged.
- If not, set the expiration and stale timeout to large values. Then, reduce the initial timeout incrementally until the problem resolves.

Note

CTE must be restarted when a new timeout value is set, in order for the value to take effect.

Keep the new value until the problem is resolved. Then, once the network problems have been fixed, reset the timeout values back to the initial values.

vmutil

Usage

```
vmutil <options> <operations>
```

Options

Option	Function	Description
-a	--agent <name>	Specify agent type (vmd or pkcs11)
-d	--extdir <string>	Specify location of external certificate and key set
-e	--error <string>	Specify one or more errors for state report
-h	--help	Display help and exit
-l	--loglevel <level>	Specify log output level (debug, info, warn, error or fatal)
-f	--force enabled	Force option for delete host operation
-v	--version	Display program version and exit

Operations

Operation	Description
certexpiry	Report the certificate expiration date for this agent
deletehost	Delete this client from the server
renewcerts	Renew certificate set for this agent
reportstate	Report agent state and error conditions to server
unregister	Unregister this agent/client from the server
updatecerts	Update external certificate and key set for this agent/client

vmd utility

The **vmd** utility displays CTE software version information.

The **vmd** utility is located in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin` and a symbolic link to this file is placed in `/usr/bin/vmd`.

Syntax

vmd [OPTIONS...]

-h show utility syntax

-v display CTE version

-f runs **vmd** in the foreground

Display the Installed Version

To display the installed CTE version, type:

```
vmd -v
Version 6
<Release.build-number>
2022-02-04
Copyright (c) 2009-2025, Thales.. All rights reserved.
```

vmsec Utility

The **vmsec** utility allows you to manage security aspects of CTE on the host. On Linux hosts, the **vmsec** utility is located in:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/vmsec
```

vmsec Syntax

Syntax	Description
<code>checkinstall</code>	Show vmd kernel status
<code>challenge</code>	Enter the dynamic host password
<code>vmdconfig</code>	Display the vmd configuration
<code>check_hwenc</code>	Display kernel configuration
<code>hwok</code>	Report status of hardware signature
<code>passwd [-p <password>]</code>	Enter the static host password
<code>version</code>	Display CTE version

vmsec Examples

- Display CTE Challenge String
- Display CTE Status
- Entering a Password
- Display Kernel Status
- Display CTE Build Information
- Display Contents of Conf files

Display CTE Challenge String

To display a CTE password challenge string and enter the response string when the CipherTrust Manager is not network accessible, use the `vmsec challenge` command. This command displays a challenge string that you can send to your key manager administrator, who will then send you back the correct response information.

For example:

```
vmsec challenge
Contact a Security Server administrator for a response.
Your host name is "Host120" Your challenge is: HPTQ-ZYLK
Response -> IHFY-W7WG-PDA0-QKKQ
```

Contact your key manager administrator and give them the challenge string. The administrator will give you the response string. Enter the response string in the **Response** field and press **Enter**. You have 15 minutes to enter the response string.

Tip

If you are using CipherTrust Manager, the ability to change the contact string will be added in a future release. For CipherTrust Manager, the contact string says "Contact your CM administrator".

Display CTE Status

This utility shows you if CTE is configured and running. If it is not running, you might need to start it manually. To display CTE status, use the `vmsec checkinstall` command. For example:

```
vmsec checkinstall
The kernel component is installed and running.
```

Entering a Password

To enter the CTE static host password, use the `vmsec passwd` command. For example:

```
vmsec passwd
Please enter password:
OK passwd
```

To enter CTE static host password on the command line so you can specify it in a batch script, specify the password using the `-p` option. For example:

```
vmsec passwd -p myPass123
OK passwd
```

Display Kernel Status

To display the kernel status, use the `vmsec status` command. For example:

```
vmsec status
FILE_FORMAT=2
FILE_GENERATED=08/27/2019 18:54:10
SA_QOS_STATUS=0
SA_HOST_CPU_UTIL=0
GP_1_Policy=27
GP_1_Dir=/gp
GP_1_lock=1
GP_1_type=1
GP_1_gtype=manual
GP_1_opt=gtype=2,policy=27,lock=1,type=1,dir=/gp/
GP_1_config_state=unguarded
GP_1_status=not guarded
GP_1_statuschk_tm=0-00-00 00:00:00
GP_1_config_op_retry_cnt=0
```

```

GP_1_config_op_attempt_tm=0-00-00 00:00:00
GP_1_flags=0
GP_1_reason=Inactive
GP_1_usage=free
TOTAL_GP=1
KEYS_AVAILABLE=TRUE
sdk_version=<Release.build-number>
sdk_builddate=2019-08-19 15:16:46 (PDT)
coreguard_locked=false
system_locked=false
logger_upload_url=https://thl602-2114.qa.com:8447/upload/logupload,https://thl602-2116.qa.com:8447/upload/logupload
logger_cert_dir=/opt/vormetric/DataSecurityExpert/agent/vmd/pem
hostname_for_logging=vmd
QOS_PAUSED=false
vmd_STRONG_ENTROPY=false
vmd_URL=https://thl602-2114.qa.com:8446
vmd_SRV_URLS=https://thl602-2114.qa.com:8446, https://thl602-2116.qa.com:8446
vmd_PRIMARY_URL=https://thl602-2114.qa.com:8446
vmd_SUPPORTS_F8P=TRUE
vmd_SUPPORTS_CR256=TRUE
vmd_RANDHP=TRUE
learn_mode=false
concise_logging=false
vmd_listening_port=7024
vmd_initialization_time=2019-07-25 12:07:14.514
vmd_last_server_update_time=2019-07-25 12:12:04.747 policy_name_27=aes256
policy_version_27=0
policy_keyvers_27=0
policy_type_27=ONLINE
policies=27
logger_suppression_VMD=SUPPRESS
logger_intervaltime_VMD=600
logger_repeat_max_VMD=5
logger_suppression_POL=SUPPRESS
logger_intervaltime_POL=600
logger_repeat_max_POL=5
CONFIG_SA_1=27
TOTAL_CONFIG_SA=1
SA_1_NAME=27
SA_1_ALIAS=aes256
SA_1_TYPE=0
SA_1_REF=1
SA_1_HIP_REG_TIME=0
SA_1_FLAGS=1
TOTAL_SA=1
TOTAL_AUTH=0
AUTHBIN_1=|authenticator|/usr/sbin/sshd B92A3D7EEF67B82230F7F76097D65159FCF5722A4
154A249EFDC22C20F1B572C
AUTHBIN_2=|authenticator|/bin/login 4F210D1B83ACD79B006BCF7DB247ED002A45FC892C427
20390BFA6AE21AEA8DC
TOTAL_AUTHBIN=2

```

Display CTE Build Information

To see the CTE build version, use the `vmsec version` command. For example:

```
vmsec version
Version 7
7.8.0.128
2025-03-17 15:15:23 (PDT)
Copyright (c) 2009-2025, Thales. All rights reserved.
```

Display Contents of Conf files

To display the contents of the `agent.conf` and `.agent.conf.defaults` files, use the `vmsec vmdconfig` command. For example:

```
vmsec vmdconfig
appender_syslogdest Syslog_Appender_0=127.0.0.1
VMSDK_AGENT_CONFIG_FILE=/opt/vormetric/DataSecurityExpert/agent/vmd/etc/agent.conf
appender_layout Syslog_Appender_0=Syslog_Layout
VMSDK_AGENT_VERSION=7.8.0.128
VMSDK_AGENT_BUILD_ID=28
PREV_URLS=https://srv.my.thales.com:8443
syslog_appender_myhost name=dev.my.thales.com
VMD_PORT=7024
...
...
appenders=Upload_Appender, File_Appender, Syslog_Appender_0
layouts=Upload_Layout, File_Layout, Syslog_Layout, Simple
CONNECT_TIMEOUT=180000
URL=https://srv.my.thales.com:8443
STRONG_ENTROPY=false
```

CipherTrust in-Place Data Transformation for Linux

This section contains the following topics:

- [Introduction to in-Place Data Transformation \(IDT\)](#)
- [Requirements for IDT-Capable GuardPoints](#)
- [The CTE Private Region and IDT Device Header](#)
- [IDT-Capable GuardPoint Encryption Keys](#)
- [Guarding an IDT-Capable Device on Linux](#)
- [Changing the Encryption Key on Linux IDT-Capable Devices](#)
- [Guarding an IDT-Capable Device with Multiple IO Paths on Linux](#)
- [Linux System and IDT-Capable GuardPoint Administration](#)
- [Resizing Guarded IDT Devices](#)

-
- Alerts and Errors on Linux

Introduction to in-Place Data Transformation (IDT)

CTE offers in-Place Data Transformation (IDT) Capable Device GuardPoints on Linux. IDT-Capable GuardPoints allow you to guard devices by transforming the plain-text data to cipher-text on the host device. The data transformation process is called in-Place Data Transformation (IDT). The term “IDT-Capable” refers to the data transformation capability available on IDT-Capable GuardPoints.

IDT is not the same as the legacy offline data transformation. IDT is a block level data transformation with built-in resiliency to recover from system crashes during the data transformation process. IDT uses the CTE Private Region to manage the entire transformation process (For details, see [The CTE Private Region and IDT Device Header](#)).

IDT partitions the data on a device in segments of 1 MB in size and transforms one or multiple segments, up to 60 segments, in parallel. The IDT process preserves existing data in a segment during transformation in the CTE Private Region, and then transforms the data in-place. IDT also maintains the segments undergoing transformation in the CTE Private Region. In the event of system crash, IDT will recover the segments undergoing transformation at the time of crash and then resume the transformation process.

Another advantage of IDT over legacy offline data transformation is that IDT does not require a separate policy for data transformation. Instead, IDT allows you to initialize each device as either a “new device” with no existing data or as an “existing device” with existing data that needs to be transformed. You can then apply any IDT policy to any combination of new and existing devices and IDT will immediately guard the new devices while starting the IDT transformation process on the existing devices. New devices are immediately available for use while existing devices are inaccessible until the IDT process completes and all data has been converted from plain-text to cipher-text.

Requirements for IDT-Capable GuardPoints

- IDT-Capable GuardPoints are available for Linux with CTE 6.3.1 or subsequent versions. All versions of CipherTrust Manager work with IDT-Capable GuardPoints.
- The host server must use the Advanced Encryption Standard instruction set (AES-NI).
- The policy assigned to the IDT-Capable GuardPoint must be an **in-Place Data Transformation** policy and use an XTS/CBC-CS1 AES 256 encryption key.
- In order to create an IDT-Capable GuardPoint on a raw device, the device must be either:
 - Exported from an external storage system to the host device.
 - On a locally-attached disk.
- Devices protected by an IDT-Capable GuardPoint cannot currently be initialized/added as physical volumes for use by LVM. When LVM support is added, it will be announced in the CTE Release Notes.
- Existing devices divided into one or more logical partitions cannot be guarded as IDT-Capable Device GuardPoints. Logical partitions in such devices cannot be accessed or separately guarded after guarding the device.

For example, the logical partition `/dev/sda1` or `/dev/sda2` inside `/dev/sda` cannot be accessed after

guarding `/dev/sda` as IDT-Capable GuardPoint. Using `/dev/secvm/dev/sda1` is invalid as `/dev/secvm/dev/sda1` is not a GuardPoint and cannot be guarded, and, as such, would not provide access to clear-text data on `/dev/sda1`. However, you can guard individual partitions, such as `/dev/sda1` or `/dev/sda2`, as IDT-Capable GuardPoints without guarding the entire `/dev/sda` device.

- IDT-Capable GuardPoints requires XTS-AES mode of the AES algorithm for encryption.
- CTE only supports IDT on servers with microprocessors integrated with Advanced Encryption Standard instruction set (AES-NI).

The CTE Private Region and IDT Device Header

IDT-Capable GuardPoints require a small amount of disk space in the standard CTE Private Region. The reserved space is where CTE stores metadata information to identify IDT-Capable GuardPoints and to perform all data transformation and rekey operations in a resilient manner to avoid data loss or integrity issues due to system failures. The IDT-specific reserved space within the CTE Private Region is known as the IDT Device Header. By default, when you initialize a device as an IDT-Capable GuardPoint, CTE reserves 63 MB of space starting at the first sector on the device for the CTE Private Region.

CTE writes the IDT Device Header into the CTE Private Region when the device is guarded for the first time. If there is existing data on the device, the data at the start of the device is relocated to the available free space on the device and CTE creates the CTE Private Region starting at the first sector. For details, see [Initialize a Linux Device with Existing Data](#).

CTE Private Region Location

Normally, CTE requires that the CTE Private Region be embedded at the beginning of the device. IDT, however, allows you to specify that the CTE Private Region for an IDT-Capable GuardPoint should be located in a central CTE metadata directory on the host called `/vte/vte-metadata-dir` (default: `/opt/vte/vte-metadata-dir`). If you use this option, CTE stores the CTE Private Region and IDT Device Header for the device in this directory. The location of the CTE Private Region for a device is determined when you first initialize the device as an IDT-Capable GuardPoint. For details, see [Initializing an IDT-Capable Device](#).

Warning

Access to the CTE metadata directory is local to the CTE protected host. Devices whose access is shared across multiple CTE protected hosts in a cluster *must* be configured with the CTE Private Region embedded in those devices. Using a centralized metadata directory for shared devices will lead data corruption.

The location of the CTE Private Region does not affect CTE's functionality, but there are some considerations if you choose to use the centralized metadata directory `/vte/vte-metadata-dir`:

- Thales recommends that you keep the metadata for the device on the device if at all possible. You should only use the centralized metadata directory if the device cannot be expanded to accommodate the CTE Private Region.
- The centralized CTE metadata directory must be guarded by the Administrator to prevent accidental

modification or deletion of the CTE metadata. If the CTE metadata directory is not guarded, any attempt to configure or enable an IDT-Capable GuardPoint using the centralized metadata directory will be rejected. The policy associated with the metadata directory must:

- Deny all users (including the root user) the ability to modify or remove any files in the metadata directory.
- Use the key rule `clear_key` so that the metadata is stored in clear text.
- You must back up this directory whenever you back up a device that uses the directory. You will not be able to restore a protected device without access to its corresponding metadata in `/vte/vte-metadata-dir`.
- Devices with existing data do not need to be resized to accommodate the CTE Private Region, so there are no disk size discrepancies between system utilities such as `fdisk` and any other applications. However, Thales still recommends that you do not shrink an IDT-Capable GuardPoint even if the CTE Private Region is not embedded on the device.

Device Size

If you embed the CTE Private Region on the device itself, after configuring and guarding the IDT-Capable GuardPoint on the device, the device size reported to applications is the size of the device minus the space reserved for the CTE Private Region. This can lead to a discrepancy between the disk size reported by some applications versus the size reported by system utilities such as `fdisk`.

Warning

Do not shrink IDT-Capable GuardPoints. Due to the relocation of user data from the CTE Private Region, if you shrink the device, you may corrupt data on the device.

The IDT Device Header contains both the available device size and the size of the CTE Private Region. To view the IDT Device Header, use the `voradmin idt status <device-name>` command. The **Exported Disk Size** field shows the disk size available for use by other applications. The **Private Region Size** field shows the disk size reserved for CTE. For example:

```
voradmin idt status /dev/sdc2
IDT Header on /dev/secvm/dev/sdc2
Version:                1
Change:                 0
Private Region Size:    129024 sectors
Exported Device Size:   9627648 sectors
Key UUID:               9cc3c8e4-7ea7-310f-85c7-6f911de1ab52
Mount Path:             None
```

The `voradmin idt status` command also reports the UUID of the XTS/CBC-CS1 AES 256 key applied to the device.

IDT-Capable GuardPoint Encryption Keys

IDT-Capable GuardPoints must be encrypted using XTS/CBC-CS1 AES 256 keys. An XTS/CBC-CS1 AES 256

type key is a 512-bit key composed of two components:

- The first 256 bits of the key is the AES 256 encryption key component.
- The second 256 bits is the tweak component.
- Create XTS keys on CM in the Keys menu.
- For CM, refer to [“Creating a New Key”](#) for more information.

The Key Manager (CipherTrust Manager) generates a UUID, along with other relevant attributes, for each newly-added key. It then provides the key and its attributes to the CTE protected host when the policy containing the key is pushed to the host device. CTE stores the key and its attributes, including the key's UUID, in the IDT Device Header. The first time a device is guarded as an IDT-Capable GuardPoint, CTE writes the IDT Header on the device before data transformation takes place, if data transformation is required.

Key Attributes - Example

The following describes the parameters you should specify to add a new XTS/CBC-CS1 AES 256 key named `IDT_DEMO_KEY_1`. Note the algorithm and encryption mode specified for the key.

- Algorithm: **AES**
- Size: **256**
- Encryption Mode: **XTS/CBC-CS1**

Note the UUID of the key. This UUID is stored in the IDT Device Header on all devices encrypted with this key, allowing you to verify which key is being used on each device.

Policy Requirements for IDT-Capable GuardPoints

IDT-Capable GuardPoints require a policy of type **in-Place Data Transformation** with a single key rule specifying the key names for **Current Key** and **New Key**. The **Current Key** name is `clear_key` or an XTS/CBC-CS1 AES 256 key name, depending on whether the data on the device has already been encrypted.

- If there is no existing data on the device or if the existing data on the device has not yet been encrypted, specify `clear_key` for **Current Key**. In the **New Key** field, specify the name of the XTS/CBC-CS1 AES 256 key that you want to use to encrypt the data on the device.
- If the existing data on the device has already been encrypted, specify the name of the key used to encrypt the data in the **Current Key** field and the name of the new XTS/CBC-CS1 AES 256 key you want to use to rekey the data in the **New Key** field. When the policy is pushed to the host, CTE will rekey the data on the device using the key specified in **New Key**. In other words, the **New Key** field specifies the XTS/CBC-CS1 AES 256 production key name to apply to the device.

In all cases, the **New Key** field specifies the XTS/CBC-CS1 AES 256 production key name that you want to use to encrypt the data on the device. After you guard an existing device with an in-Place Data Transformation policy, CTE transforms the existing data using the New Key. When the process is finished, the New Key becomes the Current Key for that device, and all data will be encrypted or decrypted with that key. The IDT Device Header contains the UUID of the key currently being used to encrypt/decrypt data on the device. To view the current key UUID, use the `voradmin idt status <device-name>` command.

You may add security rules to restrict certain user/process access to protected devices. For suggestions, see [Use Cases Involving IDT-Capable GuardPoints.md](#){:target="_blank"}.

A simple IDT policy requires:

- **Policy type:** in-Place Data Transformation
- **Rule:** Simple security rule that permits access to all users and programs
- **Current key:** `clear_key`
- **New key:** an IDT_KEY for encrypting the data on any device associated with the policy

Guarding an IDT-Capable Device on Linux

In order to guard an IDT-Capable device, you need to:

1. Make sure the devices you intend to guard meet the requirements for IDT-Capable GuardPoints. For details, see [Requirements for IDT-Capable GuardPoints](#).
2. Install the CTE Agent and register the host with the Key Manager if it is not already registered. IDT does not require any special registration options or licenses.
3. Initialize the device using the `voradmin idt config [new|xform]` command to specify whether there is any existing data on this device that needs to be encrypted and to configure the location of the CTE Private Region. For details, see [Initializing an IDT-Capable Device](#).
4. Log on to the Key Manager to apply an IDT-Capable GuardPoint to the device. For details, see [Guard the Linux Device with an IDT-Capable GuardPoint](#).

Warning

For devices with shared access across multiple CTE Protected hosts in a cluster, you must designate one and only one of the nodes in the cluster as the node on which you plan to initialize and guard the device for the first time. The designated node must be the only one that accesses the device until the entire initial data transformation process has completed. This requires guarding each shared device at the designated host level rather than at the host group level if you are using a host group to manage the CTE Protected nodes in your cluster. DO NOT initialize or guard any device on multiple nodes in the cluster simultaneously, because multiple nodes attempting to transform the same data can corrupt the data on the entire device.

Initializing an IDT-Capable Device

When you initialize an IDT-Capable storage device, the process specifies:

- Whether there is existing data on the device that needs to be encrypted.
- Where you want to store the CTE Private Region, which contains the IDT Device Header along with metadata

that identifies the IDT-Capable device as a guarded device. You can embed the CTE Private Region on the device itself or in the central CTE metadata directory on the host. (For details, see [The CTE Private Region and IDT Device Header](#).)

How you initialize the device depends on whether it is a new device or an existing device that already has data that needs to be transformed into cipher-text. For details, see:

- [Initialize a New Linux Device](#)
- [Initialize a Linux Device with Existing Data](#)

Initialize a New Linux Device

Run the `voradmin idt config new` command to initialize a new device. The `new` option specifies that the device does not hold user data so no initial data transformation is required. For a shared device that is accessed from multiple protected hosts, you must initialize the device only once and on only one protected host.

Note

To configure devices with multiple IO paths for Linux, see [Changing the Encryption Key on Linux IDT-Capable Devices](#).

1. Log into the device as `root`.
2. Run the `voradmin idt config [-external] new [-c <n>] <device-name>` command, where:
 - `-external` is an optional parameter that tells CTE you want to use the centralized CTE metadata directory instead of embedding the CTE Private Region on the device itself. If you use this option, you must have configured and guarded the centralized CTE metadata directory as described in [CTE Private Region Location](#).
 - `new` (required) indicates that the device contains no data (it is a new disk). As soon as you push the IDT policy, the device will be available as a guarded IDT-Capable GuardPoint.
 - `-c <n>` (optional). If you use this option, CTE sets the number of data transformation jobs to run in parallel to the number specified in `<n>`. `<n>` can be an integer between 1 and 60 (default: 8).

Each data transformation job transforms 1MB worth of data and requires CPU resources in addition to three I/O operations as part of data transformation. Each job reads 1MB of data from the device, preserves the data in the CTE Private Region, rekeys the data to cipher-text, and writes the transformed data to the device. If you increase the number of parallel jobs, the data transformation process will complete faster but there will be an increased performance impact on the system. Only increase the `-c` option if you are certain that the system resources are available to handle the additional load.

The value for the `-c` option you specify here remains in effect for all subsequent data transformations (such as any data rekeys) until you specify a new value.

- `<device-name>` (required). Specifies the device name. For example, `/dev/sdc2`.

For example, if you want to initialize a new Linux disk named `/dev/sdc2` using 10 parallel data transformation jobs with the CTE Private Region embedded on the device, you would specify:

```
voradmin idt config new -c 10 /dev/sdc2
```

If you want to initialize a new Linux disk named `/dev/sdc2` using the default number of parallel data transformations but with the CTE Private Region in the centralized CTE metadata directory, you would specify:

```
voradmin idt config -external new /dev/sdc2
```

3. To verify that the disk has been initialized, run the `voradmin idt status` command.

```
voradmin idt status /dev/sdc2
Device /dev/sdc2 is configured to guard as IDT-Capable GuardPoint
```

4. At this point the Administrator can protect the device as an IDT-Capable GuardPoint through the Key Manager. For details, see [Guard the Linux Device with an IDT-Capable GuardPoint](#).

Note

The initialization process prepares the device to be guarded but does not actually guard it. You need to assign an IDT-Capable GuardPoint to the device in the Key Manager before the device is actually protected.

Initialize a Linux Device with Existing Data

If the device has existing data, you need to use the `voradmin idt config xform` command to initialize the disk for CTE. Unless you are using the centralized CTE metadata directory, this command examines the current disk size and computes the size required to hold the existing data plus the CTE Private Region at the beginning of the device. After the CTE initialization is complete, you then need to resize the device before you can guard it with an IDT-Capable GuardPoint.

Warning

If access to the device is shared access across multiple CTE Protected hosts in a cluster, be sure to initialize the device on one and only one of the CTE hosts.

The following procedure describes how to initialize the device for CTE. Note that the existing data is not altered in any way until after you perform this procedure and you guard the data with an IDT-Capable GuardPoint. CTE does *not* begin transforming the data from clear-text to cipher-text until the IDT-Capable GuardPoint has been

applied and the encryption key has been pushed to the device through the GuardPoint Policy.

1. Log into the device as `root`.
2. Run the `voradmin idt config [-external] xform [-c <n>] <device-name>` command, where:
 - `-external` is an optional parameter that tells CTE you want to use the centralized CTE metadata directory instead of embedding the CTE Private Region on the device itself. If you use this option, you will not have to resize the device but you must have configured and guarded the centralized CTE metadata directory as described in [CTE Private Region Location](#).
 - `xform` (required) indicates that the device contains existing data. CTE will transform all existing data on the device from clear-text to cipher-text as soon as you guard the device. The device will be inaccessible until the transformation is complete, and the device must remain offline during the entire transformation process. No user access will be permitted until all data has been transformed.
 - `-c <n>` (optional). If you use this option on Linux, CTE sets the number of data transformation jobs to run in parallel to the number specified in `<n>`. `<n>` can be an integer between 1 and 60 (default: 8).

Each data transformation job transforms 1MB worth of data and requires CPU resources in addition to three I/O operations as part of data transformation. Each job reads 1MB of data from the device, preserves the data in the CTE Private Region, rekeys the data to cipher-text, and writes the transformed data to the device. If you increase the number of parallel jobs, the data transformation process will complete faster but there will be an increased performance impact on the system. Only increase the `-c` option if you are certain that the system resources are available to handle the additional load.

The value for the `-c` option you specify here remains in effect for all subsequent data transformations (such as any data rekeys) until you specify a new value.

- `<device-name>` (required). Specifies the device name. For example, `/dev/sdc3`.

For example, if you want to initialize an existing Linux disk named `/dev/sdc3` using 10 parallel data transformation jobs with the CTE Private Region embedded on the device, you would specify:

```
voradmin idt config xform -c 10 /dev/sdc3
Device /dev/sdc3 must be resized to at least 9893888 sectors (4831 MBs) before
guarding as IDT-Capable GuardPoint
```

In this case you must manually resize the Linux disk by at least 9893888 sectors before you can guard it. After you guard the disk, you can expand it again later but you cannot shrink it unless you remove the GuardPoint.

If you want to initialize the same device using the centralized CTE metadata directory, you would specify:

```
voradmin idt config xform -external -c 10 /dev/sdc3
```


Note that you do not get a message about resizing the device because the CTE Private Region will not be embedded on the device.

3. To verify that the disk has been initialized, run the `voradmin idt status` command.

```
voradmin idt status /dev/sdc3  
Device /dev/sdh is configured to guard as an IDT-Capable GuardPoint
```

4. If you are embedding the CTE Private Region on the device, at this point, you need to resize the device using your standard disk management tools before you can guard it. Make sure you increase the device size by at least the amount shown in the `voradmin idt config xform` message.

You cannot assign an IDT-Capable GuardPoint to the device until it has been resized. If you do not resize the device, the GuardPoint assignment will fail.

5. After the device has been resized or the centralized CTE metadata directory has been configured and guarded, the Administrator can protect the device as an IDT-Capable GuardPoint through the Key Manager as described in [Guard the Linux Device with an IDT-Capable GuardPoint](#).

Note

The initialization process prepares the device to be guarded but does not actually guard it. You need to assign an IDT-Capable GuardPoint to the device in the Key Manager before the device is actually protected. In addition, the initialization process is only kept in memory until the device is guarded or rebooted. If the device is rebooted before you guard it, you will need to perform the initialization procedure again.

Guard the Linux Device with an IDT-Capable GuardPoint

After the device has been initialized, you can guard the device as an IDT-Capable GuardPoint from the Key Manager. For existing devices, as soon as the GuardPoint configuration has been pushed to the host and the status changes to guarded, CTE begins transforming the data on the disk using the encryption key associated with the GuardPoint Policy.

Warning

If access to the device is shared access across multiple CTE Protected hosts in a cluster, be sure to guard the device on one and only one of the CTE hosts.

Note

For details about how to create a GuardPoint in CM, see, “[Managing GuardPoints](#)”, [CTE Administration Guide](#).

To see the data transformation progress, use the `voradmin idt xform status <device-name>` command, as described in [Viewing Device Status and the IDT Device Header](#).

After the device is initialized and guarded, the protected device must be accessed through the CTE device pathname. This pathname corresponds to the secvm device. For example, the Linux device pathname `/dev/sdc2` becomes `/dev/secvm/dev/sdc2` as soon as the process is complete.

Note

- Be sure to use the secvm device name when using file system management tools such as `mkfs` and `fsck`.
- Do not use the device mapper names corresponding to IDT-Capable GuardPoints for GuardPoint administration on protected hosts.

Data Relocation and Transformation on Existing Linux Devices

When you add an IDT-Capable GuardPoint to a device that has been initialized with the `voradmin idt xform` command and you opted to embedded the CTE Private Region on the device, CTE first relocates existing data in the region of the device designated as CTE Private Region. The data is relocated to the end of the device, into the new space allocated when you resized the device. The relocation occurs once when the device is guarded for the first time. No relocation is necessary for subsequent rekeys on the device.

Relocation of data is transparent to applications accessing data through the IDT-Capable GuardPoint. CTE will map application I/O requests over the private region to the relocated region. After guarding the device, you can grow the device size further if necessary. However, you cannot shrink the device size.

IDT does not require a separate policy for data transformation. If you initialized the device with the `xform` option, CTE starts the IDT process when transformation is required. During the IDT process, access to the device is blocked until the IDT process completes and all the data on the device has been encrypted.

```
voradmin idt status xform /dev/sdc3
Status:          In-Process
                Relocation Zone 9764864 (relocated = 1)
                SegSpc 27, Xformation Range: 3217 ... 4799, SegIDs: 4795 4796 4791 4792 4
797 4798 4799
                KeyID:          2793      Key Name:      IDT_DEMO_KEY_1
                Old KeyID:       0         Old Key Name:  clear_key

# dd if=/dev/secvm/dev/sdc3 of=/dev/null bs=512 count=1
dd: failed to open 'dev/secvm/dev/sdc3': Resource temporarily unavailable
```

```
# voradmin idt status xform /dev/sdc3
Status:          Complete
                Relocation Zone 9764864 (relocated = 1)
                SegSpc 27, Xformation Range: 3217 ... 20189, SegIDs: none
                KeyID:          2793      Key Name:      IDT_DEMO_KEY_1
                Old KeyID:       0         Old Key Name: clear_key

# dd if=/dev/secvm/dev/sdc3 of=/dev/null bs=512 count=1
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.000989039 s, 518 kB/s
```

Thin-Provisioned Devices

IDT skips transforming thin-provisioned regions of a device. Data returned to IDT as sequence of clear-text zeros, in sector size granularity, is indication of possible sparse or un-allocated regions of the device that do not have to be transformed.

IDT Recovery From Crash

IDT is fault tolerant in the event of system crashes. IDT keeps track of the transformation process over the entire device. In the event of a crash, IDT will automatically resume transformation from the point of failure as soon the GuardPoint is enabled after system startup.

If you find the transformation status set to **In-Progress** when the GuardPoint is not enabled, the **In-Progress** state reflects an earlier system crash after which the GuardPoint has not been enabled to recover from the interruption in the IDT process.

Example of Creating an IDT-Capable GuardPoint on an Existing Linux Device

The following example shows the process of initializing an existing Linux device using `voradmin idt config xform` and guarding it as an IDT-Capable GuardPoint from the viewpoint of the Linux root user. In this example, all files in `/bin/*` are copied to a temporary location outside the device, then compared with the corresponding files on the device after the device has been resized and encrypted. The comparison proves that the file system is unchanged after the encryption process has completed.

First, we verify that the device is not protected, then we check the current size of the disk and create the copy of the files in `/bin/*`. After that, we run the `voradmin idt config xform` command to initialize the device.

```
voradmin idt status /dev/sdc1
Device /dev/sdc1 is not configured as IDT-Capable
# fdisk -l /dev/sdc1
Disk /dev/sdc1: 21.1 GiB, 21103640576 bytes, 41218048 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes
# mkfs.xfs /dev/sdc1
meta-data=/dev/sdc1          isize=256    agcount=4, agsize=1288064 blks
                        =               sectsz=512   attr=2, projid32bit=1
                        =               crc=0        finobt=0, sparse=0
data        =               bsize=4096   blocks=5152256, imaxpct=25
                        =               sunit=0     swidth=0 blks
```

```

naming    =version 2                bsize=4096    ascii-ci=0 ftype=1
log        =internal log            bsize=4096    blocks=2560, version=2
          =                        sectsz=512    sunit=0 blks, lazy-count=1
realtime  =none                    extsz=4096    blocks=0, rtextents=0
# mount -t xfs /dev/sdc1 /xfs
# cp /bin/* xfs
# voradmin idt config xform /dev/sdc1
Device /dev/sdc1 must be resized to at least 41347072 sectors (40378 MBs) before
guarding as IDT-Capable GuardPoint

```

At this point, you need to resize the device using your device management tools. You must increase the size by at least 41347072 sectors (40378 MBs). After the device has been resized, you can verify the new size:

```

fdisk -l /dev/sdc1
Disk /dev/sdc1: 21.2 GiB, 21169700864 bytes, 41347072 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes

```

After the device has been resized, the Administrator can guard the device with the desired in-Place Data Transformation policy. If the Administrator chooses Auto Guard, data transformation begins as soon as the policy is pushed to the host. If the Administrator chooses Manual Guard, data transformation does not begin until the Linux root user initiates it with the `secfsd -guard` command. Once data transformation begins, the Linux root user can check the progress using the `voradmin idt status xform` command.

```

secfsd -guard /dev/sdc1
secfsd: Path is guarded
# voradmin idt status xform /dev/sdc1
      Status:          In-Process
      Relocation Zone  9764864 (relocated = 1)
      SegSpc 27, Xformation Range: 3217 ... 4799, SegIDs: 4795 4796 4791 4792 4
797 4798 4799
      KeyID:           2793      Key Name:      IDT_DEMO_KEY_1
      Old KeyID:       0         Old Key Name: clear_key

```

After the status has changed to completed, you can compare the current version of the files in `/bin/*` with the ones you copied earlier.

```

voradmin idt status xform /dev/sdc1
      Status:          Complete
      Relocation Zone  9764864 (relocated = 1)
      SegSpc 27, Xformation Range: 3217 ... 20189, SegIDs: none
      KeyID:           2793      Key Name:      IDT_DEMO_KEY_1
      Old KeyID:       0         Old Key Name: clear_key
# voradmin idt status /dev/sdc1
IDT Header on /dev/secvm/dev/sdc1
      Version:          1
      Change:           0
      Private Region Size: 129024 sectors
      Exported Device Size: 41218048 sectors
      Key UUID:         9cc3c8e4-7ea7-310f-85c7-6f911de1ab52
      Mount Path:       None
# mount -t xfs /dev/secvm/dev/sdc1 /xfs
# for file in `ls /bin/sfx`; do cmp /bin/$file /xfs/$file; done

```

```
# umount /xfs
```

Changing the Encryption Key on Linux IDT-Capable Devices

To meet various compliance requirements, you may want to change the key that CTE has used to encrypt IDT-Capable GuardPoints. Thales refers to this changing of encryption keys as “Key rotation” or “Rekey”. Unlike the Live Data Transformation product offered by Thales for file systems on traditional storage devices, to change the encryption key on an IDT-Capable GuardPoint, the device must be taken offline. The data on the device will be inaccessible during the key rotation process.

For CipherTrust Manager, see [Key Version Modify Request](#) for more information.

Warning

For devices with shared access across multiple CTE Protected hosts in a cluster, you must designate one and only one of the nodes in the cluster as the node on which you plan to initialize and guard the device for rekey. The designated node must be the only one that accesses the device until the entire rekey process has completed. This requires guarding each shared device at the designated host level rather than at the host group level if you are using a host group to manage the CTE Protected nodes in your cluster. **DO NOT** initialize or guard any device on multiple nodes in the cluster simultaneously, because multiple nodes attempting to transform the same data can corrupt the data on the entire device.

1. Log on to the Key Manager.
2. Make sure that you know what Policy you want to associate with the GuardPoint or create a new **in-Place Data Transformation** policy if needed. The key rule must specify the current XTS/CBC-CS1 AES 256 key that the GuardPoint is currently using as well as the new XTS/CBC-CS1 AES 256 key that you want to use to transform the protected data.

You can either create a new in-Place Data Transformation policy or you can change the keys assigned to an existing in-Place Data Transformation policy. If you use an existing policy however, the new key you specify cannot have been previously used to encrypt the IDT-Capable GuardPoint. If you want to rekey the GuardPoint using a previously-used key, you must create a new policy in order to do so.

Include both the current key and the new key in the policy to ensure that both keys will be available during the rekey process, even if the key information stored in the CTE Private Region becomes unavailable.

Do not push this policy to the host yet.

3. Shut down any applications accessing the GuardPoint you are planning to rekey. If the GuardPoint is mounted as a file system, you must also unmount the file system.
4. Once the data can no longer being accessed, you can unguard the GuardPoint on the Key Manager.
 - a. If the GuardPoint is a manual device GuardPoint, you must first unguard it using the `secfsd -unguard` command on the CTE host before you unguard it on the Key Manager. If it is an automatic GuardPoint, you can skip this step and simply unguard the GuardPoint in the Key Manager.

The following example checks the guard status of `/dev/sdc1` and gets the current key name, then unguards the device.

```
secfsd -status guard
GuardPoint  Policy                Type                ConfigState  Status  Reason
-----
-----
/dev/sdc2    IDT_DEMO_POLICY_1  rawdevice          guarded      guarded  N/A
/dev/sdc3    IDT_DEMO_POLICY_1  rawdevice          guarded      guarded  N/A
/dev/sdc1    IDT_DEMO_POLICY_1  manualrawdevice    guarded      guarded  N/A
# voradmin idt status xform /dev/sdc1
      Status:      Complete
      Relocation Zone 0 (relocated = 0)
      SegSpc 27, Xformation Range: 4294967295 ... 4294967295, SegIDs: none
      KeyID:      2793      Key Name:      IDT_DEMO_KEY_1
      Old KeyID:   0        Old Key Name:  clear_key
# secfsd -unguard /dev/sdc1
secfsd: Path is not guarded
# secfsd -status guard
GuardPoint  Policy                Type                ConfigState  Status  Reason
-----
-----
/dev/sdc2    IDT_DEMO_POLICY_1  rawdevice          guarded      guarded  N/A
/dev/sdc3    IDT_DEMO_POLICY_1  rawdevice          guarded      guarded  N/A
/dev/sdc1    IDT_DEMO_POLICY_1  manualrawdevice    unguarded    not guarded  Inactive
```

- b. Return to the Key Manager, select the GuardPoint in the GuardPoints table, and click **Unguard** to unguard the device in the Key Manager.

Wait until the GuardPoint has been removed from the Key Manager.

5. Return to the device and run the `voradmin idt rekey` command. After you run the `voradmin` command, the IDT Device Header is temporarily removed from the device.

```
voradmin idt rekey /dev/sdc1
Enter YES to prepare device /dev/sdc3 for rekey -> YES
# voradmin idt status /dev/sdc1
Device /dev/sdc1 is configured to guard as IDT-Capable GuardPoint
```

Note

For manual GuardPoints, you must unguard the device both using `secfsd -unguard` and the Key Manager before you can use the `voradmin idt rekey` command.

6. In the Key Manager, guard the device with the new **in-Place Data Transformation** policy you created earlier. If you selected a Manual GuardPoint, use `secfsd -guard` to activate the new policy and start the data transformation to the new key.

During the IDT process, user access to the GuardPoint is blocked until IDT completes the transformation process.

The following example shows how to use `secfsd -guard` on manual GuardPoint `/dev/sdc1`, and the status messages that occur during the rekey process. If you are using an automatic GuardPoint, you do not need to use the `secfsd -guard` command. Instead, the rekey process starts as soon as you push the new policy from the Key Manager.

```
secfsd -guard /dev/sdc1
secfsd: Path is guarded
# secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
/dev/sdc2	IDT_DEMO_POLICY_1	rawdevice	guarded	guarded	N/A
/dev/sdc3	IDT_DEMO_POLICY_1	rawdevice	guarded	guarded	N/A
/dev/sdc1	IDT_DEMO_POLICY_2	manualrawdevice	guarded	guarded	Data transformation in progress

```
# voradmin idt status xform /dev/sdc1
      Status:                In-Progress
      Relocation Zone 0 (relocated = 0)
      SegSpc 27, Xformation Range: 3987 ... 3993, SegIDs: 3991 3987 3988 399
2 3989 3990 3993
      KeyID:                2921      Key Name:      IDT_DEMO_KEY_2
      Old KeyID:            2793      Old Key Name: IDT_DEMO_KEY_1
```

7. After the `xform` status shows as completed, you can restart all application workloads on the guarded device.

```
voradmin idt status xform /dev/sdc1
      Status:                Complete
      Relocation Zone 0 (relocated = 0)
      SegSpc 27, Xformation Range: 4768 ... 4768, SegIDs: none
      KeyID:                2921      Key Name:      IDT_DEMO_KEY_2
      Old KeyID:            2793      Old Key Name: IDT_DEMO_KEY_1
```

```
# secfsd -status guard
GuardPoint  Policy                Type                ConfigState  Status  Reason
-----
/dev/sdc2   IDT_DEMO_POLICY_1  rawdevice          guarded     guarded  N/A
/dev/sdc3   IDT_DEMO_POLICY_1  rawdevice          guarded     guarded  N/A
/dev/sdc1   IDT_DEMO_POLICY_2  manualrawdevice    guarded     guarded  N/A
```

Guarding an IDT-Capable Device with Multiple IO Paths on Linux

Each individual IO path from a server node to a storage controller is treated as a separate device on the host. DM-Multipath on a Linux host provides a management framework to group the individual IO paths to the same LUN into a single multipath device. If you use DM-Multipath to manage devices on the protected host, the individual devices that correspond to each IO path to the LUN cannot be configured for guarding as IDT-Capable, as those devices are under control of DM-Multipath. To guard such devices, you must guard the device mapper generated by DM-Multipath (multipathd) under the `/dev/mapper` directory.

Note

IDT is the only feature of CTE that exclusively supports guarding of a device mapper generated device under DM-Multipath framework.

The following example illustrates the procedure for guarding a device mapper generated device with the alias name `/dev/mapper/mpathA`.

1. Create an **in-Place Data Transformation** policy using an XTS/CBC-CS1 AES 256 key as the key rule.
2. On the host, prepare the device to be configured as IDT-Capable using the `voradmin idt config [-external] new|xform [-c n] <mapper-alias-name>` command.

For example, if the disk is a new disk with no existing data, you would enter:

```
voradmin idt config new /dev/mapper/mpathA
```

If the disk has existing data that you want to encrypt, you would enter:

```
voradmin idt config xform /dev/mapper/mpathA
```

3. Guard `/dev/mapper/mpathA` as Device GuardPoint using the policy created above. Be sure to check the **in-Place Data Transformation** check box.
4. For Manual Guard configuration, enable the GuardPoint using the `secfsd` command as follows:

```
secfsd -guard /dev/mapper/mpathA
```

5. For Auto Guard, wait for the `/dev/mapper/mpathA` device to be guarded on the protected host.
6. Once the device is guarded, provide the pathname of the secvm device to applications and/or file system operations. For example, `/dev/secvm/dev/mapper/mpathA`.

Viewing Device Status and the IDT Device Header

After you guard a device, you can view the status of that device using the `voradmin idt [xform] status <device-name>` command, where:

- `xform` (optional). If you specify this option, CTE shows the status of any data transformation processes happening on the device. If you do not specify this option, CTE displays the IDT Device Header for the device.
- `<device-name>` (required). The standard Linux name of the device whose status you want to view. (For example, `/dev/sdc2`.)

For example, if you want to view the IDT Device Header for the Linux device `/dev/sdc2`, you would enter:

```
voradmin idt status /dev/sdc2
IDT Header on /dev/secvm/dev/sdc2
      Version:                1
      Change:                 0
Private Region Size:         129024 sectors
Exported Device Size:        9627648 sectors
      Key UUID:               9cc3c8e4-7ea7-310f-85c7-6f911de1ab52
      Mount Path:             None
```

If you want to view the data transformation status on `/dev/sdc2`, you would enter:

```
voradmin idt status xform /dev/sdc3
      Status:                 In-Process
      Relocation Zone 9764864 (relocated = 1)
      SegSpc 27, Xformation Range: 3217 ... 4799, SegIDs: 4795 4796 4791 4792 4
797 4798 4799
      KeyID:                   2793      Key Name:      IDT_DEMO_KEY_1
      Old KeyID:               0         Old Key Name:  clear_key
```

The **Status** field displays **In-Progress** if a data transformation process is running, and **Completed** if the process has finished.

Linux System and IDT-Capable GuardPoint Administration

Note

For details about how to create a GuardPoint in CM, see the chapter, “Managing GuardPoints”, CTE Administration Guide.

Voradmin IDT Commands on Linux

The `voradmin` command is a command line utility for management of CTE specific configuration and status reporting. The `voradmin` command also supports configuration management related IDT-Capable GuardPoints (IDT).

For details about the Linux `voradmin idt` command options, see the man page for the `voradmin` command.

File System Mount Points on Linux

You can create and mount a file system on an IDT-Capable GuardPoint. CTE imposes one restriction on the mount point pathname selected for a device. Once you mount the device on a pathname, you cannot change the mount point to a different pathname. This restriction is enforced to allow the file system mount point to be guarded using a separate policy to enforce access control rules on the mounted file system namespace.

The following example shows the mount point of the IDT-Capable GuardPoint as the `/xfs` directory. The example also shows a failed attempt to mount the file system on a different directory pathname.

```
voradmin idt status /dev/sdc1
IDT Header on /dev/secvm/dev/sdc1
    Version:                1
    Change:                 0
Private Region Size:      129024 sectors
Exported Device Size:     9627648 sectors
    Key UUID:              9cc3c8e4-7ea7-310f-85c7-6f911de1ab52
Mount Path:               /xfs
# umount /xfs
# mkdir /other-xfs
# mount -t xfs /dev/secvm/dev/sdc2 /other-xfs
mount: permission denied
# mount -t xfs /dev/secvm/dev/sdc2 /xfs
```

Auto Mount Options for File System Devices on Linux

IDT-Capable GuardPoints containing file systems can also be added to the `/etc/fstab` configuration file for auto mount at startup or unmount at shutdown. An entry can be for a GuardPoint configured for either Auto Guard or Manual Guard. For more information about Auto and Manual Guard options, see [Guard the Linux Device with an IDT-Capable GuardPoint](#).

Use the device path corresponding to an IDT-Capable GuardPoint device when specifying `fstab` entries, such as `/dev/secvm/dev/sdh`. Do not use the native device pathnames, such as `/dev/sdh`, or device mapper device names. You must also include several settings in the `fstab` entry for each IDT-Capable GuardPoint, as shown in the following table:

Option	Description
<code>x-systemd.requires= secvm-barrier.service</code>	Ensure that the IDT-Capable GuardPoint is enabled before the device is mounted at startup and disabled after the device is unmounted at shutdown. The <code>secvm-barrier.service</code> service is a proxy for all the services that make up CTE.
<code>nofail</code>	The system boot will proceed without waiting for the IDT-Capable device if it can't be mounted successfully.

Option	Description
<code>x-systemd.wanted-by=<idt device>.device</code>	Required for Linux distributions running <code>systemd</code> 242 or later. Instructs <code>systemd</code> to add a <code>wants=</code> dependency on the IDT-Capable device to ensure that, when the device becomes available, this mount operation is executed. <code><idt device>.device</code> is the name of the device specified in <code>fstab</code> with the <code>/</code> replaced with <code>-</code> . For example, <code>/dev/secvm/dev/sdb</code> becomes <code>dev-secvm-dev-sdb.device</code> .

This is an example of an entry in `/etc/fstab` for an IDT-Capable GuardPoint with an xfs file system that is mounted on `/xfs`:

```
/dev/secvm/dev/sdh /xfs xfs x-systemd.requires=secvm-barrier.service, \
x-systemd.wanted-by=dev-secvm-dev-sdh.device,nofail 0 0
```

For information about configuring `systemd` for CTE, see [CTE and `systemd`].

Linux System Utilities for Signing

The following table includes recommendations on the system and file system specific utilities for inclusion in the signature set to allow or deny root execution.

EXT Utilities	Deny/Allow	XFS	Deny/Allow	Generic Utilities	Deny/Allow
<code>badblock</code>	Allow	<code>fsck.xfs</code>	Allow	<code>mount</code>	Allow
<code>debugfs</code>	Deny	<code>mkfs.xfs</code>	Allow	<code>umount</code>	Allow
<code>e2freefrag</code>	Allow	<code>xfs_repair</code>	Allow	<code>dmsetup</code>	Allow
<code>e2fsck</code>	Allow	<code>xfs_admin</code>	Allow		
<code>e2image</code>	Allow	<code>xfs_bmap</code>	Allow		
<code>e2label</code>	Allow	<code>xfs_check</code>	Allow		
<code>e2undo</code>	Allow	<code>xfs_copy</code>	Deny		
<code>filefrag</code>	Allow	<code>xfs_db</code>	Deny		
<code>fsck.ext2</code>	Allow	<code>xfs_estimate</code>	Allow		
<code>fsck.ext3</code>	Allow	<code>xfs_freeze</code>	Allow		
<code>fsck.ext4</code>	Allow	<code>xfs_fsr</code>	Allow		
<code>logsave</code>	Allow	<code>xfs_growfs</code>	Allow		
<code>mke2fs</code>	Allow	<code>xfs_info</code>	Allow		
<code>mkfs.ext2</code>	Allow	<code>xfs_logprint</code>	Allow		
<code>mkfs.ext3</code>	Allow	<code>xfs_mdrestor</code>	Allow		

EXT Utilities	Deny/Allow	XFS	Deny/Allow	Generic Utilities	Deny/Allow
		e			
mkfs.ext4	Allow	xfs_metadump	Allow		
resize2fs	Allow	xfs_mkfile	Deny		
tune2fs	Allow	xfs_ncheck	Allow		

Resizing Guarded IDT Devices

Devices configured as IDT-Capable can be resized using the system-provided resizing utilities. If you are using a file system on the GuardPoint, you can mount the file system after resizing the device and then grow the file system to the new size using the appropriate utility such as `xfs_growfs` or `resize2fs`.

Warning

Do not shrink IDT-Capable GuardPoints. Due to relocation of user data from the CTE Private Region, if you shrink the device, you may corrupt data on the device.

1. Stop applications from accessing the IDT-Capable GuardPoint.
 - Unmount the file system if the device is mounted.
 - Unguard the IDT-Capable GuardPoint if using Auto Guard or on the host with the `secfsd unguard <device-name>` command if using Manual Guard.
2. Use the native disk management tools to resize the device.
3. After resizing the device, check the size of the device with the `fdisk -l` or similar command. Note that you cannot use the `voradmin idt status` command to verify the new size of the device at this point because the size information is not updated in CTE until the IDT-Capable GuardPoint is re-enabled.
4. If the reported size does not match what you expect, you may need to rescan your storage devices using the command appropriate for the device's connection type.
5. Once the expected size is achieved, enable the IDT-Capable GuardPoint and restart your applications.

Resizing Guarded IDT Devices

Devices configured for in-Place Data Transformation can be resized using the system-provided resizing utilities. If you are using a file system on the GuardPoint, you can mount the file system after resizing the device and then grow the file system to the new size using the appropriate utility such as `xfs_growfs` or `resize2fs`.

Warning

Do not shrink IDT GuardPoints. Due to relocation of user data from CTE private region, if you shrink the device, you may corrupt data on the device.

1. Stop applications from accessing the GuardPoint.
 - Unmount the file system if the device is mounted.
 - Disable GuardPoints: auto-guard if it is enabled on the CipherTrust Manager, or manual-guard if it is enabled on the protected host.
2. Use the native disk management tools to resize the device.
3. After resizing the device, check the size of the device. For Linux, you can use the `fdisk -l` command.
4. If the reported size does not match what you expect, you may need to rescan your storage devices using the command appropriate for the device's connection type.
5. Once the expected size is achieved, enable the GuardPoint and restart your applications.

Examples

The following example show the administrative steps to grow an XFS file system mounted on an ES GuardPoint. The example shows a device of size 41,347,072 sectors resized to 43,395,072 sectors.

```
# fdisk -l /dev/sdh

Disk /dev/sdh: 21.2 GB, 21169700864 bytes, 41347072 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes

# xfs_info /dev/secvm/dev/sdh
meta-data=/dev/secvm/dev/sdh      isize=512    agcount=4, agsize=1288064 blks
                                     sectsz=512    attr=2, projid32bit=1
                                     crc=1        finobt=0  spinodes=0
data      =                       bsize=4096    blocks=5152256, inampt=25
                                     sunit=0      swidth=0 blks
naming    =version 2              bsize=4096    ascii-ci=0 ftype=1
log       =internal              bsize=4096    blocks=2560, version=2
                                     sectsz=512   sunit=0 blks, lazy-count=1
realtime  =none                  extsz=4096    blocks=0, rtextents=0

# voradmin idt status /dev/sdh
ESG Header on /dev/secvm/dev/sdh
  Version:      1
  Change:      0
  Notifications: None
  Storage Status: None
  Private Region Size: 129024 sectors
  Exported Device Size: 41218048 sectors
  Key UUID:     81e415ed-4a1e-3a2f-b829-5893dd2fd0b0
  Mount Path:   N/A (GuardPoint not enabled)

# umount /xfs
# secfsd -unguard /dev/sdh
secfsd: Path is not guarded
```

In this example we resize the device on the storage array to 43395072 sectors. Notice that the `voradmin` command reports the old device size until the device is guarded.

```
# fdisk -l /dev/sdh

Disk /dev/sdh: 22.2 GB, 22218276864 bytes, 43395072 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes

# voradmin idt status /dev/sdh
ESG Header on /dev/secvm/dev/sdh
  Version: 1
  Change: 0
  Notifications: None
  Storage Status: None
  Private Region Size: 129024 sectors
  Exported Device Size: 41218048 sectors
  Key UUID: b1e4450d-0a5e-3a8f-b829-5893dd2fd0b0
  Mount Path: N/A (GuardPoint not enabled)

# secfsd -guard /dev/sdh
secfsd: Path is guarded

# voradmin idt status /dev/sdh
ESG Header on /dev/secvm/dev/sdh
  Version: 1
  Change: 0
  Notifications: None
  Storage Status: None
  Private Region Size: 129024 sectors
  Exported Device Size: 43264048 sectors
  Key UUID: b1e4450d-0a5e-3a8f-b829-5893dd2fd0b0
  Mount Path: /xfs
```

The final step shown in below is to mount and resize the XFS file system to include the extended space into the file system.

```
# mount -t xfs /dev/secvm/dev/sdh /xfs
# xfs_growfs /xfs
meta-data=/dev/secvm/dev/sdh      isize=512    agcount=4, agsize=1288064 blks
                                     sectsz=512    attr=2, projid32bit=1
                                     crc=1        finobt=0  spinodes=0
data      =                       bsize=4096    blocks=5152256, maxpct=25
                                     sunit=0      swidth=0 blks
naming    =version 2              bsize=4096  ascii-ci=0 ftype=1
log       =internal              bsize=4096  blocks=2560, version=2
                                     sectsz=512   sunit=0 blks, lazy-count=1
realtime  =none                  extsz=4096    blocks=0, rtextents=0
data blocks changed from 5152256 to 5408256
# xfs_info /dev/secvm/dev/sdh
meta-data=/dev/secvm/dev/sdh      isize=512    agcount=5, agsize=1288064 blks
                                     sectsz=512    attr=2, projid32bit=1
                                     crc=1        finobt=0  spinodes=0
data      =                       bsize=4096    blocks=5408256, maxpct=25
                                     sunit=0      swidth=0 blks
naming    =version 2              bsize=4096  ascii-ci=0 ftype=1
log       =internal              bsize=4096  blocks=2560, version=2
                                     sectsz=512   sunit=0 blks, lazy-count=1
realtime  =none                  extsz=4096    blocks=0, rtextents=0
```

Alerts and Errors on Linux

This section lists the alerts and errors that may be encountered during system operations.

Encryption key on device has not been made available

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the encryption key specified in the policy for the GuardPoint has not been made available to the protected host.

Solution: Check the host's connectivity with the Key Manager.

Specified policy disagrees with metadata set on the Guard Path

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the key specified in the policy for the GuardPoint does not match with the key stored in the IDT Device Header.

Solution: Un-guard the device and check the name and UUID of the key in the IDT Device Header using `voradmin idt status <device-name>` and `voradmin idt status xform <device-name>` commands and compare the name and UUID with the key name specified in the policy. Correct the discrepancy and re-guard the device.

Device has not been configured for IDT-Capable

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the device has been properly guarded as an IDT-Capable GuardPoint on the Key Manager but the device has not been initialized for guarding as IDT-Capable.

Solution: The most probable cause of this error is that you did not initialize the device for guarding as IDT-Capable on protected host. It's also possible that the guarded device has already configured for guarding as Ean IDT-Capable GuardPoint. If the device needs to be initialized for guarding as IDT-Capable, see [Initializing an IDT-Capable Device](#).

Device not resized for guarding as IDT-Capable

This message appears in the output of `secfsd -status guard` command and indicates that the IDT-Capable GuardPoint was not successfully enabled. The status indicates that the newly guarded IDT-Capable GuardPoint, which has been initialized with `xform` option of `voradmin`, has not been resized to accommodate storage space for the CTE Private Region.

Solution: Unguard the IDT-Capable GuardPoint, resize the LUN and verify that the host sees the expanded size, then guard the IDT-Capable GuardPoint from the Key Manager.

Data transformation failed

This message appears in the output of `secfsd -status guard` command and indicates that the IDT-Capable GuardPoint was not successfully guarded. The status indicates that the protected host encountered an error while transforming the data on the device during IDT.

Solution: Consult with the system and/or storage admin to check on the health of the LUN in the storage array. You may contact Thales Support for troubleshooting and recovery if there has not been a report of any error on the LUN.

Data transformation in progress

This message appears in the output of `secfsd -status guard` command and indicates that the IDT-Capable GuardPoint was not successfully enabled. The status indicates that the protected host is transforming the data on the device.

Solution: You must wait for data transformation to complete. Check the status of transformation by running `voradmin idt status xform <device name>`. Access to the device is blocked until transformation completes.

Device <device-name> is configured to guard as IDT-Capable GuardPoint

This error message is reported by the `voradmin` command when initializing a device as an IDT-Capable GuardPoint that has already been initialized for guarding as an IDT-Capable GuardPoint.

Solution: The device has already been initialized for guarding as IDT-Capable and is probably waiting to be guarded as an IDT-Capable GuardPoint through the Key Manager. Alternatively, if you want to remove the IDT-Capable configuration, use the `voradmin idt delete <device-name>` command.

Device <device-name> is configured as IDT-Capable GuardPoint

This error message is reported by the `voradmin` command when initializing a device that is already being guarded as an IDT-Capable GuardPoint.

Solution: The device is already guarded by an IDT-Capable GuardPoint.

GuardPoint for device <device-name> still guarded on Key Manager

This error message is reported by the `voradmin` command when attempting to initialize a device for rekey or removing the device as IDT-Capable.

Solution: Unguard the IDT-Capable GuardPoint, wait for the protected host to process the update, and then rerun the `voradmin` command.

Failed to open device <device-name>, error Device or resource busy

This message occurs when `voradmin` detects that the target device is busy.

Solution: The device may already be in use by other application. Rerun the `voradmin` command when the device is no longer in use.

Device <device-name> is not configured as IDT-Capable

This error message is reported by the `voradmin` command when attempting to delete a device as an IDT-Capable GuardPoint.

Solution: This message indicates that the target device has been not initialized for guarding as IDT-Capable. The message may also be reported if the specified device has been initialized for guarding as IDT-Capable but it has not been guarded yet. In this case, it removes the preparation made by `voradmin`. You can remove the IDT-Capable configuration status on the device by running `voradmin idt delete <device-name>`. You may see the same error message again, and if you do, you can ignore it.

Abort! Error: Could not stop secfs, secvm device(s) busy

This error occurs during CTE shutdown when there is a busy CTE protected device.

Solution: Verify that all applications directly accessing `secvm` protected GuardPoints have been shut down. Ensure that all file systems on top of a `secvm` protected devices are under the control of `systemd` and have been unmounted before attempting to shut down the agent.

Abort! Error: Could not unmount file systems

This error occurs during CTE shutdown when a file system under the control of `systemd` fails to unmount.

Solution: Verify that file systems on top of an IDT-Capable GuardPoint devices are not busy and then rerun the agent shut down command.

A dependency job for idt.mount failed. See 'journalctl -xe' for details

This error occurs during CTE startup when system fails to mount a file system. This error message is typically accompanied by a long timeout during the CTE startup process.

Solution: Check that the underlying device is available and that the IDT-Capable GuardPoint was successfully applied on the device. Once the device is available, the file system will automatically finish mounting.

ESG/IDT-ALERT: IO error on header for [GuardPoint]

This is an alert message to the Key Manager. It occurs when CTE encounters a general error when attempting to access the private region on an IDT-Capable device.

Solution: An I/O error attempting to read or write to the device may have been caused by errors on the host or storage array. Consult with the system and/or storage admin to check on the health of the LUN in the storage array. You may contact Thales Support for troubleshooting and recovery if there has been no report of errors on the LUN.

ESG/IDT-ALERT: Data transformation failure on [GuardPoint]

This is an alert message to the Key Manager. It occurs when protected host encounters an error transforming the data on device during IDT process.

Solution: Contact Thales Support for troubleshooting and recovery.

ESG/IDT-INFO: Data transformation complete on [GuardPoint]

This message is a notification to the Key Manager admin that the protected host has completed the data transformation of the specified IDT-Capable GuardPoint.

ESG/IDT-ALERT: Failed to resize <device-name>

This alert is a notification to the Key Manager admin that the protected host has failed to update the change to the device size in the IDT Device Header on the device.

Solution: Contact Thales Support for troubleshooting and recovery.

FSADM-ALERT: ESG/IDT required Signature Set for system utilities may have to be resigned

This alert is a notification to the Key Manager admin that the recent system upgrade to the protected host may have updated the binary files listed in the signature set for restricting root access.

Solution: Upon this notification you must immediately re-sign the affected or all the binary files to prevent them from accessing protected data.

File System is not automatically mounted after IDT completes

An IDT-Capable device with a file system that has been configured to automatically mount may fail to automatically mount while the device undergoes data transformation through IDT. Following is a sample log message in the kernel ring buffer that reports a failed attempt to access a device during IDT. You can ignore this message.

```
Vormetric SecVM: secvm_map during IDT (dc 00000000c3537611)
```

When access to a device is to mount the file system, the kernel ring buffer may also report a second error message indicating that a file system failed to mount due to data corruption. You can ignore this message. This occurs because the mount command is issued after the device has been guarded but before data transformation through IDT is complete. While IDT is in progress, the device cannot be used, so any attempt to mount the file system will fail.

Solution: Manually mount the file system after IDT is complete.

Upgrading CTE on Linux

This chapter describes how to upgrade an existing CipherTrust Transparent Encryption (CTE) client and contains the following sections:

Upgrading CTE

This section describes the generic instructions for interactively upgrading CTE. If there are any changes to this procedure for the current release of CTE, those changes will be documented in the CTE Release Notes.

If you want to schedule an upgrade to occur the next time the system boots, see [Scheduled Upgrade Feature](#).

1. Stop any application accessing files in the GuardPoint.
2. Log on to the host where you will upgrade CTE. You must have root access.
3. Copy or mount the installation file onto the host system.
4. Start the upgrade by executing the install program for the release to which you want to upgrade. If you want to automatically accept the CTE License Agreement, you can include the `-y` parameter.

For example, the following command upgrades the product to version `<Release.build-number>` after the user manually reviews and accepts the CTE License Agreement:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin
```

The following command upgrades the product to version `<Release.build-number>` but automatically accepts the CTE License Agreement:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin -y
```

5. Follow the prompts. During an upgrade, the following message displays. Enter Y at the prompt:

```
Upgrade detected: this product will be stopped and restarted.  
Do you wish to proceed with the upgrade? (Y/N) [Y]: Y  
Installation success.  
You will not do the registration steps since CTE is already registered with th  
e Key Manager.
```

6. To verify that the upgrade was successful, use the `vmd -v` command:

```
vmd -v  
Version 6, Service Pack 2  
<Release.build-number>  
2022-02-04  
Copyright (c) 2009-2022, Thales. All rights reserved.
```

Scheduled Upgrade Feature

- Warnings for CTE for Linux
- Using the Scheduled Upgrade Feature
- Performing a Manual Upgrade When an Upgrade is Already Scheduled

Note

Scheduled upgrade on reboot is not supported on HDFS nodes.

Warnings for CTE for Linux

- Prior to upgrading your system, perform a backup or take a snapshot of your system.
- As with prior CTE versions, Key Manager connectivity is required during upgrade.
- Yum updates, or OS patches, should be done prior to CTE upgrade on reboot.
- If you upgrade from a compatible kernel to an incompatible kernel, the `secfs` module will fail to load on the next reboot.
- You may see the following behavior if the upgrade on reboot fails due to a crash, or a power failure, (this is similar to a failure during a normal upgrade).
 - If a crash, or power failure, occurs before the upgrade executes, the upgrade will not take place, and the

currently installed CTE version continues to run after the reboot. Restart the system to upgrade successfully.

- If a crash, or power failure, occurs during the upgrade, CTE may enter an inconsistent state. Perform a restore from your backup, or roll back to the snapshot that you just took. Then, start the upgrade again.
- If a crash, or power failure, occurs after a successful upgrade, then the new version will run on the next reboot. No user intervention is required in this case.
- During reboot or shutdown, all applications and services dependent on CTE services must be stopped before a scheduled update takes place. Failure to stop these services can result in an aborted scheduled upgrade during the system reboot. Examples of situations that may cause an aborted upgrade are applications with open files in a CTE GuardPoint, or a third party anti-virus software doing periodic scans.

For examples of how to set up CTE start/stop dependencies with other programs, see [CTE and systemd](#).

Using the Scheduled Upgrade Feature

The following procedure describes how to use voradmin to schedule an upgrade that will be applied the next time the machine reboots.

1. If you want to check which version of CTE for Linux you currently have installed, use the `vmd -v` command:

```
vmd -v
Version 6, Service Pack 2
7.0.0.47
2022-02-04
Copyright (c) 2009-2022, Thales. All rights reserved.
```

2. To schedule an upgrade on reboot, use the following commands:

```
voradmin upgrade schedule <path_to_CTE_installer_binary> y [-t <custom_extraction_path>]
```

where:

- `<path to CTE installer>` is the full path to the CTE installation file for the release to which you want to upgrade. For example, `./vee-fs-7.8.0.75-129-rh8-x86_64.bin`.
- `-y` is an optional parameter that automatically accepts the CTE License Agreement. If you do not specify this parameter, the installer displays the CTE License Agreement and you must manually accept it before the upgrade can be scheduled.
- `[-t <custom_extraction_path>]` is an optional parameter that specifies the path to a custom binary extraction path directory in which you want CTE to store the temporary files it needs during the upgrade. The default is `/var/tmp/`, but in some systems, `/var/tmp/` is restricted and not available for use.

Exceptions: Do not use the `-t` option on protected paths, GuardPoint paths, or paths which do not have sufficient permissions to copy/extract the target binary.

For example, if you are upgrading to version 7.2.0.xx and you want to automatically accept the license agreement and use a custom directory, you would type:

```
voradmin upgrade schedule ./vee-fs-7.2.0-98-rh8-x86_64 -y -t /my_custom_dir
```

Note

The `[-t]` option is only supported by CTE v7.2 and subsequent versions.

3. If you want to verify that the upgrade was successfully scheduled, use the `voradmin upgrade show` command:

```
voradmin upgrade show
Upgrade on reboot is currently scheduled.
Current CTE version is 7.0.0.47, upgrade on reboot scheduled for CTE 7.1.0.66.
```

4. Reboot the machine, then log in and verify that the upgrade was successful.

```
vmd -v
Version 6, Service Pack 2
7.1.0.66
2022-02-04
Copyright (c) 2009-2022, Thales. All rights reserved.
```

Note

Appropriate logs will be logged in syslog.

Performing a Manual Upgrade When an Upgrade is Already Scheduled

If an administrator runs a manual upgrade after an upgrade has already been scheduled, the installer displays the following warning:

```
WARNING: upgrade on reboot is already scheduled for 7.1.0.66.

Do you want to cancel scheduled upgrade on reboot ? (Y/N) [Y] :
```

If the administrator does *not* cancel the scheduled upgrade, the scheduled upgrade takes precedence and the manual upgrade fails with the message:

```
Already scheduled upgrade on reboot remains intact.

Installation failure.
```

If the administrator wants to proceed with the manual upgrade immediately, they must enter Y at the prompt to cancel the scheduled upgrade:

```
WARNING: upgrade on reboot is already scheduled for 7.1.0.66.

Do you want to cancel scheduled upgrade on reboot ? (Y/N) [Y] : Y

WARNING: upgrade on reboot is cancelled for 7.1.0.66. Proceeding with manual upgr
ade.

Upgrade detected: this product will be stopped and restarted.

Do you wish to proceed with the upgrade? (Y/N) [Y]: Y

.....

Upgrade success.
```

To verify that the upgrade succeeded, the administrator can use the `vmd -v` command:

```
vmd -v
Version 6, Service Pack 2
7.1.0.66
2022-02-04
Copyright (c) 2009-2022, Thales. All rights reserved.
```

To cancel an existing scheduled upgrade on reboot:

```
voradmin upgrade cancel
Successfully cancelled upgrade on reboot
```

Upgrading CTE agents in an LDT Communication Group from 7.4.0 to 7.5.0 and post 7.5.0

When upgrading the CTE agent version on all nodes of an LDT Communication Group, you must stop CTE on all of the nodes to be upgraded before upgrading them.

1. Unguard the GuardPoints on the nodes to be upgraded:
 - a. Go to the CipherTrust Manager UI.
 - b. In the GuardPoint window, click the ellipsis on the right side of a GuardPoint and select disable to disable the GuardPoint.
 - c. Repeat the steps for all of the GuardPoints on the nodes to be upgraded.

2. Stop the CTE service on all of the nodes to ensure that all of the GuardPoints are unguarded.

For **Windows**:

- a. Go to **Control Panel > Services (local)**.
- b. Select **secfsd**.
- c. Select **Stop the Service**.

For **Linux**, type:

```
/etc/vormetric/secfs stop
```

3. Upgrade CTE on all of the nodes.
4. If your setup contains **manual directory** type GuardPoints, then you must run `secfsd -guard <gp>` to guard the GuardPoints again after the upgrade.
5. Verify that the GuardPoints are guarded on all of the nodes. Type:

```
# secfsd -status guard
```

Uninstalling CTE from Linux

Considerations

- The CTE Agent must be removed from the Linux host before the host is removed from the key manager with which it is registered.
- Database applications like DB2 and Oracle can lock the user space while they run. If the uninstall fails because a GuardPoint is in use, determine which applications are using the files in the GuardPoint and stop them. Then run the uninstall again.
- Commands like `fuser` and `lsof` might not reveal an active GuardPoint because they detect active usage, not locked states. Although it may appear that a GuardPoint is inactive, it may be in a locked state. Under this condition, software removal may fail with an error similar to the following:

```
/home: device is busy.
```

Procedure

1. Stop any application from accessing files in the GuardPoint.
2. In the key manager with which this host is registered, do the following:

- Decrypt any data you want to use after uninstall. After the CTE Agent software is removed, access to data is no longer controlled. If data was encrypted, it will remain encrypted. If decrypted or copied out of the GuardPoint, the data is visible as clear text.

This decryption must be done on *every* GuardPoint on the host if you want to access all existing data on the host.

- Make sure the Agent and System locks have been disabled for the host.
- Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.

Do not remove the host from the key manager yet.

3. Log on to the host as `root`.
4. Change the directory to an unguarded location (for example, `/.`).

Caution

Do not change (`cd`) into the `/opt/vormetric` directory or into any directory below `/opt/vormetric`. If you run the uninstaller from `/opt/vormetric` or any of its subdirectories, the package removal utility may fail and return the following message:

You are not allowed to uninstall from the `/opt/vormetric` directory or any of its sub-directories.
Agent uninstallation was unsuccessful.

5. Start the uninstall. Type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/uninstall
Would you like to uninstall the vee-fs package? (Y/N) [Y]: Y
.....
Success!
```

6. Remove the host record from the key manager.

Migrating Agents from CTE-U to CTE

Note

This process **only** works on NFS. It is **not** supported on a Local File System.

Assumptions

- CTE-U agents are installed on a client and registered to a CipherTrust Manager.
- GuardPoints are setup and encrypting data on the CTE-U Agent.

Migrating

When you have a CTE-U agent that is already registered with CipherTrust Manager, and you want to change it from CTE-U to CTE, you **must** perform the following steps in order:

1. Unguard the GuardPoints on the client from CipherTrust Manager.
 - a. Go to the CipherTrust Manager UI.
 - b. In the GuardPoint window, click the ellipsis on the right side of a GuardPoint and select **disable** to disable the GuardPoint.
 - c. Repeat the steps for all of the GuardPoints on the nodes to be upgraded.
2. Uninstall the CTE-U software from the agent.
3. Unenroll the client from CipherTrust Manager.
4. Delete the entry from CipherTrust Manager.
5. Add the client back into CipherTrust Manager.
6. Install and Register the new Agent.
7. Create a new LDT policy.

Note

Make sure that the policy uses the same key in CTE-U and in CTE.

8. Create new LDT GuardPoints and apply the LDT policy to the new GuardPoints on the CTE agent.



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

- CTE Agent Linux and Windows Quick Start Guide 3
 - Installation Prerequisites 3
 - Installing and Registering CTE 6
 - Installation and Registration on Linux 6
 - Installation and Registration on Linux with UEFI Secure Boot 10
 - Windows Installation 13
 - Windows Registration 14
 - Guarding a Directory with CipherTrust Manager 17
 - Access the CipherTrust Manager Domain 17
 - Identify or Create an Encryption Key 18
 - Create a Standard Policy 20
 - Create and Assign a GuardPoint 28
 - Using and Renewing Certificates 30
 - Protecting Data with CTE 32
 - Guarding a Directory with Ransomware Protection 34

CTE Agent Linux and Windows Quick Start Guide

CTE protects data at rest, residing on Direct Attached Storage (DAS), Network Attached Storage (NAS), Storage Area Networks (SAN) or in the Cloud. This can be a mapped drive or mounted disk, as well as through Universal Naming Convention paths.

CTE secures data with little impact to application performance. It requires no changes to your existing infrastructure and supports separation of duties between data owners, system administrators, and security administrators.

This section describes how to install CTE on Linux and Windows systems using the standard, interactive installation script for Linux and interactive installer for Windows. After successful installation, register that system with CipherTrust Manager and then create your policies, encryption keys, and GuardPoints using the CipherTrust Manager.

This section contains the following topics:

- [Protecting Data with CTE](#)
- [Using and Renewing Certificates](#)
- [Installation Prerequisites](#)
- [Installing and Registering CTE](#)
- [Guarding a Directory with CipherTrust Manager](#)
- [Guarding a Directory with Ransomware Protection](#)

Installation Prerequisites

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.
- CipherTrust Manager must contain an LDT Communication Group if you will use LDT to guard data over CIFS/ NFS shares using LDT policies. See [Managing LDT Communication Groups](#) for more information.

Minimum Hardware Requirements for CTE

The following requirements are the minimum for CTE. When you add LDT, or third-party applications, you need to add more storage and RAM. Refer to the [LDT guide](#) for LDT requirements and the third-party software for their requirements.

Component	CPU	CPU Cores	RAM	Storage (Free Space)
CTE-Windows	Intel/AMD x64 with AES-NI support	4 cores	8 GB	1GB
CTE-Linux	Intel/AMD x64 with AES-NI support	4 cores	8 GB	1GB
CTE-AIX	IBM PowerPC8 or higher	4 cores	8 GB	1GB

Port Configuration Requirements

The following port information applies to both Windows and Linux systems.

Communication through a Firewall

If a protected client must communicate with CipherTrust Manager through a firewall, see the CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

Communication with CipherTrust Manager

The default port for http communication between CipherTrust Manager and the CTE Agent is **443**. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

Communication for LDT over CIFS/NFS

All nodes that intend to use **LDT over CIFS/NFS** GuardPoint must have the following ports open:

- 7024
- 7025

Note

When you are registering a CipherTrust Transparent Encryption client with CipherTrust Manager, you can manually include a destination port number, (Default: 443). If you enter a port value, using the syntax **<hostname or IP address>:<port number>** then CipherTrust Transparent Encryption **does not** perform a port scan. CipherTrust Transparent Encryption uses the port number provided to verify the target server type using a TLS operation.

If you do not enter a port number, CipherTrust Transparent Encryption performs a port scan to check which ports are listening, including port 443.

Linux

Recommendations and Considerations

- The host on which you want to install CTE *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE to release 7.0.0, or any subsequent version, will fail.
- Thales recommends that you install CTE in the default location.
- Do not install CTE on network-mounted volumes such as NFS.
- Make the Installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.

For example:

```
./vee-fs-7.8.0.75-rh8-x86_64.bin -d /home/hello/
```

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the CipherTrust Manager to all clients where you install CTE.
- If the host is a virtual machine, the VM must be deployed and running.

Windows

Recommendations and Considerations

- The host on which you want to install CTE *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE to release 7.0.0, or any subsequent version, will fail.
- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the Windows system on which you plan to install CTE to the CipherTrust Manager. After the Windows system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.
- CipherTrust Transparent Encryption must also allow for connectivity of the CipherTrust Manager to all of the clients where you install CTE, as well as communication between different CTE clients that plan to enable LDT over NFS/CIFS.
- If the system is a virtual machine, the VM must be deployed and running.

Installing and Registering CTE

During the installation, you are asked a series of questions. After the installation, you are prompted to immediately register the CTE with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host.

Select the type of installation you want to do:

- Installation and Registration on Linux
- Installation and Registration on Linux with UEFI Secure Boot
- Windows Installation
- Windows Registration

Installation and Registration on Linux

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note

- If possible, Thales recommends that you use the default directory `/opt/vormetric`.
- Custom directories are **only available** for RHEL and SLES.
- Custom directories are **not available** for COS (Cloud Object Storage).

To view all installer options, use the `-h` parameter. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type **Y** and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

Welcome to the CipherTrust Transparent Encryption File System Agent Registration Program.

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>
```

```
In order to register with a CipherTrust Manager you need a valid registration token from the CM.
```

```
Do you want to continue with agent registration?(Y/N) [Y]:
```

5. Type **N** and press Enter to end the installation procedure without registering the CTE Agent with a key manager.
6. Enter **Y** to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE. For example:

CTE for CipherTrust Manager

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Please enter the primary key manager host name: 10.3.200.141
```

```
You entered the host name 10.3.200.141
```

```
Is this host name correct? (Y/N) [Y]: Y
```

CTE for CDSPaaS

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Enter the primary key manager host name of the service:
```

```
You entered the host name us1.ciphertrust.dpondemand.io
```

```
Is this host name correct? (Y/N) [Y]: Y
```

Host names:

- **Europe:** `ciphertrust.dpondemand.io`
- **North America:** `us1.ciphertrust.dpondemand.io`

Note

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: `<hostName>:<port#>`. For example, `10.3.200.141:8445`.

7. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the following list.
```

```
[1] sys31186.qa.com
```

```
[2] 10.3.31.186
```

```
Enter a number, or type a different host name or IP address in manually:
```

```
What is the name of this machine? [1]: 2
```

```
You selected "10.3.31.186".
```

8. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
```

```
Please enter the profile name for this host: My-Profile
```

```
Please enter the host group name for this host, if any:
```

```
Please enter a description for this host: RHEL7 system West Coast Datacenter
```

```
Token : 12345
```

```
Profile name : My-Profile
```

```
Host Group : (none)
```

```
Host description : RHEL7 system West Coast Datacenter
```

```
Are the above values correct? (Y/N) [Y]: Y
```

9. At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloning. The default is Y (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This

can be rectified by running this registration program again. Do you want to enable this functionality? (Y/N) [Y]:
Y

10. Type Y to support Filesystem encryption and to choose other features. Type N if you only want to support Ransomware Protection. If you type N, then LDT and COS are not supported.

```
Do you want this host to have Filesystem encryption support enabled on the server? (Y/N) [Y]:
```

11. At the LDT prompt, specify that you want this client to use CTE-LDT by typing Y and pressing Enter:

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]: Y
```

12. If you are planning to create GuardPoints on NFS shares, enter the name of the LDT Communication Group that this node will join.

```
Enter the LDT Communication Group name: LCG1
```

Warning

The registration token, profile name, client group name and LDT Communication Group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

13. The installation checks for Confidential Computing adapter types. If it finds one, it states:

```
The following confidential computing adapter types have been identified.
1. Intel Trust Domain Extensions (tdx)
Do you want this host to have confidential computing enabled? (Y/N) [N]:
```

Type Y to enable Confidential Computing.

14. At the Cloud Object Storage (COS) prompt, specify whether you want this client to use CTE COS.

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

15. Specify if you want to enable Ransomware Protection.

```
Do you want this host to have Ransomware Protection support enabled on the server?
```

```
ver? (Y/N) [N]:
```

16. CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.
Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption CTE Agent with
the CipherTrust Manager on 10.3.200.141.

Installation success.
```

17. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Installation and Registration on Linux with UEFI Secure Boot

If you want to install the CTE Agent software on a Linux system that has UEFI Secure Boot enabled, you must first download the appropriate Thales public certificate for your version of CipherTrust Transparent Encryption, and add that certificate to the MOK (Machine Owner Key) list.

Note

- The Thales public certificate is valid for three years from the date of issuance. Six months before the current public certificate is set to expire, Thales will release an advisory, along with the new certificate, that will become valid after the six month grace period expires. All future builds of CipherTrust Transparent Encryption will be built with the new certificate.

Warning

- You can only use the new certificate if the CTE build has been signed with the new certificate. If you are using an older version of CipherTrust Transparent Encryption that was signed with a previous certificate, then you **must** use that certificate with CipherTrust Transparent Encryption.

Public Certificate Naming Convention

The Thales public certificate name is `CTE_Secure_Boot_Cert_MM-DD-YYYY.der`:

Example

```
CTE_Secure_Boot_Cert_05-15-2023.der
```

Getting the Current Public Certificate

There are two options for getting the certificate:

Option 1: Install the DER file

1. Download the CipherTrust Transparent Encryption binaries to your local system.
2. Use the `-e` option to extract the public certificate from the downloaded binary:

```
./<cte-binary-name>.bin -e
```

Example

```
./vee-fs-7.8.0.75-95-rh8-x86_64.bin -e
```

3. Add the certificate to the MOK list.

Option 2: Convert the PEM file to DER

1. Download the certificate from the Thales public directory [CTE_Secure_Boot Repository](#)

```
curl -O https://packages.vormetric.com/pub/CTE_Secure_Boot/<certificate_name>.pem
```

Example

```
curl -O https://packages.vormetric.com/pub/CTE_Secure_Boot/CTE_Secure_Boot_Cert_05-15-2023.pem
```

Note

You can also download it from the [Thales Customer Support Portal: KB0027431](#).

2. Convert the certificate from a PEM file to a DER file using the following command:

```
openssl x509 -inform PEM -outform DER -in <certificate_name>.pem -out <certificate_name>.der
```

Example

```
openssl x509 -inform PEM -outform DER -in CTE_Secure_Boot_Cert_05-15-2023.pem  
-out CTE_Secure_Boot_Cert_05-15-2023.der
```

3. Add the certificate to the MOK list.

Adding the Certificate to the MOK List

Note

During this procedure, you **must** reboot the Linux host and then respond to a system prompt as soon as the host restarts.

1. Log into the host as **root**.
2. Add the certificate to the MOK list:

```
mokutil --import <cert-name>
```

Example

```
mokutil --import CTE_Secure_Boot_Cert_05-15-2023.der
```

3. Enter and confirm a password for this request when prompted.
4. Reboot the host and follow the instructions on the console when the host is back online. You will need to enter the password you created in the previous step when prompted. For detailed information, refer to the specific instructions from each linux distribution.

Note

If you do not respond to the system prompt to update the MOK when the host restarts, the prompt will time out and you will need to run the **mokutil** command again.

5. When prompted, reboot the host again.

6. After the host has rebooted for the second time, verify that the certificate has been properly added to the MOK list:

```
mokutil --test-key <cert-name>
```

Example

```
mokutil --test-key CTE_Secure_Boot_Cert_05-15-2023.der
```

Response

```
CTE_Secure_Boot_Cert_05-15-2023.der is already enrolled.
```

Windows Installation

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the **License Agreement** page, accept the License Agreement and click **Next**.
6. Click **Next** to accept the default folder. When you are done, click **Next**.

Note

- Thales recommends that you install CTE in the default installation directory, `C:\Program Files\Vormetric\DataSecurityExpert\agent\`
- You **must** install the CTE Agent on the same drive as Windows. For example, if Windows is installed on the **C:** drive, you must install the CTE Agent on the **C:** drive.

7. On the **Ready to Install** page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
8. On the **InstallShield Wizard Completed** page, make sure the **Register CipherTrust Transparent Encryption now** option is selected and click **Finish**. The installer opens the [Register CipherTrust Transparent Encryption](#) wizard.

Windows Registration

The following procedure describes how to register the CTE Agent after installation is complete.

Use the `register_host` utility to create certificate requests, exchange certificates between the CipherTrust Manager and the host, to enable ransomware detection, and to register CTE on the CipherTrust Manager. After the host is registered, if you selected to enable file system encryption, you can configure CTE, apply GuardPoints, or perform database backups. If you selected ransomware protection, you can apply the protection to volumes. Run the `register_host` utility in text mode on a terminal window.

Caution

The default host registration timeout is 10 minutes. If the host is unable to reach the CipherTrust Manager within the allotted period because of an extremely slow network connection, set the `REGISTER_HOST_TIMEOUT` environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

1. Log on to the host as a Windows user with administrative privileges.
2. Launch the CTE Registration Wizard using one of the following methods:
 - In the system tray, right click the CipherTrust Lock icon and select **Register Host**.
 - Run `...\register_host.exe -vmd -silent`.
3. Reboot the system. CTE automatically displays the registration wizard if CTE is not already registered.
4. In the Register Host dialog box, verify the host's machine name and click **Next**.

Note

For CipherTrust Data Security Platform Services, the host names of the services are:

- **Europe:** `ciphertrust.dpondemand.io`
- **North America:** `us1.ciphertrust.dpondemand.io`

5. On the **Gathering agent information** page, select one or both of the following options and click **Next**.
 - **File System:** Allows you to protect and encrypt CTE files with policies
 - **Ransomware Protection:** Protects volumes from ransomware
6. On the **Gathering Key Manager information** page, enter the FQDN or IP address of the primary CipherTrust Manager.

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: **<hostName>:<port#>**. For example:10.3.200.141:8445

When you are done, click **Next**. CTE communicates with the selected CipherTrust Manager to validate what features have been licensed and are available to the CTE Agent.

7. On the **Gathering host information** page:

File System

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see [Hardware Association Feature](#).
- If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the client, select **Enable LDT Feature**. For details on LDT, [CTE Agent Live Data Transformation](#).
- If you want the node to be an [Windows AccessOnly](#) node, select **Enable LDT AccessOnly Feature**.

Ransomware

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see [Hardware Association Feature](#).

When you are done, click **Next**.

8. On the **Gathering registration information** page, enter the following:

File System

- **Registration token:** The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name:** The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.
- **LDT Communication Group:** If you are planning on using LDT over CIFS/NFS on a CipherTrust Manager, enter the name of the LDT Communications Group that this node will join. See [Adding Clients to an LDT Communication Group](#) for more information.

Ransomware

- **Registration token:** The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name:** The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.

Warning

The registration information is case-sensitive. If any of it is entered incorrectly, the client registration will not succeed. If the registration fails, click **Back** in the installer and verify that the case is correct for all entries on this page.

When you are done, click **Register**. CTE contacts the CipherTrust Manager and attempts to register the client with the specified options. The Register Host dialog box displays a message with the results of the registration request.

If the registration completed successfully, click **Finish**.

9. Restart the client to complete the installation process on the client.
10. After the host has rebooted, you can verify the installation by checking CTE processes:
 - a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
 - b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.
 - If you are using CipherTrust Manager version 2.2 or later, you can now use CipherTrust Manager to administer CTE on the client.

If you are using CipherTrust Manager version 2.1 or earlier, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Guarding a Directory with CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

Note

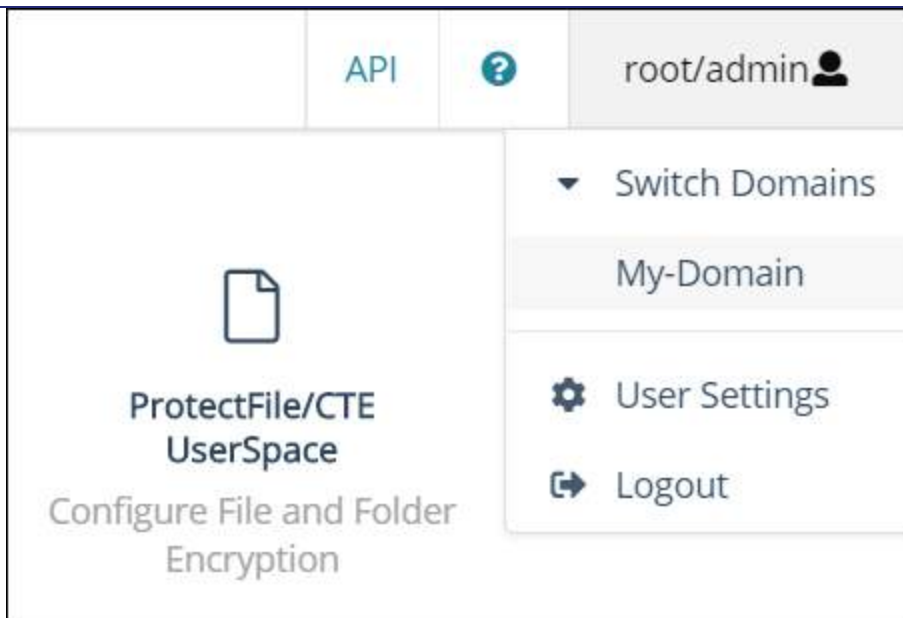
In Windows, for guarding using LDT on a local drive, or on a CIFS/Share drive, refer to the [CTE-Live Data Transformation with CipherTrust Manager](#) guide.

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

1. [Access the CipherTrust Manager domain](#) in which the client is registered.
2. [Identify or Create an Encryption Key](#) that CTE will use to encrypt the data on the device or directory.
3. [Create a Standard Policy](#) for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. [Create and Assign a GuardPoint](#) to the device or directory.

Access the CipherTrust Manager Domain

1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to [Create an Encryption Key](#). If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the user name **root/admin** on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.
 - c. The logged in user now shows the new domain name/user name.



Identify or Create an Encryption Key

1. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.

Tip

To navigate to the Products page from anywhere in the CipherTrust Manager Console, click the App Switcher icon in the top left corner.

2. Above the Key table, click **Add Key**.
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
4. In the **Key Usage** section, make sure **Encrypt** and **Decrypt** are selected.
5. Click **Add Key**. CipherTrust Manager displays the properties for the new key.
6. In the general options area, enable the **Exportable** option.

You can also enable the **Deletable** option in this section if you want a CipherTrust Manager Administrator to be able to delete the key.

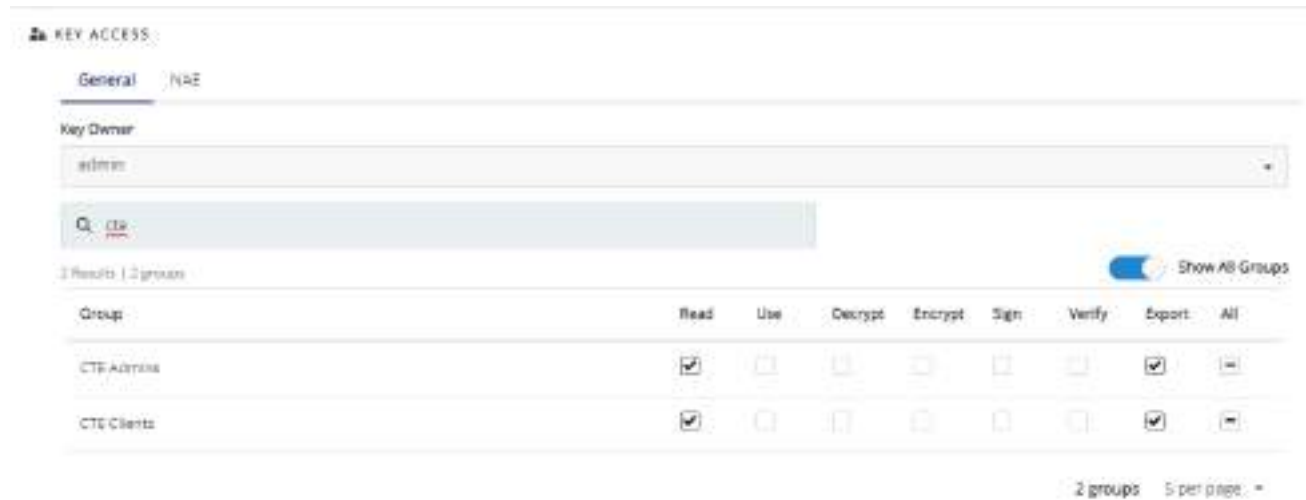
ID	2e58c582..51136313	Owner	Global	Object Type	Symmetric Key
UUID	e3ad9c3e..70d47711	Created	05 Mar 2021, 05:13	Algorithm	AES
MUID	e3ad9c3e..7b333c9f	Last Modified	05 Mar 2021, 05:13	Size	256
KeyID	N/A	Exportable	☒	Deletable	☐

7. In the **Key Access** section, do the following:

a. In the Search Groups box, type **CTE**.

If no groups display, make sure that the **Added Only** option is **disabled**.

b. Click the **Read** and **Export** option for both the CTE Admins and CTE Clients groups.



c. When you are done, click **Update**.

8. Click the **CTE** tab and set the following properties:

- **CTE Versioned:** Specify whether the key is versioned.

For a standard policy, and for CTE-U, you should clear this check box. If you do not, the key will not appear in the keys list when you add the key rule to the standard policy.

Note

CTE-U **only** supports standard and offline policies. It **does not** support LDT.

- **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.

Unselected

The keys are only stored on the disk inside the CipherTrust Manager. When required, they are downloaded to CipherTrust Transparent Encryption, but only cached in kernel memory and while encrypted. This is the default mode. The Agent continues to work even if communication to CipherTrust Manager is not active. Note that this mode requires a stable connection between CipherTrust Manager and the CipherTrust Transparent Encryption agent in case the agent is restarted, or the server is rebooted to retrieve the keys and policies from CM.

- **Selected**

In this mode, the keys are further encrypted with a derived key generated using a FIPS-approved derivation function and stored in the local protected directory which can be accessed only by CTE services and utilities. If the connection between CipherTrust Manager and CTE agent is not available, keys are recovered for service through the challenge/response mechanism.

- **Encryption Mode:** Encryption mode of the key. The options are:

- XTS/CBC-CS1
- CBC

For CTE-U, select CBC-CS1. CBC keys are supported due to legacy key requirements, but they are not recommended for CipherTrust Transparent Encryption UserSpace.

9. When you are done, click **Update**.

For creating keys through the API, see [Creating Keys](#) for more information.

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **Transparent Encryption** application.
2. In the sidebar on the Clients page, click **Policies**.
3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
4. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint.. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create.. In this example, we will create a Standard policy.
Description	A user-defined description to help you identify the policy later.. For example: Standard policy for new GuardPoints
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/LDT policies. While useful for quality assurance, troubleshooting,

Field	Description
	and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set.. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.
Data Transformation	If you select Standard as the policy type, also select the Data Transformation option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time.. This option is only displayed for Standard policies.

When you are done, click **Next**.

- On the Security Rules page, define the security rules that you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of **key_op** and the effects **Permit** and **Apply Key**. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version.

To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

When you are done, click **Next**.

- On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.

Field	Description
Current Key Name	Click Select to choose an existing key or create a new one. If the data has not yet been encrypted, select clear_key. Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select clear_key.
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

When you are done, click **Next**.

- On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click Select to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in Create an Encryption Key.

When you are done, click **Next**.

- Click **Next**.
- On the confirmation page, review the information for the policy and click **Save**.

Create Policy

1 General Info 2 Security Rules 3 Key Rules 4 Data Transformation 5 Confirmation

Review the provided policy details.

1 General Info

Name: Simple-Policy
Policy Type: Standard
Description: Standard policy for new GuardPoints

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*			key_op	permit:applykey	Yes
*					Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	Simple-Key

Back Save

Security Rule Ordering for Policies

If you want to enforce restrictions when guarding NFS/CIFS shares using an LDT or standard policy with a **CBC-CS1** key, note the following:

CipherTrust Transparent Encryption embeds the LDT and/or IV (initialization vector) attributes in the first 4K of files for NFS/CIFS shares guarded with an LDT or standard policy with a **CBC-CS1** key. Embedding CipherTrust Transparent Encryption attributes increases the actual file size by 4K. CTE hides that extra 4K when reporting the file size to users, or processes, that access the file with the Apply Key effect.

If you need the actual file size, or read/write access on the embedded header, for backup/restore processes for example, then you need a rule that permits access without Apply Key.

LDT Policies

Example 1: Permits Backup and Restore

A policy that allows backup and restore of encrypted data, clear-text access to certain processes, and denies access to all others:

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1				key_op	permit:applykey	No	
2			backup	all_ops	permit:audit	Yes	
3			authorized-processes	all_ops	permit:audit:applykey	Yes	
4				all_ops	deny:audit	Yes	

Rule	Purpose
1	Default LDT rule required for LDT policies.
2	Allows for processes in the backup Process Set to access the real file size and backup the CipherTrust Transparent Encryption attributes along with the encrypted file data.
3	Allows for processes in the authorized-processes Process Set to access the clear-text data, but it hides the additional 4K from the CipherTrust Transparent Encryption attribute.
4	Denies all other processes access to the data.

Example 2: Permits access to certain Processes

A policy that only allows certain processes clear-text access but allows all others to see the OS file attributes.

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1				key_op	permit:applykey	No	
2			authorized-processes	all_ops	permit:audit:applykey	Yes	
3				f_md_audit_md_read_r...	permit:audit	Yes	
4				all_ops	deny:audit	Yes	

Rule	Purpose
1	Default LDT rule required for LDT policies.
2	Allows for processes in the authorized-processes Process Set to access the clear-text data.
3	Allows for processes not in the authorized-processes Process Set to read the OS file and directory attributes. Note: Processes that match this rule obtain the file size with the 4K header. If a process that is not in the authorized-processes Process Set needs the file size without the header, then the Apply Key must be present in the Effect or you will need an additional rule granting Apply Key to that specific process. That rule must be defined before this rule.
4	Denies processes not in the authorized-processes

Rule	Purpose
	Process Set from reading any data from the files.

Standard Policies

Example 1: Permits access to certain Processes

A policy that allows backup and restore of encrypted data, clear-text access to certain processes, and denies access to all others:

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1			backup	all_ops	permit,audit	Yes	...
2			authorized-processes	all_ops	permit,audit,applykey	Yes	...
3				all_ops	deny,audit	Yes	...

Rule	Purpose
1	Allows for processes in the backup Process Set to access the real file size and backup the CipherTrust Transparent Encryption attributes along with the encrypted file data.
2	Allows for processes in the authorized-processes Process Set to access the clear-text data, but it hides the additional 4K from the CipherTrust Transparent Encryption attribute.
3	Denies all other processes access to the data.

Example 2: Permits access to certain Processes

A policy that only allows certain processes clear-text access but allows all others to see the OS file attributes.

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1			authorized-processes	all_ops	permit,audit,applykey	Yes	...
2				f_rd_attr_rd_sec,d_r...	permit,audit	Yes	...
3				all_ops	deny,audit	Yes	...

Rule	Purpose
1	Allows for processes in the authorized-processes Process Set to access the clear-text data.
2	Allows for processes not in the authorized-processes Process Set to read the OS file and directory attributes. Note: Processes that match this rule obtain the file

Rule	Purpose
	size with the 4K header. If a process that is not in the authorized-processes Process Set needs the file size without the header, then the Apply Key must be present in the Effect or you will need an additional rule granting Apply Key to that specific process. That rule must be defined before this rule.
3	Denies processes not in the authorized-processes Process Set from reading any data from the files.

For more information, see [Adding Security Rules](#) in the CipherTrust Manager documentation.

Using Auto Mount with Standard Policies

For CTE v7.8.0 and previous versions, Auto Mount is supported with standard policies, with CBC/CBS-CS1 keys, on both NFS and local file systems. For v7.8.0 and subsequent versions, Auto Mount will be supported with LDT.

Auto Mount is an option provided for guarding a GuardPoint. When selected, you specify the mount point, so it enables automatic guarding of the GuardPoint when accessed at that mount point, rather than immediately after policy deployment.

A GuardPoint configured with a standard policy using auto mount must use GuardPoint type: Auto Directory. The Auto Mount option is not supported with GuardPoint type: manual. When you select GuardPoint type: Auto Directory in a Linux policy, the Auto Mount option displays.

Note

For GuardPoint type: Auto raw, see [File System Mount Points on Linux](#).

Create GuardPoint[?]

Policy *

VMFSODT43-NONLDT-CONFORM-CS1

Select

Type *

Auto Directory

Path *

☒ Enter/Browse Path☐ Upload CSV

/oxf-fs1

Browse

i To apply the same GuardPoint settings to multiple paths, type paths in the Path field or specify them using the Browse button. A maximum of 200 GuardPaths can be specified.

Auto Mount



Multifactor Authentication:



Cancel

Create

Behavior of Auto Mount GuardPoints

After you push a policy on a CTE agent, if you check the status, you'll find that the auto mount GuardPoint is not yet guarded because the guard operation is not yet triggered:

```
secfsd -status guard
```

Example Response

```
GuardPoint Policy Type ConfigState Status Reason
-----
/nfs-oxf-fs1/test VMFSODT40-AUTOMOUNT-POL auto mount guarded not guarded Inactive
```

In the CTE CLI, Auto Mount is controlled by `autofs`. When `autofs` is enabled, accessing the GuardPoint

triggers the guard operation. To trigger **autofs**, type one of the following:

```
systemctl start autofs
systemd.auto mount
```

Example

```
ls /nfs-oxf-fs1/test
secfsd -status guard
```

Example Response

```

${gp} Policy Type ConfigState Status Reason
-----
/nfs-oxf-fs1/test VMFS0DT40-AUTOMOUNT-POL auto mount guarded guarded N/A

```

Note

When adding the auto mount GuardPoint, the mount point should be unmounted. If the mount point is mounted with auto mount, then you must manually **unmount** the mount point so that the next time the mount point is accessed, secfsd will guard the GuardPoint.

Limitations

- CTE does not support nested GuardPoints with auto mount enabled
- The GuardPoint path must be at the same level as the mount point when enabling auto mount on an **autofs** mount point. This ensures that auto mount unguards when the **autofs** mount point times out. If the GuardPoint path is set at any level deeper than the configured **autofs** mount point, the **autofs** mount point will never timeout because the GuardPoint will continue to keep the mount point in a busy state.

Create and Assign a GuardPoint

- Stop all applications that are accessing the directory you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:

Linux	Windows
/dir/hr/files /dir/accounting/files /dir/shared/hr /dir/shared/accounting	- C:\HR Files\ - C:\Accounting Files\ - C:\Shared Resources\HR\ - C:\Shared Resources\Accounting\

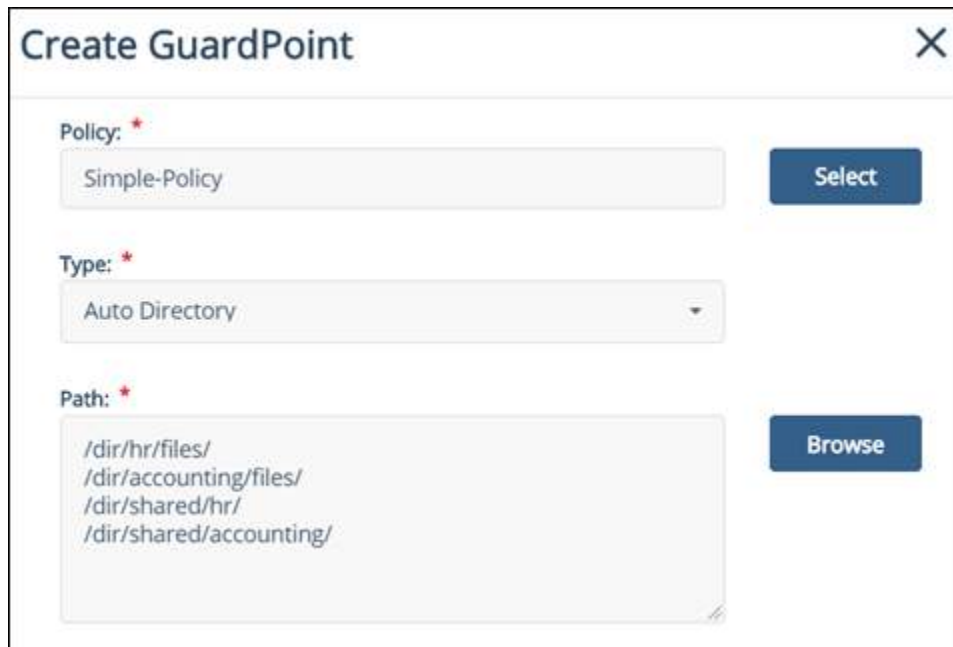
Tip

If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

2. In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
3. In the Clients table, click on the name of the client you want to protect.
4. Above the GuardPoints table, click **Create GuardPoint**.
5. In the Create GuardPoint page:
 - a. In the **Policy** field, select the policy you created earlier.
 - b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click Browse to select them from a explorer window.

If you want to enter multiple paths, put each path on its own line. For example:

Linux:



Windows:

d. Click **Create**.

e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**. For this example, click No.

The CipherTrust Manager pushes the GuardPoint configuration to the client.

6. Type the following to transform the data:

```
# dataxform --rekey --print_stat --preserve_modified_time --gp <pathToGP>
```

When the data transformation has finished, applications can resume accessing the now-protected data. (See the “CTE Data Transformation Guide” for more information.)

Using and Renewing Certificates

Certificates are used to verify the identity of a remote peer when agents communicate with CipherTrust Manager. CipherTrust Transparent Encryption and CipherTrust Manager can use internally generated or externally generated certificates.

Automatic Renewal of Client Certificates

The default lifespan of these certificates is set in CipherTrust Manager in the Registration Token section. For the automatic agent certificate renewal process to work, you must have current (not expired) and valid client certificates installed.

The system automatically renews any certificate that is **60** days or closer to expiration. VMD extracts the expiration date from the existing certificate *.pem files. If the current date is later than this renewal date, then the renewal date is the current day.

Note

- The renewal process is transparent and requires no intervention by the administrator. If multiple client agents require renewal at the same time, the clients stagger the renewal process to avoid network congestion. This staggering could introduce a delay of up to 48 hours in the renewal process.
- Certificate renewal will cause VMD to restart. When an agent restarts, or a certificate is renewed, the agent sends a system notification and a log entry.

Updating Client Certificates

You must regenerate client certificates when you:

- Configure an agent to access a new initial CipherTrust Manager
- When CipherTrust Manager updates its certificates
- Delete and reinstall agent software
- Regenerate the CA signer certificate of CipherTrust Manager

Since you are updating client certificates, the client already has certificates and the client is already registered with the initial CipherTrust Manager. The certificates on the local client will be deleted and regenerated automatically. However, you must unregister the client on the CipherTrust Manager before proceeding.

- If you are upgrading agent certificates with the same CipherTrust Manager, there is no need to disable GuardPoints.
- If you are upgrading the agent certificates with a different CipherTrust Manager, disable all configured GuardPoints for the client before proceeding. After certificate upgrade completes, assign the GuardPoints from the new CipherTrust Manager.

To update client certificates:

1. [Unenroll the client](#)
2. [Install and Register the new Agent](#)

Validating Certificates with a Local CA Certificate

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Ensure that registration by the CTE agent is serviced only by the expected key manager by providing a copy of the CA certificate that will be used to authenticate the TLS communications with the key manager.

- [Validating CipherTrust Manager and CipherTrust Transparent Encryption for Windows with a Local CA Certificate](#)
- [Validating CipherTrust Manager and CipherTrust Transparent Encryption for AIX with a Local CA Certificate](#)
- [Validating CipherTrust Manager and CipherTrust Transparent Encryption for Linux with a Local CA Certificate](#)

Replacing Certificates

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

When replacing CA certificates which have signed CTE clients, see [Certificate Renewals](#) for the proper process.

External CA Certificates

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

External certificates are used for communication between CTE and CM. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

- [AIX External Certificates](#)
- [Linux External Certificates](#)
- [Windows External Certificates](#)

Protecting Data with CTE

How to Protect Data with CTE

CTE uses policies created in the associated key manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your protected hosts. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of GuardPoints.

Policies specify:

- Whether or not the resting files are encrypted.
- Who can access decrypted files and when.
- What level of file access auditing is applied when generating fine-grained audit trails.

A Security Administrator accesses CipherTrust Manager through a web browser. You must have administrator privileges to create policies using CipherTrust Manager. The CTE Agent then implements the policies once they are pushed to the protected host.

CTE can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

How to Protect Data from Ransomware with CTE

Note

- Ransomware Protection for **Windows** is compatible with CipherTrust Manager **v2.12** and subsequent versions. It is only supported in CipherTrust Transparent Encryption v7.4.0 for **Windows** and subsequent versions.
- Ransomware Protection for **Linux** is compatible with CipherTrust Manager **v2.17** and subsequent versions. It is only supported in CipherTrust Transparent Encryption v7.8.0 for **Linux** and subsequent versions.

CipherTrust Transparent Encryption with Ransomware Protection protects data on servers and endpoints from ransomware attacks by auditing, monitoring and blocking malicious processes. Users can strengthen their security posture with CipherTrust Transparent Encryption access and encryption policies, multi-factor authentication, and Ransomware Protection for complete control of their data.

CTE Ransomware Protection is not an EDR (Endpoint Detection and Response) or XDR (Extended Detection & Response) solution which tries to prevent end-points from getting infected or track the lateral movement of the ransomware. However, CipherTrust Transparent Encryption with Ransomware Protection works well in conjunction with XDR and EDR solutions. CTE Ransomware Protection solutions performs real-time data analysis on sensitive data, calculates the entropy value of data, and determines whether the application is writing encrypted or unencrypted data. This analysis is performed using the CTE ML (Machine Learning) model and a score is assigned to the process. Based on this score, CTE either alerts the process behavior to the user or blocks process access to the data.

Warning

Ransomware Protection requires the `vmarfs.sys` driver. If you are using Ransomware Protection and you switch to the `vmfiltr.sys` driver, then you will disable Ransomware Protection.

Note

CipherTrust Transparent Encryption Ransomware Protection requires a [Flex Utility license](#) to enable Ransomware Protection within CipherTrust Manager.

Guarding a Directory with Ransomware Protection

Note

- Ransomware Protection for **Windows** is compatible with CipherTrust Manager **v2.12** and subsequent versions.
- Ransomware Protection for **Linux** is compatible with CipherTrust Manager **v2.17** and subsequent versions.

Setting Ransomware Protection GuardPoints

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

To create a Ransomware Protection GuardPoint:

1. In CipherTrust Manager, open the **Transparent Encryption** application.
2. Select the client or client group on which you want to create a GuardPoint.
 - Click an Ransomware Protection-enabled client under the **Client Name** column (**Clients > Clients**). These are the clients with either Ransomware Protection, or CTE Ransomware Protection, protection mode.
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click **Create GuardPoint**:

Note

Once Ransomware Protection is enabled during CTE registration, Ransomware Protection is applied to all GuardPoints.

Ransomware Protection is supported in 2 Protection Modes:

- **RWP:** In CipherTrust Manager, when creating a GuardPoint, you cannot assign a policy and type is automatically set to Ransomware Protection Only.
- **CTE-RWP:** On clients with **CTE RWP** mode, you can create a Ransomware Protection GuardPoint set to Ransomware Protection Only, as well as other types of GuardPoints that use policies as shown below. In Linux, Ransomware Protection is also available for other GuardPoints if the GuardPoints are set on a directory.

Status	Policy Name	Protected Path	Type	Client Group	Enabled	LSP Progress	Multi-step Authentication
+	Active	C:\Users\jdoe\Documents	Anti-Credential		Yes	100%	
+	Active	C:\Users\jdoe\Documents*.pdf	Ransomware Protection Only		Yes	100%	

4. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:

- **Enter/Browse Path:** Select this option, and enter the path by either typing or clicking the **Browse** button.

Note

- For **CTE Windows**, Ransomware Protection GuardPoints are applied at the volume level. Even if you specify the path of a folder or a file, the GuardPoint will be applied at the volume level.
- For **CTE Linux**, Ransomware Protection is applied at GuardPoint level.
- If you specify a network share, all of the network shares to be mounted subsequently will be protected.
- A CTE client administrator can configure protection of all existing GuardPoints, and those to be added to the client subsequently.
- A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

Browse Method

- Click **Browse** to select the path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths. Note that the client must be registered with CipherTrust Manager in order to browse its file system.
- In the **Enter Path** field, specify the path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.
- Click **Add**.

Manual Method

Alternatively, if you know the path, manually enter path in the given text box. Enter one path per line.

- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more paths. This is the recommended method to specify a large number of paths in one step.

Note

If a manually entered path does not yet exist, check that you entered the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.

5. Click **Create**. A message appears prompting to confirm the reuse of these GuardPoint settings on another path.
 - Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:
 - a. In the **Enter Path** field, specify the path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.
 - b. Click **Add Path**. The newly added path appears under the Paths list on the left. Similarly, add as many paths as required.
 - c. Click **OK**.
 - Click **No** if you do not want to use the same settings on another path.
6. Check the GuardPoint status, type:

```
secfsd -status guard
```



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

CTE Agent Linux Integration Guides	5
Installing CTE on Hadoop	5
Overview	6
Implementing CTE on HDFS	7
Create an Encryption Zone in HDFS Name Space for AWS EMR	8
Using the Original Information from HDFS	8
Create an HDFS Host Group and GuardPoint in CipherTrust Manager	9
Adding a New DataNode to a CTE-protected HDFS	11
Configure NameNodes	12
Take a DataNode Offline and Perform Data Transformation	15
Implementing CTE on HDFS on a Single Host	16
Deploy Cloudera Hadoop on CTE	16
HDFS Upgrade with CTE	17
Configure the Hadoop Cluster for CTE	20
Create a CipherTrust Configuration Group	20
Update the Hadoop-env Template with CTE Settings	21
Modify the HDFS IOCTL	22
Change the HDFS File Rename Check	23
User Information Push	23
Uninstalling CTE for the Hadoop Cluster	23
CTE Installation and Configuration	24
Configuring Hadoop to Use CTE	26
Deleting Metadata in HDFS when Migrating Out of LDT	28
Integrating File Activity Monitoring (FAM) with CTE Linux	30
Using CTE with Oracle	34
Basic Troubleshooting Techniques	34
Verifying Database Encryption	35
Using CTE LDT with Oracle	36
Oracle RAC ASM and ASMLib	37
Important ASM Commands and Concepts	38
Determining Best Method for Encrypting Disks	39
General Prerequisites	41
Specific Prerequisites	42
Oracle RAC ASMLib Multi-Disk Online Method	43
About Oracle RAC ASM Raw Devices	44
Oracle RAC ASM Multi-Disk Online Method	45
Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)	47
Surviving the Reboot and Failover Testing	49
Using CTE with Oracle ASM Filter Driver	50
Audience	50
Enable Oracle ASMFD for CTE	51
Configure CTE and create a guarded Oracle ASMFD	52

Convert a baseline ASMFD disk group to a CTE guarded ASMFD disk group using the Offline method	53
Convert a baseline ASMFD disk group to a CTE guarded ASMFD disk group using the Online method	55
Uninstall/ Upgrade CTE with active ASMFD Setup	58
Using Oracle with CTE-U	59
Integrating and Configuring EDB	60
Integration with Pacemaker	62
Performing CTE maintenance with an LDT GuardPoint in a Pacemaker Setup	62
Using CTE with Pacemaker	65
Using CTE with SQL Server on Linux on Red Hat 8	68
Configuring Support for SAP HANA	76
Using CTE with GlusterFS	80
NetApp Snapshot Directory	82
Using CTE with Quantum StorNext	83
Overview of using CTE with Quantum StorNext	84
CTE and Quantum StorNext Compatibility	84
Setting up CTE and Quantum StorNext Integration	86
Stop secfs Before Upgrading StorNext LAN Clients	88
Using CTE with McAfee Endpoint Security for Linux Threat Prevention	88
Using CTE and Database Activity Monitoring (DAM) Simultaneously	92
Using CTE with Trend Micro Deep Security Software	96
CTE for Cloud Object Storage	97
COS Overview and Requirements	98
CTE COS S3 Installation Overview	101
Configure the AWS CLI to use the COS Root CA Certificate	104
Guard an AWS Bucket	112
Using a COS Proxy Root CA Certificate Information	112
Protecting Python Programs with CTE	113
Enable COS on an Agent with no COS Service	115
Creating a COS Policy	115
CTE with Teradata Database Appliances	116
IDT-Capable GuardPoints and Teradata Database Appliances	117
Requirements and Considerations	117
Guarding a Teradata Database Device	120
Install CTE on the Teradata Database Appliance	121
Identify Devices to be Guarded with IDT-Capable GuardPoints	122
Select the Initial Configuration Method	122
Initialize and Guard the Database Devices Using the Standard Initialization Method	123
Automating and Reducing the Duration of Initial Data Transformation	129
Automating and Reducing the Duration of the Subsequent Data Transformations	133
Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method	136
Changing the Encryption Key on Teradata Devices	139
Access Rules to Apply on the Teradata Database Appliance	140
Replication of IDT Metadata Files Across Members of a Clique	143

Best Practices	145
Uninstalling CTE from the Teradata Cluster	146
Alerts and Errors	148
Generating IDT-capable Metadata for Teradata Storage Expansion	150
Confidential Computing: Integrating Intel® Tiber™ Trust Services and Intel TDX, with Microsoft Azure or Google Cloud Platform	151
Integrating with Intel® Tiber™ Trust Services and Intel TDX for Confidential Computing	171

CTE Agent Linux Integration Guides

This document covers the following information:

- Confidential Computing: Integrating Intel® Tiber™ Trust Services and Intel TDX, with Microsoft Azure or Google Cloud Platform
- Integrating File Activity Monitoring (FAM) with CTE Linux
- Installing CTE on Hadoop
- Using CTE with Oracle
- Integrating and Configuring EDB
- Integration with Pacemaker
- Using CTE with SQL Server on Linux on Red Hat 8
- Configuring Support for SAP HANA
- Using CTE with GlusterFS
- NetApp Snapshot Directory
- Using CTE with Quantum StorNext
- Using CTE with McAfee Endpoint Security for Linux Threat Prevention
- Using CTE with Trend Micro Deep Security Software
- Using CTE and Data Activity Monitoring (DAM) Simultaneously
- CTE for Cloud Object Storage
- CTE with Teradata Database Appliances

Solutions Guides

Solutions guides have been moved to the [Use Cases](#) section.

Installing CTE on Hadoop

This section describes how to protect an HDFS cluster with CTE. It contains the following topics:

- Overview
 - Implementing CTE on HDFS
-

-
- Deploy Cloudera Hadoop on CTE
 - HDFS Upgrade with CTE
 - CTE Installation and Configuration
 - Deleting Metadata in HDFS when Migrating Out of LDT

Overview

The Hadoop Distributed File System (HDFS) is a file system that supports large files and directory structures distributed across hundreds, or even thousands, of commodity *DataNode* hosts in a cluster. Previously, CTE could only protect directories and files on the *local file system* rather than the actual HDFS files and directories. Now, CTE can protect *HDFS* files and directories.

A CipherTrust Manager can:

- Define an encryption policy for HDFS files and directories in HDFS name space.
- Selectively encrypt HDFS folders with different keys providing multi-tenancy support.
- Define user-based I/O access control rules for HDFS files in HDFS name space.

At the heart of an HDFS cluster is the *NameNode* that provides the framework to support a traditional hierarchical file and directory organization. The NameNode is a master server that manages the HDFS name space and regulates access to files by clients.

HDFS files are split into one or more data blocks that are distributed across *DataNode* hosts in a cluster. The NameNode maintains the namespace tree and the mapping of data blocks to DataNodes. To deploy CTE, install CTE on all of the NameNode and DataNode hosts in a cluster.

Overview of CTE on HDFS

The following sections list the high-level steps for implementing CTE protection on your HDFS. The process requires that the HDFS Administrator and CipherTrust Manager to work in tandem to complete separate tasks.

You can keep the HDFS cluster alive a active if you enable HDFS data replication and activate the nodes individually. Following are the high-level steps:

HDFS Administrator

1. Compile a list of directories specified by `dfs.datanode.data.dir`. If these directories do not already exist in the NameNode local file system, create them.
2. Pass the directory list to the CipherTrust Manager.
3. Ask CipherTrust Manager to:
 - a. Add the NameNode to the HDFS host/client group.
 - b. Create a GuardPoint for the HDFS host/client group on each of these directories.

Administrator

1. Create an HDFS host/client group to contain the HDFS nodes.
2. Create a host/client group GuardPoint on each of the datanode directories obtained from the previous step.
3. Add the NameNode to the HDFS host/client group.

HDFS Administrator

1. For each DataNode, take the node offline and perform a data transformation.
2. Ask the Administrator to add the DataNode to the host group. (After the DataNode is added to the host group, it can be brought online.)
3. Repeat this process until all of the nodes have been encrypted and added to the HDFS Host Group.
4. Modify the host group policies to protect specific HDFS files and directories, as needed.

Implementing CTE on HDFS

This section describes how to implement CTE protection on your HDFS NameNode or DataNode. If you enable HDFS data replication, protecting one node at a time allows you to maintain the HDFS cluster. When all of the nodes are configured, you can create GuardPoints on specific HDFS files and directories.

These instructions require that the HDFS Administrator and Administrator work in tandem to complete separate tasks.

Note

The instructions below assume that each NameNode and DataNode exist on their own separate host. If you have a NameNode and DataNode on the same host, see [Implementing CTE on HDFS on a Single Host](#).

CTE on HDFS Implementation Assumptions

- You have installed, configured and registered CTE on all of the NameNodes and DataNodes in the Hadoop cluster.
- The HDFS Administrator has knowledge and experience with HDFS and Ambari.
- The CipherTrust Manager Administrator has knowledge and experience with CTE.
- The two can work and communicate in tandem with each other.

Create an Encryption Zone in HDFS Name Space for AWS EMR

HDFS requires the following manual steps if you want to have an encryption zone in the HDFS name space for AWS EMR, (Elastic MapReduce).

1. Add the following properties to `hdfs-site.xml`.

```
dfs.vte.ioctl.lib vorhdfs dfs.vte.rename.check true dfs.vte.ioctl.device <.sec folder name, up to the CTE installation location>
```

Note

The default .sec folder is `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec`

2. Save the file.
3. Restart HDFS NameNode and DataNode services.

Using the Original Information from HDFS

Update or add the following properties to `hdfs-site.xml` if you want CTE to use the original user information from HDFS.

1. Add the following properties to `hdfs-site.xml`.

```
<property>
  <name>dfs.block.access.token.enable</name>
  <value>true</value>
</property>
<property>
  <name>dfs.client.read.shortcircuit</name>
  <value>false</value>
</property>
<property>
  <name>dfs.vte.user.push</name>
  <value>true</value>
</property>
```

2. Save the file.
3. Restart HDFS NameNode and DataNode services.

Create an HDFS Host Group and GuardPoint in CipherTrust Manager

After configuring the NameNodes, the next steps in activating CTE on HDFS is for the security administrator. To create a client group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Click **Create Client Group**. The Create Client Group dialog box displays.
4. Enter a unique **Name** for the client group.
5. Select the **Cluster Type**: HDFS
 - a. **NON CLUSTER**: Creates a non-clustered client group.
 - b. **HDFS**: Creates a clustered client group. An HDFS client group is required to apply GuardPoints on CTE clients in an HDFS cluster.
6. (Optional, displayed if a profile already exists) From the Client Profile drop-down list, select the desired client profile. The default profile is DefaultClientProfile.
7. (Optional) Provide Description to identify the client group. The maximum length can be 256 characters.
8. Click **Create**. The client group is created.
9. Add the NameNode obtained from the HDFS Admin to the HDFS Client Group.

Note

Thales highly recommends using Auto Guard for HDFS. You can use manual guards, but this might result in data corruption if some nodes in a running cluster are guarded, while others are not.

Notes for HDFS Cluster Policies

The following screenshot depicts a valid HDFS policy. You can build a similar policy for your system:

The policy uses the following rules:

- For the user set hdfs-dev-user, the action is all_ops, the effect is Audit, Apply Key, Permit
- For other users the action is READ, the effect is Permit
- For the resource set hdfs-data-1, the key is hdfs-key-1
- For the resource set hdfs-data-2, the key is hdfs-key-2

Create Policy

1 General Info

2 Security Rules

3 Key Rules

4 Confirmation

Review the provided policy details.

1 General Info

Name: hdfs-dev-enc

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
	hdfs-dev-user		all_ops	permit,audit,applykey	Yes
			read	permit	Yes

3 Key Rules

Resource Set	Key Name
hdfs-data-1	hdfs-key-1
hdfs-data-2	hdfs-key-2

Back

Save

Additional Settings for HDFS (Linux Clients)

Depending on the Hadoop security authentication mode, additional settings are needed for CTE clients in an HDFS cluster. Add the following settings as appropriate.

!!! note

`/usr/jdk64/jdk1.8.0\_40/bin/java` is the Java executable used to launch the HDFS services. Change the Java jdk path to reflect your end-user environment.

- Sample setup when `hadoop.security.authentication` mode is simple.

```
|authenticator+arg=+class=org.apache.hadoop.hdfs.server.namenode.NameNode|/usr/
jdk64/jdk1.8.0_40/bin/java
      |authenticator+arg=+class=org.apache.hadoop.hdfs.server.datanode.Da
taNode|/usr/jdk64/jdk1.8.0_40/bin/java
```

- Sample setup when `hadoop.security.authentication` mode is Kerberos.

```
|authenticator+arg=+class=org.apache.hadoop.hdfs.server.namenode.NameNode|/usr/
jdk64/jdk1.8.0_40/bin/java
      |authenticator+arg=+class=org.apache.hadoop.hdfs.server.datanode.Se
```

```
cureDataNodeStarter|/usr/lib/bigtop-utils/jsvc
```

Adding a New DataNode to a CTE-protected HDFS

Use the following procedure to add a new DataNode to a CTE-protected HDFS. If not followed, HDFS encrypted files could be exposed in cleartext.

Note

If you already have CTE installed on the cluster nodes before Ambari installs the Hadoop software, see [Install CTE on the Cluster Nodes before Ambari Installs Hadoop](#).

1. Install the HDFS client on the host. This option is available in Ambari when adding a new DataNode to the cluster.
2. Add the new node to the CipherTrust Manager database and make sure that host/client settings of the new node is the same as existing nodes in the cluster. See the *CTE Installation for Hadoop chapter in the CTE Installation and Configuration Guide*.
3. Install CTE on the new node, register to CipherTrust Manager, and run `config-hadoop.sh` to prepare the libraries. See the *Configuring Hadoop to use CTE* section in the *CTE Installation and Configuration Guide*.
4. Make sure that the data directories (specified in `dfs.datanode.data.dir` property) exist on the new node. They must have the same permission and ownership as the other existing nodes in the cluster. If necessary, create them.
5. Add the host/client to the HDFS Host Group that is guarding the cluster. This is important: Do not rely on the DataNode to create the data directories as the data replication can occur before the GuardPoints are in effect.
6. Add the DataNode service to the new node. Again this option is available through Ambari.
7. If using Kerberos, check that the keytab files are created correctly.
8. Start the DataNode service on the new node.
9. Execute some `hdfs dfs` shell commands to ensure that encryption/decryption of data works correctly.

Install CTE on the Cluster Nodes before Ambari Installs Hadoop

If CTE is already installed on the cluster nodes before Ambari installs the Hadoop software, Ambari can mistakenly pick up the `.sec` directory in configuration steps to store the HDFS data. Make sure the following properties do not contain the `.sec` directory:

- DataNode data directory

-
- NameNode data directory
 - Secondary NameNode checkpoint directory
 - Zookeeper directory
 - `yarn.nodemanager.local-dirs`
 - `yarn.nodemanager.log-dirs`
 - `yarn.timeline-service.leveldb-timeline-store.path`
 - `yarn.timeline-service.leveldb-state-store.path`

Note

This list is not exhaustive. Depending on the Hadoop ecosystem packages installed, there can be others.

Configure NameNodes

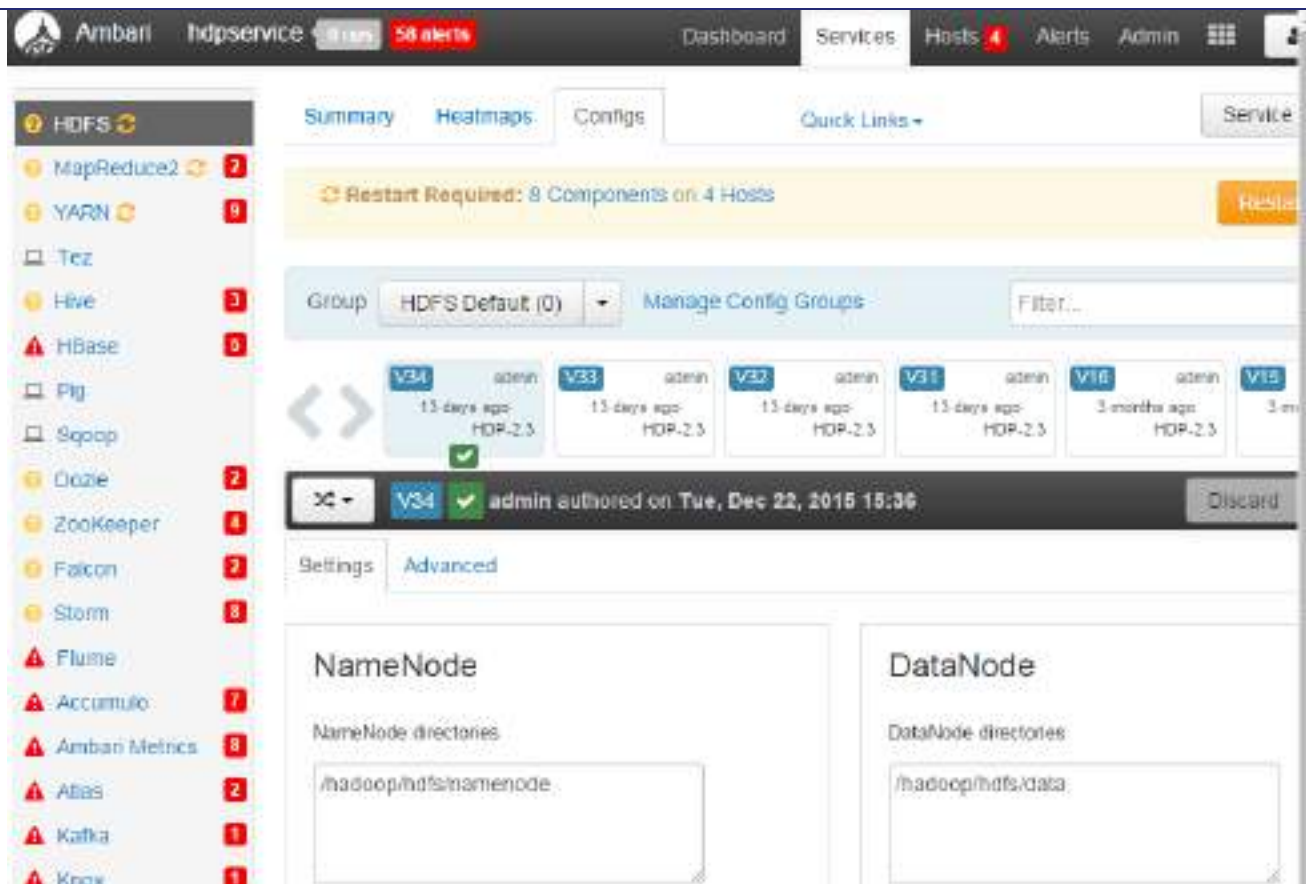
For both HDFS and Cloudera, you must configure the namenodes.

Configure the Ambari Hadoop NameNodes

The first step to implementing CTE on HDFS is for the **HDFS Administrator** to compile a list of the DataNode HDFS local file system directories, and create them on the NameNode local file systems. After this, the Administrator must add the NameNodes to an HDFS Host Group:

1. Compile a list of directories specified by `dfs.datanode.data.dir`. Obtain this from `hdfs-site.xml` or using Ambari go to:

HDFS > Configs > Settings > DataNode > DataNode directories



2. If these directories do not already exist in the NameNode local file system, create them on each NameNode in your Hadoop cluster.
3. Pass the following information to the Administrator:
 - The directory list and instructions to create a GuardPoint for the HDFS Host Group on each of these directories.
 - Instructions to add the NameNodes IP addresses or host names to the HDFS Host Group.

Create and Configure the Cloudera Hadoop Namenodes and Datanodes

Create the role groups CTE on Cloudera Manager:

1. Create a new role group for the Thales-namenode.
 - a. **Group Name:** thales-namenode
 - b. **Role Type:** NameNode
 - c. **Copy from:** NameNode Default Group
2. Move the name nodes to the group Thales-namenode.

3. Create a new role group for the Thales-datanode.
 - a. **Group Name:** thales-datanode
 - b. **Role Type:** DataNode
 - c. **Copy from:** DataNode Default Group
4. Move the data nodes to the group thales-datanode.

Configure the Thales-namenode group

1. In the **NameNode Environment Advanced Configuration Snippet (Safety Valve)** dialog, in the thales-namenode field:

```
HADOOP_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent"
```

2. In the **NameNode Advanced Configuration Snippet (Safety Valve)** for hdfs-site.xml, add the following values:

```
<property><name>dfs.vte.ioctl.device</name><value>/opt/vormetric/DataSecurityExpert/agent/secfs/.sec</value></property>
<property><name>dfs.vte.ioctl.lib</name><value>vorhdfs</value></property>
<property><name>dfs.vte.rename.check</name><value>true</value></property>
<property><name>dfs.block.access.token.enable</name><value>true</value></property>
```

Configure the Thales-datanode group

1. In the **DataNode Environment Advanced Configuration Snippet (Safety Valve)** dialog, in the thales-namenode field:

```
HADOOP_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent"
```

2. In the **DataNode Advanced Configuration Snippet (Safety Valve)** for hdfs-site.xml, add the following values:

```
<property><name>dfs.vte.ioctl.device</name><value>/opt/vormetric/DataSecurityExpert/agent/secfs/.sec</value></property>
<property><name>dfs.vte.ioctl.lib</name><value>vorhdfs</value></property>
<property><name>dfs.vte.user.push</name><value>true</value></property>
```

```
<property><name>dfs.block.access.token.enable</name><value>true</value></property>
```

Take a DataNode Offline and Perform Data Transformation

The next step in activating CTE on HDFS is to switch a DataNode to offline and transform (encrypt) its sensitive data. Once the data is transformed, the HDFS Admin can add the DataNode to the HDFS Host/Client Group. Then they can switch the DataNode back to online. Most of these procedures are completed by the **HDFS Administrator** although one is done by the Administrator.

1. **HDFS Administrator:** Switch a DataNode to offline.
2. **HDFS Administrator:** Encrypt the files in the directories specified by `dfs.datanode.data.dir` (see [Configure NameNodes](#)).
3. **Administrator:** Create encryption keys and a data transformation policy to transform the data.

**** CipherTrust Manager****

The screenshot shows the 'Create Policy' interface with five steps: General Info, Security Rules, Key Rules, Data Transformation, and Confirmation. The 'Data Transformation' step is active, showing a table of transformation rules.

General Info

Name: hdfs-dev-did
Policy Type: Standard
Description:

Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*			key_op	permit,applykey	Yes

Key Rules

Resource Set	Current Key Name
hdfs-data-1	clear_key
hdfs-data-2	clear_key

Data Transformation Rules

Resource Set	Transformation Key Name
hdfs-data-1	hdfs-key-1
hdfs-data-2	hdfs-key-2

Back Save

4. **Administrator:** After encrypting the data in those directories, add the DataNode host to the HDFS client group.

5. **HDFS Admin:** After the DataNode is added to the HDFS client group, activate the DataNode online.
6. Repeat this procedure for all of the DataNodes in your HDFS cluster.

For more information, see the [CipherTrust Manager documentation](#).

Implementing CTE on HDFS on a Single Host

It is possible, though not recommended, that an HDFS NameNode and DataNode exist as separate processes on the same host. If this is your deployment, use the following CTE deployment guidelines:

1. Configure the HDFS NameNodes (see [Configure NameNodes](#)):

Note

The directories specified by `dfs.datanode.data.dir` already exist on the local file system so you do not have to create them.

2. Pass the following information to the Administrator:
 - The `dfs.datanode.data.dir` directory list and instructions to create a GuardPoint for the HDFS Host Group on each of these directories.
 - Instructions to add the NameNodes IP addresses, or host names, to the HDFS Host Group.
3. Create an HDFS host/client group and host/client group GuardPoint:
 - a. Administrator must create an HDFS Host Group to contain the HDFS nodes.
 - b. The Administrator must create a GuardPoint for the Host Group on each of the directories specified by `dfs.datanode.data.dir`
4. Take the DataNode offline and perform a data transformation.
5. Add the NameNode/DataNode host/client to the host/client group.

Deploy Cloudera Hadoop on CTE

Deploying Cloudera Hadoop (CDP) on CTE consists of multiple steps that are documented in various locations. The following is the order that you should follow when installing CDP on CTE and links to the relevant documentation.

1. Deploy CDP 7 (Hadoop 3.1.1) cluster on RHEL 7.8 or RHEL 8.5, see the [CDP Private Cloud Base Installation Guide](#)
2. Configure Hadoop configuration for CTE, see [Configure NameNodes](#)

3. Cipher Trust Manager configuration, see [CipherTrust Manager Documentation](#)
4. CTE Installation and registration, see [CipherTrust Transparent Encryption \(CTE\) Documentation Set](#)
5. LDT, see [CTE Live Data Transformation with CipherTrust Manager](#)

HDFS Upgrade with CTE

To upgrade Hadoop, configure CTE to integrate with the new HDFS instance.

Upgrading one node at a time

Once CTE is installed and configured on the node:

1. Make sure that HDFS services are shut down on the node.
2. Upgrade **Hadoop**.
3. Type:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/bin/config-hadoop.sh -i -y
```

4. Start HDFS services on the node.

Upgrade CTE with LDT in an HDFS Cluster

If you are using LDT with HDFS cluster, follow these steps when upgrading CTE, in order to maintain your LDT GuardPoints.

1. Suspend rekey on all data nodes.
2. Shutdown your name nodes/data nodes.
3. Upgrade CTE in the name node first.

Note

Always upgrade name nodes before data nodes.

4. After CTE upgrade succeeds, type:

```
config-hadoop.sh -i -y
```

5. On the Ambari admin console, start the name node.
6. Verify that the CipherTrust java process successfully launched in the name node. (You should not see an error message.) Type:

```
ps -ef | grep java | grep vormetric
```

7. Check the CipherTrust Manager status. It should show LDT rekeyed status.
8. Check the name node status. It should display the GuardPoint status and match the state before upgrade. Type:

```
secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/hadoop/hdfs/data	LDT_HDFS_Sanity	local	guarded	guarded	N/A

9. Repeat the above steps for all of the data nodes in the HDFS cluster.

Rolling Upgrades

Hortonworks Data Platform has introduced rolling upgrades to automate the Hadoop upgrade process (<http://bit.ly/2pQrFo3>). The upgrade process is controlled by the Upgrade Pack (<http://bit.ly/2rkutvF>) that is predefined and certified by Hortonworks.

To integrate CTE with the upgrade, you need to temporarily change the Ambari scripts before performing the rolling upgrades and then restore the scripts after the upgrades.

1. On Ambari server machine, type:

```
cd /var/lib/ambari-server/resources/common-services/HDFS/2.1.0.2.0/package/scripts
```

2. Copy the utils.py file, type:

```
cp utils.py utils.py.org
```

3. Using a text editor, add the following commands to `utils.py`:

```
if action == "start":
    if name == "namenode" or name == "datanode":
        Execute(format("secfs/hadoop/bin/c onfig-hadoop.sh
        -i -h {hadoop_bin}/../ -j <java home> -p hdp -d", not_if=service_is_up,
        user=params.root_user)
```

```
# For Redhat 6.x, uncomment the following command
# Execute(format("/etc/init.d/secfs secfsd restart"),
not_if=service_is_up, user=params.root_user)
# For Redhat 7.x, uncomment the following command
# Execute(format("/secfs restart"), not_if=service_is_up,
user=params.root_user)
before
Execute(daemon_cmd, not_if=service_is_up, environment=hadoop_env_exports
The Java home of your HDFS instance should be used to replace <java home>:
if action == "start":  if name == "namenode" or name == "datanode":
Execute(format("secfs/hadoop/bin/config-hadoop.sh -i -h {hadoop_bin}
../ -j <java home> -p hdp -d"), not_if=service_is_up,
user=params.root_user)
# For Redhat 6.x, uncomment the following command
# Execute(format("/etc/init.d/secfs secfsd restart"),
not_if=service_is_up, user=params.root_user)
# For Redhat 7.x, uncomment the following command
# Execute(format("/secfs restart"), not_if=service_is_up,
user=params.root_user)
Execute(daemon_cmd,
    not_if=service_is_up,
    environment=hadoop_env_exports)
```

4. Type:

```
ambari-server restart
```

5. Perform rolling upgrades.
6. During the upgrade process, many of the intermediate service status checks can fail. Skip over them by clicking on **Proceed to Upgrade**.
7. Click **Finalize** to complete the upgrade. If the active NameNode fails to activate due to the incompatible HDFS layout version, manually start the NameNode with '**-upgrade**' option to correct the layout version file.

```
/var/lib/ambari-server/ambari-sudo.sh su hdfs -l -s /bin/bash -c 'ulimit -c u
nlimited ; /usr/hdp/current/hadoop-client/sbin/hadoop-daemon.sh --config /usr/
hdp/current/hadoop-client/conf start namenode -upgrade'
```

8. If there are excessive under-replicated blocks, run the following command to isolate them and manually start the replication:

```
su - <$hdfs_user>
```

```
# hdfs fsck / | grep 'Under replicated' | awk -F':' '{print $1}' >> /tmp/under_replicated_files
# for hdfsfile in `cat /tmp/under_replicated_files`; do echo "Fixing $hdfsfile"; hadoop fs -setrep 3 $hdfsfile; done
```

9. Restart the HDFS services. Wait for the replication to complete and the NameNodes to exit safe mode.
10. When Hbase is restarted after upgrades, it tries to rename from: `/apps/hbase/data/.tmp/data/hbase/namespace` to: `/apps/hbase/data/data/hbase/namespace`, which may cause key conflict if the GuardPoint is set incorrectly (for example, `/apps/hbase/data/data` is guarded, but not `/apps/hbase/data/.tmp`). This results in Hbase shutting down.

Before re-starting Hbase, make sure that the GuardPoint policies on the Hbase files are set correctly to cover all Hbase-related files. A broader GuardPoint (`/apps/hbase/data` instead of just `/apps/hbase/data/data` and other folders) could fix this issue.

11. Check cluster upgrade by verifying the `hadoop version`.
12. Run a few map reduce jobs and Hbase commands to make sure that the entire Hadoop stack is working properly.
13. Rename `utils.py.org` to `utils.py`

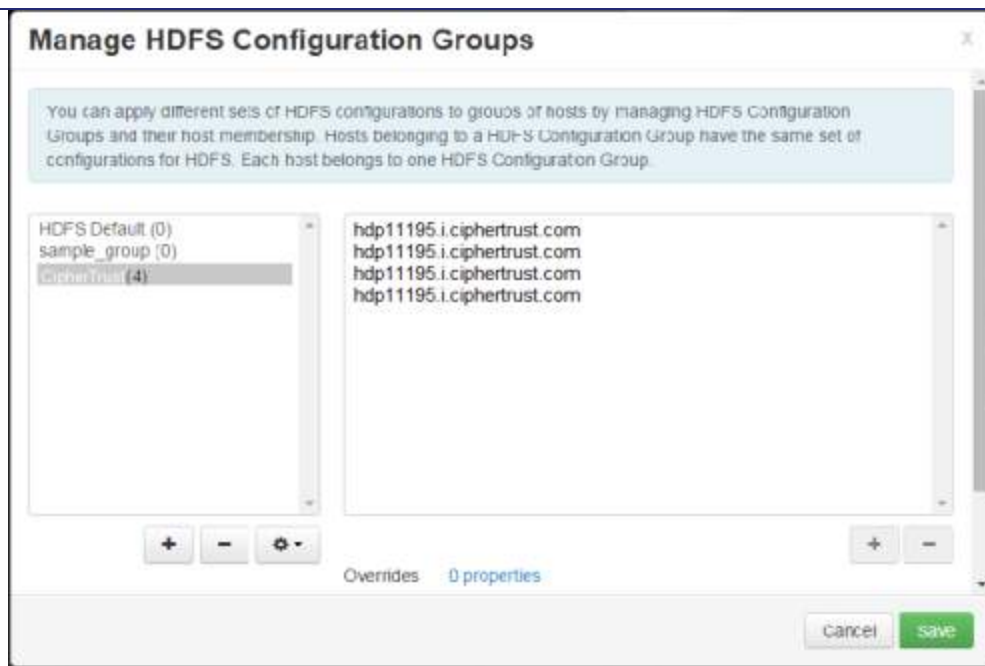
Configure the Hadoop Cluster for CTE

Configure the Hadoop cluster to use CTE before installing and configuring CTE on the nodes. Use Ambari to perform this configuration.

Create a CipherTrust Configuration Group

The CipherTrust Configuration Group will eventually contain all of the hosts in your Hadoop cluster. At first you create an empty group. Later you populate it with the hosts on which you will install and configure agents.

1. On Ambari, go to **HDFS > Configs > Manage Config Groups**.
2. Add a new configuration group: *CipherTrust*.
3. Make the group, *CipherTrust*, the current group.



Update the Hadoop-env Template with CTE Settings

1. Go to **HDFS > Configs > Advanced > Advanced hadoop-env > hadoop-env template**.
2. Copy and paste the original **hadoop-env** templates into the Thales template and add the following two export lines to specify that the CTE Java agent is instrumented into NameNode and DataNode.

```

hadoop-env template
for jarFile in `ls /usr/share/java/*mysql* 2>/dev/null`
do
    JAVA_JDBC_LIBS=$(JAVA_JDBC_LIBS) $jarFile
done

# Add libraries required by oracle connector
for jarFile in `ls /usr/share/java/*ojdbc* 2>/dev/null`
do
    JAVA_JDBC_LIBS=$(JAVA_JDBC_LIBS) $jarFile
done

export HADOOP_CLASSPATH=$(HADOOP_CLASSPATH) ${JAVA_JDBC_LIBS}

# Setting path to hdfs command line
export HADOOP_LIBEXEC_DIR=${hadoop_libexec_dir}

# Mostly required for hadoop 2.0
export JAVA_LIBRARY_PATH=${JAVA_LIBRARY_PATH}

export HADOOP_OPTS="-Dhdp.version=$HDP_VERSION $HADOOP_OPTS"

do
    JAVA_JDBC_LIBS=$(JAVA_JDBC_LIBS) $jarFile
done

export HADOOP_CLASSPATH=$(HADOOP_CLASSPATH) ${JAVA_JDBC_LIBS}

# Setting path to hdfs command line
export HADOOP_LIBEXEC_DIR=${hadoop_libexec_dir}

# Mostly required for hadoop 2.0
export JAVA_LIBRARY_PATH=${JAVA_LIBRARY_PATH}

export HADOOP_OPTS="-Dhdp.version=$HDP_VERSION $HADOOP_OPTS"

#-----vormetric-----
export HADOOP_NAMENODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_NAMENODE_OPTS}"
export HADOOP_DATANODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_DATANODE_OPTS}"
#-----vormetric-----

```

```

export HADOOP_NAMENODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_NAMENODE_OPTS}"
export HADOOP_DATANODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_DATANODE_OPTS}"

```

Modify the HDFS IOCTL

1. Go to **HDFS > Configs > Advanced > Custom hdfs-site**.
2. In the **dfs.vte.ioctl.lib** field, type: `vorhdfs`
3. In the **dfs.vte.ioctl.device** field, type:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec
```

Change the HDFS File Rename Check

1. Go to **HDFS > Configs > Advanced > Custom hdfs-site**.
2. Set **dfs.vte.rename.check** to **true**

User Information Push

You only need this configuration if you want to use the original user information with HDFS operation for IO access check.

Note

It has a performance cost.

1. Go to **HDFS > Configs > Advanced > Advanced hdfs-site** and uncheck **HDFS Short-circuit read**.
2. Set **dfs.block.access.token.enable** to **true**.
3. Go to **HDFS > Configs > Advanced > Custom hdfs-site** and set **dfs.vte.user.push** to **true**.

Uninstalling CTE for the Hadoop Cluster

This section explains how to remove CTE and restore the environment back to the non-CTE cluster environment. Thales recommends uninstalling the agent from HDFS nodes one by one, starting from the DataNode. Uninstall the agent from the NameNode last.

1. Shut down one DataNode.
2. Perform the normal agent uninstall procedure.
3. Go to Ambari, remove the DataNode host from the CipherTrust Configuration Group.
4. Start the DataNode.
5. Delete the CipherTrust Configuration Group from Ambari when agent is uninstalled from all DataNodes.
6. Repeat these steps for each DataNode.
7. Repeat these steps for each NameNode.

CTE Installation and Configuration

After configuring the Hadoop cluster for CTE:

1. Install and register CTE on the HDFS nodes.
 - You can do this to all the nodes at once, but the HDFS is unavailable during CTE installation and configuration.
 - You can also do this one node at a time. If you install and register CTE nodes one at a time, you must start from NameNode, then DataNode, and always keep NameNode service up once NameNodes are configured.
2. In either case, add the FQDN of the node to the CipherTrust Configuration Group, then proceed with agent installation and configuration. See [Installing and Configuring CTE on an HDFS Node](#).
 - Modify the Host Group. See [Modifying host settings for HDFS hosts on the CipherTrust Manager](#).
 - Configure CTE by running `config-hadoop.sh` on the HDFS node. See [Configuring Hadoop to Use CTE](#).
 - Review the SecFS configuration variables that support the HDFS name cache. [HDFS Name Cache](#).

Installing and Configuring CTE on an HDFS Node

1. Using Ambari, add the FQDN of the node to the CipherTrust Configuration Group. See [Create a CipherTrust Configuration Group](#).
2. Install, configure, and register CTE.
3. Modify the host settings for each node. See [Modifying host settings for HDFS hosts on the CipherTrust Manager](#).

Modifying host settings for HDFS hosts on the CipherTrust Manager

The Hadoop service can start as root and then downgrade to an unprivileged user. If the unprivileged user is not authenticated by password, CTE flags the user as fake. CTE cannot allow a user to access a resource protected by a user rule when the user is faked, even if the user matches the permit rule. Because of this, modify the CipherTrust Manager host/client setting as follows:

- On Ambari, go to **HDFS > Configs > Advanced > Advanced core-site** and find out if `hadoop.security.authentication` mode is set to **simple** (no authentication) or **Kerberos**.

Modifying host settings for alternate versions of Java

Sometimes, you may have more than one version of Java installed on your systems. This can create issues while using Hadoop, which uses Java to launch different services.

CipherTrust Transparent Encryption expects the following version of Java to be installed on a system:

```
/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.252.b09-2.el7_8.x86_64/jre/bin/java
```

If you have a different version of java installed on any of your systems, then you must perform a simple modification and add authenticators to the Host settings section in CipherTrust Manager for that version of Java as well. See the following section for more information.

Simple Modification

To use a **simple** modification, ask the Administrator to add the following lines to the host/client group:

```
`/usr/jdk64/jdk1.8.0_40/bin/java` is the Java executable used to launch the HDFS services. Change the Java jdk path to reflect your end-user environment.
```

```
|authenticator+arg+=+class=org.apache.hadoop.hdfs.server.namenode.NameNode|
|usr/jdk64/jdk1.8.0_40/bin/java
|authenticator+arg+=+class=org.apache.hadoop.hdfs.server.datanode.DataNode|
|usr/jdk64/jdk1.8.0_40/bin/java
```

The entire host/client settings will look like this:

```
|authenticator|usr/sbin/sshd
|authenticator|usr/sbin/in.rlogind
|authenticator|bin/login/
|authenticator|usr/bin/gdm-binary
|authenticator|usr/bin/kdm
|authenticator|usr/sbin/vsftpd

|authenticator+arg+=+class=org.apache.hadoop.hdfs.server.namenode.NameNode|usr/jdk
64/jdk1.8.0_40/bin/java
|authenticator+arg+=+class=org.apache.hadoop.hdfs.server.datanode.DataNode|usr/jd
k64/jdk1.8.0_40/bin/java
```

Modifying Host Group for HDFS NameNodes HA on CipherTrust Manager

To enable high availability (HA) for your HDFS NameNodes, ask the Administrator to add the following lines to the host/client group.

```
`/usr/jdk64/jdk1.8.0_40/bin/java` is the Java executable used to launch the HDFS services. Change the Java `jdk` path to reflect your end-user environment.
```

```
|authenticator+arg+class=org.apache.hadoop.hdfs.qjournal.server.JournalNode|us
r/jdk64/jdk1.8.0_40/bin/java
|authenticator+arg+class=org.apache.hadoop.yarn.server.applicationhistoryservic
e.ApplicationHistoryServer|usr/jdk64/jdk1.8.0_40/bin/java
|trust+arg+=+class=org.apache.hadoop.hdfs.tools.DFSZKFailoverController|usr/jdk6
4/jdk1.8.0_40/bin/java
```

The entire host/client group for HA (in this example, with Kerberos) will look like this:

```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login/
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
|authenticator|/usr/sbin/vsftpd

|authenticator+arg+class=org.apache.hadoop.hdfs.server.namenode.NameNode|/usr/jdk
64/jdk1.8.0_40/bin/java
|authenticator+arg+=+class=org.apache.hadoop.hdfs.server.datanode.SecureDataNodeSt
arter|/usr/lib/bigtop-utils/jsvc
|trust+arg+class=org.apache.hadoop.hdfs.qjournal.server.JournalNode|/usr/jdk64/jd
k1.8.0_40/bin/java
|trust+arg+=+class=org.apache.hadoop.yarn.server.applicationhistoryservice.Applica
tionHistoryServer| \
/usr/jdk64/jdk1.8.0_40/bin/java
|trust+arg+=+class=org.apache.hadoop.hdfs.tools.DFSZKFailoverController|/usr/jdk6
4/jdk1.8.0_40/bin/java
```

Configuring Hadoop to Use CTE

1. On the HDFS node, type:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/bin/config-hadoop.sh -i.
```

HDFS prompts you for the following information:

- **Hadoop product name:** (i.e. *hdp*)
- **Hadoop product version:** (i.e. *2.6.0.2.2.0.0-2041*)
- **Path to JAVA_HOME used by Hadoop:** (i.e. */usr/jdk64/jdk1.8.0_40*)

Note

Alternatively, you can use the automated installation option:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/bin/config-hadoop.sh -i -p hdp -v
2.6.0.2.2.0.0-2041 -j /usr/jdk64/jdk1.8.0_40 2.
```

2. Verify the configuration the using the -S option:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/ bin/config-hadoop.sh -s

Vormetric-Hadoop Configuration Status
PRODUCT_NAME=hdp- PRODUCT_VERSION=3.0.0.0-2557 HADOOP_HOME=/usr/hdp/current/ha
```

```

doop-client/sbin/./- HADOOP_VERSION=2.7.1 HADOOP_PRODUCT_VERSION=
2.7.1.2.3.0.0-2557- HADOOP_VERSION_MAJOR=2.7 LIBVORHDFS_S0=/usr/hdp/current/hadoopclient/sbin/./lib/native/libvorhdfs.so LIBHDFS_S0=/etc/vormetric/hadoop/lib/libhdfs.so VORMETRIC_HADOOP=/etc/vormetric/hadoop-
#-----vormetric-----
export HADOOP_NAMENODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_NAMENODE_OPTS}"v6 . . . . 62 export HADOOP_DATANODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_DATANODE_OPTS}"
#-----vormetric----- /etc/vormetric/hadoop/lib/libhdfs.so ...ok
/usr/hdp/current/hadoop-client/sbin/./lib/native/libvorhdfs.so ...ok /etc/vormetric/hadoop/gen-vor-hadoop-env.sh ...ok
/etc/vormetric/hadoop/vor-hadoop.env ...ok
Looks ok.
Vormetric Transparent Encryption Agent 6.0.3 Installation and Configuration Guide v6 . . . . .62 export HADOOP_DATANODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_DATANODE_OPTS}"
#-----vormetric ----- /etc/vormetric/hadoop/lib/libhdfs.so ...ok /usr/hdp/current/hadoop-client/sbin/./lib/native/libvorhdfs.so ...ok /etc/vormetric/hadoop/gen-vor-hadoop-env.sh ...ok /etc/vormetric/hadoop/vor-hadoop.env ...ok
Looks ok

```

Verify secfsd is Running with Hadoop Environment

Use a text editor to view the `/etc/init/secfsd-upstart.conf` file. The file should contain env entries, type:

```
cat /etc/init/secfsd-upstart.conf
```

HDFS Name Cache

Obtaining the HDFS file name from the NameNode is network intensive, so the map from HDFS block file name to HDFS file name is cached in a hash table. The following secfs configuration variables are used to support the hash cache. They are provided in case you need to tune the memory management of the name cache for better performance.

- **hdfs_cache_entry:** Default is 1,024,000, which could cover up to 125TB HDFS data because the default HDFS block size is up to 128MB (128MB * 1024000 = 125TB).
- **hdfs_cache_bucket:** Default is 10240.
- **hdfs_cache_timeout:** Default to 30 minutes.

- **hdfs_cache_interval**: Default wake up interval for a worker thread to update the cache entry whose timeout has expired is 10 seconds.

On Linux, you can configure each secfs configuration variable using the voradmin commands:

For example, to configure the variable, type:

```
voradmin secfs config hdfs_cache_interval 30
```

Note

Because HDFS rename is a metadata operation inside the HDFS NameNode and does not call into the local file system, the hash cache might contain expired data. The HDFS NameNode is coded to prevent renamed data from crossing a key boundary to prevent data corruption. However, other access checks based on the HDFS file name may give incorrect information if the name is expired. Understand this risk before using this feature.

Enabling CTE on HDFS

To enable CTE on your HDFS:

1. Restart CTE agent on the node.

- For Redhat 6.x, type:

```
/etc/init.d/secfs restart
```

- For Redhat 7.x or 8.x, type:

```
/etc/vormetric/secfs restart
```

2. Restart the Hadoop Services in the cluster.

You can now create GuardPoints to protect your entire HDFS.

Deleting Metadata in HDFS when Migrating Out of LDT

In an HDFS deployment, if you migrate from an LDT to a non-LDT environment, the administrator must delete the LDT mdstore file.

In the following example:

`/hadoop/hdfs` is the mount point

`/hadoop/hdfs/data` is the GuardPoint

To manage the migration:

1. In the CipherTrust Manager, click **Client > Client Groups**.
2. Click **<host/client group name>**. The Edit host/client group window opens.
3. Click **GuardPoints**.
4. Select the appropriate HDFS directory with an LDT GuardPoint, and click **Unguard**.
5. Using the Ambari admin console, shutdown all NameNode/DataNode one by one. Ensure that no HDFS GuardPoints are busy.
6. Ensure that no GuardPoints are configured on any HDFS node in the cluster, type:

```
secfsd -status guard
No GuardPoints configured
```

7. On the node running secfs, type:

```
voradmin ldt attr delete <guard path>
# voradmin ldt attr delete /hadoop/hdfs/data
LDT metadata has been removed from all files in GuardPoint /hadoop/hdfs/data
```

8. On the system, verify that the metadata store has been removed from the secfs mount points, type:

```
voradmin ldt rmstore <mount_point>
# voradmin ldt rmstore /hadoop/hdfs
Enter YES if /hadoop/hdfs does not include any GuardPoints associated with an
LDT policy ->YES
MDS file /hadoop/hdfs/::vorm:mds:: has been removed.
```

9. Verify that the metadata store has been removed from the secfs mount points, type:

```
ls -altr <mount_point>
# ls -altr /hadoop/hdfs
You should not see `/hadoop/hdfs/::vorm:mds::` listed.
```

10. Repeat the above steps for each node in the HDFS cluster.

Integrating File Activity Monitoring (FAM) with CTE Linux

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Software Requirements

Software	Minimum Version Required
CipherTrust Transparent Encryption	7.8.0.75
CipherTrust Manager	2.19 or subsequent versions

Overview of FAM on CTE agents

File Activity Monitoring (FAM) catalogs, monitors, and secures unstructured data (files). Unstructured data refers to any data that is not stored in databases. You can find these files locally, on the network, or in the cloud. FAM provides insights into data location, ownership, access history, permissions, protection, sharing, and sensitivity, enabling informed decisions about data protection.

For more information on FAM, see the [Introduction to the File Activity Monitoring User Guide](#)

CTE agents enabled with both File System Encryption and FAM capabilities can perform file system monitoring and audit file operations, as per the requirements of the Data Security Fabric (DSF) policies.

Scope of FAM on CTE host

Enabling FAM will also monitor activity on files outside of CTE GuardPoints.

Note

FAM will **not** monitor activity on RWP-enhanced files with CTE Ransomware Protection feature enabled

File Monitoring

The CTE agents monitor and audit user and application access to all files. Monitoring is not limited to files inside of CTE GuardPoints. Files outside of CTE GuardPoints are also monitored, except for those in the following directories:

Linux

/dev

```

/roc
/sys
/media
/opt/vormetric
/CTE-custom-install-location

```

Windows

```

\BOOT
\Windows
\Program Files*
\Users\*\APPDATA\ROAMING\MICROSOFT\WINDOWSAPPDATA\ROAMING\MICROSOFT\WINDOWS*
\Users\*\APPDATA\LOCAL\MICROSOFT\*
\Users\*\APPDATA\LOCAL\TEMP\*
\Users\*\APPDATA\LOCAL\PACKAGES\*
\Users\*\APPDATA\LOCAL\GOOGLE\CHROME\*
\PROGRAMDATA\MICROSOFT\*
\PROGRAMDATA\DELL\*

```

Also excluded from monitoring:

- VSS volumes
- DFSR private folders
- CSV volumes
- File operations performed by:
 - CTE internal processes
 - Thales Data Discovery and Classification processes
 - CTE-managed internal system operations
 - Metadata files

FAM Policies vs CTE Policies

FAM policies, which are similar to CTE policies with respect to security rules, allow you to monitor activity on specific data locations and/or by specific users. FAM policies only allow audit rules to specify/filter the content to be monitored. They do not impact access to the file.

Note

FAM policies are associated with the entire client, as compared to CTE policies which are limited to a particular GuardPoint path.

Performance Impact of FAM on CTE

File activity monitoring and audits consume system resources. This can potentially affect the performance of system and critical applications running on CTE agents. You can reduce the performance impact on the DSF management console by modifying the monitoring rules of the FAM policy applied to the CTE agent. For example:

- File operations, such as reading file attributes, are operations that are performed very frequently by applications and system utilities.
- If the CTE GuardPoint has policy rules with audit enabled, then with FAM also enabled, there may be additional overhead/performance impact due to the additional FAM policy evaluation and logging. However, the policy has no impact on file access/permissions.

Adjustments in the FAM policy to reduce, or eliminate highly frequent operations, can decrease the impact of FAM. Consult the FAM documentation for information on adjusting the FAM policy.

Enabling FAM on CTE Agent

You can enable FAM on CTE agent during CTE registration, or through the API.

Enable during Registration

After installing CTE, you enable FAM when registering, or re-registering, to CipherTrust Manager. During registration, you are prompted with the following two questions:

```
Do you want this host to have Filesystem encryption support enabled on the server? (Y/N) [Y]: Y

Do you want this host to have File Activity Monitoring support enabled? (Y/N) [N]: Y
```

Make sure that you answer **Y** to both questions.

Restart Secfs

For CipherTrust Manager v2.19 on **Linux**, post registration, you **must** restart **secfs**. This is **not** required for CipherTrust Manager v2.20 and subsequent versions. To restart secfs:

1. Type:

```
/etc/vormetric/secfs stop
```

2. Type:

```
/etc/vormetric/secfs start
```

Enable through the CM API

You can enable FAM on CTE, post registration:

- As part of the CTE upgrade on reboot process.
- Through the CM API available for CM 2.20 and subsequent versions. See the API documentation available through the CipherTrust Manager software.
- Through the DSF management console. Refer to DSF documentation for more information.

Disabling FAM on CTE

- For CipherTrust Manager v2.19, you cannot completely disable FAM once enabled. However, you can remove the FAM policy associated with the client to temporarily disable FAM audit logging/monitoring.
- For CipherTrust Manager v2.20, you can disable FAM on CTE agent through the DSF management console or through the CM API. Refer to DSF documentation for disabling FAM on CTE agents.

Voradmin Support for FAM

The `voradmin` utility allows you to gather statistics and administer CTE on a host/client. It has slightly different syntax and command capabilities depending on whether the host/client is running in Linux or Windows. The `voradmin` command provides minimal support for FAM administration on CTE agents. You can check the state of FAM and the FAM policy name applied to the CTE host.

The following command reports the state of FAM, the FAM policy name applied to the CTE host, and the DSF GW configuration for forwarding FAM audits to the DSF GWs.

```
voradmin fam show config
```

FAM Output when policy not applied

Example

```
# voradmin fam show config
```

Response

```
FAM_STATE   : DISABLED
FAM_POLICY  : Not Applied
```

FAM Output when policy applied

Example

```
# voradmin fam show config
```

Response

```
FAM_STATE    : ACTIVE
FAM_POLICY   : fam-all-ops-policy
```

Limitation

- File path names included in the FAM audits that are generated from file operations performed inside Linux containers, or namespaces, under **chroot** enforcement, are relative to the directory created by the **chroot**, or container, as the root directory.
- CTE enforces a limit of 128 characters in the FAM policy names. FAM audits resulting from policies exceeding this limit, will have the policy name trimmed to the this limit.

Using CTE with Oracle

This section describes how to install and configure CTE on Oracle RAC ASM, how to use an ASM Filter Driver Linux. It contains the following topics:

- [Oracle RAC ASM and ASMLib](#)
- [Oracle RAC ASMLib Multi-Disk Online Method](#)
- [About Oracle RAC ASM Raw Devices](#)
- [Oracle RAC ASM Multi-Disk Online Method](#)
- [Oracle RAC ASM Multi-Disk Offline Method \(Backup/Restore\)](#)
- [Surviving the Reboot and Failover Testing](#)
- [Using CTE with Oracle ASM Filter Driver](#)
- [Basic Troubleshooting Techniques](#)
- [Using Oracle with CipherTrust Transparent Encryption UserSpace](#)

Basic Troubleshooting Techniques

The following are some of the most common configuration issues that prevent the Oracle ASM configuration from working properly.

If you encountering errors similar to:

- ORA-15075: disk(s) are not visible cluster-wide
- ORA-15032: not all alterations performed

This could be the result of improper settings for the I/O layer, meaning that your disks are not properly configured.

Perform the following tasks to verify that the settings are correct:

1. On the CipherTrust Manager, in the Host Group that was created for the RAC cluster, verify that the host group for this configuration does **NOT** have the Cluster Group option set (this option is only for GPFS, which is not supported with CTE).
2. Ensure that the GuardPoints for the block devices are set at the Host Group level. This ensures that each node receives identical GuardPoints.
3. Verify that the GuardPoints are active on all nodes. When the GuardPoints are set, go to each node and verify that they are set and guarded, using the WebUI or the `secfsd -status guard1` command. If they do not guard correctly:
 - Verify that the udev rules are set correctly, as described in [Modify the UDEV Rules](#)
 - Make sure the device names are the same across all nodes.
4. From ASM, make sure that the `asm_diskstring` parameter is modified to include the CTE devices and that the proper pathname is used, see [Altering ASM_DISKSTRING on ASM](#).

Verifying Database Encryption

Option 1

The best way to verify the state of the data, without impacting anything in the existing environment, is to use the Oracle `kfed` command. You can run this command against the native path of the existing GuardPoints and make sure it returns with valid header information. If it returns valid information with the GuardPoint in place, then this confirms that the data is properly encrypted. If it returns with invalid header information, then that indicates that the data is either clear, double encrypted, or not in the expected encrypted state. The syntax for running this command would look similar to the following but will vary based on your environment.

```
/app/oracle/grid/product/19.0.0/grid/bin/kfed read /dev/rdisk/<diskName>
```

If the location is properly encrypted, following is an example of the viewable output:

```
/app/oracle/grid/product/19.0.0/grid/bin/kfed read /dev/rdisk/<diskName>
```

System Response:

```
kfbh.endian:          1 ; 0x000: 0x01
kfbh.hard:             242 ; 0x001: 0xf2
kfbh.type:            124 ; 0x002: *** Unknown Enum ***
kfbh.datfmt:          66 ; 0x003: 0x42
kfbh.block.blk:       1088904227 ; 0x004: blk=1088904227
kfbh.block.obj:       1558192170 ; 0x008: file=8234
kfbh.check:           3321251423 ; 0x00c: 0xc5f6465f
kfbh.fcn.base:        932956641 ; 0x010: 0x379bc9e1
kfbh.fcn.wrap:        3040493590 ; 0x014: 0xb53a4016
kfbh.spare1:          3806015223 ; 0x018: 0xe2db2ef7
kfbh.spare2:          3794962182 ; 0x01c: 0xe2328706
```

```

60000000000D8000 01F27C42 40E75C23 5CE0202A C5F6465F
[...|B@.\#\..*..F_]
60000000000D8010 379BC9E1 B53A4016 E2DB2EF7 E2328706 [7.....:@.....2..]
60000000000D8020 CA2F30AD 522B4D21 99292639 004EBB34 [./0.R+M!.)&9.N.4]
60000000000D8030 A3896BE8 BD839D23 2204E19E 946C575C [...k....#"....lw\]
60000000000D8040 4CE2218F 35E1B101 AF751A70 780E6D6E [L!.5....u.px.mn]
60000000000D8050 5E7E6A38 C600ED5F 929047C4 DF372A8E [^~j8...._..G..7*.]
60000000000D8060 E103152D BA87CC03 11A7D963 9D72FCE1
[...-.....c.r..]
60000000000D8070 1EC6B48B 03EE869F 61D651F9 E7614957 [.....a.Q..aIW]
60000000000D8080 810E0353 9C461F49 69569733 501D19EF [...S.F.IiV.3P...]
60000000000D8090 B268002B 4F9457B6 BDB04AC5 D3D07446 [.h.+0.W...J...tF]
60000000000D80A0 FD9EE5E0 9B46CB66 30D10B22 F63AB77E [.....F.f0..."..~]
60000000000D80B0 6FF79075 4BBD1FAD 8F226188 7774300D [o..uK...."a.wt0.]
60000000000D80C0 A809B6FB E1F1C80B B5760E68 9747D97D [.....v.h.G.}]
KFED-00322: Invalid content encountered during block traversal: [kfbtTraverseBloc
k][Invalid OSM block type][][124]

```

Option 2

The second option to verify the state of the data is to use the `dd` command. This requires you to specify some blocks and write it out to a file. After this completes, read the file using the `strings` command. You can do this while the device is in use. In the example below some sectors are skipped and it only dumps 10000 counts.

For example:

```
dd if=/dev/mapper/asm_data2p1 of=/tmp/dd2.out skip=1047 count=10000
```

Option 3

The third option to verify the state of the data without impacting the existing environment is to use the `strings` command.

Note

The `strings` command cannot read a busy or large device.

You can run this command against the native path (`/dev/<deviceName>`) of the existing GuardPoints (`/dev/secvm/dev/<deviceName>`). The new path to SecVM would be similar to `/dev/secvm/dev/<deviceName>`. By executing the `strings` command against the native path `strings /dev/<devicename> | more`, this does not go through the SecVM device and therefore is not be decrypted. If it is encrypted the output should contain illegible text.

Using CTE LDT with Oracle

Oracle compatibility with LDT

Oracle is compatible with LDT with the following changes:

You must run Oracle with the following file system IO option, when mounted on NFS:

- DirectIO

Note

LDT is not supported on raw devices such as ASM.

Oracle RAC ASM and ASMLib

This section describes how to install and configure CipherTrust Transparent Encryption on an Oracle RAC ASM and ASMLib.

Using CipherTrust Transparent Encryption with an Oracle RAC ASM

You can apply CipherTrust Transparent Encryption when the Oracle DB is active or inactive. If you choose to use it while the Oracle DB is active, it eliminates any downtime. You can apply CipherTrust Transparent Encryption during low volume traffic time frames. If you choose to use this option, then use the **rebalance** function of ASM. This allows you to:

1. Migrate data off of a disk so that it can be dropped/removed from a **Diskgroup**.
2. Apply CipherTrust Transparent Encryption protection.
3. Add the disk back into the diskgroup.

Caution

You **must** drop the related ASM diskgroup first, before dropping the disk. If, for example, you drop an ASM disk before dropping an ASM diskgroup, and then add it back to the diskgroup without cleanly wiping the disk, the ASM diskname will be corrupted. To avoid this problem, clear out the disk before you add it back into the diskgroup. Example: `dd if=/dev/zero of=/dev/secvm/dev/mapper/asmdg-asmlv002 bs=32k`

ASMLib

ASMLib is an optional support library for the Automatic Storage Management feature of the Oracle Database. If the customer is using ASMLib, then management is performed through an Oracle ASM command line. Using this can be simpler than the setup required for standard ASM. The commands and details of the procedure differ as well.

Important ASM Commands and Concepts

Rebalancing Disks

When you drop/remove a disk from the diskgroup, it is important to apply the proper value for the power setting for rebalance and to use the **WAIT** command.

Example ASM Command:

```
SQL> ALTER DISKGROUP <DiskGroupName> DROP DISK <diskName> REBALANCE POWER 8 WAIT;
```

- The rebalance command moves the data off of the disk that you are removing from the diskgroup, distributing the data across the remaining DISKS.
- The power setting is a number from 1 to 11. It determines how much processing power is dedicated to the rebalance, versus normal operations. Unless the encrypting occurs during heavy traffic volume, the minimum value you should use is 6. Otherwise, consult the customer's DBA for the proper setting. An appropriate value to start with is 8.

Mapping Raw Devices

You can map raw devices for this configuration using:

- **Multipath I/O**

This is typically evident when the path for the mapped devices is set to: `/dev/mapper/<device-name>`.

- **Raw devices**

Some customers use raw devices to map a name like raw3 to a specific device name. You usually find this mapping in a file called: `/etc/sysconfig/rawdevices`.

Note

It is important to understand how the device names are used and if they are the same across all of the RAC nodes.

- **EMC PowerPath**

If using EMC PowerPath then the device names are similar to the following: `/dev/emcpowerXXXX`.

When browsing the CipherTrust Manager through the local host, you cannot find Power Path devices. You must manually input the paths. The guarded disk names are prepended with: `/dev/secvm`.

Checking Rebalance Status

The `wait` command is very important when ASM performs a rebalance. When you specify `wait`, the command prompt does not display until all of the data is rebalanced and migrated off of the disk. If you do not specify `wait`, the command prompt returns immediately, and you must issue the following ASM command to check the status of the rebalance:

```
SQL> select * from v$asm_operation;
```

This command returns information about the:

- State
- Current power level
- Current amount rebalanced
- Estimated work until completion
- Rate
- Estimated minutes
- Any error codes

Note

It is highly recommended that you always specify the `wait` command when performing a **Drop Disk** with Rebalance. If it is not specified, ASM may prematurely release the disk, thereby allowing CTE to place a GuardPoint on the disk before the rebalance completes. This action may corrupt the data.

Oracle cautions against this issue:

Caution

The `ALTER DISKGROUP...DROP DISK` statement returns before the drop and rebalance operations complete. Do not reuse, remove, or disconnect the dropped disk until the `HEADER_STATUS` column in the `V$ASM_DISK` view for this disk changes to `FORMER`. You can query the `V$ASM_OPERATION` view to determine the amount of time remaining for the drop/rebalance operation to complete. For more information, refer to the Oracle Database SQL Language Reference and the Oracle Database Reference.

Determining Best Method for Encrypting Disks

A diskgroup can contain one or multiple disks. You must determine if the diskgroup contains enough disks and free space for encryption. If the diskgroup contains only one disk, or multiple disks but not enough free space,

then you must use the **Offline** (backup/restore) method for encryption.

If the diskgroup contains more than one, you can use the **Online** (rebalancing) method. During rebalancing, additional disks allow for migrating data from the original disk so that it can be encrypted, added back into the diskgroup, and then migrated back to the source disk. Therefore, if the customer does not want to permanently add extra disks, they can add disks temporarily, just for rebalancing.

In general, once you have completed the initial setup for the operating system with which you are working, for both ASM or ASMLib, the high-level process is the same for applying CTE protection to raw devices and using them.

Online Method (No Application / Database Downtime)

Typically, when using the online method, follow these steps:

1. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.
2. Apply CTE encryption to the disk.
3. Add each protected disk to the diskgroup.
4. Restart the nodes and the failover test.
5. Repeat the previous steps for each disk in the diskgroup.

Offline Method (Backup the DB)

Typically, when using the offline method, follow these steps:

1. Backup the database.
2. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.
3. Stop the Oracle database.
4. Delete the diskgroup.
5. Apply CTE encryption to the disk.
6. Recreate the diskgroup.
7. Add the protected disk to the diskgroup.
8. Restart the nodes and the failover test.
9. Repeat the previous steps for each disk in the diskgroup.

General Prerequisites

Setup

- Verify that you have a current backup of the database
- Install and register CTE agents on all RAC node Hosts
- Create a **Host Group** and add all RAC node hosts as members
- Create an encryption key for the Oracle RAC Database / Application
- Create an Oracle policy using the proper encryption key

Note

If the raw device mappings for the disk(s) are **not** identical across all nodes in the RAC, then you cannot use a Host Group for managing the GuardPoint within the CipherTrust Manager. You **must** apply the GuardPoint to each Host individually. This is typically not optimal, as a Host Group is the most effective and consistent way to manage GuardPoints for Oracle RAC environments.

Altering ASM_DISKSTRING on ASM

ASM uses the `asm_diskstring` setting to identify the path where ASM will attempt to locate available disks to use. If you are using device names when adding the disk, you must modify the string to include the path to SecVM.

1. To retrieve the `ASM_DISKSTRING` setting, type:

```
SQL> SHOW PARAMETER ASM_DISKSTRING
```

2. To modify the setting, type:

```
SQL> ALTER SYSTEM SET ASM_DISKSTRING='/dev/mapper/*', '/dev/secvm/dev/mapper/*';
```

Where the path added is the path to SecVM.

ASMLib manages the binding, not ASM. ASMLib creates ASMLib devices on the SecVM devices and presents it to ASM. ASM automatically recognizes the new device. This creates the need to alter diskstrings for ASM. In addition, Oracle ASM sees a new device created using ASMLib and Raw, by default.

For example:

Using Oracle ASMLib to bind the device:

```
oracleasm createdisk <devicename> /dev/secvm/dev/<blockdev>
```

Using the raw command to bind the device:

```
raw /dev/raw/rawN /dev/secvm/dev/<blockdev>
```

Specific Prerequisites

Establishing a Starting Point

In many production environments, you may find that it has been a very long time since the RAC nodes have had the services restarted or have been completely rebooted. This can result in a lack of understanding of the actual state of the RAC cluster and its ability to survive a reboot on its own, prior to installing CTE.

Restarts can uncover issues in the RAC environment that are unrelated to CTE. To avoid issues after a CTE installation, Thales recommends that you restart each RAC node **AFTER** CTE is installed and **PRIOR** to establishing any GuardPoints. This may not be feasible in a single node configuration. However, by doing so, CTE is installed but inactive, and you can ensure that the platform is in a workable state prior to getting started.

The Importance of Device Mapping

It is important to use device naming and mapping in a multi-node RAC configuration. Verify the device names to ensure that the disks are mapped to the same disks on each RAC node before applying any GuardPoints. Thales recommends that RAC nodes use the same device names across all nodes. If they do not match, then problems can occur.

If the RAC nodes use the same device names, use a Host Group to create GuardPoints. If they do not match, do not use a Host Group to create GuardPoints. Set them up independently on each Host.

Important Note about Raw Devices on UNIX

In general, raw devices are created as either character or block mode devices. Any I/O performed on character devices is non-buffered, while I/O on block devices is buffered and performed in defined block sizes (that is, 4K bytes).

While the Oracle documentation for using ASM with raw devices indicates that you can use either character or block devices, **CTE REQUIRES a block device for guarding**.

Note

- Attempting to apply a GuardPoint on a character device that does not have a corresponding block device may result in a GuardPoint that never encrypts data. The status of the GuardPoint never shows as guarded.
- The WebUI does not support browsing for the character devices. You would need to manually paste the name into the WebUI.

Block Device Support

CipherTrust Transparent Encryption UserSpace block device support requires that the underlying kernel supports I/O direct mode for loop devices (`LOOP_SET_DIRECT_IO`) in order to properly flush and retrieve data from a disk. This support was not added in the kernel loop driver until **kernel 4.10**. Any distribution with a kernel level lower than that may improperly cache data and therefore, should not be used in a multi-node setup sharing block devices because stale data may be returned to the application.

Oracle RAC ASMLib Multi-Disk Online Method

The online method describes how to remove, protect and add disks to a diskgroup.

Assumptions

Using the Online Method assumes that there is enough free space in the diskgroup so that you can drop/remove, protect and then add the disk back into the diskgroup.

Note

During the initial investigation, you may want to ensure that you have the correct raw device name for each disk that you plan on protecting. Before making any changes to the ASM configuration, obtain the definitive device names for each disk by running the following from the command prompt:

```
oracleasm querydisk -p <diskName>
```

To add the disk to the diskgroup using the online method and make it ready for use:

1. Open a terminal session on both RAC Nodes.
2. On **RAC Node 1**, perform the following:
 - a. On the ASM, type the following to remove a disk for the diskgroup.

```
SQL> ALTER DISKGROUP <diskGroupName> DROP DISK <diskName> REBALANCE POWER 1  
1 WAIT;
```

- b. Delete the disk from ASM, type:

```
oracleasm deletedisk <diskName>
```

- c. Verify that the disk is deleted from the ASM and therefore, it is not listed, type:

```
oracleasm listdisks
```

Note

If you are planning to apply a GuardPoint to a raw device that is currently in an ASM diskgroup, you must remove and delete the disk from the diskgroup before you apply the GuardPoint. ASMLib will not see the guarded disk if you skip this step. When deleting the disk, make sure that the deletion completes before continuing.

About Oracle RAC ASM Raw Devices

When Not Using ASMLib

Before starting the CTE implementation, investigate how the customer is using raw devices for their ASM configuration.

Devices using Raw Bindings

Typically, a device that uses a raw binding looks like the following to ASM:

```
/dev/raw/raw1
```

If the device is mapped this way, you must locate where the mapping is performed. Typically, you can find this in the following configuration file:

```
/etc/sysconfig/rawdevices
```

The underlying binding could be to either a **standard device** name or a **multipath** I/O device name. Either way, you must find where the bind commands are run so that you can modify them for SecVM.

Note

If raw bindings are in use, then typically no changes are needed for the `asm_diskstring`. Because the binding to the actual device is created through the `bind` command, locate where the binding occurs and change the binding to SecVM.

Multipath I/O Devices

Devices using multipath I/O are typically found with the name:

```
/dev/mapper/mpath1
```

Generally, when using multipath I/O, you create SecVM on the multipath device name.

Note

- **CTE:** If you use multipath I/O devices in the ASM configuration to add its disk, you must modify the `asm_diskstring` parameter to include the `/dev/secvm/dev/*` path.
- **CTE-U:** If you use multipath I/O devices in the ASM configuration to add its disk, you must modify the `asm_diskstring` parameter to include the `/dev/secvm/*` path.

Standard Devices

In many cases the ASM configuration may be using plain device names, like the following:

`/dev/sda1`

Note

- **CTE:** If you use standard device names in the ASM configuration to add a disk, you must modify the `ASM_DISKSTRING` parameter to include the `/dev/secvm/dev/*` path.
- **CTE-U:** If you use standard device names in the ASM configuration to add a disk, you must modify the `ASM_DISKSTRING` parameter to include the `/dev/secvm/*` path.

Consistent Naming of Devices across RAC Nodes

As previously stated, if the raw device mappings for the disk(s) are **NOT** identical across all nodes in the RAC, then you **CANNOT** use a Host Group and you **MUST** apply the GuardPoints to each Host individually. This is typically NOT optimal, as a Host Group is the most effective way to manage an Oracle RAC environment.

Oracle RAC ASM Multi-Disk Online Method

Performing encryption with the online rebalancing method requires sufficient free space to allow the drop of the largest ASM disk.

Checking for Space

In the Oracle system, use the following commands to check for available disk space:

1. Check total free space in the disk group:

```
SELECT name, free_mb, total_mb, free_mb/total_mb*100 as percentage FROM v$asm_diskgroup;
```

```

NAME                                FREE_MB  TOTAL_MB  PERCENTAGE
-----
DATA                                7        2109    .331910858

```

2. Check individual ASM disk size and usage:

```

select a.name DiskGroup, b.disk_number Disk#, b.name DiskName, b.total_mb, b.free_mb, b.path, b.header_status FROM v$asm_disk b, v$asm_diskgroup a where a.group_number (+) =b.group_number order by b.group_number, b.disk_number, b.name

```

```

DISKGROUP  DISK#  DISKNAME          TOTAL_MB  FREE_MB  PATH
HEADER_STATUS
-----
DATA        0      DATA_0000        1874      1273    /dev/oracleasm/disks/D
ATA3        MEMBER
DATA        1      DATA_0001        1992      608     /dev/oracleasm/disks/D
ATA4        MEMBER
DATA        3      DATA_0003        117       0       /dev/oracleasm/disks/D
ATA2        MEMBER
            0      DATA_ENC_0000    109       28      /dev/oracleasm/disks/D
ATA1_ENC    MEMBER

```

Adding a Disk to the Diskgroup

Using the Online Method assumes that there is enough free space in the diskgroup so that you can drop/remove a disk, protect it with CTE, and then add it back into the diskgroup.

To add the disk to the diskgroup:

1. Open a terminal session on both RAC Nodes.
2. On **RAC Node 1**, on the ASM, remove the disk from the disk group, type.

```
ALTER DISKGROUP <diskGroupName> DROP DISK <diskName> REBALANCE POWER 11 WAIT;
```

3. On the CipherTrust Manager, in the Host Group, apply a GuardPoint to the Raw Device: `<rawDevice1Name>`.
4. From **RAC Node 1**, to display the status of the guarded disks, type:

```
secfsd -status guard
```

- On both **RAC Node 1 and 2** type:

```
chown oracle:oinstall /dev/secvm/<rawDevice1Name>
chmod 660 /dev/secvm/<rawDevice1Name>
```

- From **RAC Node, on the ASM**, add the protected disk to the disk group:

```
ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/<rawDevice1Name> NAME <disk1Name>;
```

The disk is now added to the diskgroup and ready for use.

- The system is now ready for a reboot and failover test. For details, see [Surviving the Reboot and Failover Testing](#).

Troubleshooting

Occasionally, settings do not persist when the system is rebooted. To ensure they do persist, edit the `/etc/rc.local` file and add the following lines:

```
Echo "Changing Permission for secvm devices"
chown oracle:oinstall /dev/secvm/dev/<rawDevice1Name>
chmod 660 /dev/secvm/dev/<rawDevice1Name>
```

Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)

Using the Offline Method assumes that there is not enough free space in the diskgroup.

- Open a terminal session on both RAC Nodes.
- On RAC Node 1, on the ASM, type the following to remove the disk group.

```
DROP DISKGROUP <diskGroupName> FORCE INCLUDING CONTENTS;
```

Note

Make sure that the disk is removed before guarding the raw devices.

- On the CipherTrust Manager, in the Host Group, apply GuardPoints to the three raw devices:

```
<rawDeviceName1>
```

```
<rawDeviceName2>
<rawDeviceName3>
```

4. On **RAC Node 1**, to display the status of the guarded disks, type:

```
secfsd -status guard
```

5. On both **RAC Node 1** and **2**, type:

CTE

```
chown oracle:oinstall /dev/secvm/<rawDeviceName1>
chmod 660 /dev/secvm/<rawDeviceName1>
chown oracle:oinstall /dev/secvm/<rawDeviceName2>
chmod 660 /dev/secvm/<rawDeviceName2>
chown oracle:oinstall /dev/secvm/<rawDeviceName3>
chmod 660 /dev/secvm/<rawDeviceName3>
```

CTE-U

```
chown oracle:oinstall <rawDeviceName1>
chmod 660 <rawDeviceName1>
chown oracle:oinstall <rawDeviceName2>
chmod 660 <rawDeviceName2>
chown oracle:oinstall <rawDeviceName3>
chmod 660 /dev/<rawDeviceName3>
```

6. From **RAC Node 1, on the ASM**, add the protected disk to the disk group, type:

```
ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/<rawDeviceName1> NAME <diskName1>;
ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/<rawDeviceName2> NAME <diskName2>;
ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/<rawDeviceName3> NAME <diskName3>;
```

The disks are now added to the diskgroup and ready for use.

7. On **RAC Node 1**, restore the database.
8. The system is now ready for a reboot and failover test. Go to the section [Surviving the Reboot and Failover Testing](#).

Troubleshooting

Occasionally, settings do not persist when the system is rebooted. To ensure they do persist, edit the `/etc/rc.local` file and add the following lines:

```
"Changing Permission for secvm devices"
chown oracle:oinstall /dev/secvm/dev/<rawDeviceName1>
chmod 660 /dev/secvm/dev/<rawDeviceName1>
chown oracle:oinstall /dev/secvm/dev/<rawDeviceName2>
chmod 660 /dev/secvm/dev/<rawDeviceName2>
chown oracle:oinstall /dev/secvm/dev/<rawDeviceName3>
chmod 660 /dev/secvm/dev/<rawDeviceName3>
```

Surviving the Reboot and Failover Testing

Preparing for Failover Testing with ASMLib

When using ASMLib with the `createdisk` command, there is no requirement to make additional changes in `rc.local` or other areas for mapping device names or to use `chmod` or `chown` for SecVM. This is because it is managed for you by the `createdisk` function and you can verify this by running the following command:

```
ls -l /dev/oracleasm/disks
```

CTE Load Order and Startup Scripts

The last change is to ensure that CTE starts before ASM starts in the startup scripts.

Failover Testing

Confirm that everything is functional:

- Ensure that the GuardPoints are all operational.
- Ensure that you receive valid results when you query the database.
- Verify that the load order ensures that CTE starts before ASM.

Once verified, you can start the failover testing for each RAC Node.

1. Reboot the RAC Node 1 and monitor the startup.
2. Once the restart is clean, reboot RAC Node 2 and monitor the startup.

Issues with Device Mapper and Invalid Guard Path

If CTE is unable to apply a GuardPoint on a raw device, the logs may generate an error similar to the following:

```
[SecFS, 0] EVENT: Failed to guard /dev/mapper/devicename (reason: Invalid Guard Path flags 0x2 gypped 0x4 status 0x11) - Will retry later
```

If you receive this error, use the setup command to check the status of the disks, type:

```
setup info <deviceName>
```

Before attempting to establish a GuardPoint, look closely at the open count value and ensure that it is 0 on all nodes.

Using CTE with Oracle ASM Filter Driver

This chapter describes how to configure CTE on Oracle Standalone and RAC ASM Filter Driver for Linux. It contains the following topics:

- How to enable CTE for Oracle ASMFD
- How to configure CTE and create a guarded Oracle ASMFD
- How to convert a baseline ASMFD disk group to a guarded ASMFD disk group
- How to uninstall/ upgrade CTE with an active ASMFD Setup

About Oracle ASM Filter Driver

Oracle ASM Filter Driver (Oracle ASMFD) is a kernel module that resides in the I/O path of the Oracle ASM disks. Oracle ASM uses the filter driver to validate write I/O requests to Oracle ASM disks.

The Oracle ASMFD simplifies the configuration and management of disk devices by eliminating the need to rebind disk devices used with Oracle ASM each time the system is restarted.

The Oracle ASM Filter Driver rejects any I/O requests that are invalid. This action eliminates accidental overwrites of Oracle ASM disks that would cause corruption in the disks and files within the disk group.

Audience

Users must be a Senior Oracle DBA administrator who is comfortable setting up a baseline ASMFD environment.

Prerequisites

The following setup allows CTE to correctly load the guarded ASMFD disks correctly after CTE is installed, upgraded, or restarted:

1. Ensure that the ASM \$ORACLE_BASE variable is assigned a value in `/root/.bash_profile`, if Oracle is already installed.
2. Ensure that a line starting with **+ASM** exists in the `/etc/oratab`.

Note

This line is added by Oracle when Oracle is configured with ASM.

Enable Oracle ASMFD for CTE

To enable Oracle ASMFD:

1. Log in as the root user and stop the Oracle Grid Infrastructure for a standalone server, type:

```
$GRID_HOME/bin/crsctl stop has
```

2. Configure Disk Discovery for AFD. Modify the following files by adding the content of `/dev/secvm/dev/sd*` to the OS files in `/etc/oracleafd.conf` and `/etc/afd.conf` with `afd_filtering` enabled, type:

```
cat /etc/afd.conf
afd_diskstring='/dev/sd*,/dev/secvm/dev/sd*'
afd_filtering=enable

cat /etc/oracleafd.conf
afd_diskstring='/dev/sd*,/dev/secvm/dev/sd*'
afd_filtering=enable
```

- a. To prevent the file from changing back to `afd_diskstring='/dev/sd*'` make it read only, type:

```
chmod 444 /etc/oracleafd.conf /etc/afd.conf
```

3. Restart ACFS before proceeding, type:

```
acfsload stop
acfsload start
```

4. Restart the Oracle Grid Infrastructure, type:

```
$GRID_HOME/bin/crsctl start has
```

5. Verify that `/dev/secvm/dev/sd*` is part of the SQL output and the state is enabled as a grid, type:

```
SELECT SYS_CONTEXT('SYS_ASMFD_PROPERTIES', 'AFD_DISKSTRING') FROM DUAL;
```

Expected Response

```
SYS_CONTEXT( 'SYS_ASMFD_PROPERTIES', 'AFD_DISKSTRING' )
-----
/dev/sd*, /dev/secvm/dev/sd*
```

Note

If using Oracle RAC (Real Application Clusters), repeat the previous steps for all of the nodes in the related RAC cluster.

Configure CTE and create a guarded Oracle ASMFD

To configure CTE and create a Guarded Oracle ASMFD:

1. Create a raw device disk, for example:

```
/dev/sdc
```

2. Partition the targeted raw device, for example:

```
/dev/sdc1
```

3. Guard the partitioned raw device, that you just created, using CTE.
4. Create an ASMFD disk on the guarded partitioned raw device, type:

```
$GRID_HOME/bin asmcmd afd_label '<disk_label>' '<guarded_raw_partition>'
```

Example:

```
$GRID_HOME/bin asmcmd afd_label 'DISK1' '/dev/secvm/dev/sdc1'
```

5. Verify that the new disk was created, type:

```
$GRID_HOME/bin asmcmd afd_alsdk
```

The disk should display in the list of disks, similar to the following:

```
Label  Filtering  Path
```



```
=====
DISK1  ENABLED  /dev/secvm/dev/sdc1
```

6. If using Oracle RAC (Real Application Clusters), repeat the previous steps for all of the nodes in the RAC cluster.
7. Now you can use the Oracle Grid ASM Configuration Assistant GUI to create the targeted guarded ASMFD disk group on the above created guarded ASMFD disk, DISK1. See the Oracle GRID documentation for more information.

Convert a baseline ASMFD disk group to a CTE guarded ASMFD disk group using the Offline method

We will use the following example scenario in this section:

Objective:

- Convert the baseline ASMFD disk group **DATA1**, to a CTE guarded ASMFD disk group.
- Current configured baseline **DATA1** disk group consists of ASMFD disk **DISK1** on a raw partitioned device /dev/sdc1.

To convert:

1. If the targeted raw disk partition to be guarded does not yet exist, create it. For example: /dev/sdd1.

Note

The capacity of /dev/sdd1 must be large enough to transfer all of the data from ASMFD disk DISK1 on /dev/sdc1.

2. Using CTE, guard the raw partitioned device.
3. Create an ASMFD disk on the guarded raw partition:

```
$GRID_HOME/bin asmcmd afd_label '<disk_label>' '<guardedRawPartition>'
```

Example

```
$GRID_HOME/bin asmcmd afd_label 'DISK2' '/dev/secvm/dev/sdd1'
```

4. Ensure that there are current backups of all of the database(s) residing on the ASMFD disk group DATA.

5. Shutdown all databases residing on ASMFD disk group DATA1.
6. In the ASM database, run the following SQL command with the rebalance option to add a guarded ASMFD disk DISK2 to ASMFD disk group DATA1, type:

```
ALTER DISKGROUP <ASMFD diskgroup name> ADD DISK 'AFD:<ASMFD disk name>' REBALANCE POWER 11 WAIT;
```

Example

```
ALTER DISKGROUP DATA1 ADD DISK 'AFD:DISK2' REBALANCE POWER 11 WAIT;
```

7. Verify the results, type:

```
col PATH for a15 col DG_NAME for a15 col DG_STATE for a10 col FAILGROUP for a10 select dg.name
dg_name, dg.state dg_state, dg.type, d.disk_number dsk_no,d.path, d.mount_status, d.FAILGROUP, d.state
from v$asm_diskgroup dg, v$asm_disk d where dg.group_number=d.group_number and dg.name = 'DATA1'
```

System Response:

DG_NAME	DG_STATE	TYPE	DSK_NO	PATH	MOUNT_S	FAILGROUP	STATE
DATA1	MOUNTED	EXTERN	0	AFD:DISK1	CACHED	DISK1	NORMAL
DATA1	MOUNTED	EXTERN	0	AFD:DISK2	CACHED	DISK2	NORMAL

8. Run the following SQL command, in the ASM database, to transfer all data from ASMFD disk DISK1 to ASMFD disk DISK 2 and then drop ASMFD disk DISK1 from ASMFD disk group DATA1, type:

```
ALTER DISKGROUP DROP DISK 'AFD: REBALANCE POWER WAIT;
```

Example:

```
ALTER DISKGROUP DATA1 DROP DISK 'AFD:DISK1' REBALANCE POWER 11 WAIT;
```

Verify the results:

```
col PATH for a15 col DG_NAME for a15 col DG_STATE for a10 col FAILGROUP for a10 select dg.name
dg_name, dg.state dg_state, dg.type, d.disk_number dsk_no,d.path, d.mount_status, d.FAILGROUP, d.state
from v$asm_diskgroup dg, v$asm_disk d where dg.group_number=d.group_number where dg.name =
'DATA1'
```

System response

DG_NAME	DG_STATE	TYPE	DSK_NO	PATH	MOUNT_S	FAILGROUP	STATE

```

-----
-----
DATA1          MOUNTED      EXTERN      0      AFD:DISK2    CACHED      DISK2      NORMAL

```

At this point, all data in the ASMFD disk group DATA1 has been transferred from the baseline ASMFD disk DISK1, to the guarded ASMFD disk DISK2. At this time, the databases that are residing in ASMFD disk group DATA1 can now be restarted.

Convert a baseline ASMFD disk group to a CTE guarded ASMFD disk group using the Online method

We will use the following example scenario in this section:

- Number of RAC nodes: 2
- Name of Diskgroup: DATA1
- Number of disks: 3

Name of baseline disks assigned to raw device:

- DISK1: /dev/sdb1
- DISK2: /dev/sdc1
- DISK3: /dev/sdd1

ASMFD disk group **DATA1** was created from baseline ASMFD disks DISK1, DISK2, and DISK3.

```

DG_NAME      DG_STATE  TYPE      DSK_NO  PATH          MOUNT_S  FAILGROUP  S
-----
DATA1        MOUNTED   EXTERN    0      AFD:DISK1     CACHED   DISK1      N
DATA1        MOUNTED   EXTERN    0      AFD:DISK2     CACHED   DISK2      N
DATA1        MOUNTED   EXTERN    0      AFD:DISK3     CACHED   DISK3      N

```

Objective:

- Convert all of the database data on ASMFD disk group DATA1 from baseline to a CTE guarded ASMFD disk group.

Note

The combined capacity of /dev/sdc1 on DISK2 and /dev/sdd1 on DISK3 must be large enough to

hold all of the data transferring from ASMFD disk DISK1 on /dev/sdb1.

To convert:

From RAC Node 1:

1. Connect locally, as the system administrator, to an Oracle ASM instance using OS authentication, type:

```
sqlplus 'as sysasm'
```

2. At the ASM prompt, drop the ASMFD disk DATA1 from the disk group DISK1, type:

```
ALTER DISKGROUP DATA1 DROP DISK DISK1 REBALANCE POWER 11 WAIT;
```

3. Verify that the ASMFD DISK2 is no longer part of the ASMFD disk group DATA1, type:

```
sqlplus 'as sysasm' col PATH for a15 col DG_NAME for a15 col DG_STATE for a10 col FAILGROUP for a10
select dg.name dg_name, dg.state dg_state, dg.type, d.disk_number dsk_no,d.path, d.mount_status,
d.FAILGROUP, d.state from v$asm_diskgroup dg, v$asm_disk d where dg.group_number=d.group_number
and dg.name = 'DATA1';
```

System Response

DG_NAME	DG_STATE	TYPE	DSK_NO	PATH	MOUNT_S	FAILGROUP
DATA1	MOUNTED	EXTERN	0	AFD:DISK2	CACHED	DISK2
NORMAL						
DATA1	MOUNTED	EXTERN	0	AFD:DISK3	CACHED	DISK3
NORMAL						

Note

Depending on the size of your data, DISK1 might take some time to no longer show in the above query.

4. From the OS command prompt, drop ASMFD disk DISK1:

```
$GRID_HOME/bin asmcmd afd_unlabel DISK1
```

- From the command prompt, verify DISK1 is no longer visible on both RAC Node 1 and 2.

```
$GRID_HOME/bin asmcmd afd_lslbl
```

- Using CTE, guard the DISK1 raw partitioned device `/dev/sdb1`.
- From the command prompt, recreate ASMFD disk DISK1, with the guarded raw device `/dev/sdb1`.

CTE

```
$GRID_HOME/bin asmcmd afd_label 'DISK1' '/dev/secvm/dev/sdb1'
```

CTE-U

```
$GRID_HOME/bin asmcmd afd_label 'DISK1' '/dev/secvmsdb1'
```

- From the command prompt, verify that DISK1 is now visible on both RAC Node 1 and 2 with the newly guarded path:

```
$GRID_HOME/bin asmcmd afd_lslbl
```

- From the ASM prompt, add the guarded ASMFD disk DISK1 back to the ASMFD disk group DATA1, type:

```
sqlplus 'as sysasm'
ALTER DISKGROUP DATA1 ADD DISK 'AFD:DISK1' REBALANCE POWER 11 WAIT;
```

- Verify that ASMFD disk DISK1 is now part of ASMFD diskgroup DATA1, type:

```
sqlplus 'as sysasm' col PATH for a15 col DG_NAME for a15 col DG_STATE for a10 col FAILGROUP for a10
select dg.name dg_name, dg.state dg_state, dg.type, d.disk_number dsk_no,d.path, d.mount_status,
d.FAILGROUP, d.state from v$asm_diskgroup dg, v$asm_disk d where dg.group_number=d.group_number
and dg.name = 'DATA1';
```

System Response

DG_NAME	DG_STATE	TYPE	DSK_NO	PATH	MOUNT_S	FAILGROUP
DATA1	MOUNTED	EXTERN	0	AFD:DISK1	CACHED	DISK1
NORMAL						
DATA1	MOUNTED	EXTERN	0	AFD:DISK2	CACHED	DISK2
NORMAL						

DATA1	MOUNTED	EXTERN	0 AFD:DISK3	CACHED	DISK3
NORMAL					

Note

Depending on the size of your data, DISK1 might take some time to display in the above query.

11. Repeat the previous steps for Baseline DISK 2 and DISK 3

Uninstall/ Upgrade CTE with active ASMFD Setup

For an Active ASMFD Standalone Setup

1. Shutdown all databases running on guarded devices.
2. Shutdown the CRS and ACFS, type:

```
crsctl stop resource -all
crsctl stop has
afdload stop
```

3. Perform CTE maintenance, uninstall or upgrade.
4. Restart ACFS and CRS, type:

```
afdload start
crsctl start has
crsctl start resource -all
```

5. Restart related databases.

For an Active ASMFD RAC Setup

To perform CTE maintenance on all ASMFD RAC nodes in a cluster:

1. Shutdown all databases running on guarded devices.
2. Shutdown CRS, ACFS, and AFD on all nodes, type:

```
$GRID_HOME/bin/crsctl stop cluster -all
$GRID_HOME/bin/acfsload stop cluster -all
```

```
$GRID_HOME/bin/afdload stop cluster -all
```

3. Perform CTE maintenance, uninstall, or upgrade on all targeted RAC nodes.
4. Restart AFD, ACFS, and CRS on all nodes, type:

```
$GRID_HOME/bin/afdload start cluster -all
$GRID_HOME/bin/acfsload start cluster -all
$GRID_HOME/bin/crsctl start cluster -all
```

5. Restart related databases.

To perform CTE maintenance on a ASMFD RAC cluster in a rolling fashion:

1. Shutdown all instances running on guarded devices on the targeted RAC node only.
2. Shutdown CRS, ACFS, and AFD on the targeted RAC node only. Type:

```
$GRID_HOME/bin/crsctl stop has
$GRID_HOME/bin/acfsload stop
$GRID_HOME/bin/afdload stop
```

3. Perform CTE maintenance, uninstall, or upgrade on the targeted RAC node only.
4. Restart AFD, ACFS, and CRS on a targeted RAC node only, type:

```
$GRID_HOME/bin/afdload start
$GRID_HOME/bin/acfsload start
$GRID_HOME/bin/crsctl start has
```

5. Restart related instances on the targeted RAC node.

Note

If AFD fails to stop, try the following OS command:

```
modprobe -r oracleafd
```

Using Oracle with CTE-U

When guarding an ASM disk with CipherTrust Transparent Encryption UserSpace, there can be a 10% drop in database performance. This occurs when the underlying device is in Oracle direct mode. This mode avoids

double-caching, which consumes memory, and therefore impacts performance on some workloads.

This issue is affected by the `block_o_direct` parameter. If that parameter is set to `0`, the IO will be reported as complete, (meaning committed to disk) before it actually is. This is a data integrity risk for a database, because the normal mode is to mark as journal complete as soon as the data is safe on a disk. This incorrect reporting could result in a race that could lead to a journal being cleared before the data is on the disk. If a crash occurs during this window, the data would be lost.

In this scenario, data integrity and performance are at odds. You must choose which one to highlight.

1. To set CTE-U for **optimal data integrity**, type the following command:

```
voradmin secfs config block_o_direct 1
```

2. To set CTE-U for **optimal performance**, type the following command:

```
voradmin secfs config block_o_direct 0
```

Note

The commands listed in the steps above will change the `block_o_direct` parameter in CipherTrust Transparent Encryption UserSpace, in the `config.yaml` file located in: `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/conf/secfs_config.yaml`

Integrating and Configuring EDB

This chapter describes how to configure and integrate Enterprise DB Postgres Advanced Server (EDB) with CTE in Linux. It contains the following sections:

- [Preparing to Create GuardPoints](#)
- [Integration with CTE](#)

Overview

EDB provides database management software to get more functionality from PostgreSQL. EDB offers secure, scalable, advanced and enterprise-class PostgreSQL solutions. Advanced Server extends PostgreSQL with the security and performance features that enterprises need. It's also compatible with Oracle databases.

Prerequisites

Refer to [EDB documentation](#) for information on how to setup and configure EnterpriseDB.

Preparing to Create GuardPoints

Before you can safely reboot your machine, create GuardPoints, and administer any of the services, you must perform the following steps:

1. Stop the EDB service.
2. Open the `/lib/systemd/system/edb-as-13.service` file.
3. Below the `[Unit]` section, add the following line: `Requires=secfs-fs-barrier.service`.
4. Save the file and exit.
5. Open the file: `/lib/systemd/system/secfs-fs-barrier.service`.

Note

If using CTE-U, open the file: `secfs-fuse.service`.

6. At the end of the `[Before]` clause, add `edb-as-13.service`.
7. Save the file and exit.
8. Type: `systemctl daemon-reload`.
9. Type: `systemctl start edb-as-13.service`.
10. Reboot the system.
11. Stop the EDB.
12. Restart SecFS.
13. Start the EDB service again.

Integration with CTE

The following describes how to integrate EDB with CTE using an offline dataxform policy:

1. Enable and start EDB.
2. Create a database with sample data.
3. Install the latest CTE build. Refer to the [CTE Agent Linux Quick Start Guide](#) for more information.
4. Register CTE with a CipherTrust Manager.

5. Stop the EDB service.
6. Guard the EDB data and log directories with a Dataxform policy.

For example, create a policy that transforms from Clear key to AES256.
7. Perform a data transformation on both directories.
8. After Dataxform finishes, guard both directories with a policy using the correct key.

For example, use AES256 on both directories.
9. After the database and log directories are guarded, start the EDB service again.

Integration with Pacemaker

This document covers the following information:

- Using CTE with Pacemaker
- Performing CTE maintenance with LDT GuardPoints and a Pacemaker Setup

Performing CTE maintenance with an LDT GuardPoint in a Pacemaker Setup

Unguard the LDT GuardPoint with Pacemaker setup

1. Stop the SQL server, type:

```
sudo systemctl stop mssql-server
```

2. Delete the existing resource constraints from LDT and the colocation from the Pacemaker setup.

Example

A. If it exists, get the ID of the PCS constraint co-location. In the example below the, ID is: `co-location_set_msmsmt`

```
sudo pcs constraint show --full
.
.
.
Resource Sets:
set mssql_fs mssql_gpfs mssql_gpldt sequential=false (id:co-location_set_msmsmt_set) setoptions score=INFINITY (id:co-location_set_msmsmt)
```

B. Remove the PCS constraint co-location and PCS resource, type:

```
sudo pcs constraint remove co-location_set_msmsmt
sudo pcs resource delete mssql-ldtmgp
```

Expected Result: Current LDT GuardPoint status should be now be: unguarded.

Example

```
secfsd -status guard
```

Response

GuardPoint s	Reason	Policy	Type	ConfigState	Statu
-----	-----	-----	----	-----	
-----	-----				
/var/opt/mssql/LDT		LDT_clear_to_CS1_aes256_onhost	manual	unguarded	not g
uarded	Inactive				

3. Unguard the LDT GuardPoint from the Cluster Host Group in CipherTrust Manager.

Expected Result: The LDT GuardPoint should no longer be displayed when `secfsd -status guard` is executed.

Perform CTE maintenance

Now you can perform CipherTrust Transparent Encryption maintenance tasks that require stopping secfs such as:

- Stop CipherTrust Transparent Encryption
- Upgrade CipherTrust Transparent Encryption
- Uninstall CipherTrust Transparent Encryption
- Create a new baseline database for LDT on the same LDT &{gp}

See [CTE Agent for Linux Advanced Configuration](#) for more information.

Note

Before creating a new baseline database for LDT: Ensure that your target LDT GuardPoint path does not have an `ldt xattr` value on it so that the directory can trigger the initial rekey at the start of guarding. If it does have an `ldt xattr` value from a previous setup, then use the command `voradmin`

```
ldt xattr delete` to remove the old xattr value.
```

Re-Enable LDT GuardPoint with Pacemaker Setup

1. Re-enable the LDT GuardPoint from the Cluster Host Group in CipherTrust Manager. Wait until the GuardPoint is visible again and in the `unguarded` state before moving to the next step below.

Example

```
# secfsd -status guard
```

Response

GuardPoint	Policy	Type	ConfigState	Statu
s Reason				
-----	-----	----	-----	
-----	-----			
/var/opt/mssql/LDT	LDT_clear_to_CS1_aes256_onhost	manual	unguarded	not g
uarded Inactive				

2. Add the resource `mssql-ldtmgp` back into the Pacemaker setting and verify that it has started:

Example

```
sudo pcs resource create mssql-ldtmgp ocf:heartbeat:mgp mgpdir=/var/opt/mssql/LDT --group Apache_Grp-fs
```

The LDT GuardPoint should now be automatically active again in Pacemaker.

```
# secfsd -status guard
```

Response

GuardPoint	Policy	Type	ConfigState	Statu
s Reason				
-----	-----	----	-----	
-----	-----			
/var/opt/mssql/LDT	LDT_clear_to_CS1_aes256_onhost	manual	guarded	guard
ed N/A				

3. Start SQL server, type:

```
sudo systemctl start mssql-server
```

4. Add the LDT resource constraints and co-location back into the Pacemaker setting.

Example

- A. Add failover resource constraints back:

```
sudo pcs constraint order start mssql_gp1dt then start mssql-ldtmgp  
sudo pcs constraint order stop mssql-ldtmgp then stop mssql_gp1dt
```

- B. If constraint co-location was used, add it back:

```
sudo pcs constraint co-location set mssql_fs mssql_gpfs mssql_gp1dt sequentia  
l=false
```

5. Restart Pacemaker so that it can pick up the newly created resource configurations.

- A. Stop SQL server, type:

```
sudo systemctl stop mssql-server
```

- B. Reboot Pacemaker, type:

```
sudo systemctl restart pacemaker
```

- C. Re-start SQL server, type:

```
sudo systemctl start mssql-server
```

Using CTE with Pacemaker

This chapter describes how to configure CTE with Pacemaker and MySQL on Red Hat 7 or Red Hat 8. It contains the following sections:

- Overview
- Considerations and Requirements
- Creating GuardPoints

Overview

Pacemaker is a high-availability cluster resource manager that runs on a set of hosts (a cluster of nodes) in order to preserve integrity and minimize downtime of desired services (resources). Every resource has a resource agent that abstracts the service it provides and present a consistent view to the cluster.

Thales provides a resource agent for CTE that allows CTE to guard nodes running MySQL databases over an NFS share in a Pacemaker environment.

Considerations and Requirements

- System Requirements:
 - Red Hat 7 or Red Hat 8. Other versions of Red Hat are not supported.
 - Pacemaker with Corosync and the MySQL database service configured. Make sure that the Pacemaker properties settings for features such as STONITH and quorum are correct based on your Pacemaker environment.

Note

Other database applications may be used instead of MySQL, but Thales has only tested the CTE resource agent with MySQL.

- The CTE resource agent supports manual GuardPoints on a device or folder. Automatic GuardPoints are not supported.
- The CTE resource agent supports GuardPoints created from Standard or Live Data Transformation policies. It does not support IDT-Capable GuardPoints or CTE-Efficient StorageGuardPoints.
- If you install Pacemaker after you have installed CTE, you must copy the CTE resource agent to the `ofc` directory.

```
cp /opt/vormetric/DataSecurityExpert/agent/secfs/systemd/pacemaker_ra_mgp //CTE-U
cp /opt/vormetric/DataSecurityExpert/agent/secfs/.sec/bin/pacemaker_ra_mgp //CTE
```

- Upgrades to the CTE resource agent will require using Pacemaker to put each node into maintenance mode while the upgrade is performed.

Creating GuardPoints

1. Install the CTE Agent on each node in the Pacemaker cluster, and register that node in the same domain in your key manager. For details, see [Getting Started with CTE for Linux](#).

2. In your key manager, do the following:

- Create a manual GuardPoint for the MySQL data directory `/var/lib/mysql/` on all of the nodes in the cluster. You can use either a Standard or a Live Data Transformation policy to create the GuardPoint, but you must use the same policy on the GuardPoint for each node.
- Create any other manual GuardPoints you want to use. Each GuardPoint must be created on all nodes in the cluster and each set of GuardPoints must use the same policy.

For example, if you have three nodes in the cluster and you want to add a Standard GuardPoint for `/hr/shared/files` and a Live Data Transformation GuardPoint for `/dir/accounting/data`, on each of the three nodes in the cluster you would create:

- A Standard or Live Data Transformation GuardPoint for `/var/lib/mysql/`.
- A Standard GuardPoint for `/hr/shared/files`.
- A Live Data Transformation GuardPoint for `/dir/accounting/data`.

3. Select one of the nodes in your cluster and log into that node as `root`.

4. On the selected node, add a Pacemaker resource for the manual GuardPoint using the following command:

```
pcs resource create mysql-mgp ocf:heartbeat:mgp mgpdir=/var/lib/mysql \
[start_services=true] [stop_services=false]
```

where:

- `start_services=true` is an optional command that tells the resource agent to start the CTE services before enabling any manual GuardPoints. The options are `true` or `false`, and the default is `true`.
- `stop_services=false` is an optional command that tells the resource agent to stop the CTE services after disabling any manual GuardPoints. The options are `true` or `false`, and the default is `false`.

5. Create the required resource groups, colocation settings, and constraints.

Warning

If the resource groups and colocation constraints are not configured properly, the PCS cluster could run resources on multiple nodes. If the ordering constraints are not set properly, the cluster could fail to start because the system tries to mount the GuardPoint before the file system has been mounted or tries to unmount the file system before the GuardPoint has been disabled. Make sure that the following resource groups and constraints are set properly.

To do so:

- a. Create a MySQL file system group (`mysql-fsg`) that contains `mysql-fs` and `mysql-mgp` using the following command:

```
pcs resource group add mysql-fsg mysql-fs mysql-mgp
```

- b. Create a MySQL service group (`mysql-sg`) that contains `mysql-server` and `mysql-vip` using the following command:

```
pcs resource group add mysql-sg mysql-vip mysql-server
```

- c. Configure the colocation and ordering constraints so that:

- `mysql-sg` and `mysql-fsg` are colocated.
- `mysql-fs` starts before `mysql-mgp`.
- `mysql-mgp` stops before `mysql-fs`.
- `mysql-fsg` starts before `mysql-sg`.

To do so, use the following commands:

```
pcs constraint colocation add mysql-sg with mysql-fsg
pcs constraint order start mysql-fs then start mysql-mgp
pcs constraint order stop mysql-mgp then stop mysql-fs
pcs constraint order start mysql-fsg then start mysql-sg
```

6. To check the status of the cluster after the configuration is complete, use the `pcs status` command.

Using CTE with SQL Server on Linux on Red Hat 8

Considerations and Requirements

- **System Requirements:**
 - **SQL Server 2019:** Other versions of SQL Server are not supported with CipherTrust Transparent Encryption.
 - **Red Hat 8:** Other versions of Red Hat are not supported with CipherTrust Transparent Encryption.

Note

Other database applications may be used instead of MySQL, but Thales has only tested this feature with MySQL.

- CipherTrust Transparent Encryption agent supports manual GuardPoints on a device or folder for both standalone and cluster SQL Server database. Automatic GuardPoints are supported on a standalone SQL Server database. Automatic GuardPoints are supported on a standalone SQL Server database but not for cluster SQL Server databases.
- The CipherTrust Transparent Encryption resource agent supports GuardPoints created from standard or Live Data Transformation policies. It does not support IDT-Capable GuardPoints or in-place Device GuardPoint GuardPoints.

Create a CTE guarded standalone SQL Server database

1. Configure the target database data and log directory location as mssql, type:

```
sudo /opt/mssql/bin/mssql-conf set <filelocation.defaultdatadir> /u01/app/mssql/data
sudo /opt/mssql/bin/mssql-conf set <filelocation.defaultlogdir> /u01/app/mssql/log
sudo systemctl restart mssql-server
```

2. Guard targeted directory with standard encryption policy using CS1 or CBC keys of either 128aes or 256aes encryption.

Example

Policy Type: **Standard**

Rule	Value
** Security Rules**	
Action	all_ops
Effect	permit, audit, applykey
** Key Selection Rule**	
Key	aes128 or 256 with CS1 or CBC

```
secfsd -status guard
```

Response

GP Reason	Policy	Type	ConfigState	Status
-----	-----	----	-----	-----

```

      /u01/app/mssql/data      encrypt_cs1_aes128_all  local  guarded  guarde
d  N/A
      /u01/app/mssql/data      encrypt_cbc_aes256_all  local  guarded  guarde
d  N/A

```

3. Create a target SQL Server database on a guarded directory as mssql, type:

```

sqlcmd -S localhost -U SA -P '<password>'
CREATE DATABASE <targetdb>
go

```

4. Verify that data and log files are residing in the newly designated directory:

```

use <targetdb>
SELECT filename from sysfiles
GO

```

Expected results: Should see data/log file in a guarded directory:

```

/u01/app/mssql/data/testdb.mdf
/u01/app/mssql/log/testdb_log.ldf

```

Convert a baseline SQL Server database to a CTE GuardPoint using Dataxform

1. Shutdown the SQL Server service, type:

```

sudo systemctl stop mssql-server
systemctl status mssql-server

```

2. Create an online policy using CS1 or CBC keys of either 128aes or 256aes encryption.

Example of aes256

Policy Name: dxf_clear_to_cbc_aes250_onhost

Policy Type: Standard

Rule	Value
** Security Rules**	
Action	key_ops

Rule	Value
Effect	permit, applykey
** Key Selection Rule**	
Key	clear_key
Data Transformation	
Key	cbc_aes256_onhost

3. Add the GuardPoint with the policy `dxfclear_to_aes256_onhost` to the targeted baseline database data/log directory, type:

```
secfsd -status guard
```

Response

```
GuardPoint      Policy                                     Type  ConfigState  Statu
s      Reason
-----
-----
/u01/app/mssql/log    dxfclear_to_cbc_aes250_onhost  local  guarded      guard
ed N/A
/u01/app/mssql/data   dxfclear_to_cbc_aes250_onhost  local  guarded      guard
ed N/A
```

4. Run the `dataxform` command with the above policy as the root user.

```
dataxform --rekey --cleanup_on_success --gp /u01/app/mssql/dataxform/data
dataxform --rekey --cleanup_on_success --gp /u01/app/mssql/dataxform/log
```

Example

```
dataxform --rekey --eanup_on_success --gp /u01/app/mssql/dataxform/data
```

Response

```
Checking if `/u01/app/mssql/dataxform/data` is a guard point with a rekey poli
cy applied
`/u01/app/mssql/dataxform/data` is a guard point with a rekey policy applied
About to perform the requested data transform operation
-- Be sure to back up your data
```

```
-- Please do not attempt to terminate the application
Do you wish to continue (y/n)?y
.
.
.
Data transform for guard point /data1/oracle/oradata/xformdb finished
About to remove the data transformation status files
Do you wish to continue (y/n)?y
Removal of data transformation status files completed
```

5. Unguard GuardPoints `/u01/app/mssql/dataxform/data` and `/u01/app/mssql/dataxform/data` from policy `dxfc_clear_to_aes256_onhost`.
6. Guard these GuardPoints again with a standard policy which encrypts using the same open aes256 key policy as `dxfc_clear_to_cbc_aes256_onhost`.

```
secfsd -status guard
```

Response

GuardPoint son	Policy	Type	ConfigState	Status	Rea
-----	-----	----	-----	-----	
/u01/app/mssql/data	encrypt_cbc_aes256_all	local	guarded	guarded	N/A
/u01/app/mssql/log	encrypt_cbc_aes256_all	local	guarded	guarded	N/A

7. Start the database and then test to see if the data is accessible, type:

```
sudo systemctl start mssql-server
sqlcmd -S localhost -U SA -P '<password>'
use <targetdb>
SELECT filename from sysfiles
go
```

Expected results: You should be able to log into your targeted transformed database and query system files.

1. Enable the LDT setting in CipherTrust Manager using one of the following methods:
 - Install agent to your targeted database host with LDT enabled [Configuring CTE with CipherTrust Manager](#).
 - Enable LDT on an existing CipherTrust Transparent Encryption installed host using the [CM GUI](#).
2. Create a targeted new baseline in the SQL Server database:

Example

```
sudo /opt/mssql/bin/mssql-conf set filelocation.defaultdatadir /var/opt/mssql/LDT/data
sudo /opt/mssql/bin/mssql-conf set filelocation.defaultlogdir /var/opt/mssql/LDT/data
sudo systemctl restart mssql-server
systemctl status mssql-server
sqlcmd -S localhost -U SA -P '<password>'
CREATE DATABASE `<targetdb>`
SELECT Name from sys.Databases
go
```

3. Create an LDT encryption policy using CS1 or CBC keys of either 128aes or 256aes.

Example

Field	Value
Name	LDT_clear_to_CS1_aes256_onhost_key
Expiration Date	<target date>
Algorithm	AES256 or AES128
Encryption Mode	CBC_CS1 or CBC
Key Type	Cache on Host
Automatic Key Rotation	Selected
Key Version Life Span (days)	<target #>

4. Create an online LDT policy using the key created in the previous step.

Example for CBC_CS1 with AES256

Policy Name: LDT_clear_to_CS1_aes256_onhost

Security Rules

Rule	Action
Order 1	
Action	key_op
Effect	Permit, Apply Key
Browsing	No

Rule	Action
Order 2	
Action	all_ops
Effect	Permit, Audit, Apply Key
Browsing	Yes

Rule	Action
Order 3	
Action	all_ops
Effect	Deny, Audit
Browsing	Yes

Key Selection Rule:

Key	Description
Order 1	
Current Key	clear_key
Transformation Key	LDT_clear_to_CS1_aes256_onhost_key
Exclusion Rule	No

5. Stop the SQL Server, type:

```
sudo systemctl stop mssql-server
systemctl status mssql-server
```

6. Guard the new LDT baseline database with the LDT policy created in the previous step.

```
secfsd -status guard
```

Response

```
GuardPoint          Policy          Type          Con
figState  Status  Reason
-----
/var/opt/mssql/LDT/data  LDT_clear_to_CS1_aes256_onhost  local  guarded
```

```
guarded N/A
```

Wait for the Rekey Status in CipherTrust Manager to display: **Rekeyed**.

7. Run LDT with the same policy to verify the transformation of the baseline database.

```
voradmin ldt attr get <data/log directory of baseline database>
```

Example:

```
voradmin ldt attr get /var/opt/mssql/LDT/data
```

Response

```
LDT stats: version=6, rekey_status=rekeyed
  Number of times rekeyed:          1 time
  Rekey start time:                 2022/09/02 05:41:26
  Last rekey completion time:       2022/09/02 05:41:28
  Estimated rekey completion time:  N/A
  Policy key version:               0
  Pushed Policy key version:        0
  Policy ID:
    1001
  Data stats:
    total=16.0MB, rekeyed=11.0MB
    truncated=0.0MB, sparse=5.0MB
  File stats:
    total=2, rekeyed=2, failed=0
    passed=0, skipped=0, created=0, removed=0, excluded=0
```

Expected results:

- No errors in output
- rekey_status=rekeyed

Note

Do not start the next step until rekey_status = rekeyed.

8. Restart the SQL Server, type:

```
su - mssql
sudo systemctl start mssql-server
systemctl status mssql-server
```

9. Access the targeted database and query the data, type:

```
sqlcmd -S localhost -U SA -P '<password>'
use <targetdb>
use <targetdb>
SELECT filename from sysfiles
go
```

Expected results: You should be able to log into your targeted database and query system files.

Configuring Support for SAP HANA

This section describes SAP HANA, which provides automatic host-failover support. It contains the following topics:

- [Overview](#)
- [Customizing CTE for SAP HANA in HA Mode](#)
- [Using SAP HANA with LDT](#)
- [Setting Memory Allocation](#)

Overview

SAP HANA provides automatic host-failover support. CTE works with HANA fibre storage systems to enable and disable GuardPoints when a protected host starts, stops, or fails over to standby host.

CipherTrust Transparent Encryption - SAP HANA (CTE-SAP HANA) supports non-shared storage where each HANA node has its own separate storage volumes. CTE-SAP HANA provides customized scripts to support startups, shutdowns, and fail overs.

HANA attaches logical unit number (LUNs) or logical volume management (LVMs) using a Fibre Storage Connector (fcClient) providers. Thales provides hooks that are called by the HANA fcClient providers that manage guarding or unguarding of storage locations.

Note

Thales recommends using host groups to manage configuring in a clustered host environment.

Customizing CTE for SAP HANA in HA Mode

Caution

The following procedure only applies if multiple HANA nodes are configured in a high availability (HA) environment. If you are installing CTE on a single HANA node, do not change the default HANA or CTE settings.

1. Go to the installation directory:

```
cd /opt/vormetric/DataSecurityExpert/agent/secfs/saphana
```

2. If required, edit the appropriate CTE `fcClient` refined script:

Script file	Use
<code>fcClientRefinedVTE.py</code>	fcClient provider for LUN
<code>fcClientLVMRefinedVTE.py</code>	fcClientLVM provider for LVMs

3. Copy the appropriate script file to a shared location that is accessible to all nodes. In a HANA cluster environment, all nodes require access to the CTE scripts.
4. Edit the storage section of the `global.ini` file to indicate the corresponding CTE `fcClient` as the High Availability (HA) provider and to point to the location of the CTE script.

LUN Example

```
[storage]
  ha_provider = fcClientRefinedVTE
  ha_provider_path = /hana/shared/myFcClient
```

If necessary, enable debug tracing:

```
[trace]
  ha_provider = debug
  ha_fcclient = debug
  ha_fcclientrefinedvte = debug
```

LVM Example

```
[storage]
```

```
ha_provider = fcClientLVMRefinedVTE
ha_provider_path = /hana/shared/myFcClient
```

If necessary, enable debug tracing:

```
[trace]
  ha_provider = debug
  ha_fcclientlvm = debug
  ha_fcclientlvmrefinedvte = debug
```

5. Use the same CTE agent with all hosts, including standby hosts.
6. Ensure that `/etc/sudoers` includes the following:

```
<sid>adm ALL=NOPASSWD: /usr/bin/secfsd
```

7. Enable the guard paths at the mount-point level.

For example, individual guards were placed on `/hana/data/HAN/mnt00001`, `/hana/data/HAN/mnt00002`, and so forth.

- a. Use a similar naming practice for log partitions, such as `/hana/log/HAN/mnt00001`, and so forth.
 - b. Place the guard at the mount-point level. The guarded paths must match the corresponding data and log mount paths.
8. Configure GuardPoints as type `manual`. You must enable and disable the GuardPoints immediately after the device is attached, or just prior to detachment.

The reason for manual GuardPoints is that it invokes guarding and unguarding from within the HANA during the startup, shutdown, or failover process. The process resembles that of mounting and unmounting guarded auto-mount points.

9. Configure all GuardPoints so that they are available in the standby host, so that any data and log partitions that fail over from any host can be guarded on the standby.

Thales recommends that you configure all GuardPoints on all hosts, because a failed-over active host can then become the new standby, and will require all available GuardPoints.

Example

The following is an example of the data and log volumes for the host that are mounted.

```
/dev/mapper/VG_HAN_DATA_1-LV_HAN_DATA_1      793971096   3059712  750579916   1%
/hana/data/HAN/mnt00001
```

```

/hana/data/HAN/mnt00001          793971096  3059712  750579916  1% /han
a/data/HAN/mnt00001
/dev/mapper/VG_HAN_LOG_1-LV_HAN_LOG_1  496233160  2461764  468564152  1% /han
a/log/HAN/mnt00001
/hana/log/HAN/mnt00001          496233160  2461764  468564152  1% /han
a/log/HAN/mnt00001

```

Note that partition `mnt00002` is also configured, although not currently mounted by HANA. The `secfsd` status output should show the GuardPoint configuration as follows:

GuardPoint	Policy	Type	ConfigState	Status	Reason
/hana/data/HAN/mnt00001	my-pol	manual	guarded	guarded	N/A
/hana/log/HAN/mnt00001	my-pol	manual	guarded	guarded	N/A
/hana/data/HAN/mnt00002	my-pol	manual	unguarded	not guarded	Inactive
/hana/log/HAN/mnt00002	my-pol	manual	unguarded	not guarded	Inactive

For more information, see [SAP HANA Fiber Channel Storage Connector Admin Guide](#).

Using SAP HANA with LDT

SAP HANA is compatible with LDT with the following changes:

- You must add additional CTE commands to the HANA administrator entry. Using a text editor, edit `/etc/sudoers` and add entries for `/usr/bin/voradmin` and `/usr/bin/vmsec`:

```

hanadm ALL=NOPASSWD: /usr/bin/secfsd,/usr/bin/voradmin,/usr/bin/vmsec,/sbin/mu
ltipath,/sbin/multipathd,/etc/init.d/multipathd,/usr/bin/sg_persist,/bin/moun
t,/bin/umount,/bin/kill,/usr/bin/lsof,/sbin/vgchange,/sbin/vgscan

```

- If you are using an `ext3` file system, you must mount it with extended attributes. Using a text editor, edit the storage section of the `global.ini` file, type:

```

partition_*_data__mountOptions = -o user_xattr
partition_*_log__mountOptions = -o user_xattr

```

Setting Memory Allocation

There is a limitation in memory allocations for SAP HANA with asynchronous direct I/O. When you use CTE in conjunction with applications like SAP HANA that can process large numbers of direct I/O writes through the Linux AIO interface, CTE can allocate more memory than is desirable.

To limit the amount of memory that CTE consumes for AIO buffers, use the following configuration to limit the amount of memory CTE consumed for AIO buffers:

```
max_aio_memory_limit <MB>
```

The MB value specifies how much memory to allocate to temporary DIO buffers.

Note

If you do not specify a value, the default is 0, which has no memory bounding effect.

Set the option by echoing a value into the `/opt/vormetric/DataSecurityExpert/agent//secfs/.sec/conf/` configuration file. For example:

```
echo 1024 > /opt/vormetric/DataSecurityExpert/agent/ secfs/.sec/conf/max_aio_memory_limit
```

This limits the memory consumed by AIO buffers to 1GB.

Note

You **must restart** CTE after changing any values in the configuration directory to make the changes effective.

Using CTE with GlusterFS

This chapter describes how to configure CTE with GlusterFS. It contains the following sections:

- Overview
- Considerations and Requirements
- Configuring GlusterFS for CTE

Overview

GlusterFS is a scalable network file system suitable for data-intensive tasks such as cloud storage and media streaming. The Gluster share can also be mounted as an NFS client.

Thales provides support for GuardPoints in a Gluster environment.

Considerations and Requirements

- Gluster is supported on Red Hat 8 and Red Hat 9. Other versions of Red Hat are not supported.
- Clients must have gluster-fuse installed.
- Encryption keys for GlusterFS GuardPoints must use the CBC or CBC-CS1 encryption mode.

- The following CTE features are not supported in GlusterFS:
 - Auto-mounted file systems.
 - CTE-Live Data Transformation.
 - IDT-Capable GuardPoints.

Note

In a multi-node configuration, Thales has tested only the close-to-open consistency for GlusterFS. Other consistencies offered by GlusterFS are not guaranteed to work with CTE.

Configuring GlusterFS for CTE

1. On the Gluster server, configure the following Gluster volume properties for all configurations:

- `performance.flush-behind` should be off.
- `network.remote-dio` should be disabled.
- `performance.strict-o-direct` should be on.

For example, if the Gluster volume name is `MyGlusterVolume`, you would enter the following commands:

```
gluster vol set MyGlusterVolume performance.flush-behind off
gluster vol set MyGlusterVolume network.remote-dio disable
gluster vol set MyGlusterVolume performance.strict-o-direct on
```

2. If you want to use CBC-CS1 encryption keys, configure the following additional Gluster volume properties on the Gluster server:

- `performance.read-ahead` should be off.
- `performance.cache-size` should be 1GB.
- `performance.write-behind` should be off.
- `performance.client-io-threads` should be on.

For example:

```
gluster vol set MyGlusterVolume performance.read-ahead off
gluster vol set MyGlusterVolume performance.cache-size 1GB
```

```
gluster vol set MyGlusterVolume performance.write-behind off
gluster vol set MyGlusterVolume performance.client-io-threads on
```

3. On the clients, do the following based on your configuration:

- If the kernel version is *earlier* than version 4.0.0, the Gluster share must be mounted with the `use-readdir=no` mount option.

```
mount -t glusterfs -o acl,use-readdir=no MyGlusterVolume /gluster
```

- If you want to use CBC-CS1 encryption keys, the Gluster share must be mounted with the `direct-io-mode=enable` mount option.

```
mount -t glusterfs -o acl,direct-io-mode=enable MyGlusterVolume /gluster
```

- If you are using only CBC encryption keys with kernel versions 4.0.0 and later, no changes need to be made on the clients.

NetApp Snapshot Directory

This section describes SecFS support for NetApp .snapshot directory over NFS. It contains the following topics:

- [Overview](#)
- [Accessing Snapshots](#)
- [Enabling Snapshots](#)
- [Dataxform Considerations](#)

Overview

The NetApp snapshot directory contains ONTAP snapshot data entries for a specific live volume. Each snapshot is a read-only volume that is automatically mounted over NFS.

A snapshot copy is a read-only image of a traditional, or FlexVol volume, or an aggregate, that captures the state of the file system at a specific point in time.

Data ONTAP maintains a configurable snapshot copy schedule that creates and deletes snapshot copies automatically for each volume.

Accessing snapshots

By default, every volume contains a directory named .snapshot through which users can access previous versions of files. Users can gain access to snapshot copies depending on the file-sharing protocol used, NFS or CIFS. You can also prevent access to snapshot copies.

Snapshot files carry the same read permissions as the original file. A user who has permission to read a file in the volume, can also read that file in a snapshot copy. A user without read permission to the volume cannot read that file in a snapshot copy.

Note

Snapshot copies do not have write permissions.

Snapshot directories only display at the mount point, although they actually exist in every directory in the tree. This means that the `.snapshot` directory is accessible by name in each directory, but is only seen in the output of the `ls` command at the mount point. The snapshots are stamped with the date and time.

Enabling Snapshots

The NetApp storage administrator, or the OnTap device, must configure this feature. No configuration is required through CTE. CTE guards the client directory mounting the OnTap data volume over NFS.

Note

The NetApp documentation is located here: [NetApp Product documentation](#)

Dataxform Considerations

You cannot transform snapshot directory entries with Dataxform with a new key, because the snapshots are read only. You must keep previous keys and alter the running security policy accordingly to maintain access to the older snapshot entries alongside any new snapshots taken with the new key.

Also, any snapshots that get created during the data transform process (this may take a long time) have to be discarded/deleted as it may contain a mix of data blocks encrypted with both old and new keys.

Best Practices

Maintaining keys for access to older snapshots can be tedious and cumbersome. Therefore, the simplest and safest practice is to delete all old snapshots once the data is transformed with a new key.

This allows for all new snapshots to be readable with the new key while old keys can be discarded, unless used in other security policies.

Using CTE with Quantum StorNext

This chapter describes how to configure CTE and Quantum StorNext devices to interoperate to allow CTE policies to apply to storage managed by Quantum StorNext.

This section contains the following topics:

- [Overview of using CTE with Quantum StorNext](#)

- CTE and Quantum StorNext compatibility
- Setting up CTE and Quantum StorNext integration
- Stop secfs before upgrading StorNext LAN clients

Overview of using CTE with Quantum StorNext

Quantum StorNext Fibre Channel-connected devices provide shared file access to third party storage for workstation clients and are optimized for simultaneous access to very large files such as video files. The Quantum StorNext file system is known as SNFS or by its older name, CVFS.

You can encrypt and control access to SNFS files with policies by installing CTE Agents on Linux clients that are configured for access to the SNFS file system. Some limitations apply to this integration, such as supported operating systems, supported SNFS features, concurrent read/write access by multiple clients, and GuardPoint settings (see the next section for more information about these limitations).

CTE and Quantum StorNext Compatibility

The following sections list the supported operating systems and CTE settings supported for use with Quantum StorNext file systems. Important unsupported configuration parameters are also listed.

Supported StorNext Server and Client Configurations

The CTE integration with SNFS file systems works only with certain SNFS versions, SNFS storage policies, and client operating systems.

Configuration parameter	Linux
StorNext (SNFS) operating system version	6.x
StorNext metadata controller (MDC) server OS type	Linux MDC supported
StorNext replication policy	Not supported
StorNext deduplication policy	Not supported
StorNext truncation	Supported
StorNext full and partial backup	Supported
StorNext expand file system	Supported
StorNext data migration	Supported
StorNext read-ahead cache	Disable for use with CTE
Client operating systems	Red Hat Enterprise Linux (RHEL) 7.x
StorNext LAN client	DLC
StorNext mount method: locally mounted directory	Supported
StorNext mount method: CIFS	Not supported
StorNext mount method: NFS	Not supported

Supported GuardPoint and Key Settings for SNFS File Systems

When configuring CTE GuardPoints and keys for SNFS, keep in the mind the compatibility limitations listed in the following table.

!! note

Because AES-CBC-CS1 keys are not supported on Windows, do not create a policy on Linux that uses AES-CBC-CS1 keys if access to the same SNFS GuardPoint is required by both Windows and Linux LAN clients.

Configuration element	Linux
Offline data transformation	Supported
Live Data Transformation (LDT)v	Not supported
Key manager compatibility	See the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> or the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> for your CTE version
Guard unstructured data	Supported
Guard structured data	Not supported
GuardPoint type: Directory (including entire SNFS volume)	Supported
GuardPoint type: Raw device	Not supported
GuardPoint type: Block device	Not supported
GuardPoint mount option: manual guard	Supported
GuardPoint mount option: auto guard	Supported
GuardPoint mount option: automount	Not supported
AES-CBC key type	Supported
AES-CBC-CS1 key type	Supported

Supported Concurrent Access Read/Write Scenarios

If you want to allow access by multiple clients (users) to CTE-protected SNFS files under the same GuardPoint, just read-only access is supported. StorNext file locking is not implemented in CTE, so there is currently no way to prevent concurrent conflicting writes to the same file. As a result, Thales does not support write access to the same GuardPoint from multiple clients.

To enable read access to the same GuardPoint from multiple clients, ensure that all clients are configured to use the same policy and key.

Configuration parameter	Linux
Read/write access from a single LAN client to a GuardPoint	Supported

Configuration parameter	Linux
Read/write access from two or more LAN clients to the same GuardPoint	Not supported
Read-only access from one, two, or more LAN clients to the same GuardPoint	Supported

Setting up CTE and Quantum StorNext Integration

For the most part, CTE integration with Quantum StorNext is the same as for any standard file system. The next section provides an overview of the steps involved in making CTE work with SNFS. Later sections provide more information about the steps that are new or differ significantly from a typical CTE setup.

Integration Task Overview

The table below provides an overview of the steps involved in setting up SNFS and CTE to work together. As noted in the table, some of these tasks are described in the documentation for your selected key manager. Some of these steps may need to be performed by other staff members at your organization if you have divided the security administration duties as recommended by Thales and you don't have access to the key manager.

Task	Key configuration notes	For more information
Install and configure a Quantum StorNext MDC server for use with CTE	Disable the StorNext read-ahead cache. Only certain StorNext policies, features, and mount types are supported. See Supported StorNext Server and Client Configurations .	See Installing and Configuring a Quantum StorNext MDC Server for Use with CTE .
Install and configure Quantum StorNext clients for use with CTE	Ensure that SNFS starts before secfs. See Ensuring that the StorNext SNFS File System Starts Before secfs . Only certain operating systems are supported. See Supported StorNext Server and Client Configurations .	See Installing and configuring Quantum StorNext DLC Clients for Use with CTE .
Create a domain for one or more SNFS hosts, or add them to an existing domain	No difference from standard CTE agent configuration.	See "Domain Management" in your key manager documentation.
Add the host to the key manager	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager documentation.
Install and register the CTE Agent on the host system	No difference in installation.	See Getting Started with CTE for Linux
Create encryption keys (optional)	No difference from standard CTE agent configuration.	See "Managing Keys" in your key manager documentation. For information about AES-CBC-CS1 keys, see Enhanced Encryption Mode .
Configure host groups containing one or more StorNext LAN clients	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager

Task	Key configuration notes	For more information
(optional)		documentation.
Configure policies (including user, process, and resource sets) to control access or enable encryption	No difference from standard CTE agent configuration.	See “Configuring Policies” in your key manager documentation.
Configure one or more GuardPoints	Some GuardPoint settings are not supported. See Supported GuardPoint and Key Settings for SNFS File Systems .	See “Managing GuardPoints” in your key manager documentation

Installing and Configuring a Quantum StorNext MDC Server for Use with CTE

Install and configure a Quantum StorNext metadata controller (MDC) server using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Linux StorNext MDCs. Ensure that you configure the StorNext server to work with the settings supported by CTE as listed in [Supported StorNext Server and Client Configurations](#). For example, you must disable the StorNext read-ahead cache and only certain StorNext policies, features, and mount types are supported.

Installing and Configuring Quantum StorNext DLC Clients for Use with CTE

Install and configure Quantum StorNext DLC clients using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Linux StorNext DLCs.

Ensure that you configure DLC clients to work with the settings supported by CTE as listed in [Supported StorNext Server and Client Configurations](#). For example, only certain operating systems are supported.

Note

Read-only access is supported if multiple StorNext LAN clients will access files in the same GuardPoint. For more information, see [Supported Concurrent Access Read/Write Scenarios](#).

Ensuring that the StorNext SNFS File System Starts Before secfs

For CTE to function properly for Linux SNFS clients, the SNFS service must start before the CTE `secfs` service. Add an entry for the SNFS file system to `/etc/fstab` on each Linux client that has a CTE agent installed on it. Use the following format:

```
/snfs_share /stornext/snfs1 cvfs defaults,diskproxy=client 0 0
```

In this example, `/snfs_share` should be a share that has been exported from the StorNext Server. It should not be a local disk. You may have completed this configuration step as part of the StorNext LAN client installation. See the [Quantum StorNext documentation](#) for more details.

Installing the CTE Agent on Each StorNext LAN client

Install a CTE Agent on each computer that is set up as a StorNext LAN client and for which you want to set policies. For supported operating systems, see the table in [Supported StorNext Server and Client Configurations](#).

Use any installation method supported for your operating system. For details, see [Getting Started with CTE for Linux](#).

Stop secfs Before Upgrading StorNext LAN Clients

Before you upgrade StorNext Linux LAN clients, disable or stop the CTE `secfs` service. To stop the `secfs` service, follow these steps:

1. Log in as root on the computer that contains the LAN client that you want to upgrade.
2. Type the following command: `/etc/vormetric/secfs stop`

After you upgrade the StorNext client, start `secfs` again by logging in as root and running the `/etc/vormetric/secfs start` command.

Using CTE with McAfee Endpoint Security for Linux Threat Prevention

McAfee Endpoint Security for Linux Threat Prevention detects malware such as viruses and handles the malware according to policies that you configure in McAfee ePO. This chapter describes how to configure McAfee and CipherTrust Transparent Encryption to work together.

This section contains the following topics:

- [Supported McAfee Versions and Linux Operating Systems](#)
- [Ensuring the Correct McAfee Service Startup and Shutdown Order](#)
- [Excluding CTE protected directories with McAfee 10.5.x](#)
- [Updating McAfee](#)
- [Virus Scanning Behavior Differences for CIFS and NFS GuardPoints](#)

Supported McAfee Versions and Linux Operating Systems

In general, Thales has verified that CipherTrust Transparent Encryption is compatible with McAfee version 10.6.5 and later on Red Hat Enterprise Linux (RHEL) 7 and RHEL 8. See the most recent *Compatibility Matrix for CipherTrust Transparent Encryption Agent with CipherTrust Manager* or *Compatibility Matrix for CipherTrust Transparent Encryption Agent with Data Security Manager* for details about the versions of McAfee Endpoint Security for Linux Threat Prevention that have been verified to work with CipherTrust Transparent Encryption.

Ensuring the Correct McAfee Service Startup and Shutdown Order

CipherTrust Transparent Encryption services and McAfee services must be started and stopped in the correct order to prevent problems with any data that is guarded by CipherTrust Transparent Encryption. This order is important any time these services need to be started or stopped, such as:

- During the normal startup and shutdown of your Linux host.
- Before enabling a scheduled upgrade of CipherTrust Transparent Encryption.
- Before performing a manual upgrade of CipherTrust Transparent Encryption.
- As needed for maintenance or troubleshooting.

Ensuring the Correct McAfee Service Order in systemd

Configuring the proper startup and shutdown order of CipherTrust Transparent Encryption and McAfee services in `systemd` ensures that the services start in the right order during system startup and shutdown. This is also important if you configure a scheduled upgrade of CipherTrust Transparent Encryption, as CipherTrust Transparent Encryption services will need to be shut down during the upgrade.

The following McAfee services must be configured to start after CipherTrust Transparent Encryption services:

- For McAfee 10.6.6 or later:
 - `mfetpd.service`
 - `mfeespd.service`
- For McAfee 10.6.5 or earlier:
 - `isectpd.service`
 - `isecespd.service`

To configure this behavior, add these services to the `Before=` line in the `secfs-fs-barrier.service` file on your system. The order of these services on the `Before=` line in the `secfs-fs-barrier.service` file does not matter. For more information, see [Location of Application Unit Configuration Files] and [Adding Applications to the `secfs-fs-barrier.service` File].

Starting or Stopping McAfee and CipherTrust Transparent Encryption Manually

When you manually start or stop McAfee and CipherTrust Transparent Encryption, you must do so in the correct order.

To manually stop McAfee and CipherTrust Transparent Encryption:

1. Stop McAfee services using one of the following:

For McAfee 10.6.6 or later:

```
systemctl stop mftpd.service mfeespd.service
```

For McAfee 10.6.5 or earlier:

```
systemctl stop isecesp.service isectpd.service
```

2. Stop CipherTrust Transparent Encryption:

Linux distributions that support <code>systemd</code>	<code>/etc/vormetric/secfs stop</code>
Linux distributions that do not support <code>systemd</code>	<code>service secfs stop</code>

To manually start McAfee and CipherTrust Transparent Encryption:

1. Start CipherTrust Transparent Encryption:

Linux distributions that support <code>systemd</code>	<code>/etc/vormetric/secfs start</code>
Linux distributions that do not support <code>systemd</code>	<code>service secfs start</code>

2. Start McAfee services using one of the following:

For McAfee 10.6.6 or later:

```
systemctl start mftpd.service mfeespd.service
```

For McAfee 10.6.5 or earlier:

```
systemctl start isecesp.service isectpd.service
```

Excluding CTE protected directories with McAfee

Starting with CipherTrust Transparent Encryption v7.2.0, two conflicts exist between McAfee's On-Access Scan and CipherTrust Transparent Encryption when both applications are installed, regardless of installation order. This conflict occurs because McAfee's On-Access Scan tries to scan files in the initial startup (protected) directory, `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/` whenever those files are accessed by CipherTrust Transparent Encryption's own processes and utilities. Access to a CipherTrust Transparent Encryption protected directory, and its subdirectories, is restricted so that no other process or utility can access them.

The fix is to add the CipherTrust Transparent Encryption protected directories to the McAfee On-Access Scan exclusion list:

1. Change the directory. At the command line, type:

- For **McAfee 10.6.5** or prior versions:

```
#cd /opt/isec/ens/threatprevention/bin/
```

- For **McAfee 10.6.6** or subsequent versions:

```
#cd /opt/McAfee/ens/tp/bin
```

2. Add the exclusion to McAfee's On-Access Scan, type:

```
'--addexclusionrw --excludepaths "/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/" --excludesubfolder'
```

The entire exclusion list command should look like the following:

- **McAfee 10.6.5** or prior versions:

```
./isecav --setoasprofileconfig --profile standard --addexclusionrw --excludepaths "/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/" --excludesubfolder
```

- **McAfee 10.6.6** or subsequent versions:

```
./mfetpcli --setoasprofileconfig --profile standard --addexclusionrw --excludepaths "/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/" --excludesubfolder
```

Note

You only need to run this command once.

Updating McAfee

It is not necessary to shut down CipherTrust Transparent Encryption services when you update McAfee Endpoint Security to a new version. Follow the update procedure described by McAfee. Before updating, ensure that the new version of McAfee is compatible with CipherTrust Transparent Encryption as described in [Supported McAfee Versions and Linux Operating Systems].

Note

When you upgrade McAfee, make sure that the current McAfee services are configured to start *after* the CipherTrust Transparent Encryption services in **systemd**. The McAfee service names depend on the version of McAfee that you are using. For details, see [Ensuring the Correct McAfee Service Order in systemd].

Virus Scanning Behavior Differences for CIFS and NFS GuardPoints

By default, on McAfee Endpoint Security, on-access virus scanning for remotely mounted file systems such as CIFS and NFS, is disabled. However, for GuardPoints configured on CIFS and NFS volumes, this default is ignored. So on-access virus scanning is always on for GuardPoints configured on CIFS and NFS volumes. This means that if a process attempts to save an inCipherTrust Transparent Encryption file to a GuardPoint configured on a CIFS or NFS volume, the inCipherTrust Transparent Encryption file will be discovered immediately, if it matches the McAfee malware detection algorithm and handled according to the appropriate malware policy in McAfee ePO.

Using CTE and Database Activity Monitoring (DAM) Simultaneously

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Security administrators can protect execution of processes/binaries on CTE agents from a ptrace attachment. This prevents process injection attacks through ptrace system call. Refer to [Blocking ptrace system calls to prevent process injection attacks](#) for more information.

Using Ptrace and DAM

Thales CipherTrust Transparent Encryption and Imperva Database Activity Monitoring (DAM) can operate simultaneously on the same system if the ptrace attachment is not blocked on the system. Choose one of the following two configuration options from the **Advanced Security Configuration** that do not affect DAM agent functionality.

- **Disabled_for_all**
- **Enabled_for_Authenticators (Default setting)**

Disabling ptrace protection for Imperva DAM processes when setting to Enabled for All

During Imperva DAM and Thales CTE integration testing, Thales discovered that when the **ptrace_configuration** option is set to **enabled_for_all** in CTE, the DAM audit logs do not generate. This is because the **enabled_for_all** option blocks ptrace injection for all system binaries. Imperva DAM uses InjectionManager to inject shared libraries into database processes to monitor database activity. Since CTE blocks all ptrace injections in this mode, DAM fails to inject these shared libraries into the database processes. As a result, no logs are generated or sent to the gateway server.

The solution is for CTE to exempt certain applications from ptrace protection using client settings. You need to specify the binary that performs the tracing, and tag it with **|allow_ptrace|** in the client settings in CipherTrust Manager. If the binary is also listed under a host setting, the tag must be combined accordingly. For example, if the binary falls under the Authenticator client setting, the tag in the client settings should be:


```
|Authenticator+allow_ptrace|
```

Ensuring the Correct CTE/DAM Service Startup and Shutdown Order

CipherTrust Transparent Encryption services and DAM services must be started and stopped in the correct order to prevent problems with any data that is guarded by CipherTrust Transparent Encryption. This order is important any time these services need to be started or stopped, such as:

- During the normal startup and shutdown of your Linux host.
- Before enabling a scheduled upgrade of CipherTrust Transparent Encryption.
- Before performing a manual upgrade of CipherTrust Transparent Encryption.
- As needed for maintenance or troubleshooting.

Starting or Stopping DAM and CipherTrust Transparent Encryption Manually

Warning

CTE cannot be stopped while the DAM agent is running.

CTE Commands for Stopping and Starting the Agent

Command	Command syntax for Linux distros that support systemd	Command syntax for Linux distros that DO NOT support systemd
Start	<code>/etc/vormetric/secfs start</code>	<code>service secfs start</code>
Restart	<code>/etc/vormetric/secfs restart</code>	<code>service secfs restart</code>
Stop	<code>/etc/vormetric/secfs stop</code>	<code>service secfs stop</code>
Check status	<code>/etc/vormetric/secfs status</code>	<code>service secfs status</code>

DAM Commands for Stopping and Starting the Agent

Command	Command syntax	Comment
Start	<code><DAM-remote-agent-install-</code>	

Command	Command syntax	Comment
	<code>directory>/ragent/bin/ rainit start</code>	
	<code><DAM-remote-agent- install- directory>/installer/bin/ rainstallerinit start</code>	Required if it exists
Stop	<code><DAM-remote-agent- install- directory>/ragent/bin/ rainit stop</code>	
	<code><DAM-remote-agent- install- directory>/installer/bin/ rainstallerinit stop</code>	Required if it exists

See [Adding Dependencies to systemd Unit Configuration Files](#) for more information.

Ensuring the proper order

Perform the following steps in this exact order:

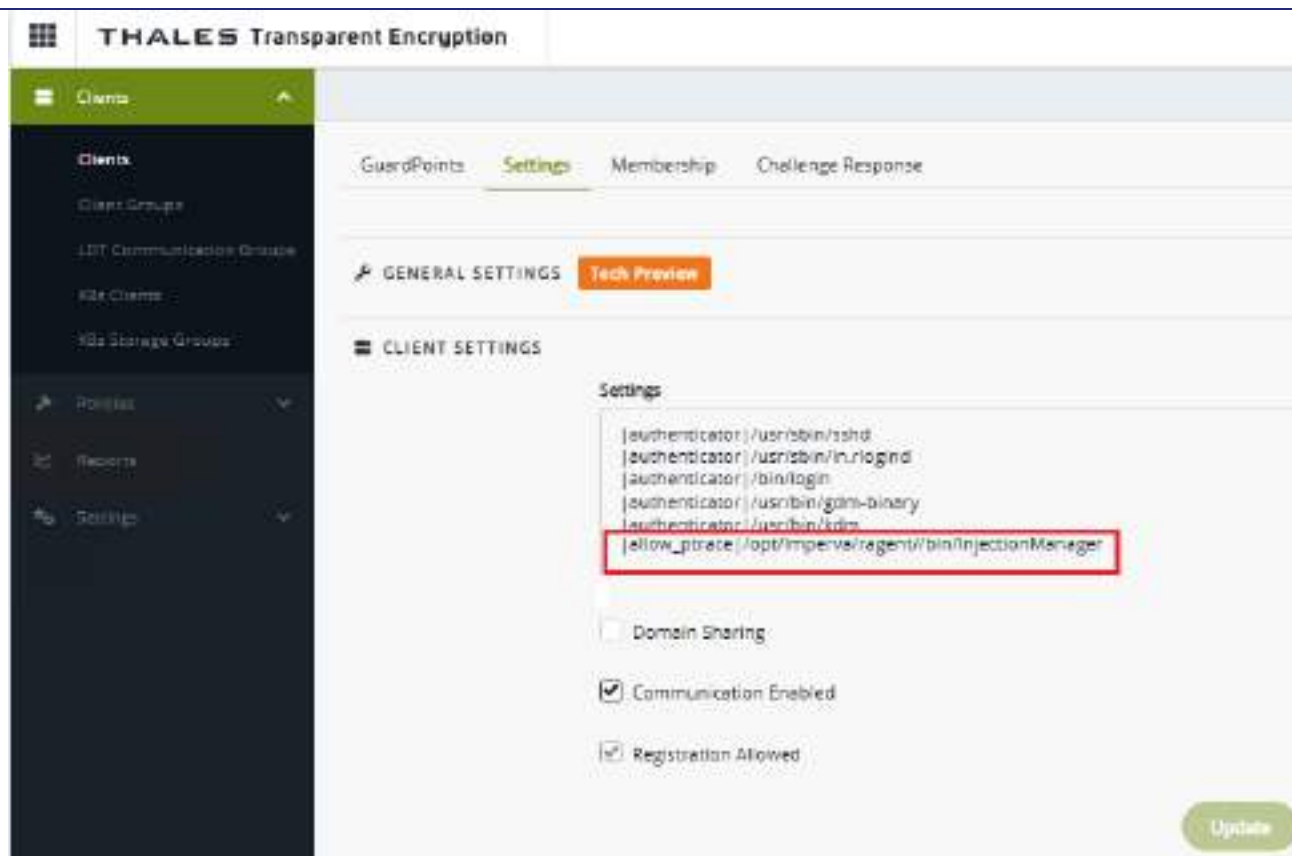
1. Stop the DAM agent monitoring.
2. Stop CipherTrust Transparent Encryption.
3. Perform the CTE or DAM upgrade or maintenance.
4. Start DAM agent monitoring.
5. Start CipherTrust Transparent Encryption.

Prerequisites

1. [Install CTE v7.8.0](#) on the agent and register it with CipherTrust Manager.
2. Ensure that Imperva DAM is installed and configured correctly on the MX server.

Exempting Applications

1. Update the client settings to include the `allow_ptrace` tag for the InjectionManager binary.

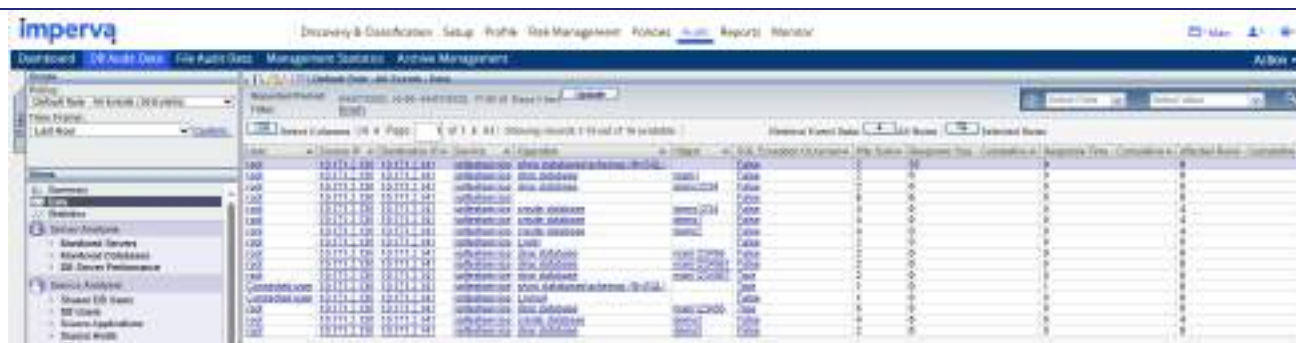


2. In the Client window, click **Advanced Security Configuration** and ensure that **Enabled_For_All** is selected.
3. Restart the MX server agent and database service to apply the updated CTE client settings:
 - a. Stop the DAM agent service.
 - b. Stop the database service.
 - c. Start the database service.
 - d. Start the DAM agent service.

Note

Consult the Imperva documentation for more information.

4. Perform any activity on the database. You should now see this activity reflected in the MX server DB audit logs.



Using CTE with Trend Micro Deep Security Software

Trend Micro's Deep Security software provides comprehensive security in a single solution that is purpose-built for virtual, cloud, and container environments. Thales has verified certain versions of this Trend Deep product for compatibility with CTE on Red Hat Enterprise Linux (RHEL) 7 and RHEL 8.

This section contains the following topics:

- Ensuring Correct Deep Security Service Startup Order
- Updating Deep Security

Ensuring Correct Deep Security Service Startup Order

CTE services and Deep Security services must be started and stopped in the correct order to prevent problems with your data that is guarded by CTE. This order is important any time these services need to be started or stopped, such as:

- During normal startup and shutdown of your Linux host.
- Before enabling a scheduled upgrade of CTE.
- Before performing a manual upgrade of CTE.
- As needed for maintenance or troubleshooting.

Ensuring Correct Deep Security Service Startup Order in systemd

Configuring the proper startup and shutdown order of CTE and Trend Micro's Deep Security services in `systemd` ensures that the services start in the right order during system startup and shutdown. This is also important if you configure a scheduled upgrade of CTE.

The following Deep Security service must be configured to start after CTE services:

`ds_agent.service`

To configure this behavior, add this service to the `Before=` line in the `secfs-fs-barrier.service` file on your system. The order of these services on the `Before=` line in the `secfs-fs-barrier.service` file does not matter. See [Location of Application Unit Configuration Files](#) for the location of the `secfs-fs-barrier.service` file on your system. See [Adding Applications to the secfs-fs-barrier.service File](#) for information about how to add services to the `secfs-fs-barrier.service` file.

Ensuring Correct Deep Security Service Startup Order Manually

Perform the following commands in this order if you need to stop Deep Security and CTE services manually:

1. Stop Deep Security services:

```
systemctl stop ds_agent.service
```

2. Stop CTE:

Linux distributions that support systemd	<code>/etc/vormetric/secfs stop</code>
Linux distributions that do not support systemd	<code>service secfs stop</code>

Perform the following commands in this order if you need to start Deep Security and CTE services manually:

1. Start CTE:

Linux distributions that support systemd	<code>/etc/vormetric/secfs stop</code>
Linux distributions that do not support systemd	<code>service secfs stop</code>

2. Start Deep Security services:

```
systemctl start ds_agent.service
```

Updating Deep Security

It is not necessary to shut down CTE services when you update Trend Micro Deep Security to a new version. Follow the [Update Deep Security software](#) described by Trend Micro.

CTE for Cloud Object Storage

Note

For CipherTrust Transparent Encryption and CipherTrust Transparent Encryption UserSpace, using, configuring and installing Cloud Object Storage works identically. The product names, CTE and CTE-U, are used interchangeably in the following sections.

This section discusses how to configure CTE for Cloud Object Storage buckets. It contains the following topics:

- [COS Overview and Requirements](#)

-
- CTE COS S3 Installation Overview and Requirements
 - Configure the AWS CLI and COS S3
 - Guard an AWS Bucket
 - Using a COS Proxy Root CA Certificate Information
 - Protecting Python Programs with CTE
 - Creating a COS Policy

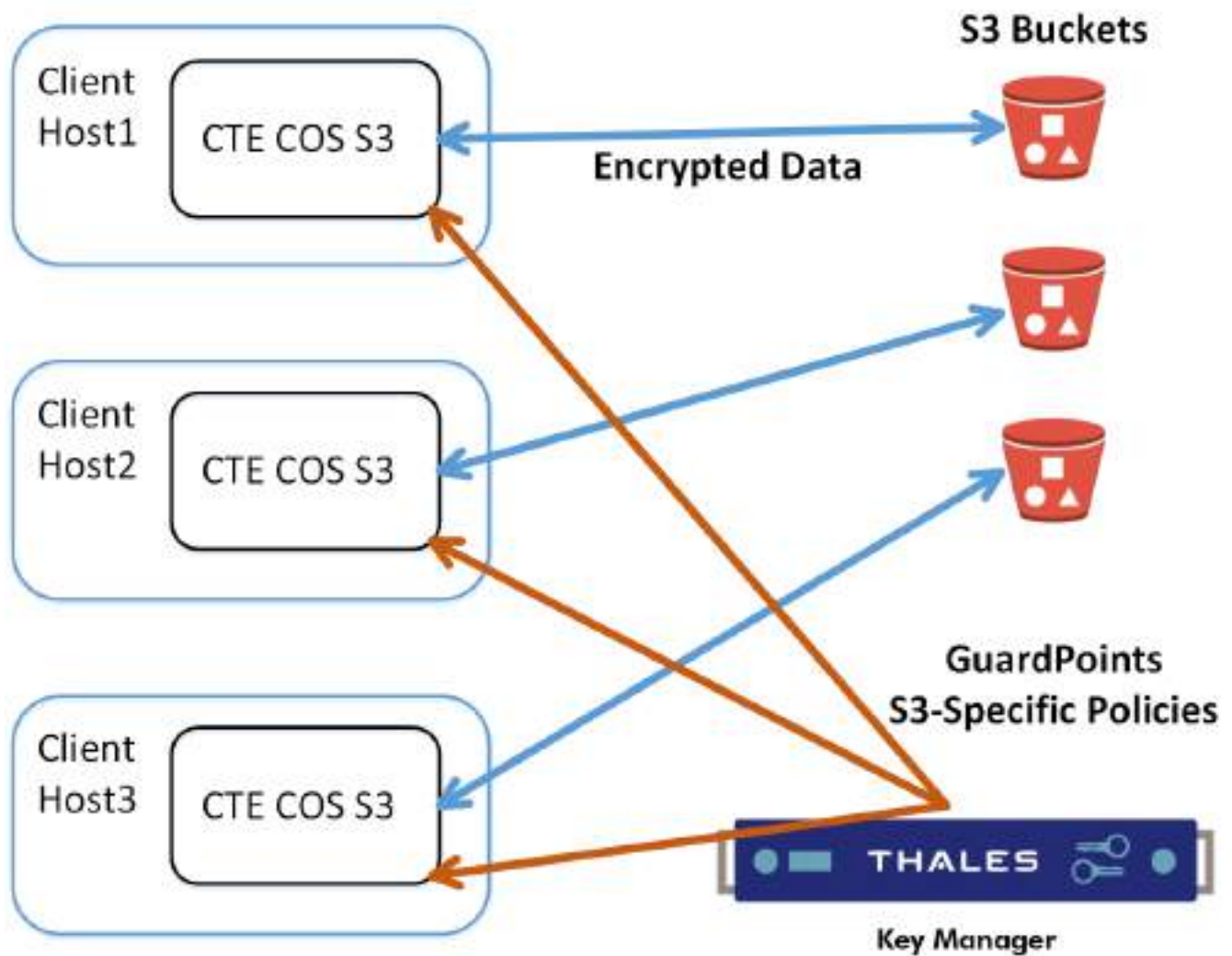
COS Overview and Requirements

CipherTrust Transparent Encryption for Cloud Object Storage (CTE COS) is an object storage service that you can use to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. CTE COS provides management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements.

CTE COS for Amazon Simple Storage Service (CTE COS S3) is an extension to CTE for inline encryption and local host access controls involving applications performing REST-API-based operations to S3 object stores.

CTE COS S3 is not a replacement for AWS IAM access controls which are enforced independently at the AWS server end.

The following diagram shows the high-level CTE COS S3 architecture:



Supported operations

- CTE COS S3 will process only AWS S3 REST https calls issued by applications. The interception is done by a bundled TLS proxy with additional CTE services.
- CTE's traditional access controls and inline encryption are transparently applied during the following operations:
 - Create a bucket
 - Write an object
 - Read an object
 - Delete an object
 - List objects

Limitations

- CTE COS S3 is supported only on RHEL 8 and RHEL 9.
- Only REST API based S3 protocol-aware applications are supported.
- Only locally generated self-signed COS Proxy CA Certificates are supported.
- AWS S3 URL path validations are not currently implemented. CTE COS S3 requires that the user must specify the correct URLs for bucket paths.
- CTE COS S3 permits only AES CBC-CS1 encryption. Encrypted files in protected buckets therefore will prepend the 4K embedded header used in CTE's AES CBC-CS1 encryption. The key manager will enforce usage of AES CBC-CS1 keys within S3 bucket policies.

Multi-part Upload Restrictions

- All upload operations for a multi-part upload must be conducted from the same host.
- Maximum file size upload is 5TB.
- Part sizes during uploads must be identical. The part numbering must be in sequence starting with 1, e.g. 1,2,3,4,... Not 10, 20, 30, etc.
- The part size specified in CTE S3's AWS credential file must match the part size specified within the application.
- Thales recommends that the Content-MD5 header be included in the request message.

System and Software Requirements

- The RHEL 8, or 9 Linux hosts must meet the standard CTE requirements.
- You must have an AWS account
- We recommend that you guard the bucket by restricting it with a CTE COS S3 Role to prevent accidental data corruption from connections outside the control of CTE COS S3. For details, see [Optionally Configure a CTE COS S3 Role for Guarded Buckets](#).
- You must download and install the pre-requisite rpm packages before you install CTE COS S3. For details, see [Install Required Linux Packages](#).
- The CTE Agent must be installed in the default directory on the host. You cannot change the default path if you also enable CTE COS S3.

Client Software Requirements

- Clients must exist on the same host as CTE COS S3. External Client connections will be rejected by the COS Proxy.
- Clients must be AWS S3 protocol aware, and can directly connect to a S3 bucket without the use of an intermediary service, such as the AWS S3 Management Console website.
- Clients must be configured to divert outgoing network connection to a COS proxy (default is localhost:3128 or 127.0.0.1:3128). For more information, see [Configure the AWS CLI Network Proxy](#).
- Clients must use the TLS 1.2 / TLS 1.3 network encryption protocol over TCP/IP to establish connections to the COS proxy.
- Clients must be configured to use the COS CA Root Certificate of the COS proxy to verify and authenticate TLS connections. For more information, see [Configure the AWS CLI to use the COS Root CA Certificate](#).

CTE COS S3 Installation Overview

In order to configure CTE COS S3, you must complete the following tasks.

Note

The AWS CLI is used as a sample application to explain the detailed installation procedure.

1. Install the required packages for CTE COS S3. For details, see [Install Required Linux Packages](#)
2. Install CTE and generate the local COS Proxy CA Certificate. For details, see [Install CTE with COS Service](#)

Note

You can only install the Cloud Object Storage feature during CTE installation. You cannot install it post installation.

3. Configure the client to use the COS Proxy CA Certificate. For details, see [Configure the AWS CLI to use the COS Root CA Certificate](#).
 4. Configure the client to use the COS proxy port. For details, see [Configure the AWS CLI Network Proxy](#).
 5. Configure CTE COS S3 with AWS Credentials. For details, see [Configure CTE COS S3](#).
 6. Optionally configure Role & IAM policies for CTE COS S3 for guarded buckets. For details, see [Optionally Configure a CTE COS S3 Role for Guarded Buckets](#).
-

7. Configure the guarded buckets. For details, see [Guard an AWS Bucket](#).

Install Required Linux Packages

CTE COS S3 requires the following prerequisite packages:

- `boost-regex`
- `boost-system`
- `boost-thread`
- `libcurl`
- `libtool-ltdl`
- `libxml2`
- `epel-release`.
- `cryptopp` // This package must be installed after `epel-release`.
- `log4cpp` // This package must be installed after `epel-release`.

For example:

```
sudo yum install boost-regex boost-system boost-thread libcurl libtool-ltdl libxml2 epel-release
sudo yum install cryptopp log4cpp
```

CTE COS S3 supports both Python2 and Python3. If both versions of Python are available, CTE COS S3 will use Python3. For either Python package, you also need to install the Python modules "`boto3`" and "`future`" after you install the main python package.

Example for Python2

```
sudo yum install python-pip
sudo pip install boto3 future
```

Example for Python3

```
sudo yum install python3 python3-pip
sudo pip3 install boto3 future
```

Install CTE with COS Service

Note

- You can only install the Cloud Object Storage feature during CTE installation. You cannot install it post installation.
- Do *not* change the default CTE installation directory. CTE must be installed in the default location if you enable Cloud Object Storage.

When the installer asks about Cloud Object Storage, type **Y** and follow the prompts as shown.

```
Do you want this host to have Cloud support enabled on the server? (Y/N) [N]: Y

CTE COS CA Cert is located in /opt/vormetric/DataSecurityExpert/agent/squid/etc/cosCA.crt
Clients must be updated to use the new CA Certificate

Generating certificate signing request for the kernel component...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done. Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.

The following is the fingerprint of the EC CA certificate. Please verify that it matches the fingerprint shown on the Dashboard page of the Management Console.
If they do not match, it can indicate an unsuccessful setup or an attack.
B0:93:C7:67:07:C9:CB:09:E2:21:F1:5C:8A:C8:79:8F:03:86:21:F2
Do the fingerprints match? (Y/N) [N]: Y

Successfully registered the CipherTrust Transparent Encryption Agent with the primary CipherTrust Data Security Server on security.manager.example.com.
Starting CTE Cloud Service
Installation success.
```

Enable COS on an Agent with no COS Service

To enable COS on a system that has CTE installed but no COS Service:

- Uninstall CTE completely.
- Reinstall CTE and select **Yes** when asked:

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]: Y
```

Uninstall COS from an Agent

Currently, the only method for uninstalling COS is as follows:

1. Uninstall CTE completely.
2. Delete the host/client from CM.
3. Re-register the host/client.
4. Reinstall CTE and select **NO** when asked:

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]: N
```

Configure the AWS CLI to use the COS Root CA Certificate

You must configure the AWS CLI to use the COS root CA certificate. To do so, edit `~/.aws/config` and add the following line to the AWS cli configuration file:

```
ca_bundle = /opt/vormetric/DataSecurityExpert/agent/squid/etc/cosCA.crt
```

For example:

```
cat ~/.aws/config
[default]
output = json
Region = us-west-1
ca_bundle = /opt/vormetric/DataSecurityExpert/agent/squid/etc/cosCA.crt
```

Configure the AWS CLI Network Proxy

All communications between client applications and the AWS server must be done through the COS proxy and the environment variable `HTTPS_PROXY` or `https_proxy` should be set. If both variables are defined, then the AWS CLI will use `https_proxy`.

For example:

```
export HTTPS_PROXY=localhost:3128
```

Configure CTE COS S3

In order for CTE COS S3 to do transparent encryption and decryption, all requests sent to the AWS S3 server must be generated and signed using valid AWS credentials. In order to retrieve these credentials for CTE COS S3, you can use any of the following methods:

- **The User Supplies the Credentials for the User's AWS Account**

The application can send the long-term credentials from the user's AWS account to CTE COS S3. These credentials do not expire.

For the AWS CLI, the credentials are in the credential file `~/.aws/credentials`. The user credentials consists of an Access Key ID and a Secret Access Key. For details about accessing the user's credentials, see your AWS documentation.

To add the AWS credentials to CTE COS S3, use the `voradmin cos s3 cred add` command:

```
voradmin cos s3 cred add [<aws_key_id> <aws_secret_key>]
```

where:

- `<aws_key_id>` is the AWS secret key ID from the `.aws/credentials` file.
- `<aws_secret_key>` is the AWS secret key from the same file.

For example:

```
voradmin cos s3 cred add AKIA****P KQSm****D
```

The User Supplies Temporary Security Credentials

You can use temporary security credentials, which expire after a short period of time. Usually temporary security credential are obtained through IAM roles and other features of the AWS Security Token Service.

Use the `voradmin cos s3 cred add` command, described above, to add the temporary credential to CTE COS S3.

CTE COS S3 Captures Temporary Credentials

CTE COS S3 can capture a temporary, newly generated, security credential and automatically add it to CTE COS S3 if the application generates the temporary security credential using the AWS Security Token Service with one of the following 3 actions and `HTTPS_PROXY` is set to `localhost:3128`.

- `AssumeRole`
- `AssumeRoleWithSAML`
- `AssumeRoleWithWebIdentity`

No other action is required from the application or user.

CTE COS S3 Retrieves Credentials from EC2 Instance Metadata Service

When CTE COS S3 is installed on AWS EC2 instance with an attached role, CTE COS S3 automatically retrieves the credential from Instance Metadata Service and uses it. However, if CTE COS S3 already has a valid credential given by the user or admin using the `voradmin` command, then that credential will be used instead. For information about setting up an IAM Role, see your AWS EC2 documentation.

No action is required from application or user.

Setting the Default Chunk Size

Note

If a chunk size is configured in the AWS CLI configuration, you must configure the same chunk size for CTE COS S3.

The default chunk size for multi-part uploads is 8 MB. To change the chunk size, use the following command:

```
voradmin cos s3 chunk [<aws_key_id> <aws_secret_key>] [<chunk_size>]
```

where:

- `<aws_key_id>` is the AWS secret key ID from the `.aws/credentials` file.
- `<aws_secret_key>` is the AWS secret key from the same file.
- `<chunk_size>` is the number of MB per chunk that you want to use for multi-part uploads. Enter an integer between 5 and 5120.

The `voradmin` command prompts for any of the optional parameters that you do not specify on the command.

For example, to set a chunk size of 250MB, you would enter:

```
voradmin cos s3 chunk AKIA****P KQSm****D 250
```

Optionally Support other 3rd Party S3 Compatible Storage

CTE COS S3 has a configuration file that lists all supported S3 compatible cloud storages. It is located at:

```
`<installation_directory>/agent/squid/etc/cos.conf`
```

To support a new 3rd party S3 compatible storage:

1. Add a new section to the configuration file with its name and endpoint base url. The following is an example with Wasabi Cloud Storage.

```
[wasabi]
endpoint = wasabisys.com
```

2. Restart CTE COS service using the following command:

```
voradmin cos service stop
voradmin cos service start
```

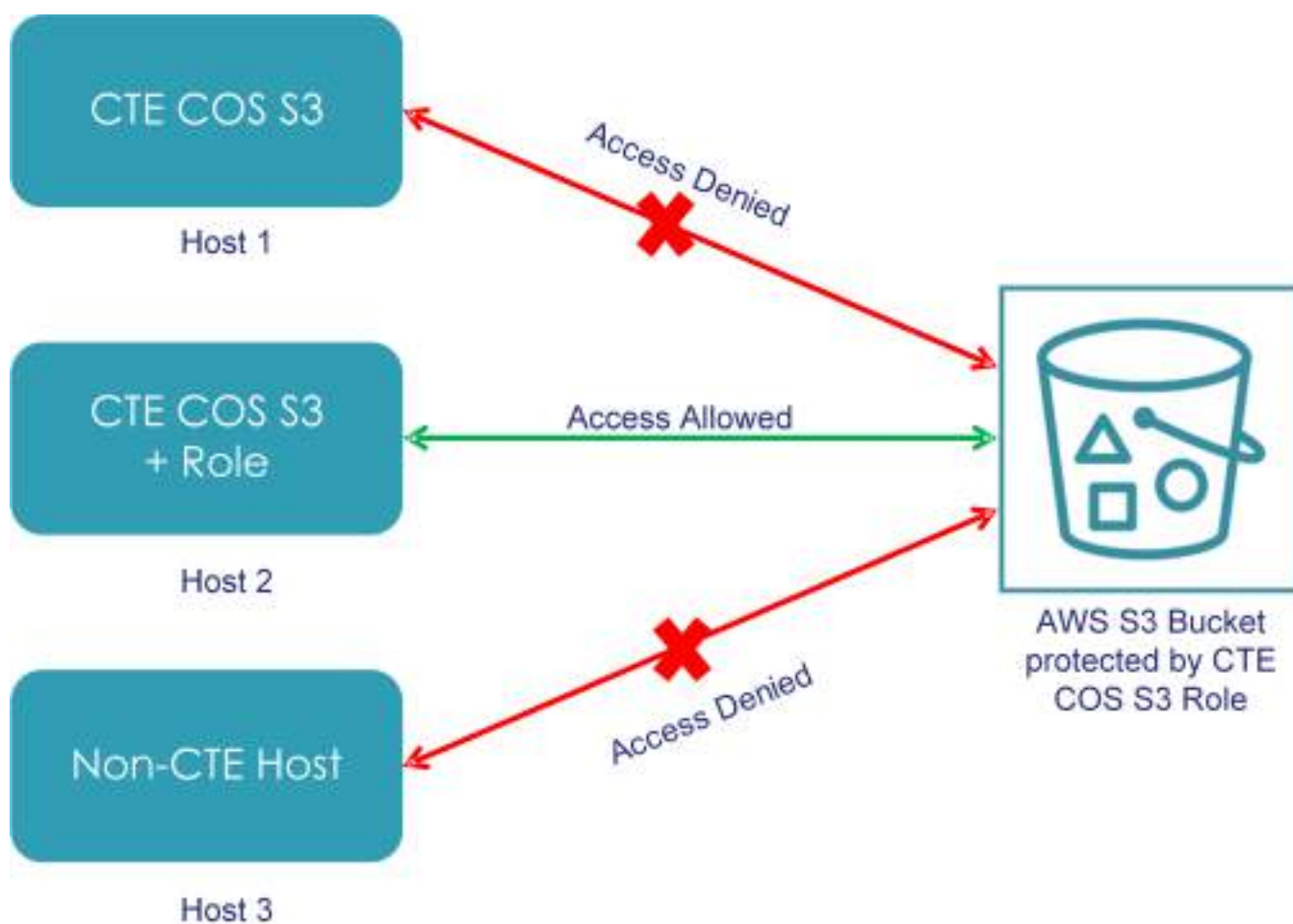
3. Configure credentials and other needed items following the guideline for the 3rd party S3 compatible storage.

Configure a CTE COS S3 Role for Guarded Buckets

AWS provides the IAM Role feature that contains certain specific permissions. A user can assume the IAM Role and therefore take on those permissions. CTE COS S3 provides a special feature using this IAM Role to prevent access to one or more buckets outside the CTE COS S3 protection as shown in the following diagram:

Note

This step is optional.



Only hosts that are configured with the CTE COS S3 Role can access the protected buckets. All other access attempts from any hosts where the CTE COS S3 Role is not configured, including attempts made through the AWS S3 Console, are blocked for the protected buckets.

This is a one-time configuration process. After the CTE COS S3 Role is configured on a host by the system or security administrator, all authorized users in the host can access the protected buckets.

Prerequisites

To set up a CTE COS S3 Role, you need a delegated IAM user, role, and policy. The delegated IAM user should be created by the AWS Administrator without any specific privileges. The role and policy must be created by a user who has at least the following privileges:

- `iam:ListPolicies`
- `iam:CreatePolicy`
- `iam:GetPolicyVersion`
- `iam:ListRoles`
- `iam:ListRolePolicies`
- `iam:ListAttachedRolePolicies`
- `iam:AttachRolePolicy`
- `iam:UpdateAssumeRolePolicy`
- `iam:CreateRole`
- `iam:GetRole`

Procedure

1. In the IAM Management Console, create a policy that allows access to specific S3 resources. You can leave the policy open to include all S3 resources in the account or include only those buckets that require CTE protection. Make sure you name the policy something that you will remember.

Tip

You can also create the policy as an inline policy after you create the CTE COS S3 Role later in this procedure.

For example, you can create a policy called `VTE_S3_Role_Policy` that allows access to the single S3 bucket `vte-cos-s3-rtb`. To verify that the policy restricts access to that bucket, you can look at the Resource allocation in the Policy summary.

The full JSON for the `VTE_S3_Role_Policy` is:

```
{  
  "Version": "2012-10-17",
```

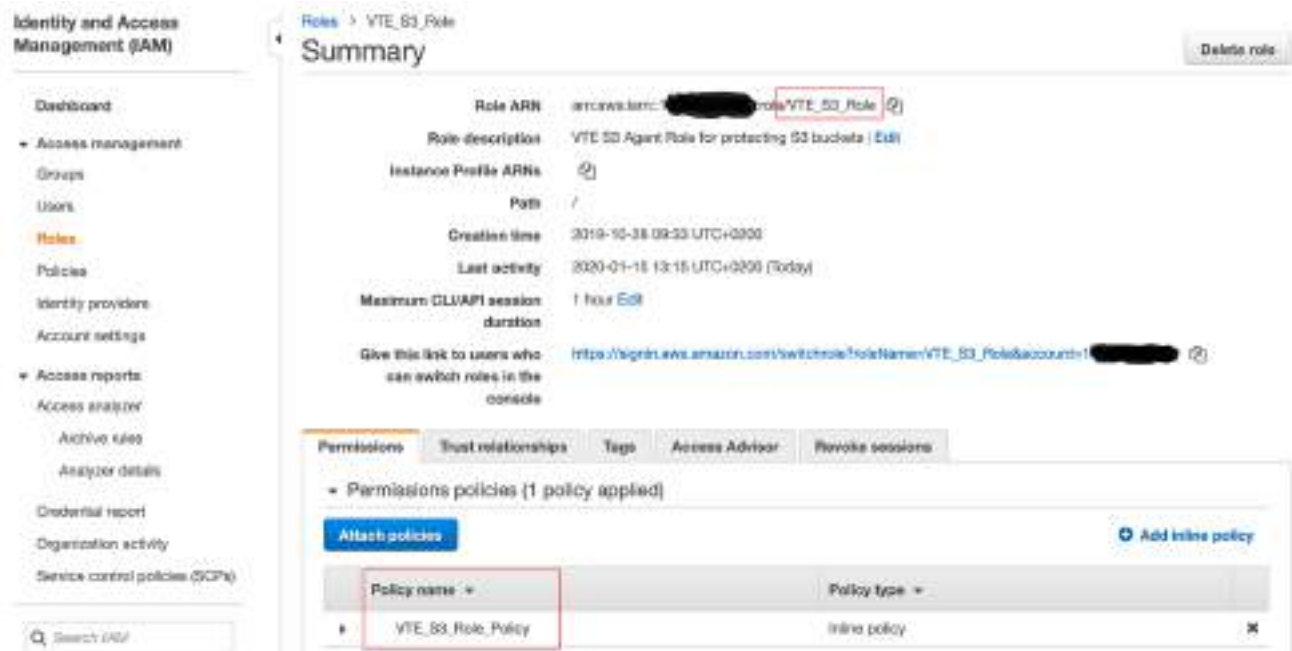


```

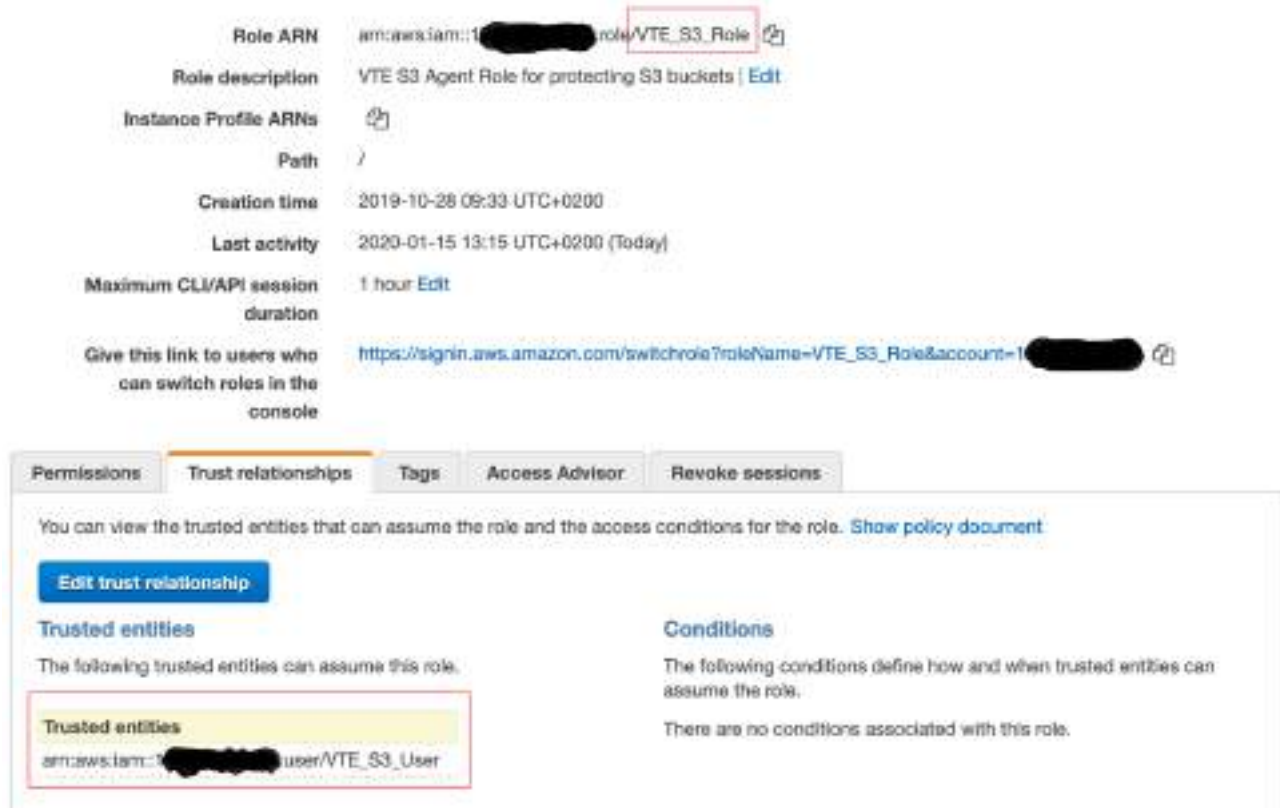
"Statement": [
  {
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": [
      "arn:aws:s3::vte-cos-s3-rtb",
      "arn:aws:s3::vte-cos-s3-rtb/*"
    ]
  }
]
}

```

2. Create a new role that you can use for the CTE COS S3 Role. For example, you could call the role VTE_S3_Role.
3. Assign the CTE COS S3 policy you created to the role, or click **Add inline policy** to create a new policy. For example:



4. Create a delegated IAM user for the CTE COS S3 Role. The user does not require any privileges because its only job is to assume the CTE COS S3 Role. The delegated IAM user can either be in the same account as the role or it can be in a different trusted account. For example, you could create a user called VTE_S3_User with no privileges.
5. Set "Trusted Entities" to the delegated IAM user on the **Trust relationships** tab. For example:



- Configure the CTE COS S3 Role with the credentials of the delegated IAM user you created earlier by entering the following command in the command line on the host system:

```
voradmin cos s3 role config [<aws_key_id> <aws_secret_key> <user_arn> <role_arn>]
```

where:

- `<aws_key_id>` is the AWS secret key ID for the delegated IAM user that you created.
- `<aws_secret_key>` is the AWS secret key or the delegated IAM user that you created.
- `<user_arn>` is the Amazon Resource Name for the delegated IAM user that you created.
- `<role_arn>` is the Amazon Resource Name for the delegated IAM Role that you created.

If you omit any of the optional parameters, the **voradmin** command prompts you for that information.

For example, if the AWS account number for the delegated IAM user is 1XXXXXXXXXXXX, the user name is VTE_S3_User, and the CTE COS S3 Role is VTE_S3_Role, you would enter:

```
voradmin cos s3 role config AKIA****P KQSm****D arn:aws:iam::1XXXXXXXXXXXX:user/VT  
E_S3_User arn:aws:iam::1XXXXXXXXXXXX:role/VTE_S3_Role
```

After you configure the user and assign the CTE COS S3 Role, CTE will access the S3 bucket through the delegated IAM user account using temporary credentials that CTE regenerates periodically. These credentials are

maintained entirely by CTE and are never exposed to end users.

Secure an S3 Bucket with the CTE COS S3 Role

When you enable the CTE COS S3 Role for a bucket, the associated bucket policy prevents unauthorized users from accessing the contents of the bucket. To enable the CTE COS S3 Role for a bucket, use the following command:

```
voradmin cos s3 role secure-bucket <key_id> <secret key> <cos name> <region> <bucket_name>
```

where:

- `<aws_key_id>` is the AWS secret key ID for the delegated IAM user that you created.
- `<aws_secret_key>` is the AWS secret key for the delegated IAM user that you created.
- `<cos name>` is the cloud service name from CTS COS configuration file, `<installation directory>/agent/squid/etc/cos.conf`.
- `<region>` is the region where the S3 bucket is located in the targeted cloud storage service.
- `<bucket_name>` is the name of the S3 bucket on which you want to enable the CTE COS S3 Role.

For example, if the bucket name is `vte-cos-s3-rtb`, you would enter:

```
voradmin cos s3 role secure-bucket AKIA****P KQSm****D aws us-west-1 vte-cos-s3-rtb
```

Disable the CTE COS S3 Role for an S3 Bucket

To remove the CTE COS S3 Role restrictions associated with a bucket, use the following command:

```
voradmin cos s3 role release-bucket <key_id> <secret key> <cos name> <region> <bucket_name>
```

where:

- `<aws_key_id>` is the AWS secret key ID for the delegated IAM user that you created.
- `<aws_secret_key>` is the AWS secret key for the delegated IAM user that you created.
- `<cos name>` is the cloud service name from CTS COS configuration file, `/agent/squid/etc/cos.conf`.
- `<region>` is the region where the S3 bucket is located in the targeted cloud storage service.
- `<bucket_name>` is the name of the S3 bucket on which you want to disable the CTE COS S3 Role.

For example, if the bucket name is `vte-cos-s3-rtb`, type:

```
voradmin cos s3 role release-bucket AKIA****P KQSm****D aws us-west-1 vte-cos-s3-rtb
```

Guard an AWS Bucket

To Guard an AWS bucket, you must:

1. Create a CBC_CS1 key. For CM, see [Creating a New Key](#) in the [CM Administrator Guide](#).
2. Create a Cloud Object Storage (COS) policy. See [Creating a COS Policy](#).
3. Apply the policy to the host. For CM, see [Managing GuardPoints](#) in the [CTE Administrator Guide](#).

Using a COS Proxy Root CA Certificate Information

The CTE COS CA Certificate, not to be confused with the Kernel and VMD Kernel Certificates, is used with the COS internal Proxy Certificate Authority and must be used by Clients to validate Certificates received during their TLS connection handshake. The default COS CA Self-Signed root CA is automatically created using a locally generated Public/Private Key with the following parameters:

```
CERT_FIELD_PARAM="/C=OZ/ST=Munchkin-land/L=Emerald City/O=ACME Inc/OU=ACME Deliveries/CN=localhost"

SUBJECT_ALT_NAME_PARAM="DNS.1:localhost,IP.1:127.0.0.1"
```

To view the currently installed Certificate for the COS Proxy CA, use the `voradmin cos ca_cert display` command.

In the context of the internal COS Proxy CA, the FQDN of 'localhost' would be the correct value, as well as the loop-back IP address of 127.0.0.1 This results in the following locally generated Root CA Certificate.

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
2a:28:2c:c5:d6:3b:05:11:fe:6e:32:1d:aa:35:29:44:e5:0d:ce:bf
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=OZ, ST=Munchkin-land, L=Emerald City, O=ACME Inc, OU=ACME Deliveries, CN=localhost
Validity
Not Before: Feb 11 18:19:33 2020 GMT
Not After : Feb 10 18:19:33 2021 GMT
Subject: C=OZ, ST=Munchkin-land, L=Emerald City, O=ACME Inc, OU=ACME Deliveries, CN=localhost
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:b9:e6:60:c9:00:f8:00:83:b7:1b:ff:b2:31:eb:
66:5a:eb:21:87:1c:aa:3d:71:b8:08:42:4d:82:6c:
9a:5c:c7:d0:ad:ec:11:9b:be:80:15:55:ab:bc:38:
11:9c:80:c4:1e:63:31:ae:b7:33:8f:88:0b:c2:ca:
```

```

e9:e8:0d:78:5a:19:e3:d9:45:fd:4c:b4:81:24:ea:
d3:d4:b9:d2:14:07:e0:33:df:b9:75:36:57:16:4d:
6e:ee:bf:5f:1d:13:14:10:d1:ba:29:0e:1e:11:38:
84:78:8a:e8:ed:1a:24:f7:6a:ac:87:66:9b:21:23:
7b:2c:44:b3:33:6c:04:b7:aa:8c:d3:64:d2:5e:b6:
56:b5:46:54:a9:37:06:c8:e5:30:5f:2a:ba:78:00:
4a:2f:f1:66:a0:1f:fd:26:05:8d:e0:da:23:1e:1b:
1e:a8:ee:77:73:76:32:3c:5e:01:aa:0f:d5:8b:ac:
a9:08:7e:50:63:5e:88:95:e5:5f:dc:1d:7b:b0:59:
50:c1:56:ba:e6:11:da:c6:c5:79:3e:a6:46:f2:39:
db:6a:9d:aa:da:ff:68:d0:39:9c:fd:5a:d5:0e:3e:
41:07:62:32:c0:be:4f:92:56:34:92:c8:1d:bd:87:
ec:e5:3b:44:a0:8f:8c:09:f9:37:40:df:b3:24:bb:
8d:67
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Key Usage:
Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
C5:19:E5:41:B7:69:E7:10:27:2D:F6:49:0D:46:0A:4B:FE:8C:7E:CB
X509v3 Authority Key Identifier:
keyid:C5:19:E5:41:B7:69:E7:10:27:2D:F6:49:0D:46:0A:4B:FE:8C:7E:CB
X509v3 Subject Alternative Name:
DNS:localhost, IP Address:127.0.0.1
X509v3 Issuer Alternative Name:
DNS:localhost, IP Address:127.0.0.1
Signature Algorithm: sha256WithRSAEncryption
2d:3c:2b:93:c0:61:1d:35:d7:f2:5f:5c:e8:0d:61:57:f2:a8:
e0:ec:98:74:02:b5:c4:78:a4:2f:b5:2b:b4:96:56:17:93:89:
eb:45:ac:df:1e:1b:e0:d5:38:da:55:62:61:97:5b:d9:9e:31:
9b:71:f1:17:37:31:5d:12:0f:5e:c1:ea:29:ee:b2:97:6e:7c:
c0:97:a9:8d:a9:2c:c0:68:e4:fa:b1:21:f8:50:b8:c0:2e:51:
fd:f2:5b:4d:41:72:0c:48:a2:db:47:14:66:20:c7:62:bd:33:
e8:a4:f4:22:c9:07:0f:0d:58:a0:9e:a1:f9:96:9c:97:c1:28:
6a:18:6f:ea:b9:28:42:48:5a:5c:da:98:22:9f:05:59:27:82:
3f:3d:4e:0b:9d:37:04:76:0e:ec:d9:f1:25:c8:78:78:fc:31:
d0:cb:24:db:47:96:7c:fa:dc:0d:14:6c:13:44:8d:87:5b:82:
d2:0f:a9:8c:48:bd:a6:b1:b9:0c:bb:50:14:70:d0:8b:7b:8c:
a5:e5:52:83:47:25:15:d6:d0:17:e0:9f:f7:99:d0:2e:17:93:
c5:38:e0:b8:c8:d4:f2:ed:39:99:ec:19:cf:5e:39:78:7b:5f:
07:48:4b:df:ec:d9:94:c5:aa:df:4d:a9:a5:a9:e3:88:74:0e:
d7:74:83:87

```

If you want to change the defaults, you can use the silent install option with the `CERT_FIELD_PARAM` and `SUBJECT_ALT_NAME_PARAM` set to the desired values, or you can replace the default Certificate using the `voradmin cos ca_cert` command. For more details, see the `voradmin` manpage.

Protecting Python Programs with CTE

CTE uses SHA-256 to generate binary signatures that can be used to allow certain trust levels for a customer application. Capturing the signature of a binary allows CTE to determine if the application's binary has changed in any way, because those changes might mean the security of the binary has been compromised.

While this mechanism works well for executable binaries to verify an application's validity at run time, this mechanism does *not* work for applications implemented with interpreter languages because CTE can only access

the interpreter's signature to validate the file. The program itself is something that is executed by the interpreter and thus CTE cannot hook into this process. Scripting languages like Python are particularly difficult because many Python programs include other Python files, which means there is no single program signature that defines the execution path.

While CTE cannot use signature sets to protect traditional Python programs, tools like PyInstaller allow for the creation of a self-contained Python executable that CTE can sign and protect.

Benefits of Using PyInstaller with CTE

Using PyInstaller allows the creation of self-contained Python binary packages. These packages contain the Python interpreter, the Python program, and all required modules and libraries. Because each package includes all of the files it needs, it is immune to changes to the Python modules or libraries on the system. This not only allows CTE to sign the binary but it also adds extra protection against an attacker trying to gain access through modifications of the underlying libraries.

Another benefit is that it provides security administrators with a stable process that is reasonably immune to system updates done by a system administrator. Once the application binary has been created and signed, the behavior of the program will not change because of updates made through the OS packaging system or Python's PIP package manager.

Getting PyInstaller

PyInstaller is an OpenSource project. The instructions for installing PyInstaller, as well as the documentation, are available on the [project page](#).

Example Usage

The exact usage of PyInstaller arguments varies based on the details of the Python program being packaged into an executable. This example shows what is needed to generate a self-contained AWS CLI binary with PyInstaller. It uses the `--onefile` flag to generate a single, self-contained binary. It assumes that the pip3 Python package manager is already installed on the system.

Installing PyInstaller

The following command installs PyInstaller in `${HOME}/.local/bin/PyInstaller`:

```
pip3 install --user PyInstaller
```

Installing the Amazon AWS Command Line Utility

The following command installs the AWS utility in `${HOME}/.local/bin/aws`:

```
pip3 install --user awscli
```

Creating a Runtime Hook

The following command creates a runtime hook that changes the Python `botocore` root directory within the packaged binary. This is necessary to make sure that we use the `botocore` packaged by PyInstaller. The hook is save to a file named `change-botocore-root.py`. For more information on runtime hooks, see the

PyInstaller documentation.

```
cat <EOF> ${HOME}/change-botocore-root.py
import sys
import boto3

if getattr(sys, 'frozen', False):
    boto3.BOTO3_ROOT = sys._MEIPASS
EOF
```

In order to get the AWS CLI utility working with PyInstaller, we need to specify some hidden imports as well as add some folders from the `awscli` and `boto3` packages into the executable. For more information about hidden imports and adding files to the executable, see the PyInstaller documentation.

```
${HOME}/.local/bin/PyInstaller --onefile \
--hiddenimport=awscli.handlers \
--hiddenimport=pipes \
--add-data=${HOME}/.local/lib/python3.6/site-packages/awscli/data:data \
--add-data=${HOME}/.local/lib/python3.6/site-packages/boto3/data:data \
--runtime-hook=${HOME}/change-botocore-root.py \
${HOME}/.local/bin/aws
```

The resulting binary will be saved in the current working directory as `dist/aws`.

Enable COS on an Agent with no COS Service

To enable COS on a system that has CTE installed but no COS Service:

1. Uninstall CTE completely.
2. Reinstall CTE and select **Yes** when asked:

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]: Y
```

Creating a COS Policy

Prerequisites for a COS Policy

1. Install Required Linux Packages
2. Generate a self-contained AWS CLI binary with PyInstaller

Make sure to:

- a. Install PyInstaller
- b. Install the Amazon AWS Command Line Utility
- c. Create a Runtime Hook

3. Configure a CTE COS S3 Role for Guarded Buckets

User Set

- [Create User Sets by Adding Members Manually](#)

Key Rule

- [Add Key Rules](#)
- For COS keys:
 - **Algorithm:** AES
 - **Object Type:** Symmetric Key
 - **Size:** 256
 - **Encryption Mode:** CBC-CS1
 - **Key Usage:** Encrypt, Decrypt
 - **Exportable:** On

Process Set

- The **Directory** is the directory where you created the binary when you generated a self-contained AWS CLI binary with PyInstaller in step 2 of the prerequisite section above.
- The **File** is the file created during that process.

CTE with Teradata Database Appliances

CipherTrust Transparent Encryption (CTE) offers IDT-Capable GuardPoints on Linux for protecting data on raw devices. The IDT solution offers data encryption, data transformation, and access control on storage devices. The principles behind CTE's IDT-Capable GuardPoints can also be applied to protect Teradata Database Appliances. (For details about IDT, see [CipherTrust In-Place Data Transformation for Linux](#).)

This section contains the following topics:

- [IDT-Capable GuardPoints and Teradata Database Appliances](#)
- [Requirements and Considerations](#)
- [Guarding a Teradata Database Device](#)
- [Changing the Encryption Key on Teradata Devices](#)
- [Access Rules to Apply on the Teradata Database Appliance](#)

-
- [Replication of IDT Metadata Files Across Members of a Clique](#)
 - [Generating IDT-capable Metadata for Teradata Storage Expansion](#)
 - [Best Practices](#)
 - [Uninstalling CTE from the Teradata Cluster](#)
 - [Alerts and Errors](#)

IDT-Capable GuardPoints and Teradata Database Appliances

The Teradata Database Appliance must be protected by an IDT-Capable GuardPoint. The In-Place Data Transformation (CTE-IDT) feature offers capabilities such as initial data transformation and access control on protected raw devices. The transformation capability transforms existing clear-text data on a device to cipher-text, and allows for subsequent re-transformation using another encryption key.

You must be familiar with CTE and CipherTrust Manager support for IDT-Capable GuardPoints before you can configure CTE to work with Teradata. For details about CTE-IDT, see [CipherTrust In-Place Data Transformation for Linux](#).

Requirements and Considerations

Location of the CTE Private Region

The CTE Private Region contains the metadata CTE requires in order to support initial transformation of data on the device and subsequent data transformation to other encryption keys. By default, CTE creates the CTE Private Region at the beginning of the guarded device. If data already exists on the device, CTE requires that the device be expanded by 63 MB to make room for the CTE Private Region. The existing data in the first 63MB of the device is then migrated into the expanded space and the beginning of the device is reserved for the CTE metadata. This data relocation is completely transparent to applications and users.

With a Teradata Database Appliance, however, CTE cannot create the CTE Private Region at the beginning of the Teradata pdisk devices because the disks in the Appliance cannot be expanded. Therefore, for Teradata Databases, CTE stores the metadata in a special directory called the CTE Metadata Directory located at: `/var/opt/teradata/vormetric/vte-metadata-dir`. This directory contains all of the metadata for every Teradata Database device that is protected by CTE.

While this does not affect the functionality of CTE, it does affect the way administrators need to back up the Teradata Database because both the Teradata Database and the metadata directory must be backed up together. You will not be able to restore a Teradata Database without access to the associated metadata in the CTE metadata directory.

Metadata File Access and Teradata Clusters

A Teradata cluster can contain multiple hosts. The members of a cluster that share access to pdisk devices belong to a clique. When you create an IDT-Capable GuardPoint on a pdisk, the metadata for that GuardPoint must be available to all members of the clique. CTE automatically replicates the metadata files across the members of a clique when the metadata is created or changed. For details, see [Replication of IDT Metadata Files Across Members of a Clique](#).

Additional Requirements and Considerations

- The Teradata kernel must be at minimum version 4.4.140-96.54.TDC-default on every node of the Teradata Database Appliance on which you plan to install CTE. Refer to the release notes document for CTE releases for compatibility requirements between the kernel releases from Teradata, and the CTE releases.

Caution

- Be sure the version of the Teradata Database is fully compatible with CTE.
 - The Parallel Upgrade Tool (PUT) component of Teradata Database has been enhanced to discover CTE protected devices. The Parallel Upgrade Tool (PUT) component of Teradata (TDput) must be version TDput-03.09.06.09 or higher. This PUT component must be available in your Teradata Database.
- The Parallel Database Extensions (PDE) component of Teradata (ppde) must be version ppde-16.20.53.07 or higher. This PDE component must be available in your Teradata Database.
- The Teradata I/O Scheduler (tdsched) component must be version 01.04.02.02-1 or higher. This I/O Scheduler component must be available in your Teradata Database.
- Contact your Teradata Customer Support Representative if you are unsure of the availability of this functionality in your Teradata cluster.

- The CTE Agent must be installed in `/opt/teradata/vormetric` on every node in the Teradata cluster. In order to specify this location, use the `-d` option when installing CTE. For example:

```
./vee-fs-7.8.0.75-sles12-x86_64.bin -d /opt/teradata/vormetric
```

Note

The CTE Agent can be installed without stopping the Teradata Database service.

- The CTE metadata directory `/var/opt/teradata/vormetric/vte-metadata-dir` must be guarded by the Administrator to prevent accidental modification or deletion of the CTE metadata files. If the CTE metadata directory is not guarded, any attempt to configure or enable an IDT-Capable GuardPoint on the Teradata appliance will be rejected.

The standard CTE policy associated with the metadata directory must:

- Deny all users (including the root user) the ability to modify or remove any files in the metadata directory.
- Specify the key `clear_key` in the key rule so that the metadata is stored in clear text.

- The following table displays how to set up your policy for guarding the CTE metadata directory:

Security Rules	
Action	Effect
Read	Permit, Audit
all_ops	Deny, Audit
Key Selection Rules	
Key	
clear_key	

- Stop the Teradata Database service when upgrading an existing CTE Agent installation, type:

```
tpareset -x Stopping Database
```

- Stop the Teradata Database service so that CTE can rekey any guarded devices. The service must remain stopped until CTE has finished rekeying all of the guarded devices on the appliance.

Calculate Encryption/Key Rotation Time for Teradata Databases

The Thales Engineering team has a set of scripts which help to calculate the estimated encryption time for CTE on a Teradata database cluster.

Using the **dd** command, the scripts simulate the I/O sequences for encrypting **pdisks** during initial encryption. The scripts perform only read operations for simulation. Two parameters are required for simulation: the amount of data to read from each **pdisk**, and the IDT concurrency level to be applied during simulation. The larger the data size, the more sample performance data will be available for estimation. Thales recommends a minimum of 4GB for data size.

The concurrency level is the IDT concurrency level for encrypting IDT configured devices. You can specify the number of segments to transform concurrently using **-c** option of the **voradmin** command when initializing the device. By default, CTE-IDT transforms 8 segments concurrently, if the concurrency level has not been specified through the voradmin command. You can specify 16 for concurrency level if the backend storage for **pdisks** uses high speed flash drives, otherwise use 8.

Note

When choosing the concurrency level for your system you **must** consider the number of CPU cores, the total IOPS of your storage system, the size of the device to transform, and the duration for the data transformation.

The scripts collect the performance data in log files during execution. The logs are saved in **/tmp/cte_data** and **/tmp/perfmon_cte_dd.log**. The Thales team will need those logs to help you with encryption time estimation.

Obtaining the Scripts and Calculating Encryption Time

1. Download the scripts:
 - `con-pdisks-dd.sh`
 - `con-pdisks-test.sh`
2. Modify the bash variable `PDISKS` in the script: `con-pdisks-dd.sh`

Example

```
PDISKS="list of pdisks assigned to this node ..."  
PDISKS="/dev/sda1 /dev/sda2 /dev/sdb1 /dev/sdb2"
```

3. Divide the disks assigned to the clique, equally amongst the nodes of the clique.
4. Copy all of the scripts to the same directory on each Cluster.
5. Run `cond-pdisks-test.sh` concurrently on all of the nodes with the selected devices.

```
# sh con-pdisks-test.sh `<number of GBs to read from each `pdisk`>` `<concurr  
ency level to be applied when reading `pdisks`>`
```

Example

```
# sh con-pdisks-test.sh 4 16
```

6. Contact [Thales Technical Support](#). They will need the collected data to calculate encryption time.

Note

1. The scripts only perform read operations to generate IO load similar to the IDT encryption process, meaning, there is no write operations. Thales factors in a few parameters to estimate rekey time.
2. Thales recommends executing the scripts when the database is not busy.
3. If there are multiple cliques, and if the user requires estimation for each clique, collect the data for each clique separately.

Guarding a Teradata Database Device

To guard a Teradata Database device:

- Install CTE on the Teradata Database Appliance
- Identify Devices to be Guarded with IDT-Capable GuardPoints
- Select the Initial Configuration Method
- Initialize and Guard the Database Devices Using the Standard Initialization Method
- Automating and Reducing the Duration of Initial Data Transformation
- Automating and Reducing the Duration of Subsequent Data Transformation
- Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method

Note

You must use the **In-Place Data Transformation** policy type when guarding Teradata devices.

Install CTE on the Teradata Database Appliance

CTE must be installed on every node in the Teradata cluster, including any Hot Standby Nodes. When you install CTE on every node in your Teradata cluster and register each node with CipherTrust Manager, the following are required:

- You must have AES-NI key available on the host.
- The Teradata kernel must be at version 4.4.140-96.54.TDC-default, or higher, on the Teradata Database Appliance on which you plan to install CTE. Refer to CTE release notes for compatibility between CTE and the Teradata kernel releases.
- Your version of Teradata Database must be fully compatible with CTE for supporting the pdisk devices protected as IDT-Capable GuardPoints.
- The CTE Agent must be installed in `/opt/teradata/vormetric`. In order to specify this location, use the `-d` option when installing CTE. For example:

```
./vee-fs-7.8.0.75-sles12-x86_64.bin -d /opt/teradata/vormetric
```

Warning

Before you install or upgrade CTE, you must stop the Teradata Database and any other applications that access the database devices directly or through the database service. Failure to stop the applications will result in a failure to install or upgrade CTE.

Caution

Be sure to install the CTE Agent in a file system with sufficient free storage space. The minimum available free space is the number of pdisks in your cluster multiplied by 63MB.

Identify Devices to be Guarded with IDT-Capable GuardPoints

Storage devices in Teradata clusters are known as pdisks. A pdisk is a slice of a LUN exported from the backend storage system attached to the nodes in a cluster. For example, the pdisk named `/dev/pdisk/dsk304` is a symbolic link to the slice on the LUN called `/dev/disk/by-id/`

`tdmp-360080e500043092c0000b46f5c34c018-part3`, as shown below:

```
ls -l /dev/pdisk/dsk304
lrwxrwxrwx 1 root root 70 May 18 12:21 /dev/pdisk/dsk304 -> /dev/disk/by-id/tdm
p-360080e500043092c0000b46f5c34c018-part3
```

CTE guards the devices represented by the pdisks in the Teradata cluster. In the example above, the device that you must configure and guard as an IDT-Capable GuardPoint is `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`.

Note

You cannot use the symbolic link name when initializing or guarding the storage devices.

To identify the disks available to the Teradata cluster and require CTE protection, look in `/dev/pdisks` on each node in the cluster. Any symbolic links that point to a Linux device path are the disks that should be initialized.

Caution

Do *not* enter the path name of the pdisk device when initializing it for guarding or in the CipherTrust Manager when you actually guard the device.

Select the Initial Configuration Method

Select the initial configuration method that you want to use. Thales supports two methods for the initial configuration of Teradata Database devices:

- **Standard Initialization Method**

This method configures devices for initial encryption of existing clear-text data on the database devices. The time required to encrypt may take hours or even days, depending on the volume of data, the number of database devices and nodes, and the bandwidth of the storage back-end of database devices. For details, see

Initialize and Guard the Database Devices Using the Standard Initialization Method.

- **Backup/Restore Initialization Method**

This method skips the initial encryption step but requires a full backup of the database and the engagement of Teradata Customer Support to assist you with some configuration steps at the Teradata database level in preparation for the full restore of the database after the database devices are protected. The length of time required for this method depends on the length of time it takes to back up, and then fully restore, your Teradata database. For details about using this method, see [Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method](#).

Initialize and Guard the Database Devices Using the Standard Initialization Method

The following procedure describes how to perform the initial configuration of your database devices using the Standard Initialization Method. This procedure encrypts the existing data in place and does not require you to backup your Teradata database when initially deploying CTE. It may, however, take several hours, or even days, to complete depending on the volume of data, the number of database devices and nodes, and the bandwidth of the storage back-end of database devices.

Warning

For each device, you must designate *one and only one* of the nodes in the cluster as the initial node. This is the node on which you plan to initialize and guard the device for the first time. The designated node must be the only one that guards the device until the entire initial data transformation process has completed. **DO NOT** initialize or guard any device on multiple nodes in the cluster simultaneously, because multiple nodes attempting to transform the same data can corrupt the data on the entire device.

1. Shut down the Teradata Database. You cannot initialize an online database device.
2. For each device, designate one of the nodes in the cluster as the initial node that you will use for the initial data transformation when the device is guarded for the first time.
3. Log into the designated node in the Teradata Database Appliance. Type:

```
voradmin idt config [-external] [new|xform] [-c <n>] <device-name>
```

- **[new|xform]** (required)

Indicates whether data already exists on the device. If the device contains no data, specify **new**. If the device contains data that you want to keep, specify **xform**. Most installations of Teradata Appliance are expected to have pdisks populated with data, therefore, most often you will use the **xform** option. When you use **xform**, CTE will transform all existing data on the device from clear-text to cipher-text as soon as you guard the device on the Appliance. The device will be inaccessible until the transformation is complete, and the device must remain offline to the Teradata Database service during the entire transformation

process. No user access will be permitted until all of the data has been transformed.

- **-external** (required)

You *must* use this option when initializing any Teradata device. With this option, CTE writes the CTE Private Region to a metadata file located in the CTE metadata directory. For details, see [Location of the CTE Private Region](#).

- **-c <n>** (optional)

If you use this option, CTE sets the number of data transformation jobs to run in parallel to the number specified in **<n>**. **<n>** can be an integer between 1 and 60, (default: 8).

Each data transformation job transforms 1MB worth of data and requires CPU resources in addition to three I/O operations as part of data transformation. Each job reads 1MB of data from the device, preserves the data in the CTE private region, rekeys the data to cipher-text, and writes the transformed data to the device. If you increase the number of parallel jobs, the data transformation process will complete faster but there will be an increased performance impact on the system. Only increase the **-c** option if you are certain that the system resources are available to handle the additional load.

The value for the **-c** option you specify here remains in effect for all subsequent data transformations (such as any data rekeys) until you specify a new value.

- **<device-name>** (required)

The name of the Teradata Database device that you want to initialize.

For example:

```
voradmin idt config -external xform -c 20 \  
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

4. Repeat the **voradmin idt config** command for each device that you want to initialize. If you want to distribute the initial data transformation or subsequent rekey load on all of the disks across all the nodes in the cluster, make sure that you run the **voradmin idt config** command for each device on the node you designated for data transformation, *excluding* the HSN node. The node on which you run the **voradmin idt config** command is the node that performs the data transformation on the device. Do *not* designate the HSN node for data transformation because the devices on the HSN node may be reserved and therefore not available for IO operations.

Guard the Devices as IDT-Capable GuardPoints

Warning

For each device, you must designate a node in the cluster as the initial node on which you plan to initialize and guard the device for the first time. The designated node must be the only one that accesses the device until the entire initial data transformation process has completed. This requires guarding each device at the designated client level rather than at the client group level. DO NOT initialize or guard any device on multiple nodes in the cluster simultaneously, because multiple nodes attempting to transform the same data can corrupt the data on the entire device.

To create an IDT GuardPoint:

1. On the **GuardPoints** tab, click **Create GuardPoint**.
2. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field.
 - b. Select an *In-place Data Transformation* policy. If no policy exists, create one, as described in [Creating Policies](#).

Name	Type	Version
☐ testcospic	Cloud Object Storage	0
☐ testpolicy	Standard	1
☐ idtpic	Live Data Transformation	0
☒ test-idt-plc	In-place Data Transformation	0

- c. Click **Select**.

Note

When an IDT policy is selected, the **In-place Data Transformation** toggle is displayed on the Create GuardPoint dialog box.

3. Select the **Type** of device to protect. This is a mandatory field. The options for a **In-place Data Transformation** policy are:

Type	Description
Auto Raw or Block Device	Select for IDT policies for raw (block) devices.
Manual Raw or Block Device	Select for IDT policies for raw (block) devices to be guarded manually.

Note

Manual Raw or Block Device are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd -unguard` commands.

4. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:

- **Enter/Browse Path:** Select this option, and enter the GuardPoint paths by either typing or clicking the **Browse** button.

Note

A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

- Click **Browse** to select a path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths.

File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

- Alternatively, if you know the path, manually enter full paths of one or more directories in the given text box. Enter one path per line.

Create GuardPoint



Policy: *

test-idt-plc

Select

Type: *

Auto Raw or Block Device

Path: *

☒ Enter/Browse Path ☐ Upload CSV

/dev/sdb/

Browse

i To apply the same GuardPoint settings to multiple paths, type paths in the Path field or specify them using the Browse button. A maximum of 200 GuardPaths can be specified.

In-place Data Transformation: ☒

Efficient Storage: ☐

5. Make sure the In-place Data Transformation option is selected.
6. Click **Create**. A message appears prompting to confirm the reuse of these GuardPoint settings on another path.
 - Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:
 - a. Specify a new **Path**.
 - b. Click **Add Path**. The newly added path appears under the Paths list on the left. Similarly, add as many paths as required.
 - c. Click **OK**.
 - Click **No** if you do not want to use the same settings on another path.

CipherTrust Manager pushes the policy and the GuardPoint configuration to the node in the cluster. The CTE agent on the node writes the IDT Device Header into the CTE Private Region in the local CipherTrust Transparent Encryption metadata directory on the node.

If this is a new device, the status immediately changes to guarded. If there is existing data on the device, CTE begins transforming the data from clear-text to cipher-text as soon as the GuardPoint configuration is available and the device status changes to guarded. The device will remain inaccessible until this data transformation completes. The length of time required to transform the data depends on the amount of existing data and the number of parallel data transformation jobs specified in the `voradmin idt config` command. To see the data transformation progress, use the `voradmin idt xform status <device-name>` command, as described in [Viewing Device and Data Transformation Status](#).

Devices with existing data are transformed from clear-text to cipher-text using the encryption key specified in the selected policy through the In-Place Data Transformation (CTE-IDT) process. For details on how CTE does data transformation on IDT GuardPoint, see [CipherTrust in-Place Data Transformation for Linux](#).

After the device is initialized and guarded, the protected device must be accessed through the device pathname corresponding to the secvm device. For example, if you guard the Linux device `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`, the pathname becomes `/dev/secvm/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3` as soon as the process is complete.

7. After all of the Teradata Database devices have been guarded, disable the guarded IDT-GuardPoints on each designated node and then enable those GuardPoints at the Client Group level on all the nodes in the clique.
8. After guarding your devices and before starting your database, you must change the current configuration of your cluster to reflect the status of the pdisk devices guarded as IDT GuardPoint. See the **Rebuild Vconfig Only** option of the Teradata Parallel Upgrade Tool (PUT) service to apply the guarded status of the pdisk devices into your database configuration. The **Rebuild vconfig** process applies the guarded configuration status of each pdisk and resets the pdisk symbolic link to the CipherTrust Transparent Encryption `secvm` device.

Warning

You must complete this step before starting your database. Failure to do so will result in database failures and potential corruption of your database.

For example, the pdisk `/dev/pdisk/dsk304` is linked to the secvm device after **Rebuild Vconfig Only** commits the guarded status of pdisk on each node:

```
# ls -l /dev/pdisk/dsk304
lrwxrwxrwx 1 root root 70 May 18 12:21 /dev/pdisk/dsk304 -> /dev/secvm/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part
```

9. After all of the Teradata Database devices have been guarded in the clique and the **Rebuild Vconfig Only** on TDput has been executed, start the Teradata Database, type:

```
# /etc/init.d/tpa start
```

Viewing Device and Data Transformation Status

After you guard a Teradata Database device, you can view the status of that device using the `voradmin idt status [xform] <device-name>` command, where:

- **xform** (optional)

If you specify this option, CTE shows the status of any data transformation processes happening on the device. If you do not specify this option, CTE displays the IDT Device Header for the device.

- **<device-name>** (required)

The name of the Teradata Database device that you want to initialize. This must be the actual device name and not the symbolic pdisk name.

For example, if you want to view the status of device `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`, you would enter:

```
voradmin idt status /dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

If you want to check the data transformation progress on the device `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`, you would enter:

```
voradmin idt status xform \
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

The **Status** field displays **In-Progress** if a data transformation process is running, and **Completed** if the process has finished.

Automating and Reducing the Duration of Initial Data Transformation

CTE for Teradata allows Teradata customers to run their database services on top of a high performing encrypted storage infrastructure, solving many security and compliance concerns. Teradata systems are usually mission critical and cannot afford to be offline for significant periods of time. The problem, therefore, is how to convert an existing Teradata system from one that is unencrypted, to one that is encrypted. Thales calls this conversion process rekeying, or data transformation.

The following steps outline the process the Teradata operations team should follow to encrypt the platform while minimizing system downtime and operational disruptions. The process leverages the fact that a Teradata system is composed of multiple disks, which create a redundant platform, and effectively approaches the conversion process by breaking it into smaller, more manageable, and less disruptive steps. Operators should prepare for data transformation and schedule time to complete the transformation process while the Teradata database services are down. The process supports recovery from unexpected IO failure during the transformation process of migrating data from unencrypted to encrypted. This document describes the procedure and execution of the transformation process using a script that orchestrates the entire transformation process across multiple nodes in a clique, and significantly reduces the entire data transformation time.

Warning

Thales recommends that you backup the Teradata database before starting the transformation process.

Use the `cte-pdisk-idt.sh` script to perform the initial rekey using embedded metadata on the Teradata `pdisks` that will be configured for IDT using external metadata. This reduces the time needed to encrypt the `pdisks` because the external metadata is a bottleneck when performing rekey on multiple concurrent devices. The script works by saving the last 63 MB of a device to a file, and then configuring the device as IDT with embedded metadata. The last 63 MB is saved because devices configured for IDT with embedded metadata relocate the first 63 MB to the end of the device to make space for the metadata. Upon completion of rekey, the script then restores the first 63 MB from the end of the device and the last 63 MB for the saved file before converting the device to IDT with external metadata.

Note

- This script **only** works for CTE 7.3.0 or subsequent versions
- This script **only** works for initial rekey.

Getting Help

Recovery from interruption during the preparation step requires manual intervention. Recovery from unexpected failure occurs when the GuardPoints are guarded again. You can then restart the script in the monitor mode to resume monitoring the transformation progress.

In the event that the script is interrupted, or a system crash, contact [Thales Support](#). If possible, include the following information to facilitate recovery:

- Output of the script
- Output of the `secfsd -status guard` command (if the interruption did not crash the system)
- Contents of the `/tmp/pdisks.list` file
- Contents of the `/tmp/monitor-idt.disks` file
- Contents of the `/opt/teradata/vormetric/agent/secfs/.sec/conf/sod_config` file
- Contents of the `/var/opt/teradata/vormetric/vte-metadata-dir` directory (including file sizes)

Prerequisites

- Your policy for the external metadata directory **must** allow read/write access for the `dd`, `mv`, `rm`, and `stat` functions.

- Your policy for the raw device **must** allow read/write access with apply key effect for the **dd** function.

Install and Setup

1. Install the agent in `/opt/teradata/vormetric` and setup the external metadata directory `/var/opt/teradata/vormetric/vte-metadata-dir` on all nodes in the clique.
 - See [Install CTE on the Teradata Database Appliance](#) for more information on installing CTE on Teradata.
2. Copy the `cte-pdisk-idt.sh` script from `/opt/teradata/vormetric/agent/secfs/.sec/bin/` to `/root`.
3. Shutdown Teradata, type:

```
tpareset -x -f 'Setting up CTE'
```

4. Generate a list of disks to encrypt, type:

```
ls -l /dev/pdisk/dsk* | awk '{ print $(NF) }' > /tmp/all_pdisks.list
```

Note

This command generates a file with a list of disks in the format: `/dev/disk/by-id/*`.

5. Divide `/tmp/all_pdisks.list` into separate files based on the number of active (non-HSN) nodes in the clique. For example, if the list contains 300 disks and there are 4 active nodes, there should be 4 files with 75 disks in each.
6. Copy each file as `/tmp/pdisks.list` to the corresponding host that will oversee encrypting those disks. For example, if there are 300 disks in a 4-node clique, each node should have a unique list of 75 disks.
7. Add a manual IDT GuardPoint on each node for the disks in `/tmp/pdisks.list`

Note

The script only toggles the GuardPoints in the `/tmp/pdisks.list` file so it is safe to add manual GuardPoints for all of the devices on all of the nodes. However, automated metadata distribution does not work if the GuardPoint is present on all nodes as it expects the node performing transformation to be the only node with the GuardPoint at this point.

Configure and Initialize

1. To configure the devices for IDT on each node, save the last 63 MB, and start the initial rekey, type:

```
/root/cte-pdisk-idt.sh -m pre -y -f /tmp/pdisks.list
```

2. To monitor transformation with the following and wait for transformation to complete, type:

```
/root/cte-pdisk-idt.sh -m mon
```

3. To finish the setup, type:

```
/root/cte-pdisk-idt.sh -m post -f /tmp/pdisks.list
```

This restores the data to the first and last 63 MB of the device, restores the external metadata, and sets the `pdisk symlinks` to their associated `secvm` device.

4. Verify that identical metadata is present for all devices on all of the nodes, type:

```
ls -l /var/opt/teradata/vormetric/vte-metadata-dir | wc -l
```

If identical metadata is not present on all of the nodes in the same clique, manually synchronize the contents of the external metadata directory.

5. Unguard all of the nodes from the security server and switch to auto-guard GuardPoints.
6. Use the [Teradata PUT tool](#) to update the `pdisk` symbolic links permanently.
7. Start Teradata to verify that the database can start, type:

```
/etc/init.d/tpa start
```

8. Clean up the files created by the script, type:

```
rm -f /tmp/all_pdisks.list /tmp/pdisks.list.done /tmp/cte_pdisk_idt_pre.out
```

Script Help Output

```
/root/cte-pdisk-idt.sh -h
```

Response

```

Usage  /root/cte-pdisk-idt.sh [-h] [-y] [-t #] [-m <mon|pre|post>]
      < [-p </dev/pdisk/dsk#>] </dev/disk/by-id/scsi-...>
      -f <batch_file> >

-f <batch_file> File with list of disks to transform
File should have one entry per line
Format is,
    /dev/disk/by-id/tdmp-xxx
    /dev/disk/by-id/tdmp-yyy
    ...
or
    /dev/pdisk/dsk# -> /dev/disk/by-id/tdmp-xxx
    /dev/pdisk/dsk# -> /dev/disk/by-id/tdmp-yyy
    ...

Format for the latter option can be generated with,

    ls -l /dev/pdisk/dsk* | awk '{ print $(NF - 2), \
$(NF - 1), $NF }'

-m mon      Monitors IDT status on disks undergoing transformation started with the '-m pre' option
-m full     Performs the entire transformation process (default)
-m pre      Performs steps to set up and begin encryption of a device
-m post     Performs steps after device has been encrypted to restore borrowed space

With the 'full' mode, the script will wait while the device undergoes encryption. The 'pre' mode will start encryption and then terminate the script and wait for a user to rerun the script with the 'post' mode after encryption is complete.

-t #        Number of threads to use during IDT (default: 16, range: 1 - 60)
-p          Pdisk to link to after transformation is complete
-y          Skips user prompts
-h          Displays this help

```

Automating and Reducing the Duration of the Subsequent Data Transformations

You can use the `cte-idt-rekey.sh` script to perform subsequent rekey operations using embedded metadata on a set of IDT-Capable devices configured with external metadata. This reduces the time needed to rekey the devices, as the external metadata is a bottleneck when performing rekey on multiple concurrent devices. The script works by converting each device to IDT with embedded metadata before launching rekey. Embedded IDT metadata makes rekey operations significantly faster. The process of converting to embedded metadata is accomplished by:

1. Saving the first 63 MB of the device.
2. Copying the external metadata into the first 63 MB of the device.

3. Renaming the external metadata file to disable the use of external metadata.
4. Upon completion of rekey, the script then copies the first 63 MB out of the new external metadata file, and then restores the original 63 MB of the device that had been the backup, before the device converted it to IDT with the external metadata.

Note

- This script is **only** compatible with CTE v7.8.0.100 and subsequent versions.
- This script **only** works for subsequent rekey operations. Use the script: `cte-pdisk-idt.sh` for the initial data transformation.
- Thales recommends that you backup the data on the devices before starting the transformation process.

Prerequisites

- Your policy for the external metadata directory **must** allow read/write access for the `dd`, `mv`, `rm`, and `stat` binaries.
- Your policy for the raw device **must** allow read/write access with apply key effect for the `dd` binary.

Applying the Script

The following steps describe how to use the script for a set of devices in a clique with one, or multiple, nodes. In a multi-node clique, each node should perform the same steps with a different set of disks so that the work of rekeying all of the disks in the clique is distributed across the members.

Note

Do not run the script on Hot Standby Nodes (HSNs).

1. Copy the `/root/cte-idt-rekey.sh` from `/opt/teradata/vormetric/agent/secfs/.sec/bin` to `/root`.
2. Shutdown **Teradata**.
3. Create a list of the disks on which to perform subsequent rekey operations. The path to the disks **must be the same** as the disks that the GuardPoints are set on.
4. Create a directory, `/var/opt/teradata/vormetric/backup`, for the backups for the first 63 MB to be saved.

5. Apply a GuardPoint to that directory with a standard policy that encrypts the data and allows read/write access.
6. Modify the policy set on the external metadata directory, `/var/opt/teradata/vormetric/vte-metadata-dir`, and the devices, to allow read/write access so that the script can manipulate the external metadata files.
7. Prepare an alternate policy if needed.

If using a new policy to rekey the device, create a new policy with the current key set to the transformation key from the existing policy, and a new XTS key as the transformation key. For example, if the current policy encrypts from clear to XTS-key1; the new policy should encrypt from XTS-key1 to XTS-key2. The new policy must also allow `dd read/write access`. You can remove this access from the policy after all of the steps have been completed.

8. Run the script with the `backup` option and pass in the disk list:

```
/root/cte-idt-rekey.sh backup /<path/to/disks>.list
```

9. Wait for the script to finish the backup on all of the nodes in the clique.
10. Unguard all of the IDT device GuardPoints.
11. Alter the policy to use the new key (unless using a new alternate policy from step 8).
12. Re-guard all of the devices with manual GuardPoints.
13. Run the script with the `rekey` option and pass in the disk list:

```
/root/cte-idt-rekey.sh rekey /<path/to/disks>.list
```

14. Follow the on-screen prompts to enter the number of threads desired for rekey.
15. Wait for the script to finish rekey on all of the nodes in the clique.
16. Ensure that the external metadata files on all of the nodes in the clique are identical to the files on the node that ran the script. Verify this by running the command: `md5sum <file>` for the metadata files on all of the nodes within a clique to verify their consistency. If there is a discrepancy, overwrite the inconsistent metadata file with the file from the node used to rekey the device.
17. Remove the manual GuardPoints set in step 12 and re-guard with autoguard GuardPoints in the same manner as the original configuration.
18. Verify the data and access to the device(s) with the command: `verify_pdisks`.
19. Undo the modifications to the policy on the external metadata directory: `/var/opt/teradata/vormetric/vte-metadata-dir`.

20. Unguard and remove the backup directory `/var/opt/teradata/vormetric/backup`.
21. Start **Teradata**.

Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method

The Standard Initialization Method encrypts the Teradata database devices using In-place data transformation. Because Teradata Appliance models range in both storage and node sizes within a cluster, the time it takes to encrypt the existing data in-place on these large scale models may exceed the desired time frame.

To address this issue on an existing Teradata database, you can configure CTE on Teradata Appliances using the Backup and Restore method to retain existing data. The total time required to configure your Teradata Appliances with CTE using this method depends on how long your backup/restore application takes to restore the database.

To initialize and guard the devices using the selected initialization method, you must:

1. Backup the entire Teradata database, including all meta files, required for a full restore of that database.
2. Install and configure CTE on the Teradata database devices.
3. Work with Teradata Customer Support to initialize a `sysinit` on the Teradata Appliance cluster in preparation for a full database restore.
4. Perform a full restore of the Teradata database from the backup to the CTE protected devices. CTE automatically encrypts the data as it is restored to each protected device.

Prerequisites

Before starting this process, complete the following prerequisites:

- Make sure you have met the requirements described in [Requirements and Considerations](#).
- Create or identify the XTS/CBC-CS1 AES 256 key that you will use for the In-Place Data Transformation policy that you will apply to the IDT-Capable GuardPoints.
- Create a **Standard** policy that will be used to guard the CTE Metadata Directory (`/var/opt/teradata/vormetric/vte-metadata-dir`).
- Create an **In-Place Data Transformation** policy that will be used to guard the Teradata Database Devices. This policy must use an XTS/CBC-CS1 AES 256 key.
- Identify all of the devices that need to be guarded as described in [Identify the Devices to Be Guarded](#).

Procedure

1. Using a Teradata certified backup application, backup your entire Teradata database. The backup needs to include the Data Dictionary, the user database, and everything else that is required for a successful restore of your database. Contact your Teradata Customer Support representative for the requirements for a full backup.

2. After confirming that your backup of the Teradata database completed successfully, shutdown the Teradata database, type:

```
tpareset -x -f "shutting down for CTE installation"
```

3. Install CTE in `/opt/teradata/vormetric` on all nodes in the Teradata cluster and register them to a CipherTrust Manager server as described in [Install CTE on the Teradata Database Appliance](#).

```
./vee-fs-7.8.0.75-sles12-x86_64.bin -d /opt/teradata/vormetric
```

4. Create the CTE metadata directory (`/var/opt/teradata/vormetric/vte-metadata-dir`) on all nodes in the cluster.

```
. pcl -shell "mkdir -p /var/opt/teradata/vormetric/vte-metadata-dir"
```

5. If you are using the Teradata Intelibase model, complete the following step. If you are using the Teradata Inteliflex model, proceed to Step 6.
 - a. Log on to the CipherTrust Manager, click the **Hosts/Clients** tab, and set the GuardPoint to the CTE Metadata Directory (`/var/opt/teradata/vormetric/vte-metadata-dir`) using the Standard policy that was created for the metadata directory on all the nodes in the Teradata cluster.
 - b. On each node, identify the list of disks that will be configured and guarded as "new" devices as described in [Identify the Devices to Be Guarded](#).
 - c. On each node, configure each disk to be guarded as a new IDT-Capable device using the `voradmin idt config -external new` command.

```
voradmin idt config -external new \  
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

Note

Make sure that you configure each device using the `new` option. This option tells CTE to guard the device without transforming the data.

- d. Log on the CipherTrust Manager, click the **Hosts/Clients** tab, and select one of the host in the clique to set the GuardPoints for all the devices that have been initialized as new IDT-Capable devices using the In-Place Data Transformation policy that you created.

Repeat this step for all other hosts until all initialized devices have been guarded with an In-Place Data

Transformation policy.

6. If you are using the Teradata Inteliflex model, complete the following step. Otherwise, proceed to Step 7.
 - a. Designate one of the nodes in a clique as the node on which you will perform the first-time initialization and guarding procedures for each device. For example, if you have a 4 clique cluster, you must designate a total of 4 nodes, one from each clique.
 - b. Log on to the CipherTrust Manager, click the **Host/Client Groups** tab, and create a host group for each clique. For example, if your Inteliflex cluster has 4 cliques, you would create 4 host groups, one for each clique. For example, cluster-clique-1, cluster-clique-2, cluster-clique-3, and cluster-clique-4.
 - c. On the **Host/Client Groups** tab, click the name of one of the client groups you just created. Click on the **Members** tab and add the designated node from the clique as a member of this client group.

Repeat this step until all designated nodes have been added to the client group that matches their clique. In the previous example, you would have one designated node in each of the 4 client groups that you created.

- d. On the **Host/Client Groups** tab, click the name of one of the host groups that you just created. Click on the **GuardPoints** tab and add a GuardPoint for the CTE Metadata Directory (`/var/opt/teradata/vormetric/vte-metadata-dir`) using the Standard policy that was created for the metadata directory on all the nodes in the Teradata cluster.

Repeat this step for each Host/Client Group you created for your cliques. In the previous example, you would add the metadata directory GuardPoint in each of the 4 host groups that you created.

- e. On the designated node for each clique, identify the list of disks that will be configured and guarded as a “new” IDT device as described in [Identify the Devices to Be Guarded](#).
 - f. Configure each disk device on the designated node to be guarded as a new IDT-Capable device, type:

```
voradmin idt config -external new \
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

Note

Make sure that you configure each device using the new option. This option tells CTE to guard the device without transforming the data.

- g. For each of the other designated nodes you identified, identify the list of devices to be guarded and configure them using the `voradmin idt config -external new` command.
 - h. Repeat this configuration process until all devices on all designated nodes that you want to guard have
-

been configured as new IDT-Capable devices.

- i. On the **Host/Client Groups** tab, click the name of one of the clientgroups you just created. Click on the **GuardPoints** tab and add a GuardPoint for each device that you initialized as a new IDT-Capable device using an In-Place Data Transformation policy.
- j. Repeat this step on each one of the host groups you created.

The guarded devices will immediately be set as guarded on the designated node through the client group. However, as part of Teradata cluster support, each guarded device will have its metadata file replicated across all nodes in a clique as described in [Replication of IDT Metadata Files Across Members of a Clique](#). You must wait for metadata replication to complete for each clique in a cluster before continuing to the next step. This process takes approximately 1 second per disk that was guarded. So if you guarded 10 disks, you need to wait approximately 10 seconds. Verify that the number of metadata files on each clique matches with the designated node using the following command:

```
pcl -shell "ls /var/opt/teradata/vormetric/vte-metadata-dir | wc -l"
```

The number of metadata files on each node in the clique should also match the number of devices in that clique. For example, if you have a clique with 10 devices in it, then the results of the above `pcl` command should show 10 metadata files on each node in the clique.

- k. After metadata replication is completed on all cliques, log on the Key Manager and click the **Hosts/Client Group** tab, then click the name of one of the client groups you just created. Click the **Members** tab and add the rest of the nodes that belong to that clique to the Host Group. After all the nodes have been added, the Key Manager automatically pushes the existing GuardPoints out to the newly added members.
 - l. Repeat this step for each one of the Host Groups that you created for your cliques.
7. Verify that all of the nodes in a clique show that all of the devices as guarded.

```
pcl -shell "secfsd -status guard"
```

8. Work with Teradata Customer Support to perform a `sysinit` of the Teradata appliances in preparation for the full database restore.
9. Restore your Teradata database from backup.

Changing the Encryption Key on Teradata Devices

To meet various compliance requirements, you may want to change the key that CTE used to encrypt the Teradata Database devices. This process is called “Key rotation” or “Rekey”.

If you want to rekey a Teradata Database device, you can either:

- Follow the process for standard IDT-Capable GuardPoints. For details, see [Changing the Encryption Key on Linux IDT-Capable Devices](#).

- Use the Backup/Restore method as described in [Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method](#). The only differences between the initial configuration described in that section and rekey process are:
 - You do not need to change the policy assigned to the CTE Metadata Directory.
 - You need to create a new In-Place Data Transformation policy, that specifies a key rule with the existing key used to encrypt the Database devices in the **Current Key** field, and the new XTS/CBC-CS1 AES 256 key that you want to use to encrypt the data in the **New Key** field.
 - When you re-guard the designated node in each clique, make sure that you use the new policy so that CTE knows it needs to re-encrypt the data with the new key after you restore the devices from the backup.

Note

Make sure that you stop the Teradata database before you rekey the devices.

Warning

Rekeying a device must be executed only on *one and only one* of the nodes in the cluster. DO NOT prepare the device for rekey or guard the device with the new rekey policy on multiple nodes in the cluster because doing so initiates the data transformation process on the device on multiple nodes. The simultaneous attempts to rekey the data can cause data corruption of all of the data on the entire device.

Access Rules to Apply on the Teradata Database Appliance

This section provides the instructions for creating a sample policy and signature sets specific to a Teradata Database Appliance to deny unprivileged users access to clear-text data on guarded devices. Such a policy requires the inclusion of specific security rules to restrict access to the Teradata Device GuardPoints for specific set of users, groups, and/or processes.

Note

You **must** add binaries to client settings to allow trusted processes to access policies. Failure to do so results in a **User not Authenticated** error which prevents access for user-based policies. For example, when using `tvsa_agent` for a Teradata cluster, you must add `/usr/pde/bin/tvsa_agent` as an authenticator in the client settings.

1. In the CipherTrust Manager, edit the host/client entry for the Teradata Database Appliance.
2. Go to the **Host/Client Settings** tab and add the following entries to the list of binaries:

-
- |authenticator|/usr/pde/bin/pdmain
 - |authenticator|/opt/teradata/sm3g/bin/tdsmagent
 - |authenticator|/usr/pde/bin/pcl
 - |authenticator|/opt/teradata/TDput/bin/putservices
 - |authenticator|/usr/pde/bin/tvam
3. Create a signature set for system processes that require access to guarded devices. The following system processes on the Teradata Database Appliance must be permitted access:

- /usr/lib/systemd/systemd-udevd
- /sbin/dmsetup
- /opt/teradata/vormetric/agent/vmd/bin/get_disks
- /sbin/pvdisplay
- /sbin/lvdisplay
- /usr/sbin/parted

You can include additional processes as needed.

4. Create a signature set for Teradata Database processes that require access to guarded devices. The following directories contain the Teradata binaries that require access:

- /usr/pde/bin/*
- /usr/tdbms/bin/*
- /opt/teradata/gsctools/bin/*
- /opt/teradata/TDput/bin/*

You can include additional processes as needed.

5. Create a system-level process set to associate the system-level processes listed in step 3, with the signature set you created in step 3. In the following example, this process set is called TD-Demo-system-process.

2 Processes

Directory	File	Signature	
/opt/teradata/vormetric/agent/vmd/bin	get_disks	TD-Demo-System-Process	
/sbin/	dmsetup	TD-Demo-System-Process	
/sbin/	lvdisplay	TD-Demo-System-Process	
/sbin/	pwdisplay	TD-Demo-System-Process	
/usr/lib/systemd	systemd-udevd	TD-Demo-System-Process	

6. Create a Teradata Database process set to associate the signature set for the Teradata Database binaries created in step 4.

2 Processes

Directory	File	Signature	
/opt/teradata/TDput/bin/	*	TD-Demo-TD-Binaries	***
/opt/teradata/gsctools/bin/	*	TD-Demo-TD-Binaries	***
/usr/pde/bin/	*	TD-Demo-TD-Binaries	***
/usr/tdbms/bin/	*	TD-Demo-TD-Binaries	***

7. Create the user set for the Teradata trusted group on your appliance.
8. If you have any other trusted groups that you want to include in your security rule, add a user set for each one of those trusted groups. You can add as many user sets to the policy as you need.
9. Create a user set for the root user and any other privileged users you want to add.
10. Verify that you have the complete signature sets, process sets, and user sets as shown in the examples below.
11. Apply the policy to the Teradata Device GuardPoints.

Replication of IDT Metadata Files Across Members of a Clique

For Teradata, metadata for IDT-Capable GuardPoints is stored in external files in the CTE metadata directory. Because the Teradata appliance is a cluster of multiple hosts/clients that share access to the same devices across multiple nodes, a metadata file must be replicated across the nodes that are in the same clique within the cluster, including Hot Standby nodes. Replication is required when the initial data transformation has been completed, and it is required again during subsequent rekeys. The availability of the metadata files on all members of the clique is critical for high availability of Teradata database in the event of a node failure because the data on the device cannot be accessed without the encryption key stored in the metadata.

Upon completion of data transformation on each device, the CTE Agent on that device automatically replicates the metadata file for that device to the other nodes in the clique using the Teradata `pcl` command. CTE uses `pcl` to both determine the other members of the clique and to replicate the metadata to those other members. When the metadata is replicated on the remote nodes, any existing metadata for the recently-transformed device already on those nodes is replaced with the updated metadata files sent by the CTE Agent. This replacement is achieved by sending the updated metadata file to all of the remote nodes through `pcl` and replacing each existing metadata file on the remote nodes with the most recent metadata files.

Specific Issues to Consider

This section describes specific problems that may be encountered during data transformation and metadata replication. Manual user intervention will be required to recover from the reported issues. For troubleshooting and recovery steps, see [Alerts and Errors](#).

General PCL Error

If the `pcl` command fails during the replication process, a message indicating the error will be logged. The messages are tagged with IDT-TD-ALERT. For example:

- IDT-TD-ALERT: Node <node name> did not respond to `pcl` command
- IDT-TD-ALERT: Failed to distribute IDT-Capable metadata file to remote nodes

These errors indicate that the node specified in the first error did not respond to a `pcl` command during metadata distribution. As a result, the metadata distribution must be manually performed across the clique before access to the device is possible.

Offline Node in Clique During Data Transformation

If a node is offline during data transformation and metadata replication process, CTE will log a message that metadata replication to the target node failed. The administrator will be required to manually replicate the metadata file to the offline node when the node comes online. The metadata file must be replicated before the database is brought up.

To do so:

- Run the `voradmin td distribute <device name>` command to distribute the metadata file of each device. The command will copy, or update, the metadata file on the agent that has come online. For example:

```
voradmin td distribute \  
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

Adding a New Node to a Clique

When you add a new node to an existing clique, the metadata files of all disks shared in the clique must be manually replicated to the newly added node before any of the guarded devices on the new node are enabled. This should be done manually using the `voradmin td distribute` command, as described above, by the Teradata administrator as part of joining the cluster.

Interoperability with Host Groups

For Teradata, when you create a new IDT-Capable GuardPoint using the `voradmin idt config xform` command, or when you subsequently rekey an existing IDT-Capable GuardPoint with the `voradmin idt rekey` command, the device must be initialized and guarded on one and only one of the nodes in the cluster. That means the IDT-Capable GuardPoint cannot be part of a client group when an IDT-Capable GuardPoint is created or rekeyed because membership in a client group means that any data transformation on any member of the client group is initiated for that member on all nodes in the client simultaneously. In the case of a Teradata cluster, multiple nodes simultaneously trying to perform data transformation on a particular device can lead to data corruption of all data on the entire device.

After the device has been guarded, or rekeyed, and the metadata files have been replicated to other members of the Teradata clique, then you can then rejoin the client with the client group.

To configure a new device whose host/client is part of a host/client group:

1. Make sure that there is no GuardPoint for the device at the client group level.
2. Designate one of the nodes in the cluster as the node that you will use to initialize the GuardPoint and for the initial data transformation when the device is guarded for the first time.
3. On the designated node, initialize the device using the `voradmin idt config -external xform <device name>` command. For details, see [Initialize and Guard the Database Devices Using the Standard Initialization Method](#).
4. Guard the device on the designated node using an In-Place Data Transformation policy. For details, see [Guard the Devices as IDT-Capable GuardPoints on CM](#).
5. Wait for the data transformation to complete on the host and for CTE to replicate the metadata to the other members of the clique.
6. You can verify that the metadata file has been distributed to the other nodes in the clique by running `md5sum /var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata` on each node in the clique.
7. Remove the IDT-Capable GuardPoint you added earlier in this procedure.
8. Guard the device through the client group to make sure that all nodes in the cluster recognize it as guarded.

**** To rekey a new device whose host/client is part of a host/client group:****

1. Unguard the IDT-Capable GuardPoint through the client group and make sure that it has been removed from all nodes in the cluster.
2. Designate one of the nodes in the cluster as the node that you will use to prepare the GuardPoint for rekeying

and to perform the data transformation when the device is guarded with the new policy.

3. On the designated node, prepare the device for rekey using the `voradmin idt rekey <device name>` command.
4. On the other nodes in the clique, make sure that the device metadata has been renamed running `ls /var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata*` on each of the other nodes. On these other nodes, the metadata file for the device should be renamed to `/var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata_xforming`.
5. Guard the device on the designated node with the In-Place Data Transformation policy that specifies the new key you want to use for the device.
6. Wait for the data transformation process to complete, and then make sure that the metadata for the device has been updated on the other nodes in the clique and the renamed metadata files have been removed. Each node should have identical copies of `/var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata` and `/var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata_xforming` should *not* exist on any node.
7. Remove the IDT-Capable GuardPoint that you created earlier in this procedure on the designated node.
8. Guard the device through the client group to make sure that all nodes in the cluster recognize it as guarded.

Best Practices

- Using a of Host/Client Group to Guard Metadata Directories
- Using a Host/Client Group for Guarding Teradata Devices in a Clique
- Best Practice for Preparation for Initial Data Transformation or Rekey

Using a of Host/Client Group to Guard Metadata Directories

Thales recommends that customers use a host group exclusively for guarding and management of the CTE external metadata directories across all nodes in Teradata cluster. (For details about the CTE metadata directory, see [Location of the CTE Private Region](#).)

By using a Host/Client Group, you can apply the same policy to the external metadata directory (`/var/opt/teradata/vormetric/vte-metadata-dir`) on all of the CTE protected nodes in the cluster.

Using a Host/Client Group for Guarding Teradata Devices in a Clique

Thales recommend that customers use a Host/Client Group to guard and manage the devices shared by all CTE protected nodes in a clique. Each clique in the cluster should be associated with a separate Host/Client Group. When configuring the Host/Client Group, the members for that client group are the nodes that belong within a clique in the cluster.

Example 1: If you have a cluster consisting of 4 cliques where there are 2 nodes sharing disks in each clique, you would create 4 Host/Client Groups, one for each clique. In each Host/Client Group, you would add the 2 nodes that are associated with the clique.

Example 2: If you have a cluster consisting of 1 clique where there are 6 nodes sharing disks in the clique, you want to create 1 client group with all 6 members that belong within that clique.

Below is an example of the Host Groups for a cluster consisting of three cliques and one metadata group:

Select	Name	Cluster Group	Description
☐	TD-cluster1-clique-1		host/client group for cluster1 clique-1
☐	TD-cluster1-clique-2		host/client group for cluster1 clique-2
☐	TD-cluster1-clique-3		host/client group for cluster1 clique-3
☐	TD-cluster1-metadata-dir		host/client group for cluster1 metadata

Best Practice for Preparation for Initial Data Transformation or Rekey

With large amounts of data managed in Teradata clusters, duration of initial data transformation and/or subsequent rekey can be very long and challenging because the database must be stopped during the data transformation process. Although you cannot transform data without shutting down the database, you may be able to reduce the transformation time by distributing the transformation of the guarded devices across multiple nodes in your cluster.

Because multiple nodes in a cluster within a clique share access to the same devices, you can designate a subset of devices to each node within the clique for initial data transformation or subsequent rekey. This requires unguarding all of the IDT-Capable devices in the Host/Client Group associated with the clique, and re-enabling each IDT-Capable GuardPoint on the node designated for the data transformation of that IDT-Capable GuardPoint. The device then remains unguarded on other nodes until the data transformation completes.

After the data transformation completes, you can then enable the guarded devices at the Host/Client Group level. Enabling the guarded device at Host/Client Group level enables the guarded devices on all of the nodes within the clique to share access to the device.

After transforming data and guarding each device on all of the nodes, you can then restart the database.

As described in [Interoperability with Host Groups](#), the metadata file for each device is replicated to the hosts in the cluster that share access to the device. As noted, replication of metadata files is automatic.

Uninstalling CTE from the Teradata Cluster

The following procedure describes how to remove CTE from your Teradata cluster. Note that uninstalling CTE will unprotect the pdisk devices that CTE is protecting/encrypting. Because the data on the pdisks remain encrypted after uninstalling CTE, the entire clear-text data must be restored to the pdisks from backup. Therefore, you must have a full backup of your database to restore to your cluster before you uninstall CTE. See the Teradata Administration Guide or your Teradata Customer Support Representative for information about backing up your database in full.

Note

You must be familiar with CTE operations for protecting Teradata clusters and IDT-Capable GuardPoints.

To uninstall CTE:

1. Make sure you have access to a full database backup so that you can restore your Teradata database after uninstalling CTE.
2. Shut down your Teradata database.
3. Use the `secfsd -status guard` command to view the full list of device GuardPoints guarded by CTE on each node of your cluster. From this information, create a consolidated list of GuardPoints with one entry per device in the consolidated list. Note that the devices accessed by the nodes in the same clique are shared devices on each node. The consolidated list must include all devices that are protected in your cluster.
4. Perform the following steps on the CipherTrust Manager:
 - a. Click on the client group name associated with your Teradata cluster and then click the **GuardPoints** tab.
 - b. Select the device names listed in GuardPoints table. The devices listed in GuardPoints table are the same devices listed in the consolidated list of devices compiled in step 3.
 - c. Unguard the selected device GuardPoints on all nodes in the cluster.
 - d. Wait for device status to change from green circle to red circle in the Status column for all the selected devices.
 - e. Select the same devices.
 - f. Click **Unguard** to remove the selected device GuardPoints on all nodes in the cluster.
5. Perform the following steps on one of the nodes of every clique in your cluster:
 - a. Run the `voradmin idt delete` command to delete the IDT-Capable GuardPoint configuration recorded for each device. This command automatically deletes the GuardPoint configuration across the nodes in the same clique.

```
voradmin idt delete <device name>
```

- b. Repeat the previous step on the other devices in your cluster, if any.
6. Go back to the Key Manager and do the following:
 - a. Select the Metadata Directory GuardPoint in the GuardPoints table of the same host group.

- b. Click **Disable** to disable the Metadata GuardPoint directory on every node in the cluster.
 - c. Select the Metadata Directory GuardPoint in the GuardPoints table again and then click **Unguard** to remove the Metadata Directory GuardPoint on all the nodes in the cluster.
7. On every node in the cluster:
- a. Run the following command to stop CTE service on each node:

```
/etc/vormetric/secfs stop
```

- b. Run the following command to uninstall the CTE Agent on each node:

```
/opt/teradata/vormetric/agent/vmd/bin/uninstall
```

To restore a full backup of the database to your cluster, contact your Teradata Customer Support Representative (CSR) to perform System Initializer and do a full restore.

Alerts and Errors

This section lists the alerts and errors that may be encountered during system operations on Teradata Appliance. Refer to Alerts and Errors listed in the chapter on IDT-Capable Device GuardPoints for additional Alerts and Errors.

General Errors

The errors in this section indicate what step failed during CTE system operations for Teradata clusters and will always be paired with an operation error which indicates which CTE system operation failed. For example:

- IDT-TD-ALERT: Node <node name> did not respond to pcl command
- IDT-TD-ALERT: Failed to complete rekey on remote nodes

This pairing of errors indicates that the steps after data transformation were unsuccessful and that the `voradmin` command `voradmin td rekeyed <device name>` is the one that failed.

For details about the `voradmin td rekeyed` command, see the `voradmin` manpage.

IDT-TD-ALERT: Node <node name> did not respond to pcl command

The node listed did not respond to a pcl command to perform an operation.

Solution: Check if the node is still online and responding. If it is, run the `voradmin` command to repeat the failed operation. This error message will always be accompanied by one of the other IDT-TD-ALERTS which will determine which `voradmin` command to run to correct the error.

IDT-TD-ALERT: Node <node name> failed to perform voradmin task

The node listed failed to perform a `voradmin` command invoked through `pcl`.

Solution: Correct the issue blocking `voradmin` and run the `voradmin` command to repeat the failed operation. This error message will always be accompanied by one of the other IDT-TD-ALERTS which will determine which `voradmin` command to run to correct the error.

IDT-TD-ALERT: Failed to find clique for disk <device>

CTE failed to locate the clique for the device specified.

Solution: Verify that `/usr/lib/tmpfiles.d/pdisk.conf` is properly configured on all nodes in the Teradata cluster.

IDT-TD-ALERT: Failed to move or rename IDT-Capable metadata file on remote nodes

This error can be due to two issues; one, metadata files that have been distributed to the remote nodes cannot be moved into the metadata directory, or two, metadata files on remote nodes cannot be renamed in preparation for rekey.

Solution: For the first issue, rerun `voradmin td distribute <node name> <device name>` command once any other problems have been resolved. For the second issue rerun `voradmin td rekey <device name>` to prepare for rekey again once any other problems have been resolved.

For details about the `voradmin td` commands, see the `voradmin` manpage.

IDT-TD-ALERT: Failed to get GuardPoint status on remote nodes

The GuardPoint for the device is still present on the CipherTrust Manager for remote nodes or CTE failed to ascertain the GuardPoint status for remote nodes.

Solution: Verify that the GuardPoint for the device has been removed from the CipherTrust Manager for remote nodes and then rerun the `voradmin` command. This error message will always be accompanied by one of the other IDT-TD-ALERTS which will determine which `voradmin` command to run to correct the error.

Operation Errors

These errors indicate which CTE system operation failed and what command should be run upon resolution of the issue that caused the error.

IDT-TD-ALERT: Failed to distribute IDT-Capable metadata file to remote nodes

CTE failed to copy the IDT-Capable metadata file from the current node to all nodes in the clique.

Solution: Correct any issues blocking `pcl` or `voradmin` and then run `voradmin td distribute <node name> <device name>` to attempt copying the metadata file over to the remote node.

For details about the `voradmin td distribute` command, see the `voradmin` manpage.

IDT-TD-WARNING: Failed to delete IDT-Capable metadata file on remote nodes

CTE was unable to remove the IDT-Capable metadata file for a device from a remote node.

Solution: Run `voradmin idt delete <device name>` on the remote node after correcting issues impeding voradmin. Members of the clique that have successfully removed the metadata file will not be adversely affected if an attempt to remove an already de-configured device occurs.

IDT-TD-ALERT: Failed to complete rekey on remote nodes

CTE was unable to complete the rekey operation on remote nodes to make the device available for guarding again.

Solution: Correct the issue and run `voradmin td rekeyed <node name> <device name>` to signal the remote node that rekey is complete and provide an updated copy of the metadata file to that remote node.

Generating IDT-capable Metadata for Teradata Storage Expansion

Teradata Disk Expansion with IDT-Capable Devices

You can use the `voradmin td expand` command to configure new disks as IDT-capable devices during Teradata disk expansion.

Note

- Guard each new device using the same policy applied to an existing guarded IDT-Capable device.
- Only use this option on new disks added during Teradata disk expansion.

After the new disk is visible to all members of the clique, perform the following steps to configure the new disk:

1. Configure the new disk using the following command on any node in the clique.

```
voradmin td expand <newDiskName> <existingDiskName>
```

Note

Do not run this command on the same device on multiple nodes.

2. Guard the new device on the CipherTrust Manager on all members of the clique.

For disk expansion that includes the addition of a new node to the clique, perform the following steps:

1. Install CTE on the new node and register the node to the CM, but **DO NOT** add the node to the client group, if using one.
2. On the new node, create the CTE Metadata directory, type:

```
mkdir -p /opt/teradata/vormetric/vte-metadata-dir
```

3. On one of the existing nodes in the clique, run the `voradmin td distribute` option to copy all existing metadata to the new node, type:

```
voradmin td distribute < node1 name, node2 name, etc..> <device>
```

4. On the same node selected in step 3, use the `voradmin td expand` option to configure the new disk as an IDT-Capable device, type.

```
voradmin td expand <newDiskName> <existingDiskName>
```

Note

The `td expand` option must be run on each new disk.

5. On CipherTrust Manager, guard the new disk in the client group. You can verify that the new disk is now guarded on all nodes except the new node.
6. On the CipherTrust Manager, add the new node as a member to the client group. Once the new node is added as a member, CipherTrust Manager will push the security policy to the new node and guard all of the disks with metadata files on the new node.

Confidential Computing: Integrating Intel® Tiber™ Trust Services and Intel TDX, with Microsoft Azure or Google Cloud Platform

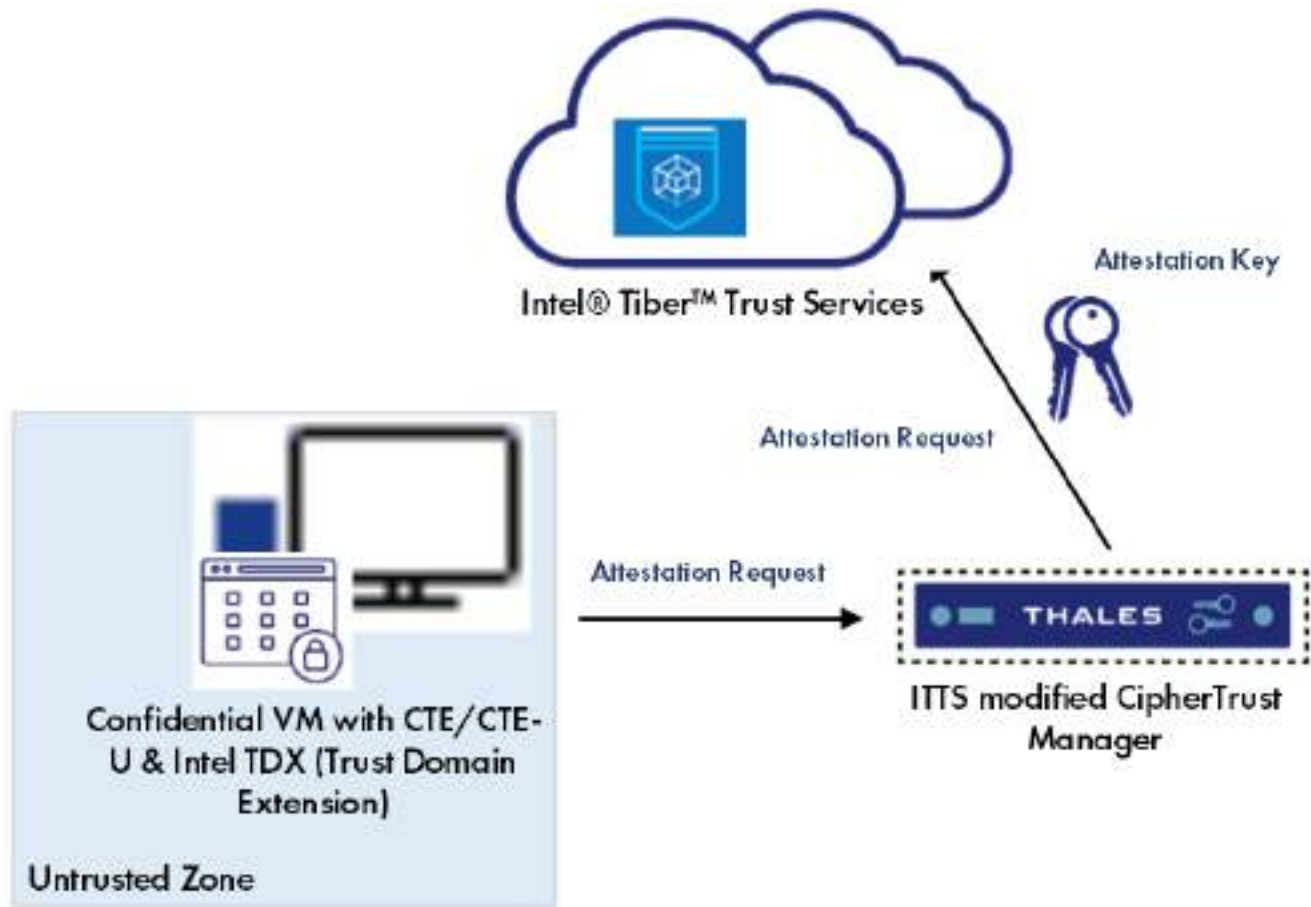
Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Confidential Computing is a cloud computing technology that can isolate and protect data on Confidential Virtual Machines (CVMs), or Trusted Domains (TDs), while it is being processed by the application, to protect it from a broad range of software attacks. Confidential Computing ensures that all data operations are executed within a Trusted Execution Environment.

Confidential Computing provisioning requires Intel® Tiber™ Trust Services (ITTS), to attest the CVMs, or TDs, and create a Trusted Execution Environment around them. ITTS is a verifier in a remote attestation application architecture. In Remote Attestation procedures, one peer (the "Attester"), produces cryptographic information about itself ("Evidence") to enable a remote peer (the "Relying Party") to decide whether or not to consider that Attester a trustworthy peer. In this case, CipherTrust Manager is the Relying Party.

When using Confidential Computing, CTE/CTE-U and CipherTrust Manager manage the attestation process to provision confidential computing on VMs running on agents to provide End-To-End Data Protection. The role of the confidential computing model is to gather the evidence and provide it to CipherTrust Manager to have it attested for by ITTS. If attestation fails, Confidential Computing prevents access to the encrypted data that it guards.



Requirements & Specifications

System	Description
Attestation Authority	Intel® Tiber™ Trust Services (ITTS)
Agent requirements	- Cloud Service Provider: Azure Cloud and Google Cloud Note Support available for the following. • Azure: Intel TDX (Trust Domain Extension) • Google Cloud: Intel TDX and Intel TDX with

System	Description
	NVIDIA H100 Operating Systems: - CTE - Ubuntu 24.04 - CTE-U - Ubuntu 24.04 - RHEL 9 & 10 Kernels (for CTE): CC is supported on cloud specific kernels. Cloud specific kernel numbers end in: -azure -gcp - See the CTE Compatibility Portal for more kernel compatibility information.
CipherTrust Manager Minimum Version	2.20
CipherTrust Transparent Encryption Minimum Version	7.8.0
CTE-U Minimum Version	10.5.0

Prerequisites

1. Install CipherTrust Manager v2.20, or a subsequent version, on a [virtual](#) or [physical](#) system.
2. Ensure that the clocks on the CipherTrust Manager, the CTE client, and the Intel server are synchronized. If they are not, see [Network Time Protocol Server Configuration](#) for more information.
3. Obtain a valid account for one of the following environments:
 - Microsoft Azure
 - Google Cloud Platform
4. Obtain an Intel® Tiber™ Trust Services account.
5. Install and configure **Microsoft Authenticator** on your mobile phone.

Note

For the purposes of this documentation, Thales has documented use of Microsoft Authenticator as the Multi-Factor Authentication (MFA) program. You can use any MFA application with the portal. See [How to Add Additional Authentication Methods](#) to set up and use an alternative MFA provider.

Creating Keys and Policies in the Intel Portal

1. Open Microsoft Authenticator on your mobile phone. The login requests an authentication code from Microsoft Authenticator to access the site.
2. Login to the Intel Portal.
3. Create an [Attestation API key](#). You can associate it with either a simple policy, or one with an MRTD (Measurement of Trust Domain) value.
 - a. In the navigation bar on the left, click **Manage Policies**.
 - b. Click **Add a Policy**. Follow the on-screen instructions for creating a policy.

Field Name	Value
Attestation Type	TDX Attestation
Policy Type	Appraisal policy with an MRTD value.

Simple Policy

```
default matches_sgx_policy = false
matches_sgx_policy = true
{
  input.tdx_is_debuggable == false
}
```

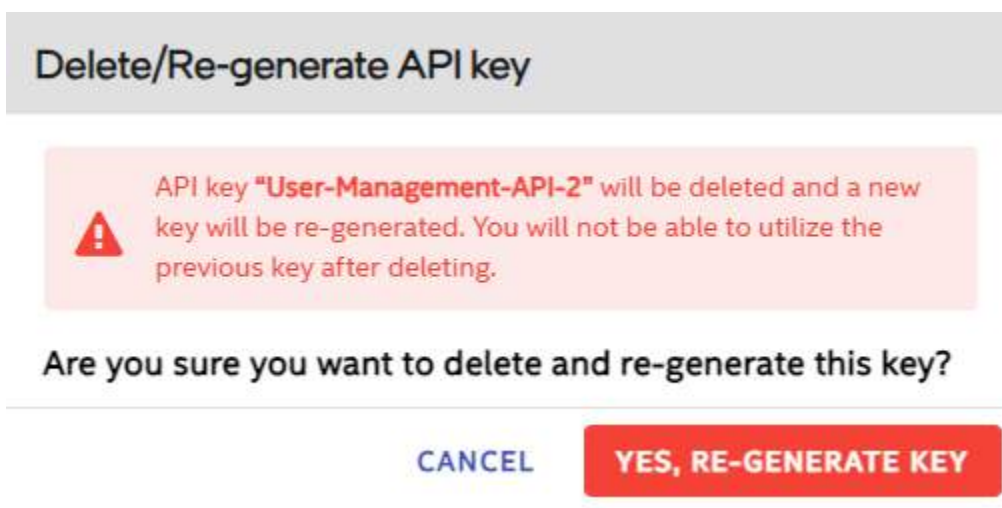
- c. To find the TDX MRTD value, on the CipherTrust Transparent Encryption agent, type:

```
sudo tpm2_nvread --offset=560 --size=48 -C o 0x01400001 | xxd -p | tr -d
'\n' | awk '{print}'
```

- d. To find the TDX MRSEAM value, on the CipherTrust Transparent Encryption agent, type:

```
sudo tpm2 nvread --offset=312 --size=48 -C o 0x01400001 | xxd -p | tr -d
```

- e. Add the policy that you created in the previous step to your API key.
4. Create an **Admin API Key**.
 - a. In the navigation bar on the left, click **Admin API Keys**.
 - b. Select the View icon () for the API key that you want to copy.
 - c. Select the Copy icon (). The API key is copied to your system memory.
 - d. Alternatively, to create a new API key, click **Delete/Regenerate API Key**.



- e. Use the API key with the Trust Services CTL CLI utility to manage admins and users.

Reference Information

To learn how to create an Intel Trust Services policy, consult the following Intel documentation:

- [Appraisal Policies](#)
- [Author a custom policy](#)
- [Policy builder tool](#)

Provisioning TDX machines

Select to provision TDX machines for either Microsoft Azure or Google Cloud Platform.

Provision a TDX machine from Microsoft Azure

1. Login to the [Azure Portal](#).
2. Open Microsoft Authenticator to obtain an authorization code.

- Enter that Microsoft Authenticator code in the dialog on the [Azure Portal](#) page.
- From the home page of the Azure portal, click **Create Resource**.
- Click **Virtual Machine** > **Create** and follow the on-screen instructions to create a VM.

Field Name	VM Type	Value
Security Type	TDX	Confidential virtual machine
OS Image	TDX	Ubuntu Server 24.xx LTS (Confidential VM) -x64 Gen 2
VM architecture	TDX	x64
Size	TDX	Standard DC4eds_v5 or larger

Note

Secure boot is enabled by default. You can disable it once **confidential VM security type** is selected. A link appears for configuring the security features. Toggle the option for **Enable secure boot** to disable it.

- Click **Review & Create**.

TDX-Azure

Virtual machine

Computer name: tdx24

Operating system: Linux (Ubuntu 24.04)

VM generation: V2

VM architecture: x64

Agent status: Ready

Agent version: 2.12.0.2

Hibernation: Disabled

Host group: -

Host: -

Proximity placement group: -

Colocation status: N/A

Capacity reservation group: -

Disk controller type: SCSI

Azure Spot

Azure Spot: -

Networking

Public IP address: 172.200.7.103 (Network interface: tdx24.28311_n1)

Public IP address (IPv4): -

Private IP address: 10.1.0.4

Private IP address (IPv6): -

Virtual network/subnet: tdx24.2-vnet/default

DNS name: [Configure](#)

Size

Size: Standard DC2asv5

vCPUs: 2

RAM: 8 GiB

Source image details

Source image publisher: canonical

Source image offer: ubuntu-24_04-lts

Source image plan: csm

Reference Information

- [Azure Confidential VM options](#)

- [Intel® Trust Authority Client Tutorial: vTPM with Intel® TDX Attestation on Microsoft Azure](#)
- [Intel® Trust Authority REST API Reference](#)

Validate TDX machine

1. List the contents for `/dev/tpm`, type:

```
ls -l /dev/tpm*
```

Result

```
crw-rw---- 1 tss root  10,   224 Aug 14 22:25 /dev/tpm0
crw-rw---- 1 tss tss  253, 65536 Aug 14 22:25 /dev/tpmrm0
```

2. Verify that Intel TDX is activated, type:

```
grep TDX
```

Result

```
[0.902814] Memory Encryption Features active: Intel TDX
```

3. Verify that the TPM (Trusted Platform Module) is valid, type:

```
grep TPM
```

Result

```
[ 0.000000] efi: ACPI=0xbfffa000 ACPI 2.0=0xbfffa014 SMBIOS=0xbff85000 SMBI
OS 3.0=0xbff83000 TPMFinalLog=0xeb39000 MEMATTR=0xbf414018 MOKvar=0xbf402000
INITRD=0xbea62c18                      RNG=0xbffd201
8                      TPMEventLog=0xb6fb3018
[ 0.070902] ACPI: TPM2 0x00000000BFFD3000 000034 (v03 VRTUAL VTPM 00000
001 MSFT 00000001)
[ 0.094058] ACPI: Reserving TPM2 table memory at [mem 0xbffd3000-0xbffd303
3]
```

Install the Trusted Platform Module tools on your Agent VM

- Download the Trusted Platform Module (TPM) tools, type:

```
apt update
apt install tpm2-tools
apt install libnsl2
apt install libatomic1
```

Provision a TDX machine from Google Cloud Platform

Prerequisites

- Obtain an image of **Ubuntu 24.xx LTS**

Use Google Cloud (GCP) to Grant access to all VM instances in a project

- Grant access to all VM instances in a project, type:

```
gcloud projects add-iam-policy-binding thl-ite-d-itecc \
--member: 'group:gcp-ite-itecc@thalescloud.io' \
--role: 'roles/iap.tunnelResourceAccessor' \
--impersonate-service-account automation@thl-ite-d-itecc.iam.gserviceaccount.co
m\
```

Note

Change the thales-related variables to values appropriate for your network.

Reference Information

- Grant access to all VM instances in a project

Check Network (VPC) and firewall flow

Warning

Your network security rules **must** allow public IP for external connection enabled. Otherwise, CTE agent registration may fail.

Create a GCP TDX VM

1. Install the gcloud SDK.

2. Login in and set up the project ID.
3. Create a network, type:

```
gcloud compute networks create tdx-default-network \
--subnet-mode=auto\
--BGP_ROUTING_MODE: REGIONAL\
--IPV4_RANGE: <for-your-network>\
--GATEWAY_IPV4: <for-your-network>
```

4. Create an SSH connection, type:

```
gcloud compute firewall-rules create allow-ssh --network tdx-default-network
--allow tcp:22
```

5. Create the VM, type:

```
gcloud compute instances create tdxvm-cpl-gcp \
--machine-type c3-standard-4 --zone us-central1-a \
--confidential-compute-type=TDX \
--on-host-maintenance=TERMINATE \
--image-family=ubuntu-2404-lts \
--image-project=tdx-guest-images \
--project cpl-tdx-l-tdxpreview-01 \
--subnet "tdx-default-network"
```

6. Connect to the VM with the gcloud sdk, type:

```
gcloud compute ssh tdxvm-cpl-gcp \
--project=cpl-tdx-l-tdxpreview-01 \
--zone=us-central1-a
```

Note

- This should create an ssh key pair. Make sure that the `/.ssh/google_compute_engine.pub` is in your list of allowed ssh keys in your VM google console. (Metadata → SSH Keys).
- If, after you log in, your prompt does not have color, username and machine name, check if the interpreter is `bash` with `echo $0`. If it is not, change it to `bash` with `sudo chsh -s /bin/bash $USER`.

TDX-GCP

Basic information

Name	tdxvm-cpl-gcp-pranay
Instance Id	2742567961464161030
Description	None
Type	Instance
Status	 Running
Creation time	Feb 27, 2024, 10:21:14 AM UTC-05:00
Location 	us-central1-a
Instance template	None
In use by	None
Physical host 	None
Maintenance status 	—
Reservations	Automatically choose (default)
Labels	None
Tags 	—
	
Deletion protection	Disabled
Confidential VM service 	Enabled
Preserved state size	0 GB

Machine configuration

Machine type	c3-standard-4 (4 vCPUs, 16 GB Memory)
CPU platform	Intel Sapphire Rapids
Minimum CPU platform	None
Architecture	x86/64
vCPUs to core ratio 	—

Shielded VM

Secure Boot 	Off
vTPM 	On
Integrity Monitoring 	On

Reference Information

- Intel Trust Authority Client Tutorial: Intel TDX Attestation on GCP

Install the Trusted Platform Module tools on your Agent VM

- Download the Trusted Platform Module (TPM) tools, type:

```
apt update
apt install tpm2-tools
apt install libnsl2
apt install libatomic1
```

CipherTrust Manager Requirements

Create an Attestation Authority Connection

Provisioning Confidential Computing on agents requires one **admin connection** (connection with administrator privileges) and one **non-admin connection** (connection without administrator privileges). The admin connection is necessary to retrieve the policies from the Attestation Authority. CipherTrust Manager uses the connection details to communicate with Intel® Tiber™ Trust Services (ITTS) for agent attestation when a request is received from the agent.

To create the **Attestation Authority** connections:

1. Log on to CipherTrust Manager.
2. In the left nav-bar, click **Access Management > Connections**.
3. Select **+ Add Connection**.
4. In the **Select Connection Type**, click **More**.
5. From the **Select Connection** dropdown, select **Attestation Authority** and click **Next**.
6. In the **General Info** section, enter the **Name** and **Description** for the connection and click **Next**.
7. In **Configure Connection**, create an Admin User Connection by selecting from the following options. Choose European or US for your URLs based on which URL is valid for your account:

Field Name	Country	Value	Description
URL for API method	US	https://api.trustauthority.intel.com	URL for connecting to the Attestation Authority.
	Europe	https://api.eu.trustauthority.intel.com	
	US: AMD	https://api.pilot.trustauthority.intel.com	Pilot for AMD

		urity.intel.com	
Base URL	US	https://portal.trustauthority.intel.com	Base URL for connecting to the Attestation Authority.
	Europe	https://portal.eu.trustauthority.intel.com	
	US: AMD	https://portal.pilot.trustauthority.intel.com	Pilot for AMD
API Key			Provide either the Admin API key, or the Attestation API key, created in ITTS to establish the connection with the Attestation Authority.
Metadata			Provide meta information in the JSON format.

8. Select **Admin User** to create a connection with administrator privileges. Click **Next**.
9. In **Add Products** section, select the **CTE** checkbox.

Note

CTE-U users should also select CTE.

10. Click **Add Connection**.
11. Repeat these steps to create the Attestation connection. **Do not** select Admin User in step 8.

Note

In CipherTrust Manager, select **Access Management > Connections**, click the ellipsis (...) to View, Edit, or Delete the connections..

Create a Global Client Profile

Create a Client Profile to associate with the Attestation Authority connection.

1. In the CipherTrust Manager dashboard, click **Access Management > Client Profiles > Add Client Profile**.
2. Enter **Profile Name** and **Description**.
3. Select **CA Type**: Local or External.
4. Select the respective Local or External CA in **Select <CA Type> CA**.
5. Enter the **Certificate Duration** (in days) for which the CA certificate remains active.
6. Expand the **CONFIDENTIAL COMPUTING** section and add the following details:

Field Name	Value	Description
Attestation Authority Identifier	Intel® Tiber™ Trust Services (ITTS)	
Attestation Connection	Select a non-admin connection	
Admin Connection	Select an admin connection	Note: Admin and non-admin type connections should belong to the same Attestation Authority.
Policy Type	Appraisal policy	These policies are fetched from the Attestation Authority server. You can select appraisal policies.
Policy Names	<policy_names>	Select one or more policies from the drop-down menu.
Cloud Provider	[Azure Google Cloud]	

7. Click **Add/Update Client Profile**.

Create a Registration Token

Create a registration token on the CipherTrust Manager. You must have administrator privileges to create registration tokens.

1. Log on to the CipherTrust Manager GUI as administrator.
2. In the left pane, click **Access Management > Registration Tokens**.
3. On the right, click **Add Registration Token**. The Create New Registration Token wizard displays.
4. Click **Begin** to start token creation. The Configure Token screen displays.
5. (Optional) Specify a **Name Prefix** for the client name. This prefix is used to construct names for clients whose names are not specified during registration with the CipherTrust Manager using this token.
 - If the name prefix is specified as `ks_client`, client names will be constructed as `ks_client#`; for

example, `ks_client1`, `ks_client2`, `ks_client3`, and so on. However, if a client's name is specified during registration, this name prefix is not used for that client.

- If the name prefix is **not** specified, the CipherTrust Manager will construct a *random* name for clients.

6. Set the **Token lifetime**. You **must** include a time unit with it such as:

Token Lifetime Span	Value
10 m	10 minutes
10 h	10 hours
10 d	10 days
unlimited	Never expires

7. Specify **Client Capacity**. This is the maximum number of clients that can be registered using this registration token. The default capacity is **100** clients.
8. Select **Add Profile** and add the client profile that you just created.
9. Click **Create Token**. The Create Token screen displays the generated registration token in **ASCII** and **Base64** encoding. CipherTrust Manager accepts the registration token in ASCII format only.
10. Click **Copy** next to the token to save the copied token. Use this token when registering and migrating clients.

Install and Register CipherTrust Transparent Encryption with a Confidential Computing VM

Prerequisites

Ubuntu Users Only

Before installing Confidential Computing, you must disable the Ubuntu unattended upgrade feature in order to prevent it from automatically upgrading to a kernel version that CipherTrust Transparent Encryption has yet to support. Once the kernel is upgraded, there does not appear to be a method to downgrade it, or choose a compatible kernel version.

To disable the Ubuntu unattended upgrade feature:

1. Type the following command:

```
dpkg-reconfigure unattended-upgrades
```

2. Choose **No** to the question about automatic updates.
3. Verify that the following configuration file shows **0** values, type:


```
cat /etc/apt/apt.conf.d/auto-upgrades
```

Expected Response

```
APT::Periodic::Update-Package-Lists "0";
APT::Periodic::Unattended-Upgrade "0";
```

Install CipherTrust Transparent Encryption

1. Install CipherTrust Transparent Encryption v7.8.0, or a subsequent version, on the VM to which you installed the TPM tools, type:

```
sudo ./vee-fs-7.8.0-88-ubuntuXX-x86_64.bin -y
```

2. During registration, select to enable Confidential Computing.
3. Log on to the host where you will install the CTE Agent as **root**. You cannot install the CTE Agent without **root** access.
4. Copy or mount the installation file to the host system. If necessary, make the file executable with the **chmod** command.
5. Install the CTE Agent. A typical installation uses the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the **-d <custom-dir>** option. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note

- If possible, Thales recommends that you use the default directory **/opt/vormetric**.
- Custom directories are **only available** for RHEL and SLES.

- Custom directories are **not available** for COS (Cloud Object Storage).

To view all installer options, use the `-h` parameter. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -h
```

6. The Thales License Agreement displays. When prompted, type **Y** and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

Welcome to the CipherTrust Transparent Encryption File System Agent Registration Program.

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>
```

```
In order to register with a CipherTrust Manager you need a valid registration token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

7. Type **N** and press Enter to end the installation procedure without registering the CTE Agent with a key manager.
8. Enter **Y** to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE. For example:

CTE for CipherTrust Manager

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Please enter the primary key manager host name: 10.3.200.141
```

```
You entered the host name 10.3.200.141
```

```
Is this host name correct? (Y/N) [Y]: Y
```

CTE for CDSPaaS

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Enter the primary key manager host name of the service:
```

```
You entered the host name us1.ciphertrust.dpondemand.io
```

```
Is this host name correct? (Y/N) [Y]: Y
```

Host names:

- **Europe:** ciphertrust.dpondemand.io
- **North America:** us1.ciphertrust.dpondemand.io

Note

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: <hostName>:<port#>. For example, 10.3.200.141:8445.

9. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the following list.
```

```
[1] sys31186.qa.com
```

```
[2] 10.3.31.186
```

```
Enter a number, or type a different host name or IP address in manually:
```

```
What is the name of this machine? [1]: 2
```

```
You selected "10.3.31.186".
```

10. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
```

```
Please enter the profile name for this host: My-Profile
```

```
Please enter the host group name for this host, if any:
```

```
Please enter a description for this host: RHEL7 system West Coast Datacenter
```

```
Token : 12345
```

```
Profile name : My-Profile
```

```
Host Group : (none)
```

```
Host description : RHEL7 system West Coast Datacenter
```

```
Are the above values correct? (Y/N) [Y]: Y
```

11. At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloning. The default is Y (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again. Do you want to enable this functionality? (Y/N) [Y]: Y

12. Type Y to support Filesystem encryption and to choose other features. Type N if you only want to support Ransomware Protection. If you type N, then LDT and COS are not supported.

```
Do you want this host to have Filesystem encryption support enabled on the server? (Y/N) [Y]:
```

13. At the LDT prompt, specify that you want this client to use CTE-LDT by typing Y and pressing Enter:

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]: Y
```

14. If you are planning to create GuardPoints on NFS shares, enter the name of the LDT Communication Group that this node will join.

```
Enter the LDT Communication Group name: LCG1
```

Warning

The registration token, profile name, client group name and LDT Communication Group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

15. The installation checks for Confidential Computing adapter types. If it finds one, it states:

```
The following confidential computing adapter types have been identified.
1. Intel Trust Domain Extensions (tdx)
Do you want this host to have confidential computing enabled? (Y/N) [N]:
```

Type Y to enable Confidential Computing.

16. At the Cloud Object Storage (COS) prompt, specify whether you want this client to use CTE COS.

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

17. Specify if you want to enable Ransomware Protection.

```
Do you want this host to have Ransomware Protection support enabled on the server? (Y/N) [N]:
```

18. CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.
Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption CTE Agent with
the CipherTrust Manager on 10.3.200.141.

Installation success.
```

19. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Validate Confidential Computing on the CTE Agent for Attestation

1. Verify that your agent is capable of confidential computing, type:

```
sudo /opt/vormetric/DataSecurityExpert/agent/vmd/bin/vmutil -a vmd cc_check
```

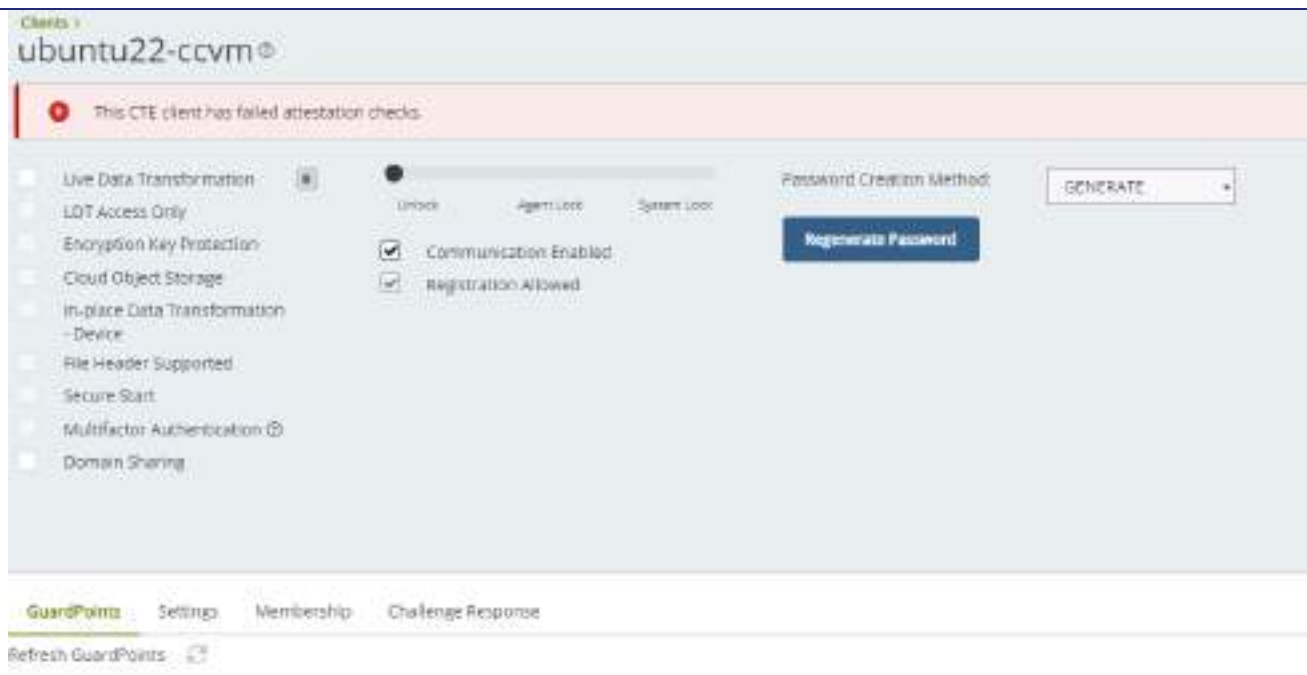
Result if validation succeeds

```
This system is capable of confidential computing.
```

Result if validation fails

```
This system is not capable of confidential computing
```

In the UI, CipherTrust Manager displays the term **warning** in the status column and displays a banner message indicating that the Agent failed attestation.



2. If using a policy with an MRTD value, validate that the MRTD value in the policy and on the Agent are the same, type:

```
sudo tpm2_nvread --offset=560 --size=48 -C o 0x01400001 | xxd -p | tr -d '\n' | awk '{print}'
```

It should be the same value as the MRTD value on this file:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/attestation.txt
```

Note

Attestations fail when the TCB status becomes out-of-date. Following is an example from the attestation report:

```
"attester_tcb_status": "OutOfDate"
```

Attestations will continue to fail until Azure rolls out a new paravisor with the updated TCB on the VM (This would also mean new measurements, such as the MRTD values, that you will need to update in the attestation policy).

To temporarily workaround this out-of-date TCB issue, remove the following line from the attestation policy:

```
input.attester_tcb_status = "UpToDate"
```

Confidential Computing Policies

There are no special CTE policies for Confidential Computing. Create standard and LDT policies as usual.

Confidential Computing GuardPoints

There are no special GuardPoints for Confidential Computing. Create GuardPoints as usual.

Integrating with Intel® Tiber™ Trust Services and Intel TDX for Confidential Computing

Caution

This feature is a technical preview for evaluation in non-production environments. Details and functionality are subject to change.

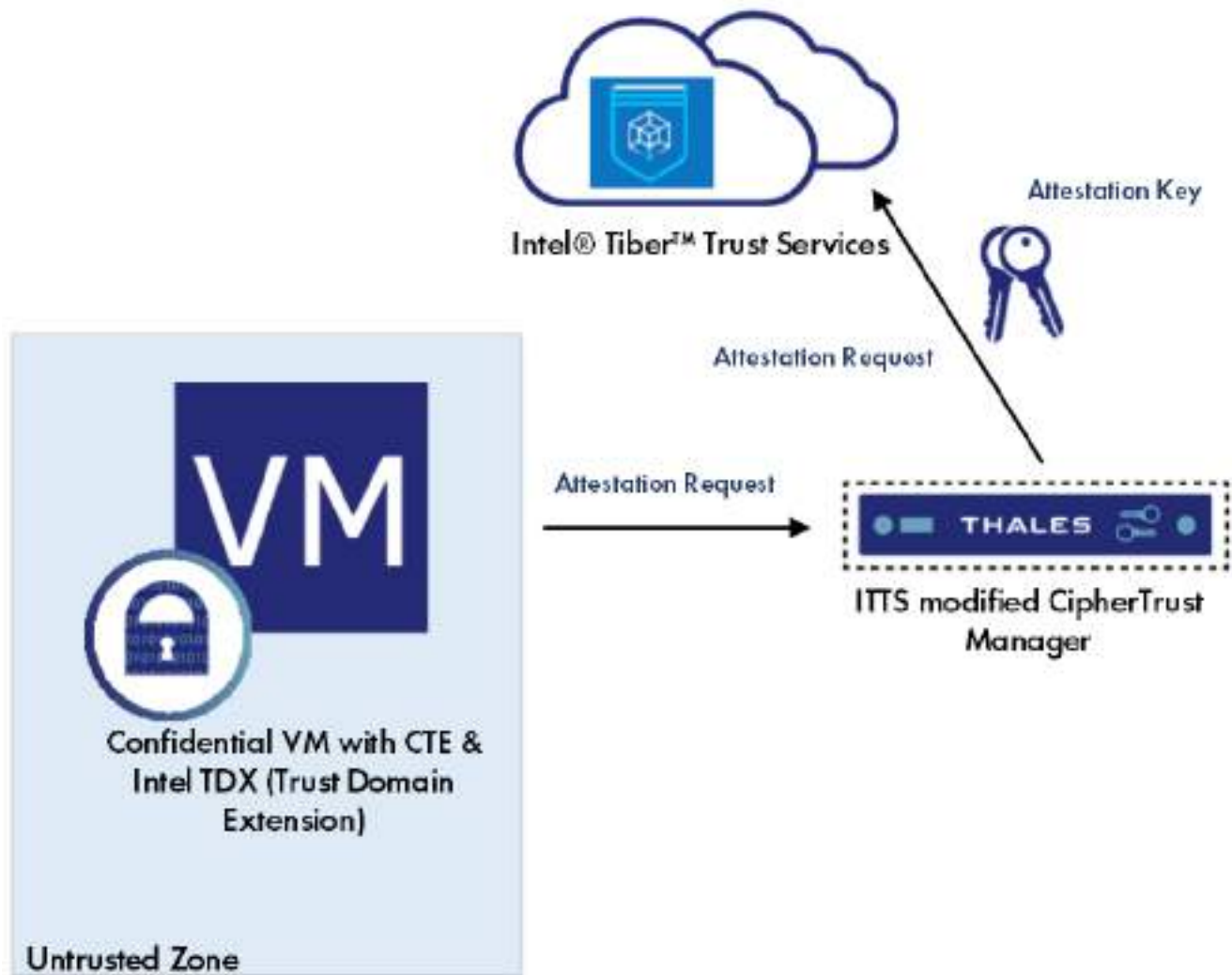
Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Confidential Computing is a cloud computing technology that can isolate and protect data on Confidential Virtual Machines (CVMs), or Trusted Domains (TDs), while it is being processed by the application, to protect it from a broad range of software attacks. Confidential computing ensures that all data operations are executed within a Trusted Execution Environment.

Confidential Computing provisioning requires Intel® Tiber™ Trust Services (ITTS), to attest the CVMs, or TDs, and create a Trusted Execution Environment around them. ITTS is a verifier in a remote attestation application architecture. In Remote Attestation procedures, one peer (the "Attester"), produces cryptographic information about itself ("Evidence") to enable a remote peer (the "Relying Party") to decide whether or not to consider that Attester a trustworthy peer. In this case, CipherTrust Manager is the Relying Party.

CipherTrust Transparent Encryption and CipherTrust Manager manage the attestation process to provision confidential computing on VMs running on CTE agents to provide End-To-End Data Protection. The role for CTE in this confidential computing model is to gather the evidence and provide that to CipherTrust Manager to have it attested for by ITTS. If attestation fails, CTE prevents access to the encrypted data that it guards.



Requirements & Specifications

System	Description
Attestation Authority	Intel® Tiber™ Trust Services (ITTS)
Agent Requirements Minimum versions listed. Subsequent versions also valid.	▪ Cloud Service Provider: Azure version 5.19 ▪ Operating System: Ubuntu 22.04 ▪ Kernel: 6.5.0-1025-azure
CipherTrust Manager Minimum Version	2.18
CipherTrust Transparent Encryption Minimum Version	7.7.0

Prerequisites

1. Install CipherTrust Manager v2.18, or a subsequent version, on a [virtual](#) or [physical](#) system.

Note

Ensure that the clocks on the CipherTrust Manager, the CTE client, and the Intel server are synchronized. If they are not, see [Network Time Protocol Server Configuration](#)

2. Obtain a valid account for [Microsoft Azure](#).
3. Obtain an [Intel® Tiber™ Trust Services](#) account.
4. Install and configure **Microsoft Authenticator** on your mobile phone.

Note

For the purposes of this documentation, we have documented use of Microsoft Authenticator as the Multi-Factor Authentication (MFA) program. You can use any MFA application with the portal. See [How to Add Additional Authentication Methods](#) to set up and use an alternative MFA provider.

Provision a TDX machine from Microsoft Azure

TDX is the remote attestation service.

1. Login to the [Azure Portal](#).
2. Open Microsoft Authenticator to obtain an authorization code.
3. Enter that Microsoft Authenticator code in the dialog on the [Azure Portal](#) page.
4. From the home page of the Azure portal, click **Create Resource**.
5. Click **Virtual Machine** > **Create** and follow the on-screen instructions to create a VM.

Field Name	Value
Security Type	Confidential virtual machine
OS Image	Ubuntu Server 22.04 LTS (Confidential VM) -x64 Gen 2
VM architecture	x64

Field Name	Value
Size	Standard DC4eds_v5 or larger

Note

Secure boot is enabled by default. You can disable it once `confidential VM security type` is selected. A link appears for configuring the security features. Toggle the option for `Enable secure boot` to disable it.

6. Click **Review & Create**.

Validate TDX machine

1. List the contents for `/dev/tpm`, type:

```
ls -l /dev/tpm*
```

Result

```
crw-rw---- 1 tss root 10, 224 Aug 14 22:25 /dev/tpm0
crw-rw---- 1 tss tss 253, 65536 Aug 14 22:25 /dev/tpmrm0
```

2. Verify that Intel TDX is activated, type:

```
grep TDX
```

Result

```
[ 0.902814] Memory Encryption Features active: Intel TDX
```

3. Verify that the TPM (Trusted Platform Module) is valid, type:

```
grep TPM
```

Result

```
[ 0.000000] efi: ACPI=0xbfffa000 ACPI 2.0=0xbfffa014 SMBIOS=0xbff85000 SMBI
OS 3.0=0xbff83000 TPMFinalLog=0xbeb39000 MEMATTR=0xbf414018 MOKvar=0xbf402000
INITRD=0xbea62c18                      RNG=0xbffd201
8                      TPMEventLog=0xb6fb3018
[ 0.070902] ACPI: TPM2 0x00000000BFFD3000 000034 (v03 VRTUAL VTPM 00000
001 MSFT 00000001)
[ 0.094058] ACPI: Reserving TPM2 table memory at [mem 0xbffd3000-0xbffd303
3]
```

Reference Information

- Create a confidential VM with the Azure CLI
- Deploy confidential VM with ARM template
- Create confidential VM in the Azure portal

Install the Trusted Platform Module tools on your Agent VM

1. Download the Trusted Platform Module (TPM) tools, type:

```
git clone https://github.com/tpm2-software/tpm2-tools
```

2. Install the Trusted Platform Module (TPM) tools on the CipherTrust Transparent Encryption agent, type:

```
apt install tpm2-tools
```

Creating Keys and Policies in the Intel Portal

1. Open Microsoft Authenticator on your mobile phone. The login requests an authentication code from Microsoft

Authenticator to access the site.

2. Login to the [Intel Portal](#).
3. Create an [Attestation API key](#). You can associate it with either a simple policy, or one with an MRTD (Measurement of Trust Domain) value.
 - a. In the navigation bar on the left, click **Manage Policies**.
 - b. Click **Add a Policy**. Follow the on-screen instructions for creating a policy.

Field Name	Value
Attestation Type	TDX Attestation
Policy Type	Appraisal policy with an MRTD value.

Simple Policy

```
default matches_sgx_policy = false
matches_sgx_policy = true
{
  input.tdx_is_debuggable == false
}
```

- c. To find the TDX MRTD value, on the CipherTrust Transparent Encryption agent, type:

```
sudo tpm2_nvread --offset=560 --size=48 -C o 0x01400001 | xxd -p | tr -d
'\n' | awk '{print}'
```

- d. To find the TDX MRSEAM value, on the CipherTrust Transparent Encryption agent, type:

```
sudo tpm2 nvread --offset=312 --size=48 -C o 0x01400001 | xxd -p | tr -d
```

- e. Add the policy that you created in the previous step to your API key.
4. Create an **Admin API Key**.
 - a. In the navigation bar on the left, click **Admin API Keys**.
 - b. Select the View icon () for the API key that you want to copy.
 - c. Select the Copy icon (). The API key is copied to your system memory.
 - d. Alternatively, to create a new API key, click **Delete/Regenerate API Key**.

Delete/Re-generate API key



API key "**User-Management-API-2**" will be deleted and a new key will be re-generated. You will not be able to utilize the previous key after deleting.

Are you sure you want to delete and re-generate this key?

CANCEL

YES, RE-GENERATE KEY

- e. Use the API key with the Trust Services CTL CLI utility to manage admins and users.

Reference Information

To learn how to create an Intel Trust Services policy, consult the following Intel documentation:

- [Appraisal Policies](#)
- [Author a custom policy](#)
- [Policy builder tool](#)

CipherTrust Manager Requirements

Create an Attestation Authority Connection

Provisioning Confidential Computing on CTE clients requires one **admin connection** (connection with administrator privileges) and one **non-admin connection** (connection without administrator privileges). The admin connection is necessary to retrieve the policies from the Attestation Authority. CipherTrust Manager uses the connection details to communicate with ITTS for agent attestation when a request is received from the agent.

To create the **Attestation Authority** connections:

1. Log on to CipherTrust Manager.
2. In the left nav-bar, click **Access Management > Connections**.
3. Select **+ Add Connection**.
4. In the **Select Connection Type**, click **More**.
5. From the **Select Connection** dropdown, select **Attestation Authority** and click **Next**.
6. In the **General Info** section, enter the **Name** and **Description** for the connection and click **Next**.

7. In **Configure Connection**, create an Admin User Connection by selecting from the following options. Choose European or US for your URLs based on which URL is valid for your account:

Field Name	Value	Description
URL for API method	https://api.trustauthority.intel.com	URL for connecting to the Attestation Authority.
Base European URL	https://portal.eu.trustauthority.intel.com	Base URL for the Attestation Authority.
Base U.S. URL	https://portal.trustauthority.intel.com	Base URL for the Attestation Authority.
API Key		Provide either the Admin API key or the Attestation API key created in ITTS to establish the connection with the Attestation Authority.
Base API European URL	https://api.eu.trustauthority.intel.com	Base URL for API connection.
Base API U.S. URL	https://api.trustauthority.intel.com	Base URL for API connection.

8. Select **Admin User** to create a connection with administrator privileges. Click **Next**.
9. In **Add Products** section, select the **CTE** checkbox.
10. Click **Add Connection**.
11. Repeat these steps to create the Attestation connection. **Do not** select Admin User in step 8.

Note

In CipherTrust Manager, select **Access Management > Connections**, click the ellipsis (...) to View, Edit, or Delete the connections..

Create a Global Client Profile

Create a Client Profile to associate with the Attestation Authority connection.

1. In the CipherTrust Manager dashboard, click **Access Management > Client Profiles > Add Client Profile**.
2. Enter **Profile Name** and **Description**.
3. Select **CA Type**: Local or External.

4. Select the respective Local or External CA in **Select <CA Type> CA**.
5. Enter the **Certificate Duration** (in days) for which the CA certificate remains active.
6. Expand the **CONFIDENTIAL COMPUTING** section and add the following details:

Field Name	Value	Description
Attestation Authority Identifier	Intel Trust Authority (ITTS)	
Attestation Type	TDX Attestation	
Attestation Connection	Select a non-admin connection	
Admin Connection	Select an admin connection	Note: Admin and non-admin type connections should belong to the same Attestation Authority.
Policy Type	Appraisal policy	These policies are fetched from the Attestation Authority server. You can select appraisal policies.
Policy Names	<policy_names>	Select one or more policies from the drop-down menu.
Cloud Provider	Azure	

7. Click **Add/Update Client Profile**.

Create a Registration Token

Create a registration token on the CipherTrust Manager. You must have administrator privileges to create registration tokens.

1. Log on to the CipherTrust Manager GUI as administrator.
2. In the left pane, click **Access Management > Registration Tokens**.
3. On the right, click **Add Registration Token**. The Create New Registration Token wizard displays.
4. Click **Begin** to start token creation. The Configure Token screen displays.
5. (Optional) Specify a **Name Prefix** for the client name. This prefix is used to construct names for clients whose names are not specified during registration with the CipherTrust Manager using this token.
 - If the name prefix is specified as `ks_client`, client names will be constructed as `ks_client#`; for example, `ks_client1`, `ks_client2`, `ks_client3`, and so on. However, if a client's name is specified during registration, this name prefix is not used for that client.
 - If the name prefix is **not** specified, the CipherTrust Manager will construct a *random* name for clients.

- Set the **Token lifetime**. You **must** include a time unit with it such as:

Token Lifetime Span	Value
10 m	10 minutes
10 h	10 hours
10 d	10 days
unlimited	Never expires

- Specify **Client Capacity**. This is the maximum number of clients that can be registered using this registration token. The default capacity is **100** clients.
- Select **Add Profile** and add the client profile that you just created.
- Click **Create Token**. The Create Token screen displays the generated registration token in **ASCII** and **Base64** encoding. CipherTrust Manager accepts the registration token in ASCII format only.
- Click **Copy** next to the token to save the copied token. Use this token when registering and migrating clients.

Install and Register CipherTrust Transparent Encryption with a Confidential Computing Azure VM

Prerequisites

Ubuntu Users Only

Before installing CipherTrust Transparent Encryption, you must disable the Ubuntu unattended upgrade feature in order to prevent it from automatically upgrading to a kernel version that CipherTrust Transparent Encryption has yet to support. Once the Azure kernel is upgraded, there does not appear to be a method to downgrade it, or choose a compatible kernel version.

To disable the Ubuntu unattended upgrade feature:

- Type the following command:

```
dpkg-reconfigure unattended-upgrades
```

- Choose **No** to the question about automatic updates.
- Verify that the following configuration file shows **0** values, type:

```
cat /etc/apt/apt.conf.d/20auto-upgrades
```

Expected Response


```
APT::Periodic::Update-Package-Lists "0";
APT::Periodic::Unattended-Upgrade "0";
```

Install CipherTrust Transparent Encryption

1. Install CipherTrust Transparent Encryption v7.7.0, or a subsequent version, on the VM to which you installed the TPM tools, type:

```
sudo ./vee-fs-7.7.0-48-ubuntu22-x86_64.bin -y
```

2. During registration, select to enable Confidential Computing.
3. Log on to the host where you will install the CTE Agent as **root**. You cannot install the CTE Agent without **root** access.
4. Copy or mount the installation file to the host system. If necessary, make the file executable with the **chmod** command.
5. Install the CTE Agent. A typical installation uses the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the **-d <custom-dir>** option. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note

- If possible, Thales recommends that you use the default directory **/opt/vormetric**.
- Custom directories are **only available** for RHEL and SLES.
- Custom directories are **not available** for COS (Cloud Object Storage).

To view all installer options, use the **-h** parameter. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -h
```

6. The Thales License Agreement displays. When prompted, type **Y** and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

Welcome to the CipherTrust Transparent Encryption File System Agent Registration Program.

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>
```

```
In order to register with a CipherTrust Manager you need a valid registration token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

7. Type **N** and press Enter to end the installation procedure without registering the CTE Agent with a key manager.
8. Enter **Y** to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE. For example:

CTE for CipherTrust Manager

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Please enter the primary key manager host name: 10.3.200.141
```

```
You entered the host name 10.3.200.141
```

```
Is this host name correct? (Y/N) [Y]: Y
```

CTE for CDSPaaS

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Enter the primary key manager host name of the service:
```

```
You entered the host name us1.ciphertrust.dpondemand.io
```

```
Is this host name correct? (Y/N) [Y]: Y
```

Host names:

- **Europe:** `ciphertrust.dpondemand.io`
- **North America:** `us1.ciphertrust.dpondemand.io`

Note

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: `<hostName>:<port#>`. For example, `10.3.200.141:8445`.

9. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the following list.
```

```
[1] sys31186.qa.com
```

```
[2] 10.3.31.186
```

```
Enter a number, or type a different host name or IP address in manually:
```

```
What is the name of this machine? [1]: 2
```

```
You selected "10.3.31.186".
```

10. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
```

```
Please enter the profile name for this host: My-Profile
```

```
Please enter the host group name for this host, if any:
```

```
Please enter a description for this host: RHEL7 system West Coast Datacenter
```

```
Token : 12345
```

```
Profile name : My-Profile
```

```
Host Group : (none)
```

```
Host description : RHEL7 system West Coast Datacenter
```

```
Are the above values correct? (Y/N) [Y]: Y
```

11. At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloning. The default is Y (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again. Do you want to enable this functionality? (Y/N) [Y]:
Y

12. Type Y to support Filesystem encryption and to choose other features. Type N if you only want to support Ransomware Protection. If you type N, then LDT and COS are not supported.

```
Do you want this host to have Filesystem encryption support enabled on the server? (Y/N) [Y]:
```

13. At the LDT prompt, specify that you want this client to use CTE-LDT by typing Y and pressing Enter:

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]: Y
```

14. If you are planning to create GuardPoints on NFS shares, enter the name of the LDT Communication Group that this node will join.

```
Enter the LDT Communication Group name: LCG1
```

Warning

The registration token, profile name, client group name and LDT Communication Group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

15. The installation checks for Confidential Computing adapter types. If it finds one, it states:

```
The following confidential computing adapter types have been identified.
1. Intel Trust Domain Extensions (tdx)
Do you want this host to have confidential computing enabled? (Y/N) [N]:
```

Type Y to enable Confidential Computing.

16. At the Cloud Object Storage (COS) prompt, specify whether you want this client to use CTE COS.

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

17. Specify if you want to enable Ransomware Protection.

```
Do you want this host to have Ransomware Protection support enabled on the server? (Y/N) [N]:
```

18. CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.  
Extracting SECFS key  
Generating EC certificate signing request for the vmd...done.  
Signing certificate...done.  
Enrolling agent with service on 10.3.200.141...done.  
Successfully registered the CipherTrust Transparent Encryption CTE Agent with  
the CipherTrust Manager on 10.3.200.141.  
  
Installation success.
```

19. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Validate Confidential Computing on the CTE Agent for Attestation

1. Verify that your CTE agent is capable of confidential computing, type:

```
sudo /opt/vormetric/DataSecurityExpert/agent/vmd/bin/vmutil -a vmd cc_check
```

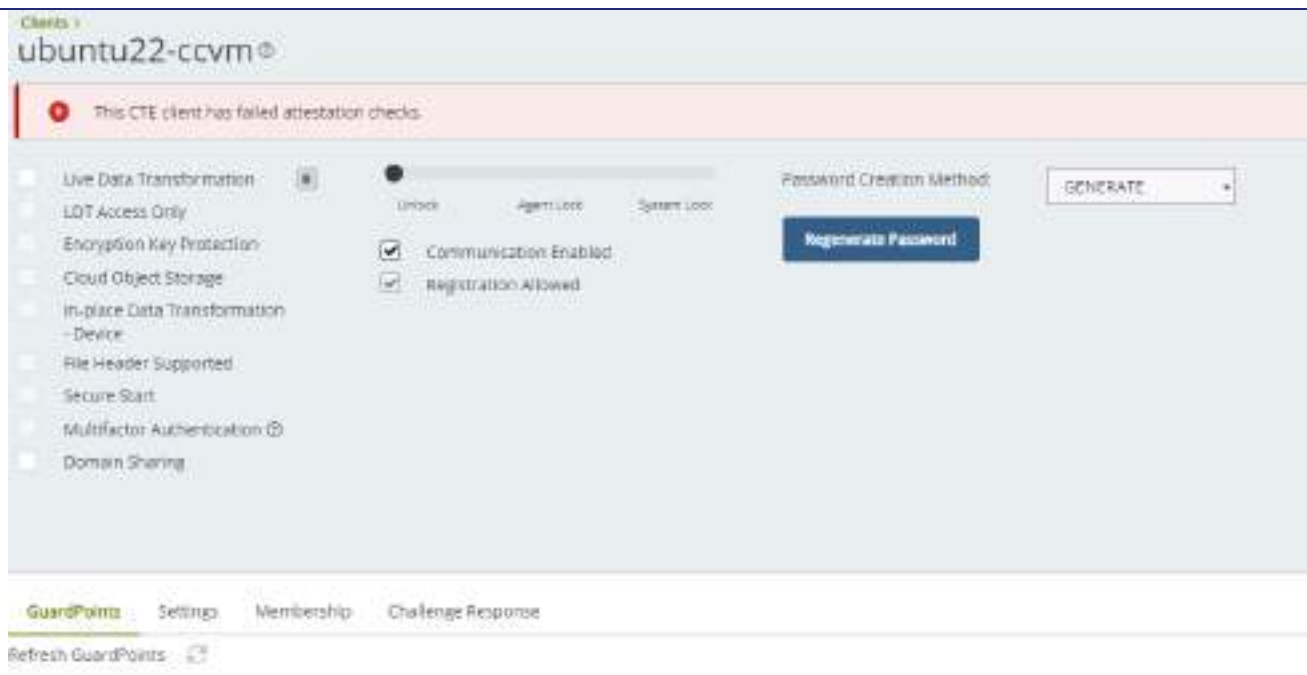
Result if validation succeeds

```
This system is capable of confidential computing.
```

Result if validation fails

```
This system is not capable of confidential computing
```

In the UI, CipherTrust Manager displays the term **warning** in the status column and displays a banner message indicating that the Agent failed attestation.



2. If using a policy with an MRTD value, validate that the MRTD value in the policy and on the Agent are the same, type:

```
sudo tpm2_nvread --offset=560 --size=48 -C o 0x01400001 | xxd -p | tr -d '\n' | awk '{print}'
```

It should be the same value as the MRTD value on this file:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/attestation.txt
```

Note

Attestations fail when the TCB status becomes out-of-date. Following is an example from the attestation report:

```
"attester_tcb_status": "OutOfDate"
```

Attestations will continue to fail until Azure rolls out a new paravisor with the updated TCB on the VM (This would also mean new measurements, such as the MRTD values, that you will need to update in the attestation policy).

To temporarily workaround this out-of-date TCB issue, remove the following line from the attestation policy:

```
input.attester_tcb_status = "UpToDate"
```

Confidential Computing Policies

There are no special CTE policies for Confidential Computing. Create standard and LDT policies as usual.

Confidential Computing GuardPoints

There are no special GuardPoints for Confidential Computing. Create GuardPoints as usual.



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

CTE Agent Live Data Transformation	6
Introduction to LDT	6
Overview of LDT	6
Versioned Keys in LDT	8
LDT Policies	8
LDT Runtime Flow	9
LDT Administrator Roles	11
Resiliency	11
Getting Started	12
Using LDT	12
Backup/Restore	13
Restrictions	13
Installing LDT	15
System Requirements	16
Installing the LDT License	19
Installing and Registering the CTE Agent Software on Linux	19
Installing and Registering the CTE Agent Software on Windows	24
Setting the Linux Kernel Time Zone	28
Enabling LDT on a Protected Host	29
Using LDT	29
Creating and Viewing Versioned Keys	30
Creating LDT Policies or converting a Standard Policy to an LDT Policy	33
Quality of Service	44
How to Set QoS	46
QoS Best Practices	49
General Best Practices for QoS	49
Select and Set Rekey I/O Rate	52
Creating an LDT GuardPoint	54
Rotating Encryption Keys (Rekey)	58
Manual Key Rotation	58
Creating a Key Rotation Schedule	59
Checking the Rekey Status	62
Obtaining Information About Keys Applied to Files	63
Showing GuardPoints During Rekey (Linux)	64
Suspending and Resuming Rekey and/or Scan Phase	64
Automatic Suspend and Resume of LDT Operations Due to Insufficient Disk Space	65
Rotating Encryption Keys While a Rekey is in Progress (Relaunch)	65
File System Operations	67
Renaming Files and Directories	67
Renaming Directories on Linux	68
Caveats	69
Example	69

Considerations	70
Deleting a File	71
File Handling (Windows Only)	71
Enabling GuardPoints in Read-Only mounted file systems (Linux)	72
Copying Files Into a GuardPoint	72
Behavior of Hard Links Inside and Outside of GuardPoints (Windows)	73
Excluding Files or Directories from Rekey	73
About the Exclusion Attribute for Files Matching an Exclusion Key Rule	73
Requirements for Exclusion Key Rules	75
Usage Notes and Limitations for Configuring Exclusion Key Rules	75
Examples of Exclusion Key Rules	79
Listing All Files Included in an Exclusion Key Rule (Linux)	81
Listing All Files Included in an Exclusion Key Rule (Windows)	81
Dynamic Resource Sets	82
Using LDT with SAP HANA Fibre Channel Systems (Linux Only)	92
LDT Administration	92
LDT Metadata in Extended Attributes	92
Listing Extended Attributes	93
MDS File (Linux)	96
Planning for LDT Attribute Storage	97
Using voradmin To Estimate Disk Space Required for LDT	98
Displaying Metadata	99
Verifying Metadata (Windows only)	99
DFS(R) and Replication (Windows)	99
Backing Up and Restoring LDT GuardPoints	100
Clear Text Backup and Restore	100
Encrypted Backup and Restore	101
LDT Policy for Encrypted Backup and Restore	102
Backup/Restore of Metadata Store File in GuardPoints Undergoing Rekey	103
Restore an Encrypted Backup	105
Restoring Non-LDT Backup Data to an LDT GuardPoint	107
Using fsfreeze (Linux only)	108
LDT Backups Using a File System or Storage-Level Snapshot Tool	108
Windows Backup and Snapshots	110
LDT Backup and Restore Troubleshooting	111
LDT Command-Line Administration: voradmin command	111
Migrating a GuardPoint to a Different LDT Policy	113
Removing LDT and Security Encryption	114
Migrating a GuardPoint Out of LDT	115
Deleting LDT Metadata (Linux)	119
Deleting LDT Metadata (Windows)	120
Removing LDT from a Host	121
Uninstalling the Agent while LDT is Rekeying GuardPoints	121
Detecting Loss of NAS connection to an LDT GuardPoint Group	122
Using LDT with CIFS/NFS shares	126

Introduction to LDT over CIFS	127
LDT over CIFS/NFS High-Level Overview	127
LDT Communication Groups and LDT GuardPoint Groups	128
Designation of Primary role and Primary Set in an LDT GuardPoint Group	134
Responsibilities of the Primary host.	139
Failover for the LDT Communication Group Master and the LDT GuardPoint Group	141
LDT GuardPoint Group Commands	148
Sharing LDT NFS/CIFS GuardPoints between Linux and Windows	150
Limitations	151
Prerequisites	154
Supported Versions	154
Administering LDT over CIFS/NFS with CipherTrust Manager	155
Adding a CIFS Connector for CipherTrust Manager	155
LDT AccessOnly nodes	157
CTE Windows Deployment for LDT AccessOnly nodes	157
Configuring LDT for CIFS shares Mapped to Multiple IP addresses	161
Policy and GuardPoint Management	163
Creating a GuardPoint on a CIFS Share Drive on CipherTrust Manager	166
Pausing and Resuming LDT per host and per GuardPoint	168
Migrating GuardPoints over NFS from or to an LDT Policy	169
Multiple GuardPoint Pathnames	170
Key Rotation Commitment	171
LDT Metadata Management Over NFS/CIFS Shares	171
Backup and Restore LDT on NFS GuardPoints	173
Upgrading CTE agent in an LDT Communication Group	173
Upgrading the LDT Agents in an LDT Communication Group from 7.2.0 to 7.3.0	175
New Terminology	176
Upgrading CTE agents in an LDT Communication Group from 7.4.0 to 7.5.0 and post 7.5.0	180
Quality of Service for LDT CIFS/NFS GuardPoints	181
Alerts	182
Troubleshooting LDT CIFS	185
Troubleshooting LDT	185
Monitoring and Statistics	186
Obtaining Statistics with GuardPoint Status	186
Obtaining LDT Statistics at the Command Line	186
Obtaining a Rekey Report	187
Monitoring Ongoing LDT Operations at the Command Line (Windows only)	188
Protecting LDT GuardPoints against Failure in Underlying File Systems (Linux)	188
Recovery Alerts	189
Alerts Playbook	190
Failure to Enable GuardPoints	190
Failure to Suspend or Resume LDT Operation	193
Insufficient Resources	193
Failed to Update LDT Attribute	194
Rekey Stopped	195

Incomplete Key Rotation	195
Skipped Key Rotation	196
Failed to Update LDT Metadata During Scan Phase.	196
File system inconsistencies after system crash.	197
Error Messages	197
Warning and Info Messages	200
Recommendations and Considerations	203
All Platform Recommendations and Considerations	203
Windows Recommendations and Considerations	205
Troubleshooting LDT Encryption Failures	206

CTE Agent Live Data Transformation

- Introduction to LDT
- Getting Started
- Installing LDT
- Using LDT
- LDT Administration
- Using LDT with CIFS/NFS shares
- Troubleshooting LDT

Note

File Name Change

The metadata storage (MDS) file name has changed from `::vorm_mds: :_` to `__vorm_mds__`. GuardPoints will automatically rename the MDS file when guarding with a CTE 7.6.0 agent. LDT NFS GuardPoints will rename once all of the hosts, with the same share guarded, have been upgraded.

Introduction to LDT

This section contains the following topics:

- Overview of LDT
- Versioned Keys in LDT
- LDT Policies
- LDT Runtime Flow
- LDT Administrator Roles
- Resiliency

Overview of LDT

CipherTrust Transparent Encryption - Live Data Transformation (LDT) is an optional, separately licensed feature of CipherTrust Transparent Encryption (CTE). With LDT, after enabling a GuardPoint, a Administrator can encrypt, or rekey, GuardPoint data without blocking user or application access to the data. In LDT, *rekey* means decrypting data with the current cryptographic key and then encrypting it with a new cryptographic key. The concept of rekey,

and how LDT rekeys data, is described in this document.

After enabling GuardPoints, LDT performs *initial* encryption or rekeying in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block application and user access to data during encryption or rekey operations, which can seriously inconvenience users and affect operational efficiency.

With LDT, the Administrator can create a single LDT policy for both initial encryption and subsequent rekeying. The same policy applies to production access and security rules without restricting user or application access to data. Applications have continuity of access to GuardPoint data during LDT.

Warning

To prevent data loss or corruption, you must stop all applications and users that are accessing files inside a GuardPoint before enabling a Live Data Transformation encryption policy for that GuardPoint. Terminating the applications closes all files that are currently being accessed inside the GuardPoint.

Unlike non-Live Data Transformation policies, however, you do not need to keep the GuardPoint offline while data transformation takes place. Instead, you can restart all applications as soon as the GuardPoint has been applied to the host, and CTE will perform the data encryption in the background. This is the only application service downtime required when using LDT.

Note

While LDT is supported on platforms with SELinux enabled in enforcing mode, you may run into interoperability issues with certain SELinux policies that may be enforcing rules against CTE access. If you experience issues running CTE with SELinux enabled, contact your system administrator for assistance. Thales Technical Support will recommend that you disable or change the mode to permissive mode to rule out SELinux when investigating reported issues.

Use Cases

This section provides a summary of typical uses for LDT. The concepts mentioned in this section are described in more detail throughout the rest of this guide.

1. Encrypt unprotected data.

When protecting files in a directory, you must encrypt them. This process is called *initial* data encryption.

2. Convert non-LDT GuardPoints to LDT GuardPoints.

Use when you have existing GuardPoints that are protected with policies created before you started using LDT.\

3. Rekey process.

Changing the key from one version to another version of the same key provides more security. Using LDT, you can change the encryption keys to more secure keys.

-
4. Transform the encrypted data to clear data.

Versioned Keys in LDT

LDT uses *versioned* keys. Each version of a particular versioned key has the same key name and encryption algorithm, but its own unique cryptographic material. That means that data encrypted with version 3 of a key named **LDT-Key** *cannot* be decrypted by any other version of **LDT-Key**, even though the key name remains the same.

Versioning allows you to add one key to your LDT encryption policy and then use different versions of that same key to periodically re-encrypt your data over time. LDT uses the new key material to transform data to the new key version, as part of the same Live Data Transformation policy that also protects the data. The process of re-encrypting data with a new version of the existing key is called *Key Rotation*.

In CipherTrust Manager, you can create a versioned key and then add that key to one or more Live Data Transformation policies. When you use CipherTrust Manager to create a new version of the key, CipherTrust Manager automatically pushes the new key version to any CTE clients associated with the Live Data Transformation policies that contain the key. As soon as the CTE Agent receives the new key, it begins transforming the data to the new key version in the background.

You can also create a Key Rotation Schedule in CipherTrust Manager that automatically rotates your keys periodically. When the scheduled rekey date is reached, CipherTrust Manager automatically creates a new key version and pushes it to any CTE clients that are associated with any policies that include the key. When CTE receives the new key version, it automatically starts the rekey process on the affected LDT GuardPoints.

Rekey | Key Rotation

In LDT, *rekeying* or *key rotation* means decrypting the data with a previous version of the key and re-encrypting it with a new version of the key. LDT allows users and applications to access data while LDT is rekeying the data. Rotating the key and re-encrypting the GuardPoint data with the new version of the key helps to maintain a high level of data security.

Most often, the rekey happens automatically based the Key Schedule defined in CipherTrust Manager, but you can also generate a new version of the key whenever you want to rekey the GuardPoints associated with that key.

LDT Policies

In LDT, you define a single policy for initial data encryption and subsequent rekeying. The policy specifies:

- **Current key**
Associated with data that you want to protect using LDT. This is either a non-versioned key from an earlier policy, or `clear_key`, which means that the data is not currently encrypted.
- **Transformation key**
The versioned key that LDT applies to transform the data from the key used for initial data transformation. When the transformation key rotates, it transforms the data from a previous version of the transformation key to a new version.

Note

Transformation key and versioned key are used interchangeably throughout this document.

As soon as LDT applies the policy to a GuardPoint and enables protection for it, LDT triggers an initial transformation from the current key to the transformation key.

When the transformation key expires, it generates the next version of the versioned key with new cryptographic material. The CipherTrust Manager then pushes the policy to the hosts. The policy now contains the new version of the key. This initiates a rekey process on the GuardPoint to transform data to the new version of the transformation key specified in the policy.

Users and applications can continue accessing data without any interruption during initial encryption and subsequent key transformations.

Note

During LDT policy creation, you must use the Apply Key effect in your policy. If you do not, then end users can see the clear text data until the file is transformed.

LDT Runtime Flow

This section presents an overview of how LDT works and what to expect when LDT is enabled and running in your environment. All of the tasks mentioned here are described in more detail later in this chapter.

First, the administrator completes LDT setup:

1. Upload the LDT license on the CipherTrust Manager.
2. Register LDT hosts with the CipherTrust Manager and be sure that the hosts are licensed for LDT.
3. Create one or more versioned keys.
4. Optionally create a Key Rotation Schedule or add your new keys to an existing schedule.
5. Define Live Data Transformation policies which use the versioned key(s) and contain rules governing LDT operations.
6. Optionally provide Quality of Service (QoS) settings for the LDT hosts. The QoS settings control the:
 - Window of time in which LDT operations are allowed to run.
 - Percentage of CPU resources that LDT can use, or the amount of data to transform according to the QoS setting per the Administrator.

Note

Configuring the QoS settings is highly recommended as a best practice.

When these items are set up, LDT is ready to transform and encrypt data by applying policies to GuardPoints for live initial transformation and subsequent rekeys, as well as enforcement of security rules.

LDT goes through the following phases after the keys and Live Data Transformation policies are defined:

1. Initial data transformation starts

LDT begins when an Live Data Transformation policy is first applied to a GuardPoint or an LDT key is automatically rotated through a key rotation schedule in CipherTrust Manager. When a client that uses the associated policy contacts CipherTrust Manager, CipherTrust Manager sends the new policy, or the the key rotation notification, to the client. (If the same versioned key is used in multiple policies, *all* of the clients associated with the policies that contain the key are notified when the key changes.)

2. New key version triggers a rekey on the affected GuardPoints

On each host/client , CTE determines which GuardPoints are using the key that has just rotated to a new version. CTE starts an LDT rekey on each of those GuardPoints.

On Windows, you must wait for the current key rotation process to finish before you can launch another rekey request. On Linux, if another rekey is already underway on that GuardPoint, the new rekey is queued for later execution. For details, see [Rotating Encryption Keys While a Rekey is in Progress \(Relaunch\)](#).

3. Scan for files

On each GuardPoint where CTE has started a rekey, LDT determines which files to transform. LDT takes inventory of files encrypted with earlier versions of the rotated key and makes a persistent list of the files for transformation.

The scan phase might be interrupted, such as by a host reboot. In this case, when the host reboots and the GuardPoint is enabled again, the scan operation starts over from the beginning.

4. Rekey/Key Rotation

- a. Each file, from the persistent list of files, is decrypted using the old version of the key. The old key is applied to each file and then re-encrypted using the new version of the key. Note that new files created during the LDT process do not need to be rekeyed, as they inherit the new version of the key. Multiple files and multiple regions of files are rekeyed simultaneously.
- b. The LDT extended attribute of each file is updated. (For more about extended attributes, see [LDT Metadata in Extended Attributes](#).)
- c. You can suspend and resume the LDT rekey operation manually, or through the QoS schedule. This manages the impact LDT has on other applications and processes.

If system errors occur during rekeying, such as IO errors or crashes, LDT can manage and recover from them after the system error is fixed.

5. Finish

When all of the required files in the GuardPoint have been rekeyed, the system and storage resources used by LDT are released, except for the storage required for the extended attributes.

LDT creates a rekey report, listing all of the files that were rekeyed. For more information, see [Obtaining a Rekey Report](#).

Upon completion of rekey, the Rekey Status in the GuardPoint Status window of the CipherTrust Manager Console shows Rekeyed.

LDT Administrator Roles

Using LDT requires coordination and collaboration between several different administrators. Security, system, application performance and backup schedules are critical factors that affect planning. It is very important for the **CipherTrust Manager Administrator** to coordinate with the **system administrator** and the **backup administrators**. The following table describes the roles and responsibilities for these administrators.

LDT Administrators

Role	Responsibility	Actions
CipherTrust Manager Administrator	Administers CipherTrust Manager	Coordinates with system and backup administrators. Creates security policies, key rotation schedules, and rules for LDT. Defines Quality of Service settings for LDT, applications, and backups.
System administrator	Administers servers on which CipherTrust Transparent Encryption (CTE) is deployed	Coordinates with the CipherTrust Manager Administrator to create Quality of Service schedule, taking into consideration the backup schedules.
Backup administrator	Manages data backups for data encrypted by CTE	Coordinates with the CipherTrust Manager Administrator to create Quality of Service schedule, taking into consideration the backup schedules.

Resiliency

CipherTrust Transparent Encryption - Live Data Transformation is resilient to many user actions and system occurrences. Since it is designed to run periodically without intervention, it includes various features to provide this resilience.

Before LDT enables a GuardPoint, it checks for any inconsistencies in files that were undergoing rekey at the time when system operations were interrupted. If it finds any inconsistencies, LDT corrects them before it enables the GuardPoint. It should only take a few seconds to identify and correct any inconsistency. On Windows, this process

is delayed until applications access the affected files.

During rekey, if an issue such as an I/O problem or system crash occurs, the resiliency features of LDT ensures the consistency of user data. Such issues can cause an interruption in the middle of a rekey operation. When system operations resume, LDT corrects the problems and then resumes rekeying.

Getting Started

This section contains the following topics:

- [Using LDT](#)
- [Backup/Restore](#)
- [Restrictions](#)

Using LDT

Note

- If you are new to CTE and LDT, read the CipherTrust Manager documentation first to familiarize yourself with the concepts of GuardPoints and Policies.
- Before installing LDT, see the [Linux Kernel Support](#) to verify that your version of Linux is supported.

The following list contains the steps for successfully setting up and using LDT.

1. Install the LDT License on the CipherTrust Manager.

CipherTrust Transparent Encryption - Live Data Transformation is a separately-licensed feature of CTE. Before you can use it, you have to install the license to activate it. LDT is licensed for a specific number of hosts.

For details about licensing, see the CipherTrust Manager documentation.

2. Install the CTE Agent and select the LDT feature during the install. For more information, see [Installing and Registering the CTE Agent Software on Linux](#) or [Installing and Registering the CTE Agent Software on Windows](#).

If the client is already registered with CipherTrust Manager, you can enable LDT on the client through the CipherTrust Manager Console. For more information, see [Enabling LDT on a Protected Host](#).

3. Create Versioned Keys.

LDT uses *versioned keys*. A versioned key rotates to the next version of the key generating new key material automatically without policy change. LDT encrypts data with keys that use encryption standards like AES-256.

This allows data to be re-encrypted without users having to edit the policy.

For more information, see [Keys in LDT \(Versioned Keys\)](#) and [Creating and Viewing Versioned Keys](#).

4. Optionally create a Key Rotation Schedule that will automatically rotate the versioned keys periodically. For more information, see [Creating a Key Rotation Schedule](#).

5. Create LDT Policies.

LDT uses a single Live Data Transformation policy to address both initial encryption and subsequent rekeying. The same policy applies to production access and security rules without restricting user or application access to data. Applications have continuity of access to GuardPoint data during LDT.

For more information, see [Creating LDT Policies](#).

6. Set QoS Settings.

QoS enables administrators to manage and control LDT impact to application workloads by monitoring and controlling the use of host system resources, such as memory or I/O utilization, during CipherTrust Transparent Encryption - Live Data Transformation. Administrators can also choose schedules for data transformation, or manually pause or resume transformation operations.

For more information, see [Quality of Service](#).

7. Create GuardPoints and apply LDT policies to the GuardPoints.

A GuardPoint is a directory in the file system hierarchy, where its contents have a CipherTrust data protection policy applied to it. The CTE Agent intercepts any attempt to access anything in the GuardPoint and uses the policies obtained from the CipherTrust Manager to grant or deny the access attempt. Typically data copied into a GuardPoint is encrypted, and only authorized users can decrypt and use that GuardPoint data.

For more information, see [Creating an LDT GuardPoint](#).

Backup/Restore

Before you enable a GuardPoint with an LDT Policy, make sure that you back up your data.

For more information, see [Backup Requirements](#) and [Backing Up and Restoring LDT GuardPoints](#).

Restrictions

Remember the following restrictions when using LDT:

- LDT does not support nested GuardPoints, where a GuardPoint is contained inside another GuardPoint.
- LDT does not support nested mount points. (Nested mount points refer to filesystems mounted under another mount point). In this case, the GuardPoint is applied only at the top level.

```
/dev/mapper/testvg2-lv1 on /opt/communities type ext4 (rw,realtime)
/dev/mapper/testvg2-lv2 on /opt/communities/zookeeper-communities type ext4 (r
w,realtime)
/dev/mapper/testvg2-lv5 on /opt/communities/zookeeper-communities/data-logs typ
e ext4 (rw,realtime)
```

- For HA clusters, LDT only supports the Asymmetric (active/passive) configuration. LDT does not support Symmetric (active/active) configuration.
- If you want to create LDT GuardPoints on Linux NFS shares or Windows CIFS shares, you must register the host with CipherTrust Manager and add the host to an LDT communication group.
- LDT does not support Auto Raw or Block Device GuardPoints.

Windows Only Limitations

LDT supports GuardPoints on CIFS network shared directories with the following restrictions:

- If any files are opened exclusively by another application, LDT cannot rekey those files until the other applications have released the lock.
- If a backup is taken at the snapshot level, CTE metadata is also backed up. If a restore operation tries to restore CTE metadata, CTE agent does not allow this operation and the metadata restore fails. Do not restore the CTE metadata, or ignore the error from the restore utility, if the CTE metadata restore fails.
- LDT on a ReFS file system runs slowly because of limited support from the Extended Attributes on the ReFS file system.

Note

Customers running older versions of ReFS.sys on Windows Server 2012 R2 should be aware of the memory growth issue encountered by the Thales engineering team. This issue seems to occur only when LDT is running on a large number of files. As the system memory consumption by REFS file system increases, it can eventually make the system unresponsive. This issue does not occur with the recent versions of ReFS file system drivers available on Windows Server 2016. After consulting with Microsoft, they suggest that all customers migrate to Windows Server 2016 if they are using ReFS file.

Protecting local directories and CIFS shares Simultaneously with LDT policies/dev/mapper/testvg2-lv1 on /opt/communities type ext4 (rw,relatime)

```
/dev/mapper/testvg2-lv2 on /opt/communities/zookeeper-communities type ext4 (rw,relatime) /dev/mapper/
testvg2-lv5 on /opt/communities/zookeeper-communities/data-logs type ext4 (rw,relatime)
```

1. Ensure that CTE Windows is running with the **VMLFS** driver.
2. To check the currently installed drivers, type:

```
fltmc
```

3. If the output table contains `vmlfs`, the driver is set properly. If not, type the following, in an administrative command prompt, to switch to the `VMLFS` driver:

```
voradmin config enable vmlfs
```

Note

- The above command requires all directories to be unguarded before switching the driver
- The system requires a reboot after the driver has been changed

Linux Only Limitations

- LDT does not support Linux auto-mounted file systems.
- LDT support is limited to `ext3`, `ext4`, and `XFS` file systems when `user_xattr` mount option is enabled.
- LDT does not support system hibernation (`pm-hibernate`) on Linux hosts where LDT is in use.
- You cannot use LDT and Docker container on the same host.
- You cannot use LDT and OpenShift container on the same host.
- Mounting an NFS mount point within a standard GuardPoint, or LDT GuardPoint, is not supported.

Installing LDT

This section contains the following topics:

- [System Requirements](#)
- [Installing the LDT License](#)
- [Installing and Registering CTE Agent Software on Linux](#)
- [Installing and Registering CTE Agent Software on Windows](#)
- [Setting the Linux Kernel Time Zone](#)
- [Enabling LDT on a Protected Host](#)

System Requirements

CipherTrust Transparent Encryption - Live Data Transformation (LDT) requires the following environment.

Note

See the latest [Compatibility Matrix for CTE Agent](#) for a list of CTE versions and supported operating systems.

CipherTrust Software Requirements

- CTE Agent version 7.0.0 or higher must be installed on every client that you want to protect.
- The CipherTrust Manager with which these clients are registered must be version 2.0.0 or higher.

LDT License Requirements

- One LDT license is required for *each* protected host.

LDT Client Minimum System Requirements

Product	OS	Required Memory (RAM)	CPU
LDT	All OS	16GB for rekeying up to 4 GuardPoints concurrently.	4
		Additional 4GB for every 4 additional GuardPoints rekeying concurrently.	

Calculating Additional Disk Space Requirements

LDT requires a specific amount of disk space in the file system or NFS/CIFS share for each GuardPoint, over and above the space required for the guarded files themselves. LDT uses the additional space to store LDT metadata.

The typical minimum space requirement for a GuardPoint is the number of files in the GuardPoint multiplied by 4K, plus 256MB. To estimate the amount of free file system disk space required for a GuardPoint, type:

```
voradmin ldt space <guardpoint-name>
```

Backup Requirements

- For **Windows**, GuardPoints in local file systems or CIFS shares, the application can use Volume Shadow Copy service (VSS) or robocopy for backup and restore.

- For **Linux**, GuardPoints in local file systems, the backup application must have the capability to back up user-extended attributes. For example, Thales tested LDT with NetBackup. You can also use other applications that can back up user-extended attributes.

Backup Requirements for Linux GuardPoint backup on NFS

- You can only perform a backup or restore on the NFS client designated as the primary client for the GuardPoint. Use backup clients or tools such as tar, rsync, etc. on this client. You can backup or restore individual files, or subdirectories, within a GuardPoint namespace without an Apply Key Effect. However, this excludes MDS files and all LDT private files under `vorm_ldtprivspace`.
- Performing a backup or restore on a non-primary client is not supported and may lead to data and/or LDT metadata inconsistencies, in target files, in the backup image or in the restored files. Attempts to restore files on a non-primary client will be detected and rejected. Refer to section [Encrypted Backup and Restore](#) for additional information.
- File backup/restore can only be executed when the GuardPoint is rekeyed, or in a subsequent rekeying suspended state. File backup should **not** be executed during initial rekeying state.
- For **Linux**, GuardPoints on NFS shares, the normal procedure is to back up the NAS server that serves the NFS clients rather than backing up the individual NFS clients. Because backups on NAS servers are remote from a CTE perspective, it is extremely important that CTE is *not* performing any data transformation in any GuardPoint while the NAS server is being backed up. This includes both initial data transformation and automatic or manual data rekey.

Warning

Make sure that all live data transformation has completed on all NFS GuardPoints before you back up the NAS servers associated with the NFS shares on which those GuardPoints reside. You must also make sure that no automatic rekey tasks will start while the NAS backup is in progress.

Linux-Specific Requirements

- To use LDT on an ext3 or ext4 file system, the block size **must** be 4K. Run `dumpe2fs` to determine the block size of the ext3 or ext4 file systems before using LDT. This limitation does not apply to XFS file systems or NFS shares. You can use LDT on XFS with a block size of 1K or 2K.

Local File System Requirements

- For LDT to work properly on local file systems, the underlying file system must support and enable user-extended attributes. All of the file systems supported by LDT support these attributes. If you are using LDT with ext3 or ext4 mount points, you must explicitly enable the extended attribute mount option by editing `/etc/fstab` and adding the `user_xattr` mount option. In the other file systems supported by LDT, user extended attributes are enabled by default, so you do not have to explicitly enable them.

Example `/etc/fstab` entry for ext3 on Red Hat or SLES:

```
/dev/sdb1 /disk2 ext3 defaults,user_xattr 0 0
```

Example `/etc/fstab` entry for ext4 on Red Hat or SLES 12 (ext4 is not supported on SLES 11):

```
/dev/sdc1 /disk3 ext4 auto,users,user_xattr,exec 0 0
```

For more information about extended attributes, see [LDT Metadata in Extended Attributes](#).

NFS Share Requirements

- For GuardPoints on NFS shares, LDT embeds file specific LDT metadata in the beginning of each file during the initial data transformation phase. The size of each file becomes larger by 4096 bytes to accommodate this required metadata. Both the metadata and the file size increase are hidden from users and applications as long as the GuardPoint remains enabled.
- If a GuardPoint is disabled, the metadata remains in each file and both the metadata and the file size increase become visible to users and applications.

Note

Thales highly recommends that NFS shared directory be mounted with `sync` option.

Supported Applications in Linux

- For all of the supported operating systems for database applications, see the [Compatibility Matrix for CTE Agent](#).

Replication

- `rsync`
- Hardware/software based replication system

SAP HANA Fibre Channel Systems

- SAP HANA is compatible with LDT. See the [Compatibility Matrix for CTE Agent](#).

Windows-Specific Requirements

CIFS Share Requirements

- For GuardPoints on CIFS shares, LDT embeds file specific LDT metadata in beginning of each file during the

initial data transformation phase. This metadata remains hidden to users and other applications as long as the GuardPoint is enabled.

- If a GuardPoint is disabled, the metadata remains in each file and becomes visible to users and other applications.
- The size of each file becomes larger by 4096 bytes to accommodate the required LDT metadata.

Installing the LDT License

LDT installs with the CTE Agent software, but it is a separately-licensed CTE feature. Before you can use it, you have to install the license on the CipherTrust Manager to activate LDT on any CTE clients. LDT is licensed for a specific number of clients.

1. Obtain an LDT license from Thales. You can purchase LDT along with the CipherTrust Manager software or you can add LDT later.
2. Install the license on the CipherTrust Manager.

For details, see the CipherTrust Manager documentation.

To confirm that the LDT license is in effect:

1. In the CipherTrust Manager Applications Page, open the **Admin Settings** application.
2. Click **Licensing** in the left-hand menu bar.
3. Expand the entry for **CTE - Live Data Transformation** in the License table. CipherTrust Manager shows the total number of client licenses in the **Total Clients** field and the total number of licenses used in the **Used Clients** field.

Installing and Registering the CTE Agent Software on Linux

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

Prerequisites

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.
- CipherTrust Manager must contain an LDT Communication Group if you will use LDT to guard data over CIFS/NFS shares using LDT policies. See [Managing LDT Communication Groups](#) for more information.

Minimum Hardware Requirements for CTE

The following requirements are the minimum for CTE. When you add LDT, or third-party applications, you need to add more storage and RAM. Refer to the [LDT guide](#) for LDT requirements and the third-party software for their requirements.

Component	CPU	CPU Cores	RAM	Storage (Free Space)
CTE-Windows	Intel/AMD x64 with AES-NI support	4 cores	8 GB	1GB
CTE-Linux	Intel/AMD x64 with AES-NI support	4 cores	8 GB	1GB
CTE-AIX	IBM PowerPC8 or higher	4 cores	8 GB	1GB

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note

- If possible, Thales recommends that you use the default directory `/opt/vormetric`.
- Custom directories are **only available** for RHEL and SLES.
- Custom directories are **not available** for COS (Cloud Object Storage).

To view all installer options, use the `-h` parameter. For example:

```
./vee-fs-7.8.0.88-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type **Y** and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

Welcome to the CipherTrust Transparent Encryption File System Agent Registration Program.

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>
```

```
In order to register with a CipherTrust Manager you need a valid registration token from the CM.
```

```
Do you want to continue with agent registration?(Y/N) [Y]:
```

5. Type **N** and press Enter to end the installation procedure without registering the CTE Agent with a key manager.
6. Enter **Y** to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE. For example:

CTE for CipherTrust Manager

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Please enter the primary key manager host name: 10.3.200.141
```

```
You entered the host name 10.3.200.141
```

```
Is this host name correct? (Y/N) [Y]: Y
```

CTE for CDSPaaS

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
```

```
Enter the primary key manager host name of the service:
```

```
You entered the host name us1.ciphertrust.dpondemand.io
```

```
Is this host name correct? (Y/N) [Y]: Y
```

Host names:

- **Europe:** `ciphertrust.dpondemand.io`
- **North America:** `us1.ciphertrust.dpondemand.io`

Note

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: `<hostName>:<port#>`. For example, `10.3.200.141:8445`.

7. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the following list.
```

```
[1] sys31186.qa.com
```

```
[2] 10.3.31.186
```

```
Enter a number, or type a different host name or IP address in manually:
```

```
What is the name of this machine? [1]: 2
```

```
You selected "10.3.31.186".
```

8. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
```

```
Please enter the profile name for this host: My-Profile
```

```
Please enter the host group name for this host, if any:
```

```
Please enter a description for this host: RHEL7 system West Coast Datacenter
```

```
Token : 12345
```

```
Profile name : My-Profile
```

```
Host Group : (none)
```

```
Host description : RHEL7 system West Coast Datacenter
```

```
Are the above values correct? (Y/N) [Y]: Y
```

9. At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloning. The default is Y (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This

can be rectified by running this registration program again. Do you want to enable this functionality? (Y/N) [Y]:
Y

10. Type Y to support Filesystem encryption and to choose other features. Type N if you only want to support Ransomware Protection. If you type N, then LDT and COS are not supported.

```
Do you want this host to have Filesystem encryption support enabled on the server? (Y/N) [Y]:
```

11. At the LDT prompt, specify that you want this client to use CTE-LDT by typing Y and pressing Enter:

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]: Y
```

12. If you are planning to create GuardPoints on NFS shares, enter the name of the LDT Communication Group that this node will join.

```
Enter the LDT Communication Group name: LCG1
```

Warning

The registration token, profile name, client group name and LDT Communication Group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

13. The installation checks for Confidential Computing adapter types. If it finds one, it states:

```
The following confidential computing adapter types have been identified.
1. Intel Trust Domain Extensions (tdx)
Do you want this host to have confidential computing enabled? (Y/N) [N]:
```

Type Y to enable Confidential Computing.

14. At the Cloud Object Storage (COS) prompt, specify whether you want this client to use CTE COS.

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

15. Specify if you want to enable Ransomware Protection.

```
Do you want this host to have Ransomware Protection support enabled on the server?
```

```
ver? (Y/N) [N]:
```

16. CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.
Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption CTE Agent with
the CipherTrust Manager on 10.3.200.141.

Installation success.
```

17. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Installing and Registering the CTE Agent Software on Windows

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

Prerequisites

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.
- CipherTrust Manager must contain an LDT Communication Group if you will use LDT to guard data over CIFS/NFS shares using LDT policies. See [Managing LDT Communication Groups](#) for more information.

Minimum Hardware Requirements for CTE

The following requirements are the minimum for CTE. When you add LDT, or third-party applications, you need to add more storage and RAM. Refer to the [LDT guide](#) for LDT requirements and the third-party software for their requirements.

Component	CPU	CPU Cores	RAM	Storage (Free Space)
CTE-Windows	Intel/AMD x64 with AES-NI support	4 cores	8 GB	1GB
CTE-Linux	Intel/AMD x64 with AES-NI support	4 cores	8 GB	1GB
CTE-AIX	IBM PowerPC8 or higher	4 cores	8 GB	1GB

Installation

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the **License Agreement** page, accept the License Agreement and click **Next**.
6. Click **Next** to accept the default folder. When you are done, click **Next**.

Note

- Thales recommends that you install CTE in the default installation directory, `C:\Program Files\Vormetric\DataSecurityExpert\agent\`
- You **must** install the CTE Agent on the same drive as Windows. For example, if Windows is installed on the `C:` drive, you must install the CTE Agent on the `C:` drive.

7. On the **Ready to Install** page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
8. On the **InstallShield Wizard Completed** page, make sure the **Register CipherTrust Transparent Encryption now** option is selected and click **Finish**. The installer opens the [Register CipherTrust Transparent Encryption](#) wizard.

Registration

The following procedure describes how to register the CTE Agent after installation is complete.

Use the `register_host` utility to create certificate requests, exchange certificates between the CipherTrust Manager and the host, to enable ransomware detection, and to register CTE on the CipherTrust Manager. After the host is registered, if you selected to enable file system encryption, you can configure CTE, apply GuardPoints,

or perform database backups. If you selected ransomware protection, you can apply the protection to volumes. Run the `register_host` utility in text mode on a terminal window.

Caution

The default host registration timeout is 10 minutes. If the host is unable to reach the CipherTrust Manager within the allotted period because of an extremely slow network connection, set the `REGISTER_HOST_TIMEOUT` environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

1. Log on to the host as a Windows user with administrative privileges.
2. Launch the CTE Registration Wizard using one of the following methods:
 - In the system tray, right click the CipherTrust Lock icon and select **Register Host**.
 - Run `...\register_host.exe -vmd -silent`.
3. Reboot the system. CTE automatically displays the registration wizard if CTE is not already registered.
4. In the Register Host dialog box, verify the host's machine name and click **Next**.

Note

For CipherTrust Data Security Platform Services, the host names of the services are:

- **Europe:** `ciphertrust.dpondemand.io`
- **North America:** `us1.ciphertrust.dpondemand.io`

5. On the **Gathering agent information** page, select one or both of the following options and click **Next**.
 - **File System:** Allows you to protect and encrypt CTE files with policies
 - **Ransomware Protection:** Protects volumes from ransomware
6. On the **Gathering Key Manager information** page, enter the FQDN or IP address of the primary CipherTrust Manager.

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: `<hostName>:<port#>`. For example: `10.3.200.141:8445`

When you are done, click **Next**. CTE communicates with the selected CipherTrust Manager to validate what features have been licensed and are available to the CTE Agent.

-
7. On the **Gathering host information** page:

File System

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see [Hardware Association Feature](#).
- If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the client, select **Enable LDT Feature**. For details on LDT, [CTE Agent Live Data Transformation](#).
- If you want the node to be an [Windows AccessOnly](#) node, select **Enable LDT AccessOnly Feature**.

Ransomware

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see [Hardware Association Feature](#).

When you are done, click **Next**.

8. On the **Gathering registration information** page, enter the following:

File System

- **Registration token**: The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name**: The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.
- **LDT Communication Group**: If you are planning on using LDT over CIFS/NFS on a CipherTrust Manager, enter the name of the LDT Communications Group that this node will join. See [Adding Clients to an LDT Communication Group](#) for more information.

Ransomware

- **Registration token**: The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name**: The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the

CipherTrust Manager associates the default client profile with this client.

- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.

Warning

The registration information is case-sensitive. If any of it is entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

When you are done, click **Register**. CTE contacts the CipherTrust Manager and attempts to register the client with the specified options. The Register Host dialog box displays a message with the results of the registration request.

If the registration completed successfully, click **Finish**.

9. Restart the client to complete the installation process on the client.
10. After the host has rebooted, you can verify the installation by checking CTE processes:
 - a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
 - b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.
 - If you are using CipherTrust Manager version 2.2 or later, you can now use CipherTrust Manager to administer CTE on the client.

If you are using CipherTrust Manager version 2.1 or earlier, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Setting the Linux Kernel Time Zone

The Linux kernel contains an internal time structure that may or may not contain time zone information. On system configurations that do not contain time zone information, LDT stores and displays timestamps for rekey beginning and ending in UTC (Coordinated Universal Time) rather than the system's local time zone. If this occurs, the administrator can set the kernel's internal time zone to the local time zone if they desire timestamps in their local time zone.

To set the Linux Kernel time zone information, at boot time type:

```
hwclock --systz
```

The command sets the kernel's time zone to the local time zone and resets the System Time based on the current time zone.

Note

On systems that do not set the time zone by default, existing timestamps for completed rekeys remain in UTC, even if you run `hwclock --systz`. Only timestamps for new rekeys display the local time zone.

Enabling LDT on a Protected Host

When you install CTE on a host, you can enable LDT during the registration process as described in [Installing and Registering the CTE Agent Software on Linux](#). If you have already registered the host with CipherTrust Manager, you can enable LDT in the client entry in CipherTrust Manager.

Note

- The LDT license is valid for a certain number of clients. Once you reach this limit, you can either purchase additional LDT licenses, or reclaim a license by removing an LDT client. For details, see [Removing LDT and Security Encryption](#).
- You cannot disable LDT on a client once it has been enabled.

To enable LDT on an existing host:

1. In the CipherTrust Manager Applications Page, open the **CTE** application and click **Clients** in the left-hand menu bar.
2. Click on the name of the client on whom you want to enable LDT.
3. On the Client Details page, select the **Live Data Transformation** check box, then click **Apply** to enable LDT on the protected host.

Note

After LDT has been enabled for the host, the check box is greyed out because you cannot change this option once it has been set.

Using LDT

- [Creating and Viewing Versioned Keys](#)

- Creating LDT Policies or converting a Standard Policy to an LDT Policy
- Quality of Service
- Creating an LDT GuardPoint
- Rotating Encryption Keys (Rekey)
- File System Operations
- Excluding Files or Directories from Rekey
- Using LDT with SAP HANA Fibre Channel Systems (Linux Only)

Creating and Viewing Versioned Keys

For LDT, you create a versioned key that you can add to any number of Live Data Transformation policies. When you add a new key version, CipherTrust Manager pushes the new version to every CTE client that is associated with any of the Live Data Transformation policies that contain that key.

Use the **Keys & Access Management** application in the CipherTrust Manager Applications Page when creating or viewing versioned keys.

Caution

Make sure that all keys you create for LDT are Symmetric. LDT does not support asymmetric keys.

Creating a Versioned Key

1. Log into the CipherTrust Manager Console as an administrator.
2. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.

Tip

To navigate to the Products page from anywhere in the CipherTrust Manager Console, click the App Switcher icon in the top left corner.

3. Above the Key table, click **Create a New Key**.
4. Enter a Key Name so that you will be able to find this key easily when you want to rotate it. For example, LDT-Key-1.

Note

- When CipherTrust Manager displays the list of available keys, you cannot filter the list by versioned vs. non-versioned. Therefore, it is especially important to name the key in such a way that you can easily search for it by name.
- Using a standard naming convention will also help if you want to create an automatic key rotation schedule for all your LDT keys.

5. In the **Key Metadata > Groups for Key sharing** section, do the following:

- In the **Search** box, type "cte".
- Add CTE Admins and CTE Clients to the key sharing groups by clicking the green **Add** button. The **Key Shared?** check box is automatically selected and the **Add** button changes to a **Remove** button.
- Below the Groups table, click the **CTE Key Properties** check box.

CipherTrust Manager displays the following options for CTE keys:

- **CTE Versioned:** Specifies that this is a versioned key. Make sure this option is selected.
- **Persistent on Client:** Specifies whether the key is stored in persistent memory on the client.

If this option is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.

If this option is *not* selected, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.

- **Encryption Mode:** Encryption mode of the key. Choose one of the following for LDT keys:
 - CBC
 - CBC-CS1

Encryption using CBC-CS1 keys is known as enhanced encryption. For details, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide*.

Note

XTS encryption is not supported for protecting directory-based GuardPoints. Do not select XTS as your

encryption mode.

Groups for Key sharing

Search: cte

Group Names	Key Shared?	
CTE Admins	✓	Remove
CTE Clients	✓	Remove

2 Groups 10 per page

☐ Set as "Versioned Key" for backwards compatibility

☒ CTE Key Properties

☒ CTE Versioned ☒ Persistent on Client

Encryption Mode: CBC CS1

- In the Key Behaviors section at the bottom of the page, clear the **Prevent this key from being exported** check box. If the key cannot be exported, the key will not appear in the keys list when you add the key rule to the policy.

If want the option to delete this key later on, clear the **Prevent this key from being deleted** check box. Use caution when deleting keys, as any data encrypted with that key will be inaccessible if you delete the encryption key.

Key Behaviors

☒ Prevent this key from being deleted ☐ Prevent this key from being exported

Create Cancel

- Click **Create**. The new key appears in the Keys table.

Viewing Versioned Key Information

- Log into the CipherTrust Manager Console as an administrator.
- Open the **Keys & Access Management** application.

3. Click the **Latest Version Only** check box to show only one entry for each versioned key.
4. Find the key in the Keys table.

Tip

You can filter the list by key name using wildcard searches. For example, if you know that the key name contains "LDT", you can search for `*ldt*`. The search is *not* case sensitive.

If the **Version** for a key is 0, then this is the first version of the key and no key rotation has taken place. If the **Version** is greater than 0, the key has been rotated.

5. To find all versions of a key, click the name of the key in the **Key Name** column. CipherTrust Manager displays the ID, version number, state, and date created information for each version of the key.

Modifying Key Rules

CTE v7.4 (Windows) and CTE v7.6 (Linux), and subsequent versions, allows users to modify the Key Rules while an LDT policy is active and enforced on a client. Users can add new rules and modify the existing rules. The following use case is addressed with this change:

1. Users can prioritize and plan the encryption of large files inside a GuardPoint.
2. User can transform the excluded files by adding new Key Rules.

Warning

While making Key Rule changes, you cannot change the order of the rules, or the encryption key rules applied to the file. If the data encryption keys are mismatched, it may result in data corruption.

Note

Dynamic resource sets for CTE Linux are compatible with CipherTrust Manager v2.14 and subsequent versions.

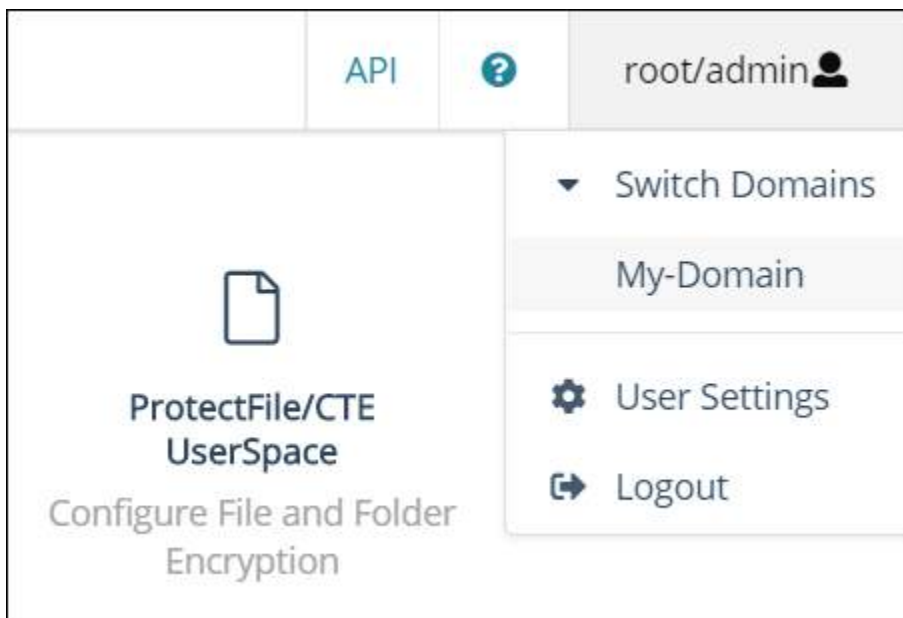
Creating LDT Policies or converting a Standard Policy to an LDT Policy

LDT uses a single Live Data Transformation encryption policy to address both data transformation and ongoing protection. In contrast, if you do not use LDT, you need a separate policy for initial data transformation, or rekey, and another policy to protect the data while it is in production use. For more information about LDT policies, see

LDT Policies.

To create an Live Data Transformation encryption policy:

1. In a web browser, navigate to the URL of the CipherTrust Manager you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to the next step. If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the domain/user name (default: **root/admin**) on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.
 - c. The logged in user now shows the new domain name/user name.



3. In the CipherTrust Manager Applications Page, open the **CTE** application.
4. In the left-hand menu bar on the Clients page, click **Policies**.
5. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
6. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. For example: LDT-Policy-West

Field	Description
Policy Type	Select Live Data Transformation.
Description	A user-defined description to help you identify the policy later. For example: LDT policy for the West Coast Datacenter.
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.

- Click **Next**.
- On the Security Rules page, define the security rules you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of **key_op** and the effects **Permit** and **Apply Key**. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version. This rule is required by LDT, so you cannot edit it, move it, or delete it.

To add additional security rules, click Create Security Rule and enter the requested information. If you want to grant user and application access to files at all times, including during initial LDT and subsequent key rotations, add a security rule with the action **all_ops** and the effects **Permit** and **Audit**.

- On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be

Field	Description
	excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one. Current key is the key applied to data that you want to protect using LDT. This is either a non-versioned key from a standard policy or a clear_key. You must use clear_key when data is not currently encrypted. When migrating a standard policy to LDT, you must enter the encryption key from the key rule of the standard policy, as the current key of LDT policy.
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. Transformation key is the versioned key that LDT applies to transform the data. For the initial transformation, the data is transformed from the Current key, to the Transformation key. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field. When rotating the Transformation key, LDT transforms the data from a previous version of the transformation key to a new version.

Note

LDT now supports dynamic resource sets. This means that you can alter the resource set, and the policy will pick up the changed resource set and apply it. However, make sure that you **do not** mix encryption keys in your edited resource set. This will cause corruption.

When you are done specifying key rules, click **Next**.

- On the Confirmation page, review the information you entered and click **Save** when you are ready to save the policy.

The following example shows a simple LDT policy that encrypts clear-text files using a versioned key named LDT-Key-1. The **key_op** and **all_ops** actions in the Security Rules panel grant user and application access to files at all times, including during initial LDT and subsequent key rotations.

1 General Info

Name: LDT-Policy-West

Policy Type: Live Data Transformation

Description: LDT policy for the West Coast Datacenter

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
▶			key_op	permit,applykey	No
▶			all_ops	permit,audit,applykey	Yes

3 Key Rules

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule
	clear_key	LDT-Key-1_xts	No

Security Rule Ordering for Policies

If you want to enforce restrictions when guarding NFS/CIFS shares using an LDT or standard policy with a **CBC-CS1** key, note the following:

CipherTrust Transparent Encryption embeds the LDT and/or IV (initialization vector) attributes in the first 4K of files for NFS/CIFS shares guarded with an LDT or standard policy with a **CBC-CS1** key. Embedding CipherTrust Transparent Encryption attributes increases the actual file size by 4K. CTE hides that extra 4K when reporting the file size to users, or processes, that access the file with the Apply Key effect.

If you need the actual file size, or read/write access on the embedded header, for backup/restore processes for example, then you need a rule that permits access without Apply Key.

LDT Policies

Example 1: Permits Backup and Restore

A policy that allows backup and restore of encrypted data, clear-text access to certain processes, and denies access to all others:

Order	Resource Set	User Set	Process Set	Action	Effect	Browsing	
▶ 1				key_op	permit,applykey	No	
▶ ☐ 2			backup	all_ops	permit,audit	No	⋮
▶ ☐ 3			authorized processes	all_ops	permit,audit,applykey	No	⋮
▶ ☐ 4				all_ops	deny,audit	Yes	⋮

Rule	Purpose
1	Default LDT rule required for LDT policies.
2	Allows for processes in the backup Process Set to access the real file size and backup the CipherTrust

Rule	Purpose
	Transparent Encryption attributes along with the encrypted file data.
3	Allows for processes in the authorized-processes Process Set to access the clear-text data, but it hides the additional 4K from the CipherTrust Transparent Encryption attribute.
4	Denies all other processes access to the data.

Example 2: Permits access to certain Processes

A policy that only allows certain processes clear-text access but allows all others to see the OS file attributes.

Order	Resource Set	User Set	Process Set	Action	Effect	Browsing	
1				key_op	permit:applykey	No	
2			authorized-processes	all_ops	permit:audit:applykey	Yes	
3				f_md_attr_md_read_r...	permit:audit	Yes	
4				all_ops	deny:audit	Yes	

Rule	Purpose
1	Default LDT rule required for LDT policies.
2	Allows for processes in the authorized-processes Process Set to access the clear-text data.
3	Allows for processes not in the authorized-processes Process Set to read the OS file and directory attributes. Note: Processes that match this rule obtain the file size with the 4K header. If a process that is not in the authorized-processes Process Set needs the file size without the header, then the Apply Key must be present in the Effect or you will need an additional rule granting Apply Key to that specific process. That rule must be defined before this rule.
4	Denies processes not in the authorized-processes Process Set from reading any data from the files.

Standard Policies

Example 1: Permits access to certain Processes

A policy that allows backup and restore of encrypted data, clear-text access to certain processes, and denies access to all others:

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1			backup	all_ops	permit:audit	Yes	
2			authorized-processes	all_ops	permit:audit,applykey	Yes	
3				all_ops	deny:audit	Yes	

Rule	Purpose
1	Allows for processes in the backup Process Set to access the real file size and backup the CipherTrust Transparent Encryption attributes along with the encrypted file data.
2	Allows for processes in the authorized-processes Process Set to access the clear-text data, but it hides the additional 4K from the CipherTrust Transparent Encryption attribute.
3	Denies all other processes access to the data.

Example 2: Permits access to certain Processes

A policy that only allows certain processes clear-text access but allows all others to see the OS file attributes.

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1			authorized-processes	all_ops	permit:audit,applykey	Yes	
2				file_audit_read_secu...	permit:audit	Yes	
3				all_ops	deny:audit	Yes	

Rule	Purpose
1	Allows for processes in the authorized-processes Process Set to access the clear-text data.
2	Allows for processes not in the authorized-processes Process Set to read the OS file and directory attributes. Note: Processes that match this rule obtain the file size with the 4K header. If a process that is not in the authorized-processes Process Set needs the file size without the header, then the Apply Key must be present in the Effect or you will need an additional rule granting Apply Key to that specific process. That rule must be defined before this rule.
3	Denies processes not in the authorized-processes Process Set from reading any data from the files.

For more information, see [Adding Security Rules](#) in the CipherTrust Manager documentation.

Using Auto Mount with LDT Policies

Auto Mount is supported with LDT policies, with CBC/CBS-CS1 keys, on both NFS and local file systems. It is an option provided for guarding a GuardPoint. When selected, it enables automatic guarding of the GuardPoint when accessed, rather than immediately after policy deployment.

Configuring and Guarding an Automount GuardPoint

1. Add this newly created directory as a GuardPoint on CipherTrust Manager using an LDT policy. A GuardPoint configured with a LDT policy using auto mount must use GuardPoint type: **Auto Directory**. The Auto Mount option is not supported with GuardPoint type: manual. When you select GuardPoint type: Auto Directory in a LDT policy, the Auto Mount option displays.

Create GuardPoint



Policy *

VMFS0DT40-AUTOMOUNT-POL

Select

Type *

Auto Directory

Path *

☒ Enter/Browse Path ☐ Upload CSV

/nfs-oxf-fs1/gp

Browse

 To apply the same GuardPoint settings to multiple paths, type paths in the Path field or specify them using the Browse button. A maximum of 200 GuardPaths can be specified.

Auto Mount

☒

Preserve Sparse Region:

☒

Multifactor Authentication:

☐

Cancel

Create

Note

For GuardPoint type: Auto raw, see [File System Mount Points on Linux](#).

2. Once the GuardPoint displays on the agent, mount the device on the GuardPoint. This should trigger guarding.
3. Verify that the GuardPoint has been enabled, that the policy is in effect, and rekey is in progress.

```
voradmin ldt attr get /nfs-oxf-fs1/gp
```

Example

```
LDT stats: version=7, rekey_status=rekeyed
Number of times rekeyed:          1 time
Rekey start time:                 2025/03/27 07:05:19
Last rekey completion time:       2025/03/27 07:05:19
Estimated rekey completion time:  N/A
Policy key version:               21
Pushed Policy key version:        21
Policy ID:
    6a4b49bd-6f34-4646-ae95-8e60e2824ff6
Data stats:
    total=0.0MB, rekeyed=0.0MB
    truncated=0.0MB, sparse=0.0MB
File stats:
    total=0, rekeyed=0, failed=0
    passed=0, skipped=0, created=0, removed=0, excluded=0
```

4. Verify that all files are rekeyed to completion as per policy key rules.

```
voradmin ldt attr get /nfs-oxf-fs1/gp
```

Example

```
LDT stats: version=7, rekey_status=rekeyed
Number of times rekeyed:          2 times
Rekey start time:                 2025/03/27 07:21:52
Last rekey completion time:       2025/03/27 07:22:14
Estimated rekey completion time:  N/A
Policy key version:               22
```



```

Pushed Policy key version:          22
Policy ID:
    6a4b49bd-6f34-4646-ae95-8e60e2824ff6
Data stats:
    total=1.0GB, rekeyed=1024.0MB
    truncated=0.0MB, sparse=0.0MB
File stats:
    total=1, rekeyed=1, failed=0
    passed=0, skipped=0, created=0, removed=0, excluded=0

```

5. Unmount. The unmount should trigger an unguard of the GuardPoint, the way it does for regular auto mount GuardPoints.

Note

Manually unmounting displays a **busy** error. This is the expected behavior, as the unguard operation is in progress. Once unguard completes, the mount point is unmounted automatically.

Example

```
umount /nfs-oxf-fs1/gp
```

Response

```
umount: /nfs-oxf-fs1/gp: target is busy.
```

Behavior of Auto Mount GuardPoints

After you push a policy on a CTE agent, if you check the status, you'll find that the auto mount GuardPoint is not yet guarded because the guard operation is not yet triggered:

```
secfsd -status guard
```

Response

GuardPoint	Policy	Type	ConfigState	Status	Reason
/nfs-oxf-fs1/gp	VMFS0DT40-AUTOMOUNT-POL	auto mount	guarded	not guarded	Not auto-mounted

In the CTE CLI, Auto Mount is controlled by `autofs`. When `autofs` is enabled, accessing the GuardPoint triggers the guard operation.

Example

```
ls /nfs-oxf-fs1/test
secfsd -status guard
```

Response

```
${gp} Policy Type ConfigState Status Reason
-----
/nfs-oxf-fs1/gp VMFS0DT40-AUTOMOUNT-POL auto mount guarded guarded N/A
```

Note

When adding the auto mount GuardPoint, the mount point should be unmounted. If the mount point is mounted with auto mount, then you must manually **unmount** the mount point so that the next time the mount point is accessed, secfsd will guard the GuardPoint.

Running Recovery on Automount GuardPoint with LDT policy

When a system crashes during an active rekey operation, the GuardPoint may enter a state that requires recovery.

```
secfsd -status guard
```

Response

```
GuardPoint      Policy      Type      ConfigState  Status      Reason
-----
/nfs-oxf-fs1/gp VMFS0DT40-AUTOMOUNT-POL automount  unguarded   not guarded  GuardPoint needs LDT recovery
```

The GuardPoint is not guarded, displays the GuardPoint status, and aborts the guard operation, while leaving the mount point mounted. This enables the admin to manually run the `voradmin ldt recover` command.

```
voradmin ldt recover /nfs-oxf-fs1/gp
```

Response

```
Enter YES to disregard failures in LDT recovery as the result of inconsistencies
in underlying file system -> YES
/nfs-oxf-fs1/gp - recovered without failure(s) - status 1
/nfs-oxf-fs1/gp - GuardPoint rkea flags 10032
Unmounted Automount GuardPoint /nfs-oxf-fs1/gp
```

After recovery, the auto mount mount point is unmounted, and the admin is prompted accordingly.

Collecting Agent Information

- Do not use `voradmin ldt list all` with the `-force-mount` option. This could create more issues.
- Change the GuardPoint type from `automount` to `manual` to enable the GuardPoint and collect the Agent information.

Limitations

- CTE does not support nested GuardPoints with auto mount enabled
- Auto mount with LDT policies only supports `auto-fs` mount points.
- The GuardPoint path must be at the same level as the mount point when enabling auto mount on an `autofs` mount point. This ensures that auto mount unguards when the `autofs` mount point times out. If the GuardPoint path is set at any level deeper than the configured `autofs` mount point, the `autofs` mount point will never timeout because the GuardPoint will continue to keep the mount point in a busy state.
- CTE **does not** remove the shadow directory created after unmount.
- CTE **does not** support auto-fs configured using direct mount with an LDT policy.
- CTE **does not** support `systemd automount` with an LDT policy.

Quality of Service

- Purpose of QoS
 - Manage LDT Impact
 - Monitor and Control CPU Usage
 - Monitor and Control Rekey/Scan I/O Rate
- QoS Scheduling During Backup/Restore

LDT runs in real time, while users actively interact with applications. This could impact performance. However, LDT is designed to not adversely affect application or system performance.

Purpose of QoS

Quality of Service (QoS) provides tools for an administrator to minimize the effect of LDT on system and application performance. It provides a set of parameters that administrators can set to control LDT use of system resources, primarily CPU and I/O bandwidth. When the QoS parameters are set appropriately, LDT stays within the defined boundaries to ensure that critical user applications are not adversely affected by LDT operations.

Manage LDT Impact

Administrators can pause or resume LDT operations to manage and control LDT impact to application workload. When data transformation occurs, either during initial or subsequent transformations, it requires substantial host CPU and I/O resources. This can cause contention for resources between the applications simultaneously running on the protected host. The administrator specifies QoS settings on each host, or at a host group level, that is using LDT. When LDT is running, QoS monitors CPU or rekey/scan rate on the host and enforces the QoS settings. QoS can also monitor and enforce an administrator imposed limit on the volume of data undergoing rekey per second. The QoS settings enable you to strike a balance between completing an LDT process and not interfering with host application performance.

Monitor and Control CPU Usage

QoS monitors and controls the use of host system resources during LDT, specifically, CPU usage and rekey/scan rate.

Note

You can control CPU usage or rekey/scan I/O rate, but not both. The CPU usage and rekey/scan I/O rate options are mutually exclusive.

Monitor and Control Rekey/Scan I/O Rate

You can choose Rekey I/O Rate as a threshold to control the LDT processing rate. When this threshold is entered, the Quality of Service continuously monitors LDT transformation and enforces the specified amount of data during:

- **Rekeying:** LDT is transforming the data on active GuardPoints based on the new key version.
- **Scanning:** LDT is analyzing files in GuardPoints. Scanning occurs:
 - Before initial transformation (Linux only)
 - Before a rekey (Linux only)
 - Following an interrupted rekey, such as a reboot on Linux or Windows, and also a directory rename or directory deletion on Windows

You can set the Rekey I/O Rate or CPU Threshold for multiple clients through the QoS Settings section in a CipherTrust Manager client profile. All clients associated with a given client profile will use the QoS thresholds set in that profile unless the thresholds are overridden locally on the individual client. (The default setting for Rekey I/O Rate in the client profile is 0 (zero), which means QoS will run full throttle.)

To set the QoS thresholds locally on a particular client, use the `voradmin ldt ior and <iorate>` command on that client. When you do so, the `voradmin` setting overrides the Rekey I/O Rate or CPU Threshold set in the CipherTrust Manager client profile. If QoS was already set locally on this client and you use `voradmin` to set the Rekey I/O Rate, LDT ignores any CPU threshold previously set.

To resume using the client profile QoS values for a client, use `voradmin ldt ior 0` to set the Rekey I/O Rate to 0 (zero). When you do so, CTE returns to using the Quality of Service settings in the client profile.

A tolerance level is associated with the Rekey I/O Rate. Together, the tolerance and Rekey I/O Rate specify a range for the LDT processing rate. The Quality of Service selects a proper tolerance for a Rekey I/O Rate provided through the `voradmin` command, and maintains the LDT processing rate at the specified Rekey I/O Rate plus or minus the tolerance. The tolerance is selected as follows:

- When the Rekey I/O Rate is less than or equal to 10MB/sec, the tolerance is 3MB/sec.
- When the Rekey I/O Rate is greater than 10MB/sec. and less than 50MB/sec, the tolerance is 4MB/sec.
- When the Rekey I/O Rate is at 50MB/sec or higher, the tolerance is 10% of the specified Rekey I/O Rate.

To set or reset Rekey I/O Rate on a single host, use the `voradmin` command as follows:

- To set the threshold of 50 MB/sec., use the following command:

```
voradmin ldt ior 50
```

- To reset the current threshold:

```
voradmin ldt ior 0
```

For more information about setting the Rekey I/O Rate using `voradmin`, see [Select and Set Rekey I/O Rate](#).

QoS Scheduling During Backup/Restore

QoS scheduling plays an important role when backing up/restoring data without the *Apply Key* rule applied to the backup/restore process. During backup/restore, you **must** pause LDT operations before taking backups. QoS scheduling allows the administrator to enter the schedule for QoS aligned with the backup schedule, and pause the LDT processes for the duration of the backup. The schedule specifies which days of the week, and what times of day, LDT is permitted to run. LDT cannot run at any time that is not permitted by the QoS schedule. QoS suspends LDT operations at all times outside of the schedule.

When setting a QoS schedule, consider your system and application peak demand periods during the day and week. Also consider your schedule for data backups. Schedule LDT to pause when you need all available system resources for other tasks, such as meeting peak user demand or performing data backups.

Note

On Windows, if your backup applications are using VSS, then you do not need to pause LDT on Windows.

How to Set QoS

To set QoS for a host to enforce a threshold on LDT based on CPU percentage:

1. Log into the CipherTrust Manager Console as an administrator.
2. Open the **CTE** application.

3. In the left-hand menu, select click **Profiles**.
4. If you want to add a new profile, click Create Profile and specify a profile name and description.
5. Click the profile name in the **Profiles** table.
6. Click the Quality of Service Configuration section heading to open the QoS options and select one of the following radio buttons:
 - **Rekey by Rate** — Specifies that you want to set a Rekey I/O Rate threshold. Enter a value between 0 and 100 in the associated **LDT QoS Rekey Rate** field. If you specify 0, CTE does not throttle the LDT rekey or scanning processes.
 - **Rekey by CPU**— Specifies that you want to set a CPU Rate threshold. Enter a value between 0 and 99 in the associated **CPU Percentage** field.

If you select this option, LDT applies a tolerance of +/- 2% on CPU threshold settings up to 7%. For threshold over 7%, LDT applies a tolerance of +/- 4%.

If CPU% is set to 0, QoS stops monitoring CPU usage and LDT operations run at maximum rekey rate within the available system resources. Setting CPU percentage to 0 does not affect LDT schedules, so LDT operations are suspended and resumed per QoS schedule.

If you do not enter CPU threshold percentage, LDT applies CPU threshold of 5% capped by default.

If CPU% is set to a very high value, such as 25%, the rekey process competes with other applications to use as many CPU cycles as it can. As a best practice, start with a setting of 10%, and increase or decrease it slowly by 5% until it reaches a reasonable level that does not adversely affect the performance of user applications. The higher the percentage, the more quickly LDT completes its processing. However, this speed causes increased competition for resources, which can significantly degrade the performance of other applications using this host.

Caution

Do not set CPU% to a very high value in an attempt to force faster data transformation. This can potentially exhaust other system resources.

When you select **Rekey by CPU**, the **Cap CPU Allocation** check box becomes available. Check this box to specify that the CPU allowance must never exceed the percentage set in CPU%. If **Cap CPU Allocation** is not checked, and additional CPU resources are available on the host, LDT consumes part of the available resources for rekey above the CPU threshold. Exceeding the threshold may impact your production workload as your production CPU resource consumption fluctuates over time.

For example, if CPU% is set to 10%, but **Cap CPU Allocation** is not set, the rekey process continues consuming available CPU cycles after reaching 10% CPU utilization, at which point the rekey process

starts contending with applications for CPU cycles.

7. In the QoS Schedules section, select the schedule you want to use from the **LDT QoS Schedule** drop-down list. This list includes the following options:

- ANYTIME
- WEEKNIGHTS
- WEEKENDS
- CUSTOM

If you select anything other than CUSTOM, CipherTrust Manager displays the time ranges in which LDT can run in the **Time Ranges** column. If you select CUSTOM, you can then click the **Create New QoS Schedule** button to create a custom schedule. Add one custom schedule entry for each time range in which you want QoS to run.

By limiting LDT to periods of low application usage, you minimize the potential for resource contention between applications and LDT.

The following example shows a profile with the CPU threshold capped at 10%. The QoS schedule is set for 1 am to 4 am on Mondays, Wednesdays, and Fridays.

QUALITY OF SERVICE CONFIGURATION

☐ Rekey by Rate
 LDT QoS Rekey Rate (MB/s)

☒ Rekey by CPU
☒ Cap CPU Allocation
 CPU Percentage

QoS Schedules

LDT QoS Schedule: CUSTOM Create New QoS Schedule

Name	Time Ranges	
CUSTOM	Monday 1:00 AM - Monday 4:00 AM	...
CUSTOM	Wednesday 1:00 AM - Wednesday 4:00 AM	...
CUSTOM	Friday 1:00 AM - Friday 4:00 AM	...

QoS Best Practices

This section gives tips and examples to help you set QoS parameters for the best results.

Related Topics

- [General Best Practices for QoS](#)
- [Select and Set Rekey I/O Rate](#)

General Best Practices for QoS

- Use Rekey I/O Rate threshold to limit LDT impact, if any, to your production workloads. Rekey I/O Rate approach is a simpler method for a Administrator or system administrator to enforce a limit on the volume of data that LDT should rekey per second. You can choose a threshold, in units of MBs per second, which is a small percentage of peak IOPS from your production workload.

Note

When choosing a threshold on CTE protected hosts with GuardPoints over NFS/CIFS shares, you must consider network bandwidth between your host and NFS/CIFS servers. QoS does not monitor the impact of LDT operations on network connections between your hosts and NFS/CIFS servers. However, the rate selected as LDT Rekey IO rate directly correlates to the network bandwidth to the target NFS/CIFS servers. In the follow-up discussions for selecting optimal rekey IO rate, you must monitor and collect the network traffic instead of disk IO transfers.

- You will see the effects of QoS settings only if the number and/or types of files in the GuardPoints stress the rekey or scan processes. On hosts with a relatively small number of files, the rekey or scan process may complete quickly without hitting a threshold and causing throttling to occur.
- Use QoS CPU parameters as an alternate method for controlling the effect LDT has on application performance.

Set limits on LDT CPU usage whenever runtime monitoring shows that user applications are affected by LDT. Start by setting the CPU parameter to 10%, then increase or decrease in 5% intervals, as needed, to tune the CPU allocation. When an acceptable level is reached, and LDT is not noticeably affecting user applications, leave the QoS CPU parameters at a constant setting.

- Use monitoring tools.

Monitor host CPU utilization with tools like `vmstat`, `top`, and `iostat` on Linux and `perform` on Windows.

You can also monitor and obtain statistics with the `voradmin ldt stats` command.

For more information about `voradmin ldt stats`, see [Obtaining LDT Statistics at the Command Line](#).

- Select CPU resource allocation for LDT from 1% to the available limit minus 5%.

If the monitoring tools indicate system CPU usage, without LDT, it is at N%, available CPU resource is M%, where $M = 100 - N$. Select a percentage within $1 - (M - 5)$ to allocate to LDT CPU usage. However, remember that QoS tolerates 2% - 4% leeway in the actual CPU usage, so adjust your selection by 2 - 4%.

- Do not set CPU resources to 0% or 99% in an attempt to minimize or stop LDT

A CPU% value of 0 or 99 is reserved for disabling the QoS CPU monitoring function. This does not stop LDT or minimize its resource usage; rather the opposite. It enables LDT to run with its maximum rekey rate. Note that when CPU % is not set, LDT clients enforce a 5% CPU threshold by default.

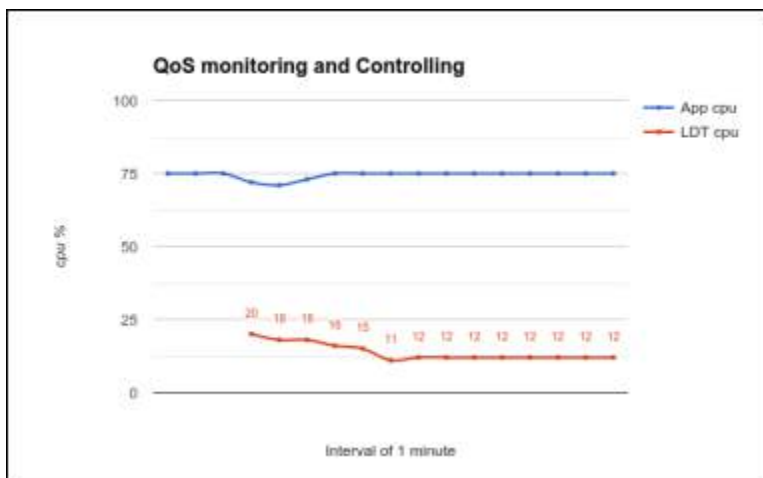
- Cap the CPU allocation.

QoS provides a **CAP CPU Allocation** parameter. Set this parameter to **True**. This ensures that LDT resource usage never exceeds the allocated percentage.

Example: Setting QoS before starting LDT

You can be proactive and set up QoS parameters before enabling GuardPoints that are protected with LDT policies. This ensures QoS starts monitoring and controlling LDT resource usage from the start. The following graph shows an example where 10% of the CPU is assigned to LDT. QoS makes sure that LDT is restricted to use only 10% of the CPU. There is a tolerance level of +/- 4%, so actual LDT usage can range between 5% and 15% of CPU. In the following example, applications use 75% of the CPU resources. As the graph shows, when LDT starts, application CPU utilization drops for a moment, because LDT exceeds the CPU threshold. QoS immediately reduces LDT's CPU usage to 12%, which is within tolerance levels for a 10% setting, and the application CPU share returns to normal.

QoS makes visible improvement immediately when LDT starts



The graph above was obtained on a Linux system running sysbench.

- To find the amount of CPU resources currently in use by applications, type:

```
top -n 1 -b | grep sysbench | awk 'BEGIN {cpu=0} {cpu += $9} END {print cpu}'
```

- To find the amount of CPU currently in use by the LDT-protected host, type:

```
top | grep Cpu
```

- To find the amount of CPU currently in use by LDT, type:

```
voradmin ldt stats | grep CPU
```

Example: Monitoring and controlling resource usage during LDT

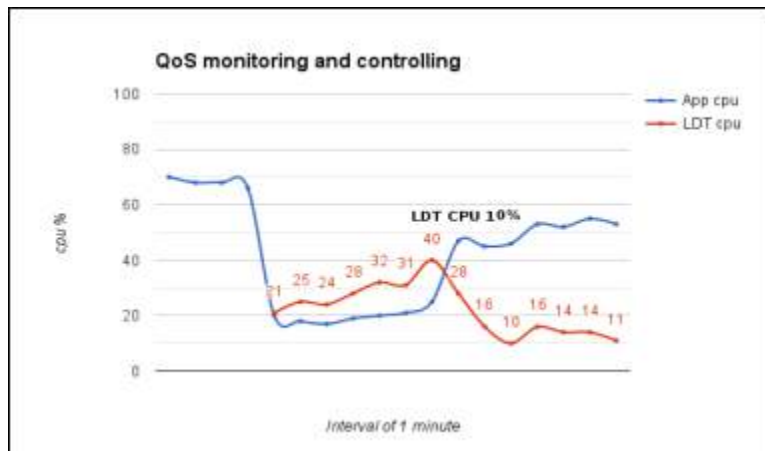
Suppose that LDT has started with CPU set to 25%, and users realize their applications are affected. For example, there might be a higher than expected level of LDT I/O operations. To return application performance to normal, reduce the CPU allocation for LDT.

- Set the **CPU parameter** to a lower value, such as 10%.
- Select the **Cap CPU Allocation** option.

QoS restricts LDT CPU usage to 10%. The application user should monitor their application. If the application's performance is still affected, reduce the CPU parameter further, such as to 5%. Repeat this procedure until application performance returns to a satisfactory level.

The following graph shows an example where QoS is not enabled to monitor and control LDT CPU usage from the start. When LDT starts, application CPU usage drops from 65% to 20%. By setting the QoS CPU parameter to 10%, application usage is greatly improved.

CPU usage allocation before and after QoS CPU parameter is set



Example: How QoS CPU settings affect I/O bandwidth

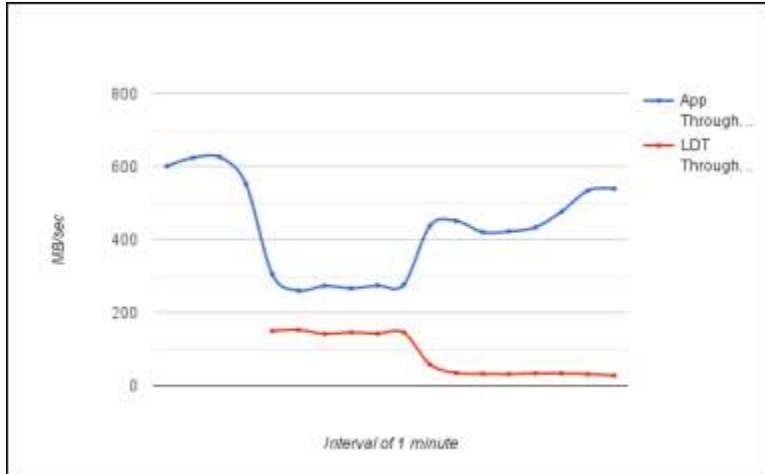
Controlling CPU utilization indirectly controls I/O bandwidth. When LDT is consuming less CPU resources, it is usually performing fewer operations of all kinds, including input and output.

The following graph shows how an application's I/O throughput is affected by LDT, and how QoS can reduce this effect through monitoring and controlling the LDT CPU resource usage.

This graph is from the same system described in [Example: Monitoring and controlling resource usage during LDT](#). No QoS parameters are set at first. When LDT starts, application I/O drops from more than 600 MB per second to below 30 MB per second. By setting the QoS CPU parameter to 10%, the LDT I/O operations drop to below the

application's ability to perform so application I/O operations is greatly improved.

I/O operations before and after QoS CPU limit is set



To obtain the data for this graph:

- Use `iostat` and benchmarking tools on an RHEL system to obtain application I/O throughput.
- Use `voradmin ldt stats` to obtain the LDT I/O throughput and rekey rate.

Select and Set Rekey I/O Rate

You can choose to set the Rekey I/O Rate to control I/O operations from LDT to minimize LDT impact to your production workload. It's assumed that you already know the maximum IOPS on your host system during your production workload. With this information, you can choose a threshold for Rekey I/O Rate and enforce the selected threshold during CipherTrust Transparent Encryption - Live Data Transformation. The work flow is as follows:

1. Set **Rekey I/O Rate** threshold using `voradmin` or in the CipherTrust Manager Console.
2. QoS retrieves the threshold and starts monitoring and controlling LDT according to the specified threshold and the tolerance factor corresponding to the threshold.
3. The selected threshold will be in effect within 2 to 4 minutes after entering the threshold.

When Rekey I/O Rate and CPU or IOWAIT thresholds are set, QoS will monitor and control the LDT processing rate based on the Rekey I/O Rate threshold. The CPU threshold will be ignored.

Set Rekey I/O Rate Threshold

1. Set **Rekey I/O Rate** threshold by using `voradmin`:

```
voradmin ldt ior 10
```

You can also set the Rekey I/O Rate for one or more managed hosts using the Quality of Service section in a client profiles. For more information about using this method, see [How to Set QoS](#).

In the `voradmin` example above, QoS enforces the threshold of 10MB/sec with the tolerance of +/- 3MB/second. Effectively, LDT attempts to rekey the amount of data in the range of 7MBs/second to 13MB/second.

On Linux and Windows, you can use `voradmin ldt ior` to report the current threshold setting without specifying a value for threshold:

```
voradmin ldt ior
QoS Rekey I/O rate threshold: 10 MB/sec
QoS Rekey I/O tolerance: 3 MB/sec
```

2. Be sure the threshold you enter is appropriate for your production workload. To verify this:

a. Observe the Rekey I/O Rate for a few minutes using `voradmin`.

On Linux, you can do this using:

```
voradmin ldt stats
Host level statistics:
File stats: rekeyed=202390, passed=0, created=0, removed=0
Data stats: rekeyed=6.2GB, truncated=0.0MB
QoS: IOR threshold=10MB/sec, tolerance=3MB/sec
current_rekey_rate=2MB/sec, current_iow=0ms
load_factor=50, delay_factor=0, delay_scan=0
```

On Windows, you can do this using:

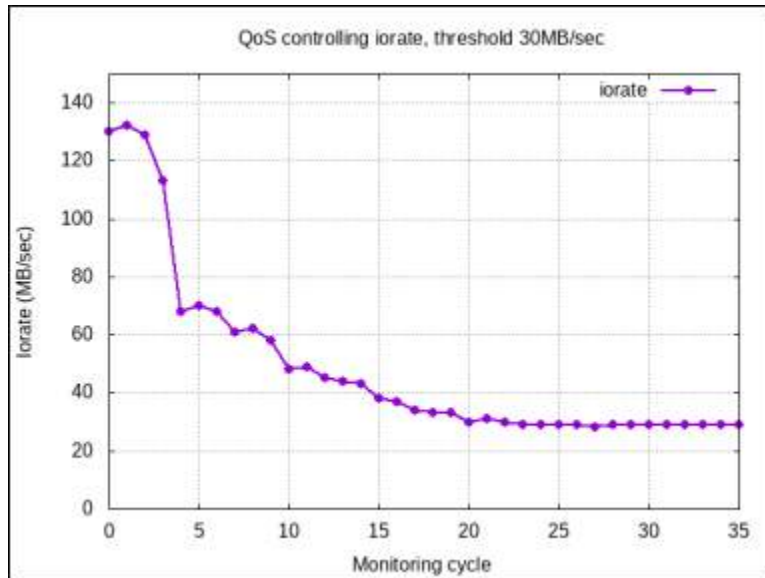
```
voradmin ldt monitor
Host Stats:
Total number of Guard Points    = 1
Rekey Status                    = Rekey done (Finished rekey on 1 out of 1 G
P's)
Total files to be transformed   = 0
Total files transformed         = 0
Total files in progress        = 0
Total transformation threads    = 0

Current rekey rate              = 0 KB/s
Rekey IO rate threshold        = 1000 MB/s
Rekey IO rate tolerance        = 4 MB/s
```

b. Set an appropriate threshold. Do not set the threshold value too high, as QoS might not be able to achieve it because of other resource bottlenecks.

3. Check the QoS controlling rekey rate.

QoS will monitor and control LDT utilization using the specified threshold. The following figure shows an example of how QoS monitors and controls LDT utilization. In this example, the threshold is 30 MB/sec. Throughput of LDT was nearly 130 MB/sec. QoS brings it down to within the range of 30 MB/second.



4. Disable QoS.

QoS will not monitor and control resources when all the thresholds, CPU, Rekey I/O rate, and IOWAIT are set to 0. When Rekey I/O Rate and IOWAIT are not explicitly set, it is considered to be set to 90 MB/second.

QoS continues to apply its schedules for suspending LDT operations at certain days and times regardless of what values are set for CPU, Rekey I/O Rate, and IOWAIT thresholds.

Summary of QoS Resources

The following table summarizes the available thresholds and the actions of QoS module to enforce the set thresholds:

Scenario	QoS Action
Only Rekey I/O Rate threshold is set	Monitor and control the LDT processing rate based on Rekey I/O Rate
Rekey I/O Rate and CPU threshold are set	Monitor and control the LDT processing rate based on Rekey I/O Rate. CPU threshold is ignored.

Creating an LDT GuardPoint

After you have installed the license and registered the LDT host (see [Installing LDT](#)), you can create an LDT GuardPoint on the host. When you create the LDT GuardPoint, you select a Live Data Transformation policy and apply that policy with its transformation keys to that GuardPoint. CTE automatically gets the Quality of Service settings from the associated Client Profile in CipherTrust Manager.

This section describes two scenarios:

- [Creating an LDT GuardPoint for an Unguarded Directory](#)
- [Converting a Standard GuardPoint to an LDT GuardPoint](#)

Creating an LDT GuardPoint for an Unguarded Directory

To create an LDT GuardPoint on what was previously an unprotected/unguarded directory:

1. Create an Live Data Transformation policy that transforms data from clear text to a versioned key. In the policy, set Current Key to `clear_key` and Transformation Key to the versioned key. For details, see [Creating LDT Policies](#).
2. Set, or modify, the Quality of Service (QoS) parameters in the Client Profile associated with the CTE client to account for LDT on all GuardPoints on this client. For details see [Quality of Service](#).

Note

Stop all applications so that they're not accessing any data in the directory that you intend to guard/protect.

3. In the CipherTrust Manager Applications Page, select the **CTE** application.
4. In the Clients table, click on the name of the client you want to protect.
5. Above the GuardPoints table, click **Create GuardPoint**.
6. In the Create GuardPoint page:
 - a. In the **Policy** field, select the LDT policy you created earlier.
 - b. In the **Type** field, select the type of device. For LDT, you can select **Auto Directory** or **Manual Directory**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a Windows-style explorer.

If you want to enter multiple paths, put each path on its own line.
 - d. Keep the **Preserve Sparse Regions** option selected if you want CTE to ignore sparse regions during data transformation.

A *sparse region* is a region within the file size that has not yet been written to. Therefore, it is not allocated with disk blocks. Any attempt to read a sparse region reads stream of zeros as data. A file may have one or more sparse regions, or an entire file may be sparse.

If you select **Preserve Sparse Regions**, LDT detects and skips transforming sparse regions. Therefore, it does not change the number of blocks utilized in the file system. This is the default.

If you disable **Preserve Sparse Regions**, LDT transforms a file without checking or skipping sparse regions, if they exist. Consequently, as LDT operations transform and fill sparse regions with encrypted stream of zeros, sparse regions are allocated with disk blocks. This increases the number of disk blocks utilized in the file system.

- e. Click **Create**.
- f. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**.

The CipherTrust Manager pushes the GuardPoint configuration to the client and CTE immediately begins transforming the data in the specified folders from clear-text to cipher-text.

7. Once the GuardPoint is in the **Active** state, you can bring applications back online. Data continues to get encrypted in the background while the application is online, according to the QoS settings defined in the policy. Once the rekeying state reaches 100%, or shows rekeyed, that means that all of the current data was successfully encrypted.

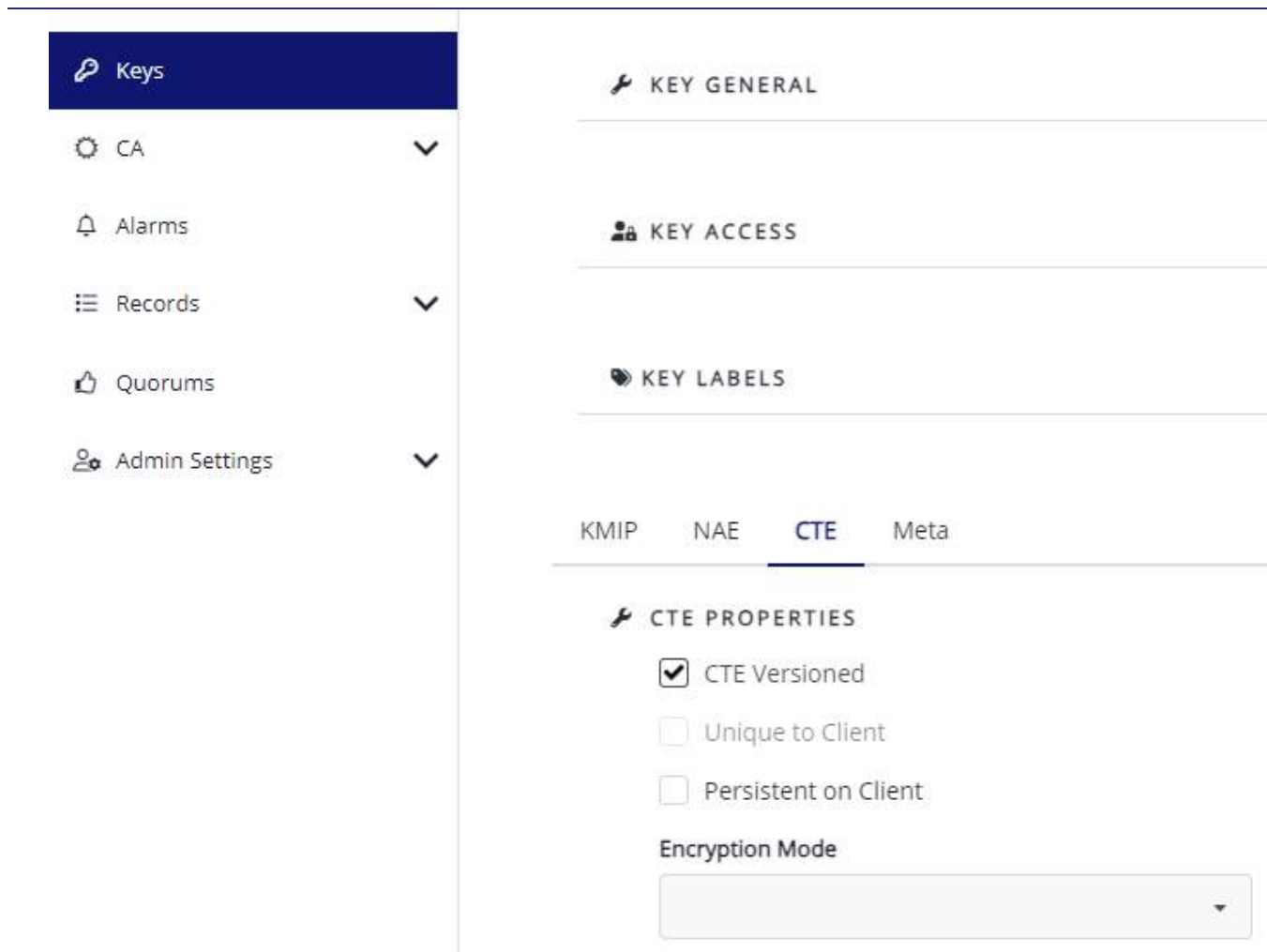
Converting a Standard GuardPoint to an LDT GuardPoint

Note

When converting a CIFS GuardPoint, ensure that the client is running the `vmarfs` driver and is a part of an LDT Communication Group. To determine which driver your node has installed, type: `fltmc` from the administrative command line. For more information, see [LDT Communication Groups and LDT GuardPoint Groups](#).

After enabling LDT on a client, you can change a standard GuardPoint to an LDT GuardPoint. LDT GuardPoints provide the advantage of allowing users to access all files in the GuardPoints while encryption is occurring. There is no downtime for the user except for the time needed to apply the GuardPoint.

1. Clone the key:
 - a. In CipherTrust Manager, navigate to the key section in the left navigation bar.
 - b. For the key that needs cloning, click the (...) button at the end of the row and select clone.
 - c. Type a unique name for the cloned key.
 - d. Toggle **CTE Versioned** to on.
 - e. Click **Clone**.
 - f. Select the key and open the CTE properties tab.
 - g. Verify that **CTE Versioned** is selected.



Note

- This is **mandatory** because keys used in Standard policies are not versioned for CTE.

2. Create a new LDT policy that transforms data from the standard/non-versioned key used in the existing GuardPoint, to an LDT versioned key.
 - **Policy name:** Make the new policy name the same as the standard policy name but append it with `_LDTPo1` or something similar to differentiate it.
 - **Security Rules:** Create the **exact same** security rules that are used in the relevant standard policy.
 - **Current key:** Use the encryption key defined in the standard policy.
 - **Transformation key:** Use the corresponding cloned/versioned Key of the current key.
3. Make sure there is no application activity within the GuardPoint.

Caution

This step is critical. Do not skip it. Make sure there is no application activity within the GuardPoint.

4. Remove/Unguard the current GuardPoints.
 - a. Open the **CTE** application and click **Clients** in the left-hand menu bar.
 - b. Click on the name of the client whose GuardPoint you want to change.
 - c. Find the GuardPoint that you want to change in the GuardPoints table, click the (...) button at the end of the row, and select **Unguard**.
5. Guard the directory again using the new LDT policy.
 - Use the steps above in [Creating an LDT GuardPoint for an Unguarded Directory](#) to guard the directory with the new policy.
6. Once the GuardPoint is in the **Active** state, you can bring applications back online. Data continues to get encrypted in the background while the application is online, according to the QoS settings defined in the policy. Once the rekeying state reaches 100%, or shows rekeyed, that means that all of the current data was successfully encrypted.

Rotating Encryption Keys (Rekey)

- [Manual Key Rotation](#)
- [Creating a Key Rotation Schedule](#)
- [Checking the Rekey Status](#)
- [Obtaining Information About Keys Applied to Files](#)
- [Showing GuardPoints During Rekey \(Linux\)](#)
- [Suspending and Resuming Rekey and/or Scan Phase](#)
- [Automatic Suspend and Resume of LDT Operations Due to Insufficient Disk Space](#)
- [Rotating Encryption Keys While a Rekey is in Progress \(Relaunch\)](#)

Manual Key Rotation

If you need to rekey your GuardPoint prior to the expiration of the current key version, you can manually start a rekey process.

On Windows, you cannot rotate a key until all current data transformations that use the same key have completed, whether those transformations are an initial data transformation or a rekey. On Linux, you can rotate the key at any time. For details, see [Rotating Encryption Keys While a Rekey is in Progress \(Relaunch\)](#).

1. In the CipherTrust Manager Applications Page, open the [Keys & Access Management] application.
2. Click **Keys** in the left-hand menu bar.
3. In the Keys table, click on the name of the key that you want to rotate.
4. On the Key Detail page, click the Add button (+) above the table to add a new version.



The new version appears in the Versions table.



Creating a Key Rotation Schedule

In CipherTrust Manager, you can create an automatic key rotation schedule that will automatically rotate all of the keys included in the schedule on a periodic basis. As soon as CipherTrust Manager creates a new version of a key, it pushes the new version to any clients associated with the policies that use the key. If the policy is a Live Data Transformation policy, CTE automatically begins rekeying the data in the LDT GuardPoint with the new version of the key.

1. In the CipherTrust Manager Applications Page, open the **Admin Settings** application.
2. Click **Schedules** in the left-hand menu bar.

CipherTrust Manager displays the existing key rotation and backup schedules that have been defined in the system. Thales strongly recommends that you look at any existing key rotation schedules to make sure that the keys you want to rotate are not already included in one of those existing schedules.

If the existing key rotation schedules do not include the keys you want to rotate, continue with this procedure

to create a new schedule.

3. On the **Schedules** page, click **Add Schedule**.
4. On the **Select Schedule Type** page, click **Key Rotation** and click **Next**.
5. Add a schedule name and description. Make sure you name the schedule as descriptively as possible so that other users can tell at a glance what keys that schedule includes. For example, you could name the schedule "Rotate-LDT-Keys" and use the description "Rotates all keys with "LDT" in their name on a yearly basis."

When you are done, click **Next**.

6. On the **Schedule Config** page, enter the following information:
 - **Duration.** Enter the day and time on which CipherTrust Manager should start using the key rotation schedule in the **Schedule Starts** field. When this day and time is reached, CipherTrust Manager looks at the date in the **Frequency** section and automatically creates a new version on that date.

Enter the day the schedule should end in the **Schedule Ends** field, or select the **Never** check box to tell CipherTrust Manager there is no end date for this key rotation schedule. If you select a date in this field, CipherTrust Manager automatically stops creating new key versions when that day and time are reached.

- **Frequency.** Select the **Basic** radio button to specify the frequency (daily, weekly, monthly, or yearly) and the UTC time at which CipherTrust Manager should automatically rotate the key after the schedule starts.

Select the **Raw (Cron)** radio button to create a cron job to control the key rotation schedule. Specify cron format in the following order:

minute, hour, day of month, month, and day of week

These five values indicate when the job should be executed. These values are mandatory and must be specified in the order given. The allowable values are:

Field	Allowed Values
minute	0-59 or * / , -
hour	0-23 or * / , -
day of month	1-31 or * / , -
month	1-12 or JAN-DEC or * / , - This field is case in-sensitive, so JAN, Jan, or jan are all equally valid.
day of week	0-6 or SUN-SAT or * / , - This field is case in-sensitive, so SAT, Sat, or sat are all equally valid.

Examples:

- December 31 at 2:35 AM UTC could be specified as: `35 2 31 Dec *`.
- On the 25th of every April, August, and December at midnight UTC could be specified as: `0 25 APR, Aug, dec *`.
- Every Monday, Wednesday, and Friday at 8:00 PM UTC could be specified as: `0 20 * * 1,3,5.`

When you enter a **Duration** and a **Frequency**, CipherTrust Manager displays the next several times the key rotation will be run under the **Frequency** field. Make sure the key rotation will be done on the days you expect.

Note

While the specified time is in UTC, the scheduled run times are shown in your local time. Therefore there may not be an exact match between the time set in the **Frequency** field and the displayed run time.

When you are done, click **Next**.

7. On the **Key Rotation Page**, specify the selection criteria you want CipherTrust Manager to use when it selects the keys it will rotate.

Caution

Make sure you are extremely careful when you specify the selection criteria so that you do not accidentally rotate keys that should not be rotated using this schedule. Whenever a new key is added to CipherTrust Manager, CipherTrust Manager compares its name and details to the filters set in all key rotation schedules defined in the Admin Settings application, and it automatically adds the new key to ALL key rotation schedules where it matches the selection criteria.

If your selection criteria is too broad, you could accidentally rotate keys that should not be rotated by this key rotation schedule.

You can enter a key name in the **Name** field, or select any of the available filters from the drop-down lists. The Selected Keys table shows the keys that will be rotated by this schedule.

CipherTrust Manager displays the current list of keys that match this criteria in the **Selected Keys** table. Make sure you go through this list carefully so that you do not rotate keys you do not want to rotate.

For example, you can rotate all keys with "ldt" anywhere in their name by specifying `*ldt*` in the **Name** field:

Add Key Rotation Schedule ✕

1 Select Schedule Type
2 General Info
3 Schedule Config
4 Key Rotation Query

A key rotation query is an object that specifies the keys that need to be rotated. All keys are rotated when it is not provided.

Name ▾ *ldt*

Q

Filters
☒ Basic
☐ Raw

Types ▾
Size ▾
Status ▾
Dates ▾

☒ Latest Version Only

Name: *ldt* ✕
Version: latest ✕

Selected Keys

Key Name	Ver	Modified	Type	Alg	Size
LDT-Key-West-Coast	2	08 Sep 2020, 10:10	Symmetric	AES	256
LDT-Key-East-Coast	3	08 Sep 2020, 10:10	Symmetric	AES	256
My_LDT_Key	0	08 Sep 2020, 10:07	Symmetric	AES	256

Back
Save

If you only want to rotate the keys whose names begin with "ldt", use the query `ldt*` in the **Name** field. In the example above, that removes `My_LDT_Key` from the list of keys that will be rotated.

The search is case insensitive, so "ldt" will also match `LDT`, `ldt`, `ldT`, or any variation thereof.

When you are certain the list of keys to be rotated is accurate, click **Save**.

Checking the Rekey Status

During a rekey, you can check the progress in the CipherTrust Manager Console, however GuardPoint status is not relayed to the CipherTrust Manager in real time. A delay of several minutes before the CipherTrust Manager displays events on the client is likely. When the number of GuardPoints on the managed host is high, for example 100+, the delay in relaying GuardPoint status is due to delays in scheduling and the execution of LDT operations on the managed host for GuardPoints.

To see the progress of a rekey and the estimated completion time:

1. In the CipherTrust Manager Applications Page, open the **CTE** application.
2. Click **Clients** in the left-hand menu bar.
3. Click the **Client Name** of the client whose LDT status you want to check in the Clients table.
4. Find an active LDT GuardPoint and click **Active** in the **Status** column.

CipherTrust Manager displays the GuardPoint Health page, which includes transformation status information such as the basic status (Rekeyed or Rekeying), the last transformation completion time, the last transformation start time, and the estimated rekey completion time.

Obtaining Information About Keys Applied to Files

Key Report Option

In the following command, you can use the `report` option of the `voradmin` command to obtain information about all of the keys in use on the GuardPoint. The report lists all keys used in the GuardPoint. For each key, it gives the key name and key version number. It lists each unique key name and version combination only once, no matter how many files use the key.

The following example shows three keys used in the GuardPoint `/oxf-fs1/gp1`:

```
voradmin ldt key report /oxf-fs1/gp1
LDT_KEY1,1
LDT_KEY2,2
LDT_KEY3,5
```

For an overview of `voradmin ldt`, see [LDT Command-Line Administration: voradmin command](#).

Key Map Option

In the `voradmin ldt key [report|map] <key_name> <guard path>` command, you can use the `map` option to obtain information about which files in a GuardPoint were transformed with a specific key, where:

- `<key_name>` is the name of the key.
- `<guard path>` is the path of the GuardPoint where the key was used.

For example, to view information about the key `LDT_KEY2` in the GuardPoint `/oxf-fs1/gp1`, you would enter:

```
voradmin ldt key map LDT_KEY2 /oxf-fs1/gp1
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
```

Keys without a version number are used by files in an exclusion key rule or files that have yet to undergo initial key rotation. Use `voradmin ldt key map` in conjunction with `voradmin ldt attr get` to determine if a file using a key without a version number is part of an exclusion key rule or awaiting initial key rotation.

Showing GuardPoints During Rekey (Linux)

Use the following command to display a list of known LDT metadata stores and any associated GuardPoints currently undergoing transformation.

```
voradmin ldt list all
MDS_1:  type=file, nguards=0, name=/disk2/___vorm_mds___
        Guard Table: version 1 nentries 0
MDS_2:  type=file, nguards=0, name=/disk3/___vorm_mds___
        Guard Table: version 1 nentries 0
MDS_3:  type=file, nguards=0, name=/disk4/___vorm_mds___
        Guard Table: version 1 nentries 0
```

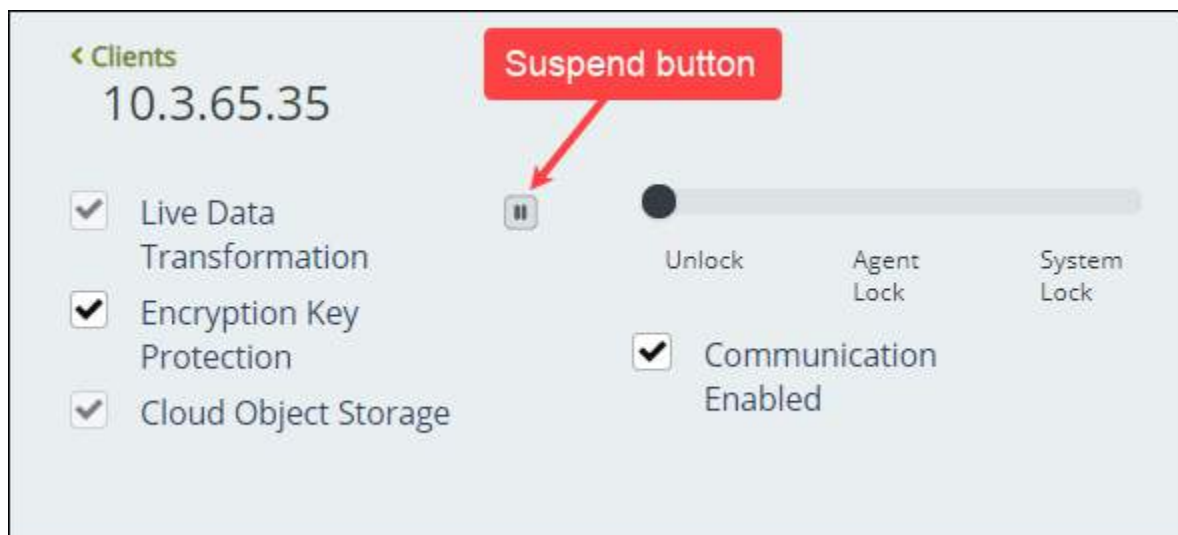
For an overview of `voradmin ldt` commands, see [LDT Command-Line Administration: voradmin command](#).

Suspending and Resuming Rekey and/or Scan Phase

The QoS schedule specifies certain time windows when LDT operations must be stopped temporarily. However, you can also suspend or resume LDT at the host/client level at any time.

To suspend LDT through the CipherTrust Manager Console:

1. Open the **CTE** application.
2. Click **Clients** in the left-hand menu bar.
3. Click the **Client Name** of the client on which you want to pause LDT in the Clients table.
4. In the Client Details area, click the **Suspend** button next to the Live Data Transformation field to suspend all LDT operations on the client.



After you pause LDT, the button turns into a Play button so that you can resume LDT operations when ready.

Considerations

- Disabling, or unguarding, an LDT GuardPoint where a rekey is in progress automatically suspends the LDT rekey operation.
- You can also use the `voradmin suspend/resume` command in Windows Powershell to suspend and resume the rekey. However, if you use the `voradmin ldt suspend` command to pause the rekey process, the LDT suspended state is not retained when the system reboots. If you want to retain the state after reboot, suspend the rekey from the CipherTrust Manager.
- On Linux, you can pause LDT during the scan phase of LDT. When paused during scan, LDT suspends operations that traverse through the namespace of GuardPoints in the scan phase of transformation. Suspending LDT during scan stops file lookup operations of LDT. This eliminates performance impact to I/O intensive production workloads, such as file serving type workloads, that access large number of files.

Automatic Suspend and Resume of LDT Operations Due to Insufficient Disk Space

LDT requires adequate storage space headroom to perform LDT operations such as rekeying on GuardPoints. On Linux, if available storage space drops below the threshold required for LDT operations to continue, the LDT operations are automatically suspended. On Windows, LDT will be suspended if there is less than 3 GB free space in the GuardPoint. Once additional storage space is available in the file system, LDT operations automatically resume.

As available space approaches the threshold for automatic suspension, LDT sends an alert to the CipherTrust Manager to notify you that you should free up more storage space before LDT operations are suspended. The alert on the CipherTrust Manager is:

```
Low space on guard point [GuardPoint], increase free space or LDT will be suspended.
```

Behavior of Automatic Suspend and Resume of LDT Operations on ext4 File Systems

By default, ext4 file systems reserve a portion of the storage space for use only by privileged processes to prevent running out of storage space in file systems. In this situation, non-privileged processes are automatically blocked from writing to the file system until the free disk space level reaches the minimum threshold. As LDT operates in privileged mode, LDT operations continue without blockage even if the free disk space threshold is low. Because of this ext4 feature, LDT operations on ext4 file systems may not be suspended due to low available storage space, even when the `df` command reports storage is 100% allocated.

Rotating Encryption Keys While a Rekey is in Progress (Relaunch)

On Linux, if a key is rotated (either manually or automatically when a key version expires) while LDT is in progress on a GuardPoint, the key rotation is processed and queued, and the GuardPoint is marked for relaunch. Relaunch indicates the need to restart LDT after the current transformation completes. If the GuardPoint has been rekeyed and is flagged for relaunch, LDT launches as soon as the GuardPoint is enabled.

When this event occurs, the following message appears in the log file: "LDT: Deferred key rotation on

GuardPoint [GuardPoint] until after completion of current transformation."

When the new key rotation request is queued, files can be in one of three states:

- **Undergoing rekey to a previous key:** Files already undergoing transformation to a previous key when the new rekey request is queued, are rekeyed to the key version already in progress.
- **Scheduled for rekey to a previous key:** Files that start transformation after the new key rotation request is queued are rekeyed to the newest key version.
- **Rekeyed to a previous key:** Files that have already been rekeyed to a previous key remain in that state until all files undergoing rekey, or scheduled for rekey, have been processed. Once the current LDT process for the GuardPoint is complete, LDT automatically relaunches to transform any files that are not rekeyed to the latest key version. This includes any files that were rekeyed before the new key rotation request was queued, or that were undergoing transformation when the new key request was queued.

For example:

```
voradmin ldt attr get /oxf-fs1/gp1
LDT stats: version=2, rekey_status=rekeying,relaunch
  Number of times rekeyed:          1 time
  Rekey start time:                 2024/03/18 16:54:00
  Last rekey completion time:       2024/03/18 16:53:38
  Estimated rekey completion time:  0 days 0 hours 6 minutes
  Policy key version:               344
Data stats:
  total=9.8GB, rekeyed=0.0MB
  truncated=0.0MB, sparse=0.0MB
File stats:
  total=1000, rekeyed=0, failed=0
  passed=0, skipped=0, created=0, removed=0, excluded=0
```

Note

Relaunch is supported on Linux only. It is not supported on Windows.

Relaunch when Directories are renamed

Prior to v7.6.0, when a user renamed a directory, LDT would set a relaunch flag on the GuardPoint during the scan phase of LDT. This relaunch flag would trigger an additional LDT process on the GuardPoint when the current transformation job completed.

As the transformation process can impose significant overhead on production workloads, subsequent relaunch of LDT, as the result of renaming directories, is not efficient.

CTE v7.6.0 records renamed directories during the scan phase, so it can locate the files relocated to other paths during the rekeying phase of LDT. This prevents the GuardPoint from going through another transformation due to the directory being renamed during the scan.

Limitation

You can only rename a maximum of 16 concurrent directories without triggering a relaunch. If more than 16 concurrent directories are renamed during the scan phase, LDT sets the relaunch flag on the GuardPoint.

File System Operations

File system operations may require attention from the Administrator. These operations are divided into the following categories:

- Renaming Files and Directories
 - Renaming Directories on Linux
 - Caveats
 - Example
 - Considerations
- Deleting a File
- File Handling (Windows)
- Enabling GuardPoints in Read-Only mounted file systems (Linux)
- Copying Files Into a GuardPoint
- Behavior of Hard Links Inside and Outside of GuardPoints (Windows)

Renaming Files and Directories

On both Linux and Windows hosts, you can rename files during initial transformation, or rekey operations.

- On Linux, you can now, as of v7.1.1, rename directories in a GuardPoint during a rekey operation.
- On Windows, LDT stops if it is transforming the contents of a folder and a user attempts to rename/move that folder.

You can change the stopping behavior of LDT using the configuration parameter `oxf_stop_on_rename`.

Using the Registry Editor, or the Windows command line, add a registry entry in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Vmmgmt\Parameters` for `oxf_stop_on_rename`.

Registry Name	Values	Comments
oxf_stop_on_rename	0 - Disabled	LDT does not stop if there is contention.
	1 - Enabled	LDT stops if there is contention.

Registry Name	Values	Comments
		Default: Enabled.

For the target folder in rename operation, LDT is never stopped.

Renaming Directories on Linux

Prior to LDT v7.1.0, you could not rename a directory within an LDT GuardPoint, during the rekeying process. However, starting in LDT v7.1.1, users and applications can now rename directories within an LDT GuardPoint, during the rekeying process.

When a directory is renamed, LDT starts performing single file rekey jobs, on files in that renamed directory. A single file rekey job is a background process that rekeys a specific file, independent of the rekey process occurring on the entire GuardPoint. This process is similar to how files marked with a lazy rekey flag are rekeyed to the latest key version upon access to the marked file. LDT supports a maximum of 16 concurrent renamed directories per GuardPoint in the scan or rekey phases. If an additional directory is renamed while there are already 16 directories being processed, the GuardPoint is marked for relaunch (See [Rotating Encryption Keys While a Rekey is in Progress \(Relaunch\)](#) for more information on the relaunch state). This will make rekey start again upon completion to pick up any additional renamed directories.

Note

If a GuardPoint is already marked for relaunch, directory renames will not trigger single file rekeys. This is because the relaunch of LDT will pick up the files in the renamed directories.

You can view rekey jobs in a GuardPoint using the command `voradmin ldt list all`. Rekey operations for files marked as lazy, as part of CipherTrust Intelligent Remediation, and for directory rename, are listed as separate single file rekey jobs. In the example below, the file `/ldt/renamed/file.0` is undergoing rekey as a single file rekey job, as the result of changing the pathname to the file.

```
voradmin ldt list all

MDS_1:  type=file, nguards=9, name=/ldt/__vorm_mds__

  Guard Table: version 1 nentries 9

  Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/ldt

    File List: count 51

  Guard 1: type=FILE, state=REKEYING DIRTY, flags=FILE LOCKED, gp=/ldt/rename
d_dir/file.0

    File List: count 1
```

LDT can run a maximum of eight concurrent single file rekey jobs for directory renaming. This limit is shared across directory renames for all of the GuardPoints on a system.

Furthermore, while directory rename is in progress on a target GuardPoint, the GuardPoint will not transition into the rekeyed state, even if LDT has completed on the rest of the files in the GuardPoint. As soon as the single file rekey jobs associated with the GuardPoint complete, the GuardPoint transitions into a rekeyed state.

Caveats

The following caveats exist when renaming directories that are in GuardPoints:

1. A directory rename operation changes path names to an unknown number of files. As such, LDT cannot accurately estimate completion time on the target GuardPoint. In such a situation, the rekey progress reflected on the key manager may show that the GuardPoint is in 100% rekeyed status, and the status remains in the 100% rekeying status, until the files in the renamed directories are rekeyed to completion.
2. Directory rename operations also affect the accuracy of LDT statistics. Those files, in a renamed directory that are not rekeyed when the directory is renamed, are no longer accessible as part of rekeying the GuardPoint. However, those files will be rekeyed as part of rekeying the renamed directory. As the GuardPoint level rekey operations fail to find those non-rekeyed files, LDT stats update to reflect those files as 'passed' and their size is added to the 'truncated' stat. When those files are rekeyed, as part of the renaming directory rekey process, the 'rekeyed' status will be correctly updated.
3. The net effect of renaming a directory during a rekey will be reflected in an inaccurate 'passed' count, and the amount of data truncated for each file not rekeyed in the renamed directory.

Example

If there are 1024 files totaling 1 GB in the directory `/ldt/gp/dir`, within the GuardPoint `/ldt/gp` when rekey starts, the stats should appear as follows:

```
ls -l /ldt/gp/dir | wc -l
1024

du -h /ldt/gp/dir
1.0G    /ldt/gp/dir

voradmin ldt stats /ldt/gp

LDT stats on /ldt/gp: version=3, rekey_status=rekeying

Number of times rekeyed:           3 times

Rekey start time:                  2021/06/14 23:53:56

Last rekey completion time:        2021/06/14 21:26:09

Estimated rekey completion time:    N/A

Data stats:

    total=13.8GB, rekeyed=726.0MB, truncated=0.0MB

File stats:

    total=1043, rekeyed=0, failed=0

    passed=0, skipped=0, created=0, removed=0, excluded=0
```

Upon renaming of the directory `/ldt/gp/dir`, any files that have not yet been processed by a GuardPoint level rekey, is added to the **passed** and **truncated** values in the stats:

```
voradmin ldt stats /ldt/gp

LDT stats on /ldt/gp: version=3, rekey_status=rekeying

  Number of times rekeyed:                3 times
  Rekey start time:                      2021/06/14 23:53:56
  Last rekey completion time:2021/06/14 21:26: 09
  Estimated rekey completion time:        N/A

Data stats:

  total=13.8GB, rekeyed=10.6GB, truncated=1.0GB

File stats:

  total=1043, rekeyed=21, failed=0

  passed=1024, skipped=0, created=0, removed=0, excluded=0
```

Considerations

Consider the following issues when renaming directories during a rekey:

- If a directory rename operation occurs during the scan phase of LDT, the GuardPoint will be marked for relaunch and LDT will be launched again at the completion of the current rekey cycle. This is because it is not possible to begin rekey jobs while LDT is in the scan phase.
- When LDT is suspended on a GuardPoint with a renamed directory, additional single file rekey jobs will not be launched until rekey resumes. However, ongoing single file rekey jobs continue until each single file rekey is completely rekeyed. Consequently, suspending LDT while single file rekey operations are in progress only suspends rekey operations at the GuardPoint level, while LDT operations on single rekey files continues without disruption. As a result, stopping CTE service, which requires suspending LDT and disabling GuardPoints, may be delayed until the files currently undergoing rekey, due to directory rename, are completed.
- Ensure that LDT is suspended at the GuardPoint level and there is no single rekey file in progress before starting operations, such as a backup, which requires suspending LDT operations. Failure to do so can result in unexpected problems.
- If files in a renamed directory are moved out of the renamed directory, those files are processed as separate rekey jobs. Those rekey jobs cannot be suspended until the rekey is completed.
- A system crash during a rekey for a directory rename, also affects how LDT performs a recovery. Normally, LDT requires that, after the crash, the recovery completes for all of the affected files in the GuardPoint, before resuming rekey operations. However, with a directory rename, it is possible for the LDT recovery to skip files

that are in the renamed directory because the path name to those files has changed since the scan phase of the key rotation. Instead, recovery for these files is deferred until the next access by LDT, or a user application, when a GuardPoint is enabled.

- LDT recovery log messages are not logged to LDT recovery log files, if the recovery log messages become necessary in the event of a failed recovery attempt. In the event of an error, LDT logs error messages in syslog, blocks access to the file that could not be recovered, and marks the file in rekey error. Files in rekey error must be restored from a backup. Additionally, as files that cannot be found for recovery are now treated as being deferred (only when the directory rename occurs prior to the crash), any orphaned files that might have been moved to the lost& found directory, in the target file system, will not be discovered as orphaned files and consequently skipped by LDT. LDT cannot discern if the orphaned files are missing or were linked to a renamed directory.

Deleting a File

When a file is removed before it is rekeyed, the file is not included in the total number of files transformed in the GuardPoint Health dialog box. Any discrepancy between total number of files to transform and those transformed is due to the removal of files from GuardPoints during LDT.

The **voradmin** command provides more detailed file level statistics related to rekey operations on the host. You can run **voradmin** to get file level statistics:

```
voradmin ldt stats <guard_path>
```

File Handling (Windows Only)

It is critical that you understand how the LDT process handles read-only, binary (executable), NTFS encrypted and NTFS compressed files.

The LDT process is subjected to all of the File System policies and attributes set on the files. In some cases, this prevents LDT from encrypting a file. If users or applications are accessing files while LDT is in progress, LDT cannot change the attributes of the files and encrypt the file. It is critical that you understand how LDT handles various types of files:

- **NTFS Encryption and Compression**

If NTFS encryption and compression is enabled on a file or folder, the LDT process cannot encrypt these files. To maintain the data coherency, LDT skips the encryption of these files. These files display as “passthrough” files in the LDT statistics.

- **Read-Only Files**

When LDT encounters read-only files, it rekeys the file by resetting the read-only attribute and then setting the attributes back again when the rekey completes. If a file is open, LDT skips this file.

- a. If the file is not opened, LDT changes the attributes of the file and stores the original attributes in the file metadata.
- b. LDT starts Rekey on this file.

- c. If a user requests to open a file for writing while rekey is in progress, access is denied. User can only open files for reading.
- d. LDT restores the attributes once rekey is done.

▪ Executable Files

If an executable is running, or files are exclusively locked by the application, the LDT process cannot encrypt those files as it is unable to acquire the required locks on the files. LDT skips these files and changes to the INCOMPLETE state.

Enabling GuardPoints in Read-Only mounted file systems (Linux)

Access to a GuardPoint enabled in a read-only mounted file system is restricted to read operations. You cannot modify data in such file systems, therefore, you cannot perform LDT operations on GuardPoints in read-only file systems. For this reason, LDT automatically suspends operations when GuardPoints are enabled on read-only file systems. LDT ignores all attempts to resume LDT operations until the underlying file system is remounted with read/write access.

Warning

You must disable a GuardPoint before changing the read/write mount options of the underlying file system. After changing the mount options, you can re-enable the GuardPoint. LDT operations adapt to the read/write options of the underlying file system when you enable the GuardPoint. Changing the mount options while a GuardPoint is enabled is unsupported and may result in unexpected errors.

Copying Files Into a GuardPoint

If you copy a file into a GuardPoint without an Apply Key rule, make sure that the file was previously copied from the same GuardPoint, or a GuardPoint protected with the same policy/versioned key. A copy operation, without an Apply Key rule, is the same as a backup or restore of a file from/to an LDT protected GuardPoint.

CTE enforces key rules of an LDT policy while a GuardPoint is enabled. CTE cannot enforce the key rules while a GuardPoint is disabled. Modifying or adding data/files inside a disabled GuardPoint is not only unsupported, but it also results in unrecoverable data corruption.

Warning

Do not add new files or modify existing files inside LDT protected GuardPoints while the GuardPoint is not enabled. This results in unrecoverable data corruption and/or files that cannot be accessed when the GuardPoint is enabled.

Behavior of Hard Links Inside and Outside of GuardPoints (Windows)

When using hard links on Windows, all of the hard links to a file must be within the boundary of a GuardPoint and must use the same key. The following scenarios provide additional details:

- If hard links to the same file are inside a GuardPoint and outside a GuardPoint, the effect on the file depends on what process accesses which hard link first. If the hard link within the GuardPoint is opened first, the file is transformed. If the hard link outside the GuardPoint is opened first, the file won't be transformed.
- If hard links to the same file exist in different GuardPoints with different keys, the file will be corrupted.
- If hard links to the same file exist in the same GuardPoint but with different keys, such as if folder-based rules are used, there will be a conflict in the key.

Note

For v7.2, hardlinks are not supported on CIFS shares.

Excluding Files or Directories from Rekey

When you add a resource set to a key rule in a policy, you can select the **Exclude Rule** option. This informs CipherTrust Manager that the directories and/or files in the resource set use the define key that is excluded from the LDT rekey process. If you specify `clear_key` for the key rule, then the directories and/or files in the resource set will be left unencrypted. Otherwise, you can select any non-versioned key to apply to those directories and/or files.

For more on Exclusion rules, see the following topics:

- [About the Exclusion Attribute for Files Matching an Exclusion Key Rule](#)
- [Requirements for Exclusion Key Rules](#)
- [Usage Notes and Limitations for Configuring Exclusion Key Rules](#)
- [Examples of Exclusion Key Rules](#)
- [Listing All Files Included in an Exclusion Key Rule \(Linux\)](#)
- [Listing All Files Included in an Exclusion Key Rule \(Windows\)](#)
- [Using Dynamic Resource Sets](#)

About the Exclusion Attribute for Files Matching an Exclusion Key Rule

Files matching an exclusion key rule have the status `rekey_excluded` in the LDT attribute. For more information about LDT attributes, see [LDT Metadata in Extended Attributes](#). To check for the exclusion attribute on a file, see [Determining if a File is Included in an Exclusion Key Rule](#).

The Exclusion Attribute is not Persistent

Exclusion from rekey is no longer a persistent property as of v7.6.0.

See [Dynamic Resource Set](#) for more information.

Determining if a File is Included in an Exclusion Key Rule

Use the `voradmin ldt attr get <path to file>` command to check whether a file is associated with an exclusion key rule.

- On Linux, an excluded file will include the status `rekey_excluded` in the `voradmin` output. For example:

```
voradmin ldt attr get /oxf-fs1/gp1/foo.txt
LDT attributes: rekeyed_size=0, rekey_status=rekey_excluded
```

- On Windows, an excluded file will include the attribute `Rekey Status Excluded` in the `voradmin` output. For example:

```
C:\> voradmin ldt attr get c:\gp1\foo.txt
LDT attributes:
Rekey Status Excluded
Initial Rekeyed Size 9 Bytes
Data Transformed 0 Bytes

Key:
Current Key Name/Version (Clear_Key)
New Key Name/Version (Clear_Key)
```

Removing the Exclusion Attribute From a File

To disassociate a file from an exclusion key rule, you must copy the file to a new file that is not associated with the resource set, or exclusion key rule, of that same source file. You can then remove the original file. The new file is created under the default key rule of whatever policy applies to the new file. Moving or renaming a file does not disassociate a file from an exclusion key rule.

For example, assume the following exclusion key rule where `Key_TextFiles` is a non-versioned key:

Exclusion Key Rule: Resource set `=*.txt`, Key = `Key_TextFiles`

If you copy the file `test1.txt` to `test1.foo`, `test1.foo` is created with whatever key is specified in the policy that matches the new file. The key for the new file could be a non-versioned key, versioned key, `clear_key`, or, no key at all if the new file is outside of a GuardPoint. The original file `test1.txt` remains unchanged and encrypted with the `Key_TextFiles` non-versioned key because the file remains in the exclusion key rule.

Rename and Restore (Linux)

The effect of rename, or backup/restore operations, involving files associated or excluded with exclusion key rules, is complex. In some cases, the operations to restore, or rename, causes conflicts between the key associated with the source file, and the key associated with the target file. For example, the result of a rename operation involving a source file, not associated with an exclusion key rule, and target file name associated with a resource set of an exclusion key rule is different from the result of the same operation when the target file name is associated with the resource set of an exclusion key rule with `clear_key`.

Note

Be sure to review the effect of the operations below and avoid administrative operations that cross associations of files across multiple resource sets with conflicting key rules.

Backup/Restore

- See [File Operations shared key Rules](#) for more information.

Rename Operation

- See [File Operations shared key Rules](#) for more information.

Requirements for Exclusion Key Rules

Keep in mind the following requirements when configuring exclusion key rules:

- Before adding an exclusion key rule to an existing policy, you must disable all GuardPoints protected with the policy. Log on to the CipherTrust Manager to disable the GuardPoint.
- You cannot choose a versioned key for the key in an exclusion key rule. Only non-versioned keys or `clear_key` (no encryption) are valid for exclusion key rules.
- All exclusion key rules must be *above* all LDT transformation key rules in the **Key Rules** area in the policy.

Usage Notes and Limitations for Configuring Exclusion Key Rules

Keep in mind the information in the following sections when configuring an exclusion key rule.

Adding an Exclusion Key Rule to an Existing Policy with Versioned Keys (Linux)

When adding an exclusion key rule to an existing policy, the exclusion rule only applies to newly created files. Existing files that match the exclusion key rule remain encrypted with the same versioned key(s) specified in the non-exclusion key rule in the policy and will be rekeyed to the key in the exclusion key rule when the versioned key(s) rotates.

To force an existing file that matches an exclusion key rule to be transformed to the key in the exclusion key rule (non-versioned in this example), use one of the following methods:

- Rotate the versioned key specified in the policy to initiate rekey operations on the GuardPoint.
- Copy the existing file within the GuardPoint. The new file will be associated with the resource set in the exclusion key rule and will be encrypted with the non-versioned key. You can then delete the original file.

To perform a similar conversion on Windows, see [Changing a Folder or Files from Versioned to Non-Versioned Key \(Windows\)](#).

Adding an Exclusion Key Rule for LDT over NFS

For an LDT over NFS GuardPoint with exclusion rules, all files, including excluded files, can only be read in clear when the GuardPoint is enabled. Excluded files on an LDT over NFS GuardPoint will not be readable when the GuardPoint is unguarded/disabled.

Adding an Exclusion Key Rule That is Part of an Active GuardPoint (Linux)

To edit and/or add an exclusion key rule to an LDT policy, all GuardPoints using the policy must first be disabled before the new key rule can be added.

Changing an Exclusion Key Rule That is Part of an Active GuardPoint (Windows)

Changes that you make to an exclusion key rule that is part of an existing policy in an active GuardPoint do not take effect until the GuardPoint that the exclusion key rule is part of is disabled and enabled again.

Overlapping Exclusion Key Rules

Multiple exclusion key rules in the same policy may overlap each other. For example on Linux, if the non-versioned key Key_A is associated with resource `/oxf-fs1/gp1/Folder_Enc_With_KEY_A` and the non-versioned key Key_B is associated with resource `*.txt`, placement of the file `/oxf-fs1/gp1/Folder_Enc_With_KEY_A/foo.txt` overlaps the two key rules. In such a case, the first rule in the policy is enforced on `/oxf-fs1/gp1/Folder_Enc_With_KEY_A/foo.txt` when the file is created and in subsequent file access.

On Windows, if the non-versioned key Key_A is associated with resource `c:\oxf-fs1\gp1\Folder_Enc_With_KEY_A` and the non-versioned key Key_B is associated with resource `*.txt`, then they would overlap on the file `c:\oxf-fs1\gp1\Folder_Enc_With_KEY_A\foo.txt`. In such a case, the first rule in the policy is enforced on `c:\oxf-fs1\gp1\Folder_Enc_With_KEY_A\foo.txt` when the file is created and in subsequent file access.

Application of Exclusion Key Rules on GuardPoint over NFS

When protecting files using an Exclusion Key Rule with `clear_key` in local file systems, files can be accessed in clear even if the GuardPoint is not enabled. Clear access is possible because data is not encrypted in such files and the LDT metadata is managed as part of the secfs extended attribute for such files. Clear access is not possible for such files in a GuardPoint over NFS because LDT metadata is part of the secfs extended attribute

that is stored in the first 4096 bytes of each file. CTE skips the embedded secfs header when reading or writing such files when a GuardPoint is enabled. With a GuardPoint disabled, access to files is not through CTE and reading or writing files in a GuardPoint will not skip the embedded secfs attribute.

Caution About Applications That Create Temporary Files (Windows)

Some applications on Windows create a temporary file version of the original file when you open and modify a file. This behavior can affect how you implement exclusion key rules.

If you have an exclusion key rule that uses a file extension to exclude files that may be opened and modified by such an application, exclude the temporary file name extension also. If you don't exclude the temporary file, the temporary file may be encrypted by another policy that matches the temporary file extension. Then the original file, which is copied from the temporary file, will be unreadable. Also keep in mind that other applications that may create temporary files with the same file extension and consider what policies should affect those temporary files.

This situation can happen with Microsoft Office files such as the `.docx` files used by Microsoft Word. When you open and modify a `.docx` file, Word creates a `.tmp` file version of that file. So for Microsoft Word you should add `*.tmp` to the exclusion key rule resource set if you add `*.docx`.

Rename Operations Crossing Key Rules (Linux)

On Linux, when a rename operation crosses key rules, the rename operation copies the source file to a new file using the new name and removes the original file. If the source file is flagged for exclusion key rule property, the target new file is disassociated with the exclusion key rule if the new name no longer matches the resource set associated with exclusion key rule. For more information, see [About the Exclusion Attribute for Files Matching an Exclusion Key Rule](#).

Using Linked Files with Exclusion Key Rules (Linux)

On Linux, do not create multiple hard links to the same target file, such that the pathname of each hard link is associated with a resource set of an exclusion key, and the key rules have different keys. Accessing the file through the pathname of each hard link results in a different key being applied to the file, resulting in data corruption in the target file due to the application of multiple keys to the same data.

If you must create hard links, be sure the hard link pathnames and the target file are within the same resource set.

Changing a Folder or Files from Versioned to Non-Versioned Key (Windows)

Exclusion key rules provide a way to convert a subset of guarded files or the contents of a folder from being encrypted by a versioned key to being encrypted by a non-versioned key. After this conversion, the excluded files or directory contents will be encrypted at the last version of the versioned key but the encryption keys for those items will not rotate to a new version when the keys for other non-excluded files are rotated. In other words, the excluded files or folder contents will be encrypted by a non-versioned key.

Follow these steps to change selected files or folder contents to a non-versioned key:

1. In the CipherTrust Manager, clone the versioned key that is used in the policy that you plan to edit. Cloning a key creates a non-versioned copy of the existing version of the versioned key.
2. In the CipherTrust Manager, disable the GuardPoint. Disabling the GuardPoint is required before modifying a

policy applied in that GuardPoint.

- Configure one or more resource sets to match the files that you want to exclude. For example, the resource set `star-dot-text` could contain `*.txt` and the resource set `sales-folder` could contain `\sales\*`.
- Add one or more exclusion key rules to convert matching files to a non-versioned key. In the following example, files matching `*.txt` and files in the `sales` folder (as defined in resource sets) will be converted from the current version of the versioned key `AES256_versioned` to `AES256_clone`, assuming `AES256_clone` is a clone of `AES256_versioned`.

Order	Resource	Current Key	Transformation Key	Exclusion Rule
1	star-dot-txt	AES256_clone	AES256_clone	Y
2	sales-folder	AES256_clone	AES256_clone	Y
3		clear_key	AES256_versioned	N

Exclusion key rules must be ordered before other rules.

- On the command line, run the following command to remove the LDT metadata from the files that you want to convert from versioned key to non-versioned key encryption:

```
voradmin ldt attr delete <path_to_files>
```

To recursively delete the LDT metadata from all files matching a pattern in all subfolders, use the following form, including `*` as a wildcard where needed:

```
voradmin ldt attr delete <path_to_files> -filter <filename>.<extension>
```

Note

Be careful when deleting the LDT metadata from files. If you delete the metadata from a file that does not match an exclusion key rule policy, the file will be unreadable after the next rekey.

Given the example exclusion key rule described in step 4, you would need to run this command on all files with the extension `.txt` (first example below) and on the files in `\sales` (second example below).

```
voradmin ldt attr delete c:\gp1 -filter *.txt
voradmin ldt attr delete c:\gp1\sales
```

For more information about using `voradmin` on LDT metadata, run `voradmin ldt attr /?` on the

command line.

6. In the CipherTrust Manager, re-enable the GuardPoint that includes the new exclusion key rule.
7. In the CipherTrust Manager, rotate the key for the policy that includes the new exclusion key rule.

Using the example exclusion key rule in step 4, after completing this procedure, files matching `*.txt` and files in the `sales` folder will have the exclusion attribute set and will be excluded from rekeying (see [About the Exclusion Attribute for Files Matching an Exclusion Key Rule](#)). Files not matching the exclusion key rule will be rekeyed to the next version of the `AES256_versioned` key.

To perform a similar conversion on Linux, see [Adding an Exclusion Key Rule to an Existing Policy with Versioned Keys \(Linux\)](#).

Examples of Exclusion Key Rules

This section describes some examples of how to use an exclusion key rule.

Encrypt Files With Exclusion Property Using a Non-Versioned Key

The following exclusion key rule applies the non-versioned key, `Key_TextFiles`, to any new files that are created with a `*.txt` extension.

Note

Existing `*.txt` files in the GuardPoint during the initial LDT data transformation process are assumed to be already encrypted with the same key that you specify in the exclusion key rule. These existing files are not transformed during the initial encryption or during any subsequent rekeys. The key you specify in the exclusion key rule is applied to new `*.txt` files only.

In the Policy, do the following:

1. Add a Key Rule.
2. In the **Resource Set** field, click **Select**.
3. Select a resource set that specifies *.txt in the File field and click the Exclude Rule** option.

Select Resource Set

Search

2 Results | 2 Resource Sets

+ Create Resource Set

Name	Updated At ↓	Description
☒ RS-all-txt-Files	06 Sep 2020, 19:02	Resource set for *.txt.
☐ LDT-Exclude	06 Sep 2020, 18:49	

2 Resource Sets 10 per page ▾

Exclude Rule: ☒

- Click **Select**. CipherTrust Manager displays the resource set name in the Resource Set field with an icon indicating that this is an Exclusion Rule.
- Select the **Key_TextFiles** key in the **Current Key Name** field.
- Click **Add**.
- Add any other key rules or exclusion key rules to the policy that you want. You must add at least one non-exclusion key rule that specifies the current encryption key and the versioned encryption key that you want to use with this Live Data Transformation policy.

For example, you could add another exclusion key rule that specifies all **.doc** files should be encrypted with the key **Key_DocFiles**, or one that specifies all **.zip** files should be left unencrypted by specifying the key **clear_key**.

Exempt Excluded Files from Encryption (Set to **clear_key**)

The following exclusion key rule sets all files in the resource set **/oxf-fs1/gp1/Clear_Files_Folder** (Linux) or **\oxf-fs1\gp1\Clear_Files_Folder** (Windows) to **clear_key** (in other words, not encrypted). Files in other directories that match other key rules in the same policy may be encrypted. This could allow unrestricted access to the files in **/oxf-fs1/gp1/Clear_Files_Folder** (Linux) or **\oxf-fs1\gp1\Clear_Files_Folder** (Windows) while access may be restricted to files in parallel directories.

- Linux Exclusion Key Rule: The Resource Set **Directory** field should contain **/oxf-fs1/gp1/Clear_Files_Folder**, and the **Key** should be **clear_key**.
- Windows Exclusion Key Rule: The Resource Set **Directory** field should contain **\oxf-fs1\gp1\Clear_Files_Folder**, and the **Key** should be **clear_key**.

Listing All Files Included in an Exclusion Key Rule (Linux)

Determining the files that match an exclusion key rule involves two steps. You list all the keys in a GuardPoint, choose the key that you're interested in, and then run a command to list the files that match that key. This process works for both standard key rules and exclusion key rules.

1. Decide on the GuardPoint that you want to check for excluded files. For example, for the GuardPoint `/oxf-fs1/gp1`, type the following on the command line:

```
voradmin ldt key report /oxf-fs1/gp1
LDT_KEY1,1
LDT_KEY2,2
LDT_KEY3,5
NON_VERSIONED_KEY
```

The number after the comma is the key version number. See [Key Report Option](#) for more information about the `voradmin` key report.

2. From the key report output, choose the key rule for which you want to list matching files. For example, to see the files associated with the `NON_VERSIONED_KEY` in the previous step, you would type:

```
voradmin ldt key map NON_VERSIONED_KEY /oxf-fs1/gp1
/oxf-fs1/gp1/file1.dat10
/oxf-fs1/gp1/file2.dat10
/oxf-fs1/gp1/file3.dat10
/oxf-fs1/gp1/file4.dat10
/oxf-fs1/gp1/file5.dat10
```

See [Key Map Option](#) for more information about the `voradmin` key map report.

Listing All Files Included in an Exclusion Key Rule (Windows)

Determining the files that match an exclusion key rule involves two steps. You list all the keys in a GuardPoint, choose the key that you're interested in, and then run a command to list the files that match that key. This process works for both standard key rules and exclusion key rules.

1. Decide on the GuardPoint that you want to check for excluded files. For example, for the GuardPoint `c:\gp1`, type the following on the command line:

```
C:\> voradmin ldt key report c:\gp1
Keys used for GP, c:\gp1 :
clear_key,0
CS1-LDT-AES256,11
```

The number after the comma is the key version number. The `clear_key` key is not versioned, so the version

number is 0.

- From the key report output, choose the key rule for which you want to list matching files. For example, to show the files associated with the `clear_key` listed above, you would type:

```
C:\> voradmin ldt key map c:\gp1 clear_key,0
Files rekey with key (clear_key,0)-
c:\gp1\file1.txt
c:\gp1\file2.txt
c:\gp1\file3.txt
c:\gp1\file4.txt
c:\gp1\file5.txt
```

Dynamic Resource Sets

The Dynamic Resource Set feature has been modified in CTE v7.8.0, with the inclusion of new key rules, when registered with CipherTrust Manager v2.17, or subsequent versions. The Dynamic Resource Set feature is also now available with Local File Systems, as well as NFS GuardPoints. Support for NFS is available starting with the patch release of CTE v7.7.100.

With Dynamic Resource Sets, you can now add a new key rule to a resource set that includes files that are not encrypted under the dynamic resource style policy. This results in the inclusion of those files for rekey and encryption. LDT launches rekey operations on the affected GuardPoints to encrypt the files associated with the resource set in the newly added key rule. Before inclusion of the key rule, those files associated with the resource set were in clear-text.

Following is an example of a policy applied to GuardPoint `/oxf-fs1/gp1` which includes subdirectories `dir1`, `dir2`, `dir3`, `dir4`. Applying this policy to `/oxf-fs1/gp1` will launch and rekey the files under `/oxf-fs1/gp1/dir1` and `oxf-fs1/gp1/dir2` using the specified key, while the remaining files in `/oxf-fs1/gp1` remain in clear-text. To rekey the files under `/oxf-fs1/gp1/dir3` and `/oxf-fs1/gp1/dir4`, you can update the policy as follows:



The screenshot shows the 'LDT-DYNRES-POL' configuration page. It has tabs for 'Local File Rules' and 'Key Rules'. Below the tabs is a table with 5 columns: 'Index', 'Resource Set', 'Current Key Name', 'Transformation Key Name', and 'Encryption Style'. There are 4 rows of data, each with a checkbox in the first column. At the bottom right, it says '4 Key Rules' and '10 per page'.

Index	Resource Set	Current Key Name	Transformation Key Name	Encryption Style
☐ 1	dir1	clear_key	LDT-KEY1	No
☐ 2	dir2	clear_key	LDT-KEY2	No
☐ 3	dir3	clear_key	LDT-KEY3	No
☐ 4	dir4	clear_key	LDT-KEY4	No

New resource sets were created for `dir3` and `dir4` before adding the new key rules in the policy. Once the updated policy is applied to the GuardPoint, the rekey is launched to encrypt the files associated with `/oxf-fs1/gp1/dir3` and `/oxf-fs1/gp1/dir4` using the encryption keys `LDT-KEY2` and `LDT-KEY3`, respectively. Remaining files in the GuardPoint remain unchanged.

New Key Rule

Files associated with resource sets are encrypted with the key specified in the corresponding key rule. Unlike files associated with the exclusion key rules, files not associated with any key rules are normally not encrypted, and not excluded from rekey, except under the few cases described below.

Following is an example of a policy applied to GuardPoint `/oxf-fs1/gp1` which includes subdirectories `dir1`, `dir2` and `dir3`. In this policy resource set, `dir1` has an exclusion key rule and resource set `dir2` has a key rule to encrypt from `clear` to `LDT-KEY-1`. Other subdirectories under `/oxf-fs1/gp1`, such as `dir3`, are not associated with any key rule.



The screenshot shows a web interface for configuring LDT-DYNRES-POL. It features a table with columns: 'Index', 'Resource Set', 'Current Key Rule', 'Transformation Key Rule', and 'Exclusion Rule'. There are two rows of data. The first row shows a resource set 'dir1' with a current key rule 'AES256' and an exclusion rule 'YES'. The second row shows a resource set 'dir2' with a current key rule 'LDT-KEY-1' and an exclusion rule 'NO'. A '+ Add Key Rule' button is visible in the top right corner of the table area.

Index	Resource Set	Current Key Rule	Transformation Key Rule	Exclusion Rule
1	dir1	AES256	AES256	YES
2	dir2	LDT-KEY-1	LDT-KEY-1	NO

Applying this policy to `/oxf-fs1/gp1` launches and rekeys the files under `/oxf-fs1/gp1/dir1` and `/oxf-fs1/gp1/dir2` using the specified key, while the files in `/oxf-fs1/gp1/dir3` remain in clear-text due to them not being associated with any key rule. This is reflected in the following examples for rekey statuses:

Example 1

```
voradmin ldt attr get /oxf-fs1/gp1/dir1/foo.txt
```

Example Response

```
LDT attributes: rekeyed_size=0, rekey_status=rekey_excluded
Key:      name=AES256, version=none
```

Example 2

```
voradmin ldt attr get /oxf-fs1/gp1/dir2/foo.txt
```

Example Response

```
LDT attributes: rekeyed_size=10485760, rekey_status=none
Key:      name=LDT-KEY-1, version=0
```

Example 3

```
voradmin ldt attr get /oxf-fs1/gp1/dir3/foo.txt
```

Example Response

```
LDT attributes: rekeyed_size=0, rekey_status=rekey_no_keyrule
Key:           name=clear_key, version=none
```

Rekeying

To rekey the files under `/oxf-fs1/gp1/dir3` you can update the policy as follows:



Once the updated policy is applied to the GuardPoint, the rekey launches to encrypt the files associated with `/oxf-fs1/gp1/dir3` using the encryption key LDT-KEY2. The remaining files in the GuardPoint remain unchanged.

Example

```
voradmin ldt attr get /oxf-fs1/gp1/dir3/foo.txt
```

Example Response

```
LDT attributes: rekeyed_size=10485760, rekey_status=none
Key:           name=LDT-KEY-2, version=0
```

As depicted above, the files previously marked as `rekey_no_keyrule` due to their association with a no rekey rule, were encrypted/rekeyed after adding the new key rule with the resource set that includes those files. Note that moving any of those files to other directories associated with key rule(s) for encryption will associate those files with the key rule corresponding to the target location, and consequently, encrypting those files in the new location under different key rules. Refer to the section below for the effect of operations, such as renaming files or directories or restoring files, to the association of the file with the resulting key rule.

Effect of Adding a New Key Rule Resulting in Rekey

Addition of a new key rule for encrypting the files associated with a resource set will increment the policy key version resulting in rekey launch on the affected GuardPoints.

Following is an example of a policy applied to GuardPoint `/oxf-fs1/gp1` which excludes subdirectory `dir1` and includes subdirectory `dir2` before adding a new key rule. The Policy Key Version is 19, before adding a new key rule.

Example

```
voradmin ldt attr get /oxf-fs1/gp1
```

Example Response

```
LDT stats: version=7, rekey_status=rekeyed
Number of times rekeyed:      1 time
Rekey start time:             2024/10/01 14:52:25
Last rekey completion time:   2024/10/01 14:52:25
Estimated rekey completion time: N/A
Policy key version:           19
Pushed Policy key version:    19
Policy ID:
    5e128f2c-3789-4985-85eb-b392c3108e25
Data stats:
    total=30.0MB, rekeyed=10.0MB
    truncated=0.0MB, sparse=0.0MB
File stats:
    total=3, rekeyed=1, failed=0
    passed=0, skipped=0, created=0, removed=0, excluded=2
```

After adding a new key rule resulting in launching rekey on the GuardPoint, the Policy Key Version of the GuardPoint changes to 20.



The screenshot shows the 'LDT-DYNRES-POL' configuration page. It has tabs for 'Security Rules' and 'Key Rules'. Below the tabs is a table titled 'Ordered Translated Key Rules'. The table has columns: 'ID', 'Resource ID', 'Custom Key Rule', 'Translation Key Rule', and 'Key Rule'. There are three rows of data. The first row has a green status icon. A '+ Add Key Rule' button is in the top right corner.

ID	Resource ID	Custom Key Rule	Translation Key Rule	Key Rule
1	1001	Custom Key Rule	AdmKey	Key
2	1002	Custom Key Rule	LDT Key 1	Key
3	1003	Custom Key Rule	LDT Key 2	Key

Example

```
voradmin ldt attr get /oxf-fs1/gp1
```

Example Response

```
LDT stats: version=7, rekey_status=rekeyed
Number of times rekeyed:      2 times
Rekey start time:             2024/10/01 14:54:57
Last rekey completion time:   2024/10/01 14:54:57
Estimated rekey completion time: N/A
Policy key version:           20
Pushed Policy key version:    20
Policy ID:
    5e128f2c-3789-4985-85eb-b392c3108e25
```

```
Data stats:
    total=30.0MB, rekeyed=10.0MB
    truncated=0.0MB, sparse=0.0MB
File stats:
    total=3, rekeyed=1, failed=0
    passed=1, skipped=0, created=0, removed=0, excluded=1
```

Feature changes for Dynamic Resource Sets after upgrading CipherTrust Transparent Encryption or CipherTrust Manager

CTE v7.6 does not differentiate between files that are not associated with any key rules, and with those associated with an exclusion key rule. As the result, files not associated with key rules are flagged as `rekey_excluded`, instead of `rekey_no_keyrule`. This behavior extends into CTE v7.7 if the CTE client is registered with CipherTrust Manager v2.16. Registering CTE v7.7, or a subsequent version, to CipherTrust Manager v2.17 or a subsequent version, enables CTE to differentiate between files associated with an exclusion key rule and those not associated with any key rule.

The following sections describe the effect of upgrading CipherTrust Transparent Encryption v7.6 and registration of a CTE client with CipherTrust Manager v2.16 and v2.17, and the new behavior when using Dynamic Resource Sets with CipherTrust Transparent Encryption v7.8.0 and CipherTrust Manager v2.17.

Scenario #1: CTE v7.6 client registers with CipherTrust Manager v2.16

When a CTE v7.6 client registers with CipherTrust Manager v2.16, or a previous version, and then CTE is upgraded to CTE v7.7, the behavior remains the same as in CTE v7.6. Note that the behavior in this scenario is that files not associated with key rules are marked as `rekey_excluded` instead `rekey_no_keyrule`.

Scenario #2: CTE v7.6 client registers with CipherTrust Manager v2.17 and then upgrades to CTE v7.7

Prior to upgrading CTE to v7.7, the files not associated with any key rule have already been marked with a `rekey_excluded` flag. As the `rekey_excluded` flag indicates exclusion from rekey, those files set to `rekey_excluded` must be reset to `rekey_no_keyrule` status after the upgrade.

If the user adds a new key rule immediately after upgrading CTE, before resetting the `rekey_excluded` flag, the files associated with the new key rule skip rekey. To avoid this, after CTE is upgraded to v7.7, run the `voradmin admin` command with the option `update-nokeyrule` to replace the `rekey_excluded` with `rekey_no_keyrule`.

Resetting `rekey_excluded` to `rekey_no_keyrule`

To reset the `rekey_excluded` to `rekey_no_keyrule` on the GuardPoint, type:

```
voradmin ldt attr update-nokeyrule ${gp}
```

Following is an example of a policy applied to GuardPoint `/oxf-fs1/gp1`, on a host with CTE v7.6, which excludes subdirectory `dir1` and includes subdirectory `dir2`.

Order	Resource Set	Current Key Name	Transformations Key Name	Exclusion Rule
1	HELLO	HELLO	HELLO	YES
2	HELLO	HELLO	LDT-HELLO	NO

In the following example, the file in `/oxf-fs1/gp1/dir3` remains in clear-text and `rekey_excluded`:

```
voradmin ldt attr get /oxf-fs1/gp1/dir3/foo.txt
```

Example Response

```
LDT attributes: rekeyed_size=0, rekey_status=rekey_excluded
Key:      name=clear_key, version=none
```

The file continues to remain in clear-text but is now marked as `rekey_no_keyrule`:

```
voradmin ldt attr get /oxf-fs1/gp1/dir3/foo.txt
```

Example Response

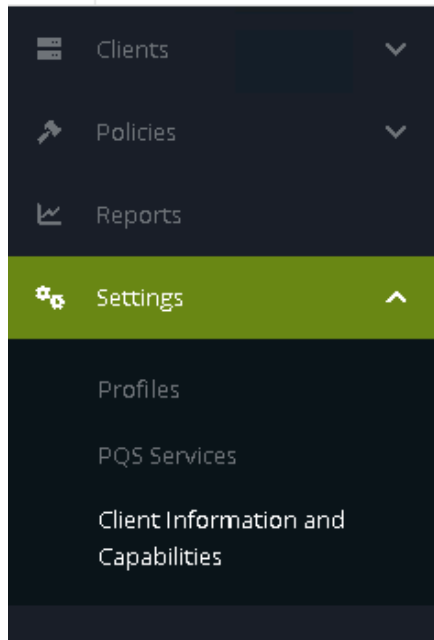
```
LDT attributes: rekeyed_size=0, rekey_status=rekey_no_keyrule
Key:      name=clear_key, version=none
```

Scenario #3: CTE v7.7 client registers with CipherTrust Manager v2.16, and then CipherTrust Manager is upgraded to v2.17, or a subsequent version

After upgrading CipherTrust Manager to v2.17, you **must** perform a capability synchronization between the CipherTrust Manager and all registered CTE agents.

To initiate a capability synchronization:

1. Go to CipherTrust Manager.
2. Click **Transparent Encryption > Settings > Client Information and Capabilities > Get Capability**



Client Information and Capabilities

Empty CTE Agent Information Log Volume ?

Remove Agent Information

Request Capabilities from All Clients ?

Get Capability

After the CipherTrust Manager upgrade is complete, the behavior remains the same as described above for CTE v7.7 with CipherTrust Manager v2.17 and subsequent versions.

File Operations Causing Key Rule Changes

Some file operations may result in changing the association of target files to a different key rule. For example, renaming a file associated with a key rule can result in changing the association. Renaming a directory can have the same result in a wider scope where all, or a subset of files, under the renamed subdirectory may share the resource set and be associated with the key rule of the resulting resource set. Another example is backing up and restoring files. Restoring a file into a different location in a GuardPoint will also change the association of the restored file to the key rule of the target location. Such operations will not only change the key rule association, but they may also change the rekey status and result in encrypting or decrypting data in the target file.

Files under an LDT policy are accessed based on their LDT attribute. As LDT attributes specify the rekey status and the encryption key applied to the data in target file, this information may not agree with the key rule associated with the file in the LDT policy.

Note

Be sure to understand the consequence of changing the association of target files to different key rules.

Restoring files Causing Key Rule Changes

As noted, restoring a file into a different location in a GuardPoint will change the association of the restored file to the key rule of the target location, as well as change the rekey status and data in the target file. The following table indicates how restoring files affects the key status and the key applied to the restored files.

- **Source Key Rule:** Key rule of the file at the time of backup
- **Target Key Rule:** Key rule of the file restored into the GuardPoint

Source Key Rule	Target Key Rule	Effect	Comment
rekey_excluded (Key A)	Encrypted Key B	rekey_excluded (Key A)	
rekey_excluded (Key A)	rekey_no_keyrule	rekey_no_keyrule (Key A)	Note 1
rekey_excluded (Key A)	rekey_excluded (Key A)	rekey_excluded (Key A)	
rekey_excluded (Key A)	rekey_excluded (clear_key)	rekey_excluded (Key A)	Note 2
rekey_excluded (clear_key)	Encrypted (Key B)	rekey_excluded (clear_key)	Note 3
rekey_excluded (clear_key)	rekey_no_keyrule	rekey_no_keyrule (clear_key)	Note 4
rekey_excluded (clear_key)	rekey_excluded (Key A)	rekey_excluded (clear_key)	Note 3
rekey_excluded (clear_key)	rekey_excluded (clear_key)	rekey_excluded (clear_key)	
rekey_no_keyrule	Encrypted (Key A)	rekey_no_keyrule, Encrypted Key A	Note 5
rekey_no_keyrule	rekey_no_keyrule	rekey_no_keyrule	
rekey_no_keyrule	rekey_excluded (clear_key)	rekey_excluded (clear_key)	
rekey_no_keyrule	rekey_excluded (Key A)	rekey_excluded (clear_key)	Note 3
Encrypted (Key A)	rekey_no_keyrule	rekey_no_keyrule (Key A)	Note 6
Encrypted (Key A)	Encrypted (Key A)	Encrypted (Key A)	
Encrypted (Key A)	rekey_excluded (Key B)	rekey_excluded (Key A)	Note 7
Encrypted (Key A)	rekey_excluded (clear_key)	Local - rekey_excluded (clear_key) NFS – rekey_excluded (Key A)	Note 8

Note

1. **rekey_excluded:** Status not preserved and changes to **rekey_no_keyrule**.
2. **rekey_excluded:** Status preserved, data remains encrypted.
3. **rekey_excluded:** Status preserved; however, data remains clear despite the key rule associated with the target location.

4. **rekey_excluded**: Status is not preserved.
5. **rekey_no_keyrule**: Status preserved on the restored file; however, the file will be encrypted during the next rekey process.
6. **rekey_no_keyrule**: Status preserved on the restored file; however, data in the file remains encrypted.
7. **rekey_excluded**: Status preserved; however, data remains encrypted to the same key despite the key rule associated with the target location.
8. Different results between GuardPoints on local and NFS.

Renaming files and shared key rules

The following table displays the results of renaming files affecting the key status and the key applied to the file under the new name. Note that renaming files may change the association of the file to another resource set.

Source Key Rule	Target Key Rule	Effect	Comment
Encrypted (Key A)	rekey_excluded (clear_key)	rekey_excluded (clear_key)	
Encrypted (Key A)	rekey_no_keyrule	rekey_no_keyrule (clear_key)	
Encrypted (Key A)	rekey_excluded (Key A)	rekey_excluded (Key A)	
Rekey_excluded (clear_key)	Encrypted (Key A)	Rekey_excluded (clear_key)	
Rekey_excluded (clear_key)	rekey_no_keyrule	Rekey_excluded (clear_key)	
Rekey_excluded (clear_key)	rekey_excluded (Key A)	Rekey_excluded (clear_key)	
Rekey_excluded (Key A)	Encrypted (Key A)	Rekey_excluded (Key A)	
Rekey_excluded (Key A)	rekey_no_keyrule	Rekey_excluded (Key A)	
Rekey_excluded (Key A)	Rekey_excluded (clear_key)	Rekey_excluded (Key A)	
Rekey_no_keyrule	Encrypted (Key A)	Rekey_no_keyrule Encrypted (Key A)	Note 1
Rekey_no_keyrule	Rekey_excluded (Key A)	Rekey_no_keyrule	Note 2
Rekey_no_keyrule	Rekey_excluded (clear_key)	Rekey_no_keyrule	

Note

1. **rekey_no_keyrule**: Preserved after file rename; however, the file will be encrypted during the next rekey process.
2. **rekey_no_keyrule**: Preserved after file rename; however, data remains clear despite the key rule associated with the target location.

Renaming directories and shared key rules

The following table indicates the result of renaming directories affecting the key status and the key applied to each file under the new directory pathname. Note that renaming files may change the association of the file to another resource set.

Source Key Rule	Target Key Rule	Effect	Comment
Encrypted (Key A)	rekey_excluded (clear_key)	Encrypted (Key A)	Note 1
Encrypted (Key A)	rekey_no_keyrule	Encrypted (Key A)	Note 1
Encrypted (Key A)	rekey_excluded (Key A)	Encrypted (Key A)	Note 1
Rekey_no_keyrule	Encrypted (Key A)	Rekey_no_keyrule Encrypted (Key A)	Note 2
Rekey_no_keyrule	rekey_excluded (clear_key)	Rekey_no_keyrule	
Rekey_no_keyrule	rekey_excluded (Key A)	Rekey_no_keyrule	Note 3

Note

1. **rekey_status** and **encryption key**: Do not immediately change after rename. During the next rekey process, LDT will decrypt the data in the renamed directory and set the **rekey_status=rekey_excluded** or **rekey_status=rekey_no_keyrule** to match the rekey status of the target key rule.
2. **rekey_status** and **encryption key**: Do not immediately change after rename. During the next rekey process, LDT will encrypt the data in the rename directory.
3. **rekey_no_keyrule**: Preserved after directory rename; however, data remains clear despite the key rule associated with the target location.

Using LDT with SAP HANA Fibre Channel Systems (Linux Only)

You must add additional CTE commands to the HANA administrator entry. To do so, edit the `/etc/sudoers` with a text editor and add entries for `/usr/bin/voradmin` and `/usr/bin/vmsec`:

Example:

```
hanadm ALL=NOPASSWD:
/usr/bin/secfsd,/usr/bin/voradmin,/usr/bin/vmsec,/sbin/multipath,/sbin/multipath
d,/etc/init.d/multipathd,/usr/bin/sg_persist,/bin/mount,/bin/umount,/bin/kill,/us
r/bin/lsof,/sbin/vgchange,/sbin/vgscan
```

If you are using an ext3 file system, you must mount it with extended attributes. To do so, edit the storage section of the `global.ini` file using a text editor and add the following lines:

```
partition_*_data__mountOptions = -o user_xattr
partition_*_log__mountOptions = -o user_xattr
```

LDT Administration

This section contains the following topics:

- LDT Metadata in Extended Attributes
- DFS(R) and Replication (Windows)
- Backing Up and Restoring LDT GuardPoints
- LDT Command-Line Administration: voradmin command
- Migrating a GuardPoint to a Different LDT Policy
- Removing LDT and Security Encryption
- Uninstalling the Agent while LDT is Rekeying GuardPoints
- Detecting Loss of NAS connection to an LDT GuardPoint Group

LDT Metadata in Extended Attributes

An *extended attribute* is a name/value pair permanently associated with a file or directory stored in a file system. CipherTrust Transparent Encryption (CTE) creates and maintains its own user extended attributes on LDT GuardPoint directories and files. The extended attributes are used to store metadata related to each file or directory that is protected using an LDT policy.

On Linux, LDT sets extended attributes on GuardPoint directories. The LDT attribute of an LDT GuardPoint stores the following metadata:

- Current key version.

-
- Rekey status.
 - Rekey start and end times.
 - Estimated completion time.
 - Total amount of data transformed.
 - Total number of files transformed.
 - Current key signature and applied key signature.

On both Linux and Windows, LDT sets extended attributes on files. The LDT attribute of a file stores the following metadata:

- Name of the current key.
- Name of the versioned key.
- Version number of the versioned key.
- LDT rekey status of the file.

In most cases, the current and new key names are the same. The exception is during initial transformation from a legacy policy to an LDT policy, when the file has been encrypted with the current key and is being transformed to the current version of the transformation key.

Note

Before you set up a GuardPoint for LDT, ensure that there is sufficient disk space available in your file system for LDT metadata. The amount of disk space you need depends on the number of files in your GuardPoint. For more information about the disk space requirement, see [Planning for LDT Attribute Storage](#).

The state of a file changes during LDT operations. The extended attributes are continually updated to reflect the current file status, which falls into one of the following categories:

- Rekeyed to the current version of the key.
- Rekeyed to the previous version of the key, or the initial key state (before the first LDT rekey has been performed).
- Partially rekeyed, where some regions of the file are rekeyed to the new key version and other regions are still keyed to the previous key version or the initial key.

Listing Extended Attributes

You can list extended attributes of files by using native operating system commands, or system calls. As part of GuardPoint administration, CTE can modify or delete extended attributes.

Note

This functionality is only available for local file systems. It is not supported for files in NFS Share GuardPoints.

In Linux, LDT attributes are set on GuardPoint directories and regular files in GuardPoint directories protected with LDT policies. The CTE extended attribute name is `::secfs:xattr:`.

The following examples use the native Linux operating system command `attr` to display the LDT attribute for the GuardPoint `/oxf-fs1/gp1` and the file `/oxf-fs1/gp1/File_1.txt`.

Example Getting File Attributes

```
attr -l /oxf-fs1/gp1/File_1.txt
Attribute "::secfs:xattr:" has a 1044 byte value for /oxf-fs1/gp1/File_1.txt
Attribute "selinux" has a 37 byte value for /oxf-fs1/gp1/File_1.txt
```

Example Getting GuardPoint Attributes

```
attr -l /oxf-fs1/gp1
Attribute "::secfs:xattr:" has a 1044 byte value for /oxf-fs1/gp1
Attribute "selinux" has a 37 byte value for /oxf-fs1/gp1
```

Example of `voradmin ldt attr get` for Linux File Attributes

In the following example, the file `/oxf-fs1/gp1/File_1.txt` has the same name for current and new keys at the same key version. In the following example, if the versioned key `LDT_KEY` is at version 755, the file is rekeyed to the latest key version under the LDT policy.

```
voradmin ldt attr get /oxf-fs1/gp1/File_1.txt
LDT attributes: rekeyed_size=4096, rekey_status=none
Key:    name=LDT_KEY, version=755
```

Example of `voradmin ldt attr get` for Linux GuardPoint Attributes

The following is example of an LDT attribute on a GuardPoint directory on Linux:

```
voradmin ldt attr get /oxf-fs1/gp1
LDT stats: version=1, rekey_status=rekeying
  Number of times rekeyed:      3 times
  Rekey start time:             2018/08/04 16:24:45
  Last rekey completion time:   2018/07/04 16:24:04
  Estimated rekey completion time: N/A
  Policy key version:           2043
Data stats:
  total=3.3GB, rekeyed=1.5GB, truncated=0.0MB
File stats:
  total=4307, rekeyed=1181,
  passed=2, skipped=0, created=0, removed=0
```

Example of `voradmin ldt attr get` for Linux NFS Share GuardPoint Attributes

The following example shows how to use the `voradmin ldt attr get` command to view the LDT attribute on GuardPoint directories over NFS shares:

```
secfsd -unguard /nfs-oxf-fs1/gp2
secfsd: Path is not guarded
voradmin ldt attr get /nfs-oxf-fs1/gp2
LDT stats: version=3, rekey_status=rekeyed
  Number of times rekeyed:          1 time
  Rekey start time:                2021/01/04 08:19:02
  Last rekey completion time:      2021/01/04 08:19:03
  Estimated rekey completion time: N/A
  Policy key version:              0
  Policy ID:                       23785
  Data stats:
    total=0.0MB, rekeyed=0.0MB
    truncated=0.0MB, sparse=0.0MB
  File stats:
    total=3, rekeyed=1, failed=0
    passed=0, skipped=0, created=0, removed=0, excluded=0
```

Example of `voradmin ldt attr get` for Windows GuardPoint Attributes

The attribute for the GuardPoint `c:\GP 1` contains the status (rekeyed) and statistics specific to the GuardPoint and LDT. Following is sample output of `voradmin` command on Windows for statistics on a file:

```
C:\> voradmin ldt attr get c:\GP\Test.txt
LDT attributes:
  Rekey Status      Rekeyed
  Initial Rekeyed Size 10 Bytes
Key:
  Key Name/Version    (LDT_KEY, 28)
```

The attribute for GuardPoint `C:\GP` contains the status (rekeyed) and statistics specific to the GuardPoint and LDT:

```
C:\> voradmin ldt attr get c:\gp\
LDT Stats
-----
  Rekey Status          LDT_ST_REKEYED
  Last rekey completion time 10/2/2017 4:26:50
  Rekey Start time        10/2/2017 4:26:17
  Estimated rekey completion time 000:00:00

File Stats:
  Total      444
  Rekeyed    444
  Skipped     0
  Errored    0
  Passed     0
  Removed    0

Data Stats:
  Total      11 GB (12649143417 Bytes)
```

```
Rekeyed    11 GB (12649143417 Bytes)
Truncated  0 Bytes
```

Example of `voradmin ldt attr get` for Windows CIFS Share GuardPoint Attributes

The following example shows how to get the LDT attributes for the CIFS GuardPoint `\\myhost\share\HR-Files\`.

```
C:\>voradmin ldt attr get \\myhost\share\HR-Files\

Live Data Transformation Stats
-----

Rekey Status          LDT_ST_REKEYED
Last rekey completion time 2/24/2021 13:42:40
Rekey Start time       2/24/2021 13:36:47
Estimated rekey completion time 000:00:00

File Stats:
Total      19087
Rekeyed    19087
Skipped     0
Errored     0
Passed      0
Removed     0
Excluded    0

Data Stats:
Total      1 GB (1083187108 Bytes)
Rekeyed    958 MB (1005006756 Bytes)
Truncated  0 Bytes
```

Example of `voradmin ldt attr get` for Windows CIFS Share File Attributes

The following example shows how to get the LDT attributes for the file `employees.doc` on the CIFS share `\\myhost\share\HR-Files\`.

```
C:\>voradmin ldt attr get \\myhost\share\HR-Files\employees.doc

LDT attributes:
Rekey Status      Rekeyed
Initial Rekeyed Size 0 Bytes

Key:
Key Name/Version   (AES_256_LDTKey_CBC,15)
```

MDS File (Linux)

In addition to LDT attributes, the LDT process on Linux requires persistent storage for additional metadata related to encrypting, or rekeying, files in GuardPoints. LDT allocates the storage space as soon as the LDT process starts on a GuardPoint. It maintains this storage space during the entire transformation process, until the GuardPoint is completely transformed.

Storage for this metadata is allocated and managed in a special file, called the MDS (metadata store) file. The

MDS file resides inside a GuardPoint directory so each GuardPoint has its own MDS file.

The MDS file is a CTE protected file with the name `__vorm_mds__`. For example:

```
ls -l /oxf-fs1/gp1/__vorm_mds__
-rwxr-xr-x. 1 root  root 31754474496 Dec  8 09:09 /oxf-fs1/__vorm_mds__
du -B 1024 /oxf-fs1/gp1/__vorm_mds__
25056    /oxf-fs1/__vorm_mds__
```

As shown above, the MDS file is sparse. In the example, the file size is approximately 30GB, however the file is allocated with approximately 25MB of disk storage. LDT automatically creates the MDS file the first time the LDT process starts on any GuardPoint in the file system namespace. It populates the MDS file with all of the metadata for the GuardPoint at the beginning of the LDT process. Disk space allocated to the MDS file is freed and the MDS file in the GuardPoint directory is removed when the LDT process completes on the GuardPoint.

Warning

The MDS file is protected. You cannot remove it unless the administrator runs the `voradmin` command to manually remove the MDS file once it is no longer needed. See [Deleting LDT Metadata \(Linux\)](#) for more information.

LDT automatically allocates and de-allocates disk space for the MDS file as part of the LDT process. De-allocation of disk space for a GuardPoint does not change the MDS file size, although it frees the disk blocks. MDS files are sparse and very large in size. The MDS file is automatically removed from GuardPoints when the files have been successfully rekeyed.

Note

The metadata storage (MDS) file name has changed from `__vorm_mds__` to `__vorm_mds__`. GuardPoints will automatically rename the MDS file when guarding with a CTE 7.6.0 agent. LDT NFS GuardPoints will rename once all of the hosts, with the same share guarded, have been upgraded.

Planning for LDT Attribute Storage

Before a GuardPoint is enabled for LDT, make sure that there is sufficient free disk space in the file system to which the GuardPoint belongs. Free space is required for LDT attributes and (in Linux) metadata in the MDS file. LDT attributes are created during the initial encryption and are never freed until the GuardPoint is permanently unguarded and removed from the protection of an LDT policy. In contrast, disk space for metadata in the MDS file is temporary, kept only during the live transformation process.

When planning how much free disk space to reserve for LDT on a GuardPoint, consider the following:

- Number of files in the GuardPoint
- (Linux) Average length of absolute pathnames of files in the GuardPoint

The LDT process pre-allocates disk space for the Linux MDS file based on a minimum of 200K files with an average pathname of 1024 bytes per GuardPoint. The minimum space amounts to 325MB of disk space for the

MDS file for each GuardPoint, even if file count is very low. (In Windows, LDT reserves the space when the file is rekeyed.)

Using voradmin To Estimate Disk Space Required for LDT

In **Linux**, you can use the `voradmin ldt space` command to estimate the amount of disk space required for LDT attributes and the MDS file. The result is rounded to the nearest MB. The syntax of the command is:

```
voradmin ldt space <guard path>
```

Note

In **Windows**, LDT requires 10% of the underlying file system space, or a minimum of 2GB disk space, for LDT to start.

The following example shows how to estimate the required disk space to perform CipherTrust Transparent Encryption - Live Data Transformation on 1501 files in the GuardPoint `/oxf-fs1/gp1`. Estimate the disk space before protecting `/oxf-fs1/gp1` using an LDT policy. For example:

```
voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 1501 files without LDT extended attributes
LDT disk space requirements: total 169MB (LDT attributes=6MB, MDS=163MB)
```

The `voradmin` command reports that 1501 files in `/oxf-fs1/gp1` without LDT attributes. These files are new to LDT. 6MB of space is required for the LDT extended attributes and 163MB for metadata in the MDS file.

The following example shows the output of the same command after encryption completes. This estimates the additional disk space needed for the next LDT rekey operation. For example:

```
voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 0 files without LDT extended attributes
LDT disk space requirements: total 163MB (LDT attributes=0MB, MDS=163MB)
```

The `voradmin` command still reports on the same 1501 files, but because encryption has occurred using LDT, the files all have their LDT attributes. No additional space is required for LDT extended attributes on the next run. However, since the MDS file is transient and deletes after it finishes encrypting the GuardPoint, it requires additional space for the next key rotation.

Note

Windows estimates space using the following equations:

```
Permanent Space = Number of Files * 4K
Temporary Space = 128K * (Number of CPU * 2)
```

Displaying Metadata

Use the following command to see LDT file attributes or GuardPoint attributes:

```
voradmin ldt attr get [<file name path> | <guard path>]
```

For an overview of `voradmin ldt`, see [LDT Command-Line Administration: voradmin command](#).

Verifying Metadata (Windows only)

Use the following command to verify if the metadata is corrupt:

```
voradmin ldt attr verify [<file name path> | <guard path>]
```

For an overview of `voradmin ldt`, see [LDT Command-Line Administration: voradmin command](#).

DFS(R) and Replication (Windows)

The Distributed File System Replication (DFS(R)) service is a multi-master replication engine used to maintain synchronized folders on multiple servers. Replicating data to multiple servers increases data availability and provides users in remote sites with fast, reliable access to files.

If you are creating GuardPoints in a DFS(R) environment, you must first add the DFS(R) private folder guard path to the exclusion list in the Windows Registry. LDT should not attempt data transformation on this read-only directory.

1. Using the Registry Editor, or the Windows command line, add a registry entry in: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Vmmgmt\Parameters` named "LDTEXCLUSIONGPLIST" of type REG_MULTI_SZ.
2. Add the `DfsrPrivate` and `System Volume Information` directory path to the `LDTEXCLUSIONGPLIST`.

For example, if the DFS(R) private directory path is `D:\data\DfsrPrivate`, add this string in `LDTEXCLUSIONGPLIST`.

3. Reboot the system to make the change take effect.

Note

LDT does not perform a rekey on the DFS(R) private directory. Its rekey status is always "N/A".

If an application, or user, is performing a rename or a delete folder operation inside a GuardPoint with an LDT policy, this may restart the rekey process. Files which are already rekeyed will not be rekeyed again.

- If a rename or a delete operation is already performed on rekeyed files/folder, then the rekey process does not

restart.

- If a rename or delete operation is performed in a folder where a rekey is in progress, LDT needs to stop the rekey process and restart the rekey again.

Backing Up and Restoring LDT GuardPoints

This section describes procedures and considerations related to backing up and restoring data in LDT GuardPoints.

In addition to the files in a GuardPoint, LDT stores metadata in extended file attributes. These LDT attributes contain information that is required for decrypting the files and for the proper operation of LDT. Therefore, it is critical that your backup application also backs up the extended attributes of the files along with file data.

Related Topics

- [Clear Text Backup and Restore](#)
- [Encrypted Backup and Restore](#)
- [LDT Policy for Encrypted Backup and Restore](#)
- [Backup/Restore of Metadata Store File \(MDS\) in GuardPoints Undergoing Rekey](#)
- [Restore an Encrypted Backup](#)
- [Restoring Non-LDT Backup Data to an LDT GuardPoint](#)
- [Using fsfreeze \(Linux only\)](#)
- [LDT Backups Using a File System or Storage-Level Snapshot Tool](#)
- [Windows Backup and Snapshots](#)
- [LDT Backup and Restore Troubleshooting](#)

Note

For backing up and restoring a CTE LDT over NFS GuardPoint, see [Backup and Restore LDT on NFS GuardPoints](#).

Clear Text Backup and Restore

A policy that applies a Security Rule with the Apply Key effect on backup/restore operations does not require any special rules for data access by backup applications. Under such a policy, backup applications always read clear data and store clear data in backup media. The backup application is not required to back up the LDT extended attributes, and a QoS schedule is not required to suspend LDT during backups.

Encrypted Backup and Restore

Note

Only the host designated as the primary host for an LDT GuardPoint Group can perform encrypted backup or restore operations on GuardPoints over NFS.

When a policy does not enforce a Security Rule with the Apply Key effect on backup/restore operations, the policy does not decrypt data on I/O operations from that backup application. Under such a policy, the backup application stores encrypted data and the LDT extended attributes of the file on the backup media.

In Linux, LDT operations must be suspended during backup. Suspending LDT completes the ongoing rekey operations on regions of files before starting the backup. During live transformation, LDT first preserves those regions of a file to be rekeyed in the MDS file. Then it updates some of the metadata in order to update the status of the data preserved in the MDS file in preparation for the rekey. Then it starts rekeying and updating those regions in the underlying file.

Suspending LDT waits for ongoing rekey operations to complete, and saves the metadata in the LDT extended attribute section of the MDS file. Suspending LDT ensures that the rekey status stored in the LDT extended attribute accurately reflects the rekey status of the data in the entire file during backup.

Note

This requirement does not apply to LDT for Windows.

The following table summarizes the state of the data in files in backup media:

LDT State of File	Security Policy	Backup Metadata or Alternate Data Streams Along with File data	Effect
Not rekeyed	Permit	Yes	Data in backup may be in clear format or encrypted with older key version.
Rekey in progress	Permit	Yes	File in backup storage is partially rekeyed. Some parts are in clear format or encrypted with older key version, and other parts are encrypted with current key version.
Rekey complete	Permit	Yes	File in backup storage is in the encrypted format with new key version.

LDT Policy for Encrypted Backup and Restore

Suppose you have an LDT policy allowing a backup user, or a backup process, to perform an encrypted backup. The backup user, or the backup process, reads encrypted data from files and stores the same encrypted data in backup media.

For example, suppose you wanted to back up GuardPoint `/oxf-fs1/gp1` protected by `My_LDT_Policy_1`. The key version before the key rotation is 8. The following steps occur:

1. Key version 8 expires and is rotated to version 9.
2. Rotating the encryption key triggers LDT to start running on the data under the GuardPoint.
3. The QoS schedule suspends LDT because a backup process is running.
4. The backup process begins, runs and later ends.
5. The QoS schedule resumes LDT.
6. LDT on the GuardPoint completes.

Note

Although the backup/restore scenarios and examples described in the rest of this section are specific to LDT on Linux platform, the concepts also apply to LDT on the Windows platform.

Consider the state of the three files in the GuardPoint during the LDT process, right after LDT is suspended in preparation for the backup. You can obtain the state of each file through the `voradmin ldt attr get` command, which examines the LDT state of each file captured in the LDT extended attributes of those files. (For an overview of `voradmin LDT`, see [LDT Command-Line Administration: voradmin command](#)).

- *File_1.dat* is rekeyed/encrypted to completion. The applied and new key versions are at version 9 of the key.

```
voradmin ldt attr get /oxf-fs1/gp1/data_files /file_1.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9
```

- *File_2.dat* is partially rekeyed/encrypted. The applied key version is at version 8 and the transformation key is at version 9.

```
voradmin ldt attr get /oxf-fs1/gp1/data_files/file_2.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=rekeying, state_saved
Current Key:    name=LDT_AES256_KEY, version=8
New Key:        name=LDT_AES256_KEY, version=9
```

- *File_3.dat* has not been rekeyed/encrypted. The applied key and transformation key are both at version 8,

which is the version before the current key rotation.

```
voradmin ldt attr get /oxf-fs1/gp1/data_files/file_3.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=8
```

While LDT is suspended on the GuardPoint, the backup process starts and archives these three files, including extended attributes, in the backup media.

```
my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_1.dat \
  /backup-media/oxf-fs1/gp1/data_files/file_1.dat
my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_2.dat \
  /backup-media/oxf-fs1/gp1/data_files/file_2.dat
my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_3.dat \
  /backup-media/oxf-fs1/gp1/data_files/file_3.dat
```

Note

- On Linux platforms, you must perform backups on a GuardPoint during periods when LDT is not actively transforming data in the GuardPoint. You must schedule backups in conjunction with LDT schedules or during periods when LDT is paused. Make sure to coordinate with the backup administrator and schedule accordingly.
- If the preferred method of backup is to create device level snapshots of the file system on the managed host or in the storage array subsystem, you must ensure that the schedule for creating snapshots pauses LDT before a snapshot is created.

Backup/Restore of Metadata Store File in GuardPoints Undergoing Rekey

- Restoring a GuardPoint from a Backup
- Potential Warnings During Restore Operation

Backing up an entire GuardPoint using commands such as `cp`, `tar`, or `rsync`, or even commercial backup products that sweep the file system namespace for backing up files is supported. This method of backup performed while LDT is in progress over GuardPoints poses some challenges when files in GuardPoints are backed up in an encrypted format. The challenge with this method of backup is the existence of the LDT Metadata Store file (MDS) in the GuardPoint during the backup or restore process, and strict protection enforced on MDS files preventing deletion or modification to MDS files.

Secondly, your backup utility must backup and restore extended attributes of files and the GuardPoint directory. Because LDT extended attributes are also protected similarly to MDS files, your backup must be enabled to restore extended attributes for files. To overcome both restrictions, your policy on the GuardPoint must include a security rule without Apply Key Effect to enable your backup utility to replace MDS files, and LDT extended attributes for files, as part of backup/restore operations. Additionally, your backup utility must be signed with a signature set from CipherTrust Manager for added security, and be executed with the option to preserve extended attribute options available with the standard Linux utilities.

The following table lists the supported backup utilities, required options to preserve extended attributes, and supported versions of the utilities.

Command	Required options	Supported version
cp	--preserve=all	OS default
tar	--xattrs	OS default
rsync	-vapIXWP --inplace	OS default
netbackup	overwrite existing files	v7.6.1 and v7.7.3

You can also backup and restore GuardPoint data, including the MDS file, if the requirements listed above on the backup utility are satisfied.

Note

You must suspend LDT on the GuardPoint before performing a backup or restore.

You can check your GuardPoint to determine if you can use this method of backup. If the directory of your GuardPoint is a mount point, MDS files reside inside your GuardPoint and you can use this method of backup for backing up or restoring your GuardPoint. However, GuardPoint directories below file system mount points must be checked and verified to use this method of backup. To verify, you can run the `voradmin` command to determine the MDS file associated your GuardPoint.

Example:

```
voradmin ldt list all
MDS_1: type=file, nguards=1, name=/oxf-fs1/gp1/__vorm_mds__

Guard Table: version 1 nentries 1
Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/oxf-fs1/gp1
File List: count 4308
```

You cannot restore to a GuardPoint during LDT, even after suspending LDT. Restoring to a GuardPoint in rekeying state will result in loss of data and potentially, data corruption. Follow the steps below to perform a full level restore of the GuardPoint.

Restoring a GuardPoint from a Backup

To properly restore GuardPoints along with the MDS file:

1. With the same tool that was used for backup, restore to the GuardPoint.
2. Once restore is complete, the GuardPoint needs to be disabled and enabled again. For manual GuardPoint, run the `secfsd` command as shown below. For auto-guards, disable and enable GuardPoints on CipherTrust Manager.

```
# secfsd -unguard <${gp}>
# secfsd -guard <${gp}>
```

- Disabling GuardPoint will remove the MDS file restored to the GuardPoint and flag the GuardPoint for RELAUNCH to restart LDT. Although the restored MDS file includes critical metadata for execution of LDT, the restored file does not hold data for any files in partial rekeyed status at the time the MDS file is restored. As such, the restored MDS file is automatically removed when GuardPoint is disabled. Once the GuardPoint is enabled, LDT is automatically relaunched on the GuardPoint as the result of RELAUNCH flag. Relaunching LDT will encrypt every file to the latest key version under LDT policy.

Potential Warnings During Restore Operation

When using `cp` for backup/restore, the `cp` command may report a failed attempt to preserve permissions on the Metadata Store File (MDS) during a restore. If you encounter the below message, continue to proceed with the restore steps since this will not affect the MDS file or dataset that is being restored.

```
cp: preserving permissions for '/oxf-fs1/gp1/__vorm_mds__ ': Permission denied
```

When using `rsync` for backup/restore, the `rsync` command may report a failed attempt to set extended attribute when restoring the MDS file on system with selinux configured in enforced mode. If user encounters the below message, continue to proceed with the restore steps since this will not affect the MDS file or dataset that is being restored.

```
rsync: copy_xattrs: lsetxattr("/oxf-fs1/gp1/__vorm_mds__ ", "security.selinux") failed: Permission denied (13)
rsync: rsync_xal_set: lsetxattr("/oxf-fs1/gp1/__vorm_mds__ ", "security.selinux") failed: Permission denied (13)
```

Restore an Encrypted Backup

[Restore a File Fully Rekeyed to the Latest Key Version](#)

[Restore a Partially Rekeyed/encrypted File](#)

[Restore a File Not Rekeyed/encrypted with an Older Key Version](#)

This section illustrates restoration of the three files from the backup media to the same GuardPoint, `/oxf-fs1/gp1`. The files are restored to a different directory under the GuardPoint.

Restore a File Fully Rekeyed to the Latest Key Version

Recall that *file_1.dat* was archived in the backup media when it was fully rekeyed to version 9 of the key. As the current version of the key is also 9, *file_1.dat* is restored from backup without any changes. After restoring the file, the state of the restored file and its applied and current key versions remain unchanged, as compared to the original file that was backed up.

```
my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files \
```



```

/file_1.dat /oxf-fs1/gp1/restored_files/file_1.dat

voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_1.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9

voradmin ldt attr get /oxf-fs1/gp1/data_files/file_1.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9

```

Restore a Partially Rekeyed/encrypted File

Recall that *file_2.dat*, archived in the backup media, was partially rekeyed between versions 8 and 9. As the current version of the key was 9 at the time of backup, *file_2.dat* is restored to the GuardPoint with the same version of the key from the time of backup. The file is flagged for *lazy rekey*, meaning that a background rekey operation is scheduled to transform the file to the latest key version the next time an application tries to access the file.

At the completion of restoration, the file is fully transformed to the key version (v9). The key version is also the latest one in the policy. Although the file is flagged for lazy rekey (LAZY_RK), the file does not need to be transformed to the latest key version because it's already there. Had the file been partially rekeyed from version 7 to version 8 of the key at the time of backup, the restored file would have completed rekeying to version 8 at the end of the restoration. Therefore, the LAZY_RK flag would initiate a background transformation to update the key version to the latest key version when the file is accessed.

If this file is not accessed by any application, the file remains unchanged in the GuardPoint. It is not transformed to the latest key version. To trigger a rekey, access the file with an application, such as a file explorer.

- Access the file with an application, such as a file explorer.

```

my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files/ \ file_1.dat /oxf-fs1/gp1/restored_files/
file_2.dat

```

```

voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_2.dat LDT attributes: rekeyed_size=1440743424,
rekey_status=lazy_rekey Key: name=LDT_AES256_KEY, version=9

```

```

voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_2.dat LDT attributes: rekeyed_size=1440743424,
rekey_status=none Key: name=LDT_AES256_KEY, version=9

```

Restore a File Not Rekeyed/encrypted with an Older Key Version

Recall *file_3.dat* was archived in the backup media when it was keyed to version 8 of the key, one version below the latest version at the time of backup. At completion of the restoration, *file_3.dat* is restored from backup to the same version, version 8, that it was keyed to when it was backed up.

However, the file is flagged for lazy rekey. After restoring the file, it is keyed to version 8 and flagged for lazy rekey (LAZY_RK). The file is rekeyed to the latest key version, version 9, as soon as an application accesses the file. If this file is not accessed by any application, the file remains unchanged in the GuardPoint.

```

my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files \
/file_3.dat /oxf-fs1/gp1/restored_files/file_3.dat

```

```

voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_3.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=lazy_rekey
Key:      name=LDT_AES256_KEY, version=8

sum /oxf-fs1/gp1/restored_files/file_3.dat
39994 1406976

voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_3.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9

```

Restoring Non-LDT Backup Data to an LDT GuardPoint

This section describes how to restore data encrypted with a non-versioned key to an LDT GuardPoint.

If the backup was performed with the Apply Key effect, the backup files are in clear text. Simply restore the clear text files to the LDT GuardPoint with the Apply Key effect. All files will be encrypted with the versioned key.

If the backup of the non-LDT GuardPoint was performed without the Apply Key effect, the backup is encrypted, and you must do the following:

Note

The following example is for a manual guarding. The steps may differ slightly if your GuardPoint is configured for auto guard.

1. Create a temporary directory for restoring the files, type:

```
mkdir -p /oxf-fs1/tmp_restore
```

2. Restore the encrypted backup files into the temporary directory, type:

```
cp -pr /backup-media/oxf-fs1/gp1/data_files/* /oxf-fs1/tmp_restore
```

3. Create a Standard Policy with the Apply Key effect for all operations, using the same key as the policy applied on the GuardPoint at the time of backup.
4. Create and enable a new GuardPoint for the temporary directory using the Standard Policy just created.

```
secfsd -guard /oxf-fs1/tmp_restore
```

5. Ensure that the temporary GuardPoint and LDT GuardPoint are both enabled.

```
secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/oxf-fs1/gp1	LDT_AES256	manual	guarded	guarded	N/A
/oxf-fs1/tmp_restore	AES256	manual	guarded	guarded	N/A

- Move the restored files from the temporary folder to the GuardPoint enabled with the LDT policy. The CTE agent encrypts the files in the LDT GuardPoint using the current key version in effect for the LDT policy.

```
mv /oxf-fs1/tmp_restore/* /oxf-fs1/gp1
```

- Unguard the temporary GuardPoint and remove the temporary restore directory.

```
secfsd -unguard /oxf-fs1/tmp_restore
rm -fr /oxf-fs1/tmp_restore
```

- Delete the temporary GuardPoint on the CipherTrust Manager.

Using fsfreeze (Linux only)

If you use the `fsfreeze` command to quiesce access to the file system before creating a snapshot, refer to the `fsfreeze` section in CTE Admin Guide in the Linux Utilities chapter on how to run the `fsfreeze` command to quiesce access to both the file system and the GuardPoint(s).

Warning

Do not use LDT schedules and do not pause LDT to align backup schedules with LDT. Instead, use the `fsfreeze` command.

- Running `fsfreeze -f` on the GuardPoint directory pauses LDT operations in-progress and freezes access to both the GuardPoint and the underlying file system.
- Running `freeze -u` reverses `freeze -f`, allowing access to underlying file system and resuming LDT operations.

LDT Backups Using a File System or Storage-Level Snapshot Tool

You can make a file system snapshot using a Logical Volume Manager service or mirroring/splitting storage level LUNs of a file system inside the storage subsystem. LDT does not have requirements for where and how you create a file system snapshot. However, it is required that you **suspend LDT processes before you take the file system snapshot**. Suspending LDT ensures data and metadata consistency between files and LDT extended attributes.

You may choose to suspend LDT manually on the managed host using `voradmin ldt suspend` command or `fsfreeze -f`, or suspend LDT on the CipherTrust Manager.

Note

Be aware that suspending LDT on the CipherTrust Manager suspends LDT on the entire host.

After creating a file system snapshot, you can resume LDT processes on the GuardPoint using `voradmin ldt resume`, or `fsfreeze -u`, or resuming LDT on the CipherTrust Manager. Do not mix the use of `fsfreeze` and `voradmin ldt suspend` to pause and resume LDT. CTE suspends or resumes LDT processes during live transformation when freezing or unfreezing GuardPoint access using `fsfreeze -f` or `-u` option.

Note

You can make sure LDT is suspended at backup time by setting the QoS schedule

You can mount a file system snapshot for data recovery. Configuration for GuardPoints must be duplicated over the mount point of the snapshot file system. Make sure to use the same LDT policy. Enabling GuardPoints over or under the snapshot mount point provides access to the protected files for recovery. You can choose to manually resume key rotation on the GuardPoints of the snapshot file system, although this is not necessary.

Following is an example of the `fsfreeze` command used to freeze access to the file system `/oxf-fs1` in order to create a snapshot of the file system device. This examples illustrates three GuardPoints enabled inside the file system namespace, `/oxf-fs1/gp-1`, `/oxf-fs1/gp-2`, and `/oxf-fs1/gp-3`. Executing the command `fsfreeze -f` targets any of the GuardPoints in the `/oxf-fs1` mount point and suspends LDT processes on all of the GuardPoints. Then it freezes access to the file system.

```
fsfreeze -f /oxf-fs1/gp-1
voradmin ldt list all
MDS_1:  type=file, nguards=1, name=/oxf-fs1/gp-3/__vorm_mds__
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/o
xf-fs1/gp-3
        File List: count 4308

MDS_2:  type=file, nguards=1, name=/oxf-fs1/gp-2/__vorm_mds__
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-2
        File List: count 4308

MDS_3:  type=file, nguards=1, name=/oxf-fs1/gp-1/__vorm_mds__
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/o
xf-fs1/gp-1
        File List: count 4308
```

After the file system snapshot is created, executing the `fsfreeze -u` command on any of the GuardPoints in the file system namespace unfreezes access to the file system and resumes LDT processes on all of the GuardPoints.

```
fsfreeze -u /oxf-fs1/gp-1
```

```

voradmin ldt list all
MDS_1:  type=file, nguards=1, name=/oxf-fs1/gp-3/___vorm_mds___
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-3
        File List: count 4308

MDS_2:  type=file, nguards=1, name=/oxf-fs1/gp-2/___vorm_mds___
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-2
        File List: count 4308

MDS_3:  type=file, nguards=1, name=/oxf-fs1/gp-1/___vorm_mds___
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-1
        File List: count 4308

```

Support for Volume Level Snapshots on NAS Shares with LDT on Linux

CTE supports volume level snapshot capabilities of NAS shares. You may choose to enable the snapshot service on an LDT-protected GuardPoint as long as the GuardPoint is enabled before the snapshot service is activated. Note that the snapshot service is deactivated before the GuardPoint is disabled. Keeping the snapshot service active when the GuardPoint is not enabled may result in data corruption or inconsistent LDT metadata at file or GuardPoint levels.

Windows Backup and Snapshots

On Windows, most backup applications use Volume Snapshot Service (VSS) for the backup. Using VSS is required for backing up files in LDT GuardPoints. VSS service provides a consistent view of the data to backup and restore applications by taking a snapshot of the volume. Windows Backup uses the snapshot volume, while other applications can continue using the original volume for normal I/O operations. VSS snapshot volume uses a “Copy on write” mechanism to provide a consistent view of the data. Some of the high-level steps of the Windows backup process are:

1. Backup application takes a snapshot of the volume using the VSS service.
2. Backup application mounts this VSS volume to read the data to be backed up.
3. The CTE Agent uses the same policy as that of the original volume to protect these snapshots.
4. The CTE Agent applies the policy and rules to all the I/O requests coming from the backup and restore applications.

Note

Make sure that you have enough disk space allocated for this procedure. When LDT rekeys files, it triggers the VSS copy-on-write technology, which makes a copy of that sector for the volume, for that previous snapshot, before it writes the new encrypted data to the original volume. This action can consume a lot of the space allocated for snapshots by VSS.

LDT Backup and Restore Troubleshooting

Restored files to a GuardPoint protected with conflicting key rules

When restoring an encrypted file from backup media to an LDT protected GuardPoint without the Apply Key effect, and the file in the backup media does not have an LDT extended attribute, the file restored to the GuardPoint is set with an LDT extended attribute that specifies the current key version of the key in the policy associated with the data in the restored file. As the key and key version in the policy do not match the key that was applied to the data at the time of backup, the file restored to the LDT protected GuardPoint is unreadable.

When restoring an encrypted file from backup media to an LDT protected GuardPoint without Apply Key effect, and the key specified in the LDT extended attribute of the file in backup media conflicts with the key rules of the policy on the GuardPoint, the restore operation fails and flags the restored file in error. You can only remove the file, or truncate it, to clear the error status on the file. Access to such files, except remove or truncate, fail with an EINVAL error.

LDT Command-Line Administration: voradmin command

Use the **voradmin** utility to gather statistics and administer LDT on a host/client . It has slightly different syntax and command capabilities depending on whether the host/client is running Linux or Windows.

To use **voradmin**:

1. Log in to the host running the CTE Agent with LDT enabled.
2. At the command line, type **voradmin**.
3. Follow the usage outputs onscreen to find the available commands and their syntax. The general syntax is:

```
voradmin ldt <command> [args]
```

Command	OS	Description
<code>voradmin ldt attr get delete <guard path> <object path></code>	W/L	Get or delete attributes for a GuardPoint or Object path.
<code>voradmin ldt exlist <add remove get> <guard path></code>	W	GuardPoint path to add in exclusion list.
<code>voradmin ldt group <check info remove repa ir comm_info> [hostname] <guard path></code>	W/L	Various info about the group.
<code>voradmin ldt ior <threshold></code>	W/L	QoS Rekey rate threshold value in MB/sec.

Command	OS	Description
<code>voradmin ldt key <report map <key> <guard path></code>	W/L	Creates a report, or map, containing statistics after each key rotation on a GuardPoint.
<code>voradmin ldt list all</code>	W/L	List all MDS files and GuardPoints undergoing LDT processing.
<code>voradmin ldt monitor [interval]</code>	W	Monitor LDT progress. If an interval is specified (in units of seconds), it continually updates the monitoring output at the specified interval.
<code>voradmin ldt rekey report <guard path> [<output file>]</code>	L	Generate a rekey report manually for a Guardpath.
<code>voradmin ldt report <guard path> <log file></code>	W	Full GuardPoint or log file path.
<code>voradmin ldt rescan <guard path></code>	W	Rescan a GuardPoint for CIP remediation.
<code>voradmin ldt resume <guard path> all</code>	W/L	Resume guarding the GuardPoint directory.
<code>voradmin ldt rmltd <guard path> voradmin ldt rmstore <guard path></code>	L	Both the <code>rmstore</code> and <code>rmltd</code> options remove the LDT metadata information remaining in a GuardPoint directory after permanent unguarding of the specified GuardPoint. The <code>rmstore</code> option removes the MDS file, if it exists. The <code>rmltd</code> removes the MDS file and the files in LDT Private Directory for GuardPoints over NFS shares. Note: GuardPoints over NFS shares are only supported if you are using the CM as your key manager.
<code>voradmin ldt skip <show> <guard path> <filename></code>	W	Display the files skipped during data transformation.
<code>voradmin ldt space</code>	W/L	Estimates disk space needed for

Command	OS	Description
<code><guard path></code>		metadata and MDS store information.
<code>voradmin ldt summary <guard path></code>	W/L	Reports the exact number of files encrypted in the GuardPoint in real time.
<code>voradmin ldt suspend <all><guard path></code>	W/L	Suspend the rekey on a specified GuardPoint, or all the GuardPoints, on this host.
<code>voradmin ldt stats [<guard path>] [<interval>]</code>	W/L	Obtains transformation LDT statistics such as: • Current rekey status • Start time • Estimated completion time • Percentage completed • Total data • Amount of data transformed • Total files • Number of files transformed • Number of files skipped • Number of files remaining for rekey

Migrating a GuardPoint to a Different LDT Policy

To change the LDT policy that an LDT GuardPoint uses, complete the following steps to ensure that the GuardPoint is migrated properly from one LDT policy to another LDT policy.

Note

This procedure is for the migration of local file system GuardPoints only. For information about migrating NFS GuardPoints to `clear_key`, see [Migrating GuardPoints over NFS from or to an LDT Policy](#).

Scenario

The GuardPoint is currently attached to LDT-Policy-1, which rekeys from `clear_key` to `LDT-Key-1`. The objective is to migrate the data in the GuardPoint to another versioned key, `LDT-Key-2`. Migration to `LDT-Key-2` requires detaching the GuardPoint from `LDT-Policy-1`, and then attaching it to `LDT-Policy-2`, assuming `LDT-Key-2` is the versioned key specified in `LDT-Policy-2`. To do so:

1. Clone the latest version of the key `LDT-Key-1` to a non-versioned key such as `LDT-Key-1-Clone`.

- a. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.

Tip

To navigate to the Products page from anywhere in the CipherTrust Manager Console, click the App Switcher icon in the top left corner.

- b. Click the name of the versioned key that you want to clone.
 - c. In the Key Details area, find the version that you want to clone.
 - d. Click the (...) button at the end of the row and select **Clone** to clone the selected version of the key.
2. Identify or create a new versioned key that you want LDT to use to re-encrypt the data. For example, **LDT-Key-2**.
 3. Create a new Live Data Transformation policy that specifies **LDT-Key-1-Clone** as the Initial Key and **LDT-Key-2** as the Transformation Key.
 4. Make sure that all data transformation has completed on the GuardPoint. To verify this, use the `voradmin ldt attr get <GuardPoint>` command.
 5. In your key manager, unguard the GuardPoint.
 6. On the host, remove the existing LDT attributes on the GuardPoint using the `voradmin ldt attr delete <GuardPoint>` command.

```
voradmin ldt attr delete /oxf-fs1/gp1
LDT metadata has been removed from all files in GuardPoint [/oxf-fs1/gp1]
LDT attributes deleted from 10 files in /oxf-fs1/gp1
LDT: Metadata has been removed from all files in guard point [/oxf-fs1/gp1]
```

7. Guard the directory using the new LDT policy.
 - If you have selected Auto Guard, data transformation begins as soon as the host gets the new policy information from the key manager.
 - If you have selected Manual Guard, use the `secfsd -guard <GuardPoint>` command on the host to begin data transformation.

Removing LDT and Security Encryption

If you want to stop using LDT on a GuardPoint or on a whole host/client , follow the instructions in the following sections.

- Migrating a GuardPoint Out of LDT
- Deleting LDT Metadata (Linux)
- Deleting LDT Metadata (Windows)
- Removing LDT from a Host

Migrating a GuardPoint Out of LDT

Migrating a GuardPoint from LDT removes the security encryption. It also provides an Administrator with the flexibility to relax the compliance requirement, when strict compliance for frequent key rotation on specific data is no longer mandatory. The following sections describe how to migrate a GuardPoint from LDT to a non-LDT policy, or to remove encryption protection from it.

Converting a GuardPoint from an LDT Policy to a Standard Policy

If you want to do more than just change the policy on a GuardPoint from an LDT policy to a non-LDT policy, see [Deleting LDT Metadata \(Linux\)](#) or [Deleting LDT Metadata \(Windows\)](#).

Note

- Converting LDT CIFS/NFS GuardPoints from Live Data Transformation policies to Standard CTE policies is not supported.
- LDT CIFS/NFS-protected GuardPoints cannot be migrated to clear_key.
- Reverse migration **is not** supported for network shares.

1. Clone the versioned key associated with the LDT GuardPoint to a non-versioned key.

The clone function creates a new key with the same cryptographic encryption material as the current version of the cloned versioned key.

This allows LDT to use the cloned key in a non-LDT policy to convert the GuardPoint from an LDT to a non-LDT managed policy.

- a. In CipherTrust Manager, click **Keys** in the navigation bar.
- b. Click the name of the versioned key that you want to clone.
- c. In the Key Details area, click the (...) button at the end of the row showing the current version of the key and select **Clone** to clone the current version.
- d. Enter a new name for the key in the **Key Name** field. Do not select the **CTE Versioned** option for the clone.

- e. Click **Clone**.
2. Open the **CTE** application and click **Clients** in the left-hand menu bar.
3. Click on the name of the client whose GuardPoint you want to migrate.
4. Find the GuardPoint you want to migrate in the GuardPoints table, then click the (...) button at the end of the row and select **Disable**.
5. After LDT disables the GuardPoint, click the (...) button at the end of the row and select **Unguard**.
6. (Linux only) Ensure that the GuardPoint is removed on the managed host:

```
secfsd -status guard  
No ${gp}s configured
```

7. LDT creates extended attributes for every file under the GuardPoint as well as the GuardPoint directory. Now that the LDT policy does not manage the GuardPoint, you must remove the extended attributes for every file in the GuardPoint, type:

```
voradmin ldt attr delete /<${gp}>
```

8. The command may take some time depending on the number of files in the GuardPoint.

Note

For all of the file system mount points that contain an LDT protected GuardPoint, you must clean up the metadata first. See [Deleting LDT Metadata \(Linux\)](#).

9. Create a non-LDT policy using the cloned key you created earlier in this procedure.
 - a. In the **CTE** application, click **Policies** in the left-hand menu bar and then click **Create Policy**.
 - b. Enter a name for the policy in the **Name** field.
 - c. In **Policy Type**, choose **Standard**.
 - d. Click **Next**.
 - e. On the Security Rules page, click **Next** to skip adding a security rule.
 - f. On the Key Selection Rules, click **Create Key Rule**.
 - g. In the **Key Name** field, select the cloned key you created earlier.

- h. Click **Add**.
 - i. Click **Next**
 - j. Confirm that the key rule is correct and click **Save**.
10. Apply the non-LDT policy to the GuardPoint.

Caution

Make sure that you have removed all of the LDT metadata from the GuardPoint before applying the non-LDT policy.

- a. Open the **CTE** application and click **Clients** in the left-hand menu bar.
- b. Click on the name of the client whose GuardPoint you want to migrate.
- c. Click **Create GuardPoint**.
- d. In the *Create GuardPoint* dialog box, select the Policy that you just created in the **Policy** field.
- e. Select the **Type: Auto Directory** or **Manual Directory**.
- f. In the **Path** field, and enter or browse to the directory to protect.
- g. When you are done, click **Create**.

Remove Protection from a GuardPoint

When compliance may no longer require protecting data in a GuardPoint, you may choose to unprotect/decrypt it. Before removing protection from your GuardPoint, you must decrypt the data in your GuardPoint by setting it to clear. You have two options to decrypt your data:

- While a GuardPoint is protected and enabled under an LDT policy, you can use copy or backup/restore commands to save files in your GuardPoint to a location outside of your GuardPoint.
- Use the `dataxform` command to transform your GuardPoint to clear in an offline transformation process.

For GuardPoints over NFS, you must backup the entire GuardPoint before you unguard the GuardPoint. Then you can restore the files from backup over the GuardPoint directory after you remove the protection on the GuardPoint.

Copying Files to Decrypt Them

If you choose to copy your files, you must create a directory outside of the GuardPoint and then copy the files into the GuardPoint directory. After finishing copying, complete the following steps:

1. Open the **CTE** application and click **Clients** in the left-hand menu bar.

2. Click on the name of the client whose GuardPoint you want to remove.
3. Find the GuardPoint you want to remove in the GuardPoints table, then click the (...) button at the end of the row and select **Disable**.
4. After LDT disables the GuardPoint, click the (...) button at the end of the row and select **Remove**.
5. (Linux only) Ensure that the GuardPoint is removed on the managed host:

```
secfsd -status guard
No ${gp}s configured
```

This completes removal of the GuardPoint under an LDT policy. You can now remove the original files and data within the GuardPoint namespace.

Using Dataxform Command to Transform the Files

If you choose to use the `dataxform` command to transform data in your GuardPoint to clear, use the `voradmin` command to verify that earlier versions of the versioned key are not in use on your GuardPoint. Complete the following steps to clear all metadata in your GuardPoint. Then, transform your GuardPoint to clear.

1. Clone the versioned key associated with the LDT GuardPoint to a non-versioned key.
 - a. In the CipherTrust Manager Applications Page, open the **Keys & Access Management** application.
 - b. Click the name of the versioned key that you want to clone.
 - c. In the Key Details area, click the (...) button at the end of the row showing the current version of the key and select **Clone** to clone the current version.
 - d. Enter a new name for the key in the **Key Name** field. Do not select the **CTE Versioned** option for the clone.
 - e. Click **Clone**.
2. Create a Standard policy using the cloned key you just created.
 - a. In the **CTE** application, click **Policies** in the left-hand menu bar and then click **Create Policy**.
 - b. Enter a name for the policy in the **Name** field.
 - c. In **Policy Type**, choose **Standard**.
 - d. Enable the **Data Transformation** option.
 - e. Click **Next**.
 - f. On the Security Rules page, click **Next** to skip adding a security rule.
 - g. On the Key Selection Rules, click **Create Key Rule**.

- h. In the **Key Name** field, select the cloned key you created earlier.
 - i. Click **Add**, then click **Next**.
 - j. On the Data Transformation page, click **Create Data Transformation Rule**.
 - k. In the **Transformation Key Name** field, select `clear_key`.
 - l. Click **Add**, then click **Next**.
 - m. Confirm that the key rule and data transformation rule are correct and click **Save**.
3. Click **Clients** in the left-hand menu bar.
 4. In the Clients table, click on the name of the client whose GuardPoint you want to remove.
 5. Find the GuardPoint you want to remove in the GuardPoints table, then click the (...) button at the end of the row and select **Disable**.
 6. After LDT disables the GuardPoint, click the (...) button at the end of the row and select **Remove**.

Before you apply the offline data transformation policy to your GuardPoint, you must clean up the LDT metadata from your GuardPoint. LDT creates extended attributes for every file under the GuardPoint, as well as the GuardPoint directory. Now that the LDT policy does not manage the GuardPoint, you can remove the extended attributes for every file in the GuardPoint.

7. Remove the extended attributes of files in a GuardPoint, type:

```
voradmin ldt attr delete <${gp}>
```

The command may take some time depending on the number of files in the GuardPoint. After metadata deletion is complete, you can apply the offline transformation policy on the GuardPoint.

8. CipherTrust Manager, guard and enable the GuardPoint with the Standard policy you created earlier.
9. After enabling your GuardPoint, run the `dataxform` command on the managed host to transform the GuardPoint to a `clear_key`, type:

```
dataxform --rekey --gp /<${gp}>/ --preserve_modified_time --preserve_access_time --cleanup_on_success
```

10. After completion of `dataxform`, unguard the GuardPoint.
11. Remove the GuardPoint from the `dataxform` policy in CipherTrust Manager.

Deleting LDT Metadata (Linux)

To remove the metadata associated with the GuardPoint, you must run the `voradmin` command on the managed

host to remove the LDT metadata associated with the GuardPoint.

Warning

Before you attempt to remove an MDS file, make sure that no LDT-protected GuardPoints remain configured under the file system mount point.

In the following example:

- `/oxf-fs1` is the mount point
- `/oxf-fs1/gp1` is the LDT-protected GuardPoint

To delete the metadata associated with the GuardPoint:

1. Ensure that the GuardPoint is not enabled on the host. Run the command below and verify that the GuardPoint pathname does not appear in the output of the `secfsd` command, type:

```
secfsd -status guard
```

2. Run the `voradmin` command to remove LDT attributes on the GuardPoint, type:

```
voradmin ldt attr delete <GuardPoint path>
```

For example:

```
voradmin ldt attr delete /oxf-fs1/gp1
LDT metadata has been removed from all files in GuardPoint /oxf-fs1/gp1
```

Deleting the LDT Private Space Directory for NFS Shares

As described in [LDT Metadata Management Over NFS/CIFS Shares](#), LDT creates and manages LDT NFS metadata in the LDT Private Space Directory inside the GuardPoint. To remove the LDT Private Space Directory and the files it contains, use the `voradmin ldt rmltd <GuardPoint>` command. For example:

```
voradmin ldt rmltd /nfs-oxf-fs1/gp1
Enter YES if GuardPoint /nfs-oxf-fs1/gp1 is no longer associated with an LDT poli
cy -> YES
LDT metadata on /nfs-oxf-fs1/gp1 has been removed.
```

Deleting LDT Metadata (Windows)

Use the following command to delete the CTE extended attribute for a file or a GuardPoint. This is useful when removing a GuardPoint from under an LDT policy (see [Migrating a GuardPoint Out of LDT](#)).

```
voradmin ldt attr delete [<file name path> | <guard path>]
```

For an overview of `voradmin ldt`, see [LDT Command-Line Administration: voradmin command](#).

Removing LDT from a Host

Once you have registered a host and enabled LDT, you cannot disable the LDT feature by unchecking the LDT box. You must unregister the host from the CipherTrust Manager, then register it again without LDT. When you remove the LDT feature from a host entirely, the host's LDT license becomes available for use on another host.

1. Stop all applications from accessing data in LDT GuardPoints on the host.
2. Migrate data in every LDT GuardPoint using the steps described in the section [Remove Protection from a GuardPoint](#).

Warning

Potential data loss. Ensure that you have decrypted the data and, optionally, copied it out of the GuardPoint. Once the CTE Agent software is removed, access to data is no longer controlled by CTE. If the data was encrypted, it remains encrypted, and there is no way to read it.

3. Remove the GuardPoints on the host from the CipherTrust Manager.
 - a. Remove the LDT metadata from those GuardPoints.
 - b. Remove the MDS files associated with those GuardPoints, if necessary. See [Deleting LDT Metadata \(Linux\)](#) for more information.
4. Remove the host from the CipherTrust Manager. For details, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
5. Re-install the agent on the host.
6. Register the host with the CipherTrust Manager. This time, do not select the CipherTrust Transparent Encryption - Live Data Transformation option. See [Enabling LDT on a Protected Host](#).

Uninstalling the Agent while LDT is Rekeying GuardPoints

You cannot uninstall the CTE Agent if LDT is rekeying any GuardPoints on that host/client .

If you want to uninstall the CTE Agent from a host/client that contains LDT GuardPoints, you must first unencrypt the files on each LDT GuardPoint using the steps noted in the previous sections.

Detecting Loss of NAS connection to an LDT GuardPoint Group

This section describes the LDT over NFS mechanism for detection of loss of a NAS (Network attached storage) connection to an LDT over NFS GuardPoint on all members of the LDT GuardPoint Group. LDT over NFS monitors LDT operations on NAS servers for detection of loss of NFS connection and implements steps to recover from loss of NAS access. This section describes the procedures and considerations for recovering an LDT over NFS GuardPoint from loss of NAS connection on a member of LDT GuardPoint Group.

Brief Overview of LDT Rekey Operations

Rekey operations within LDT GuardPoint Groups are executed on the primary host in coordination with other members of the LDT GuardPoint Group. Coordination includes interlocking access to files by applications and rekey operations. It also includes the primary host updating persistent LDT metadata on behalf of the application file or IO operations on any member of the LDT GuardPoint Group. Such active coordination is critical to the correct operations of LDT over NFS. Loss of NAS connection on any of the members in LDT GuardPoint Group disrupts the coordination between primary and other members. LDT manages loss of the NAS access on all members of the LDT GuardPoint Group to ensure data and metadata correctness with minimal impact to production workloads.

This section describes the LDT over NFS mechanism for detection of loss of NAS connection to an LDT over NFS GuardPoint on a member (primary/secondary) host of the group and also describes the procedures and considerations for recovering an LDT over NFS GuardPoint from the loss of NAS connection on a member host of the group.

Effects of loss of NAS connection on a GuardPoint

Loss of NAS connection on any member of an LDT GuardPoint Group, including primary hosts, will have negative effects on active LDT operations on the target NAS, and across the entire LDT GuardPoint Group and applications accessing files inside the affected GuardPoints. Regardless of the LDT status (active or suspended), connection loss of one member ripples through all of the LDT GuardPoint Group members. The following scenarios can occur during loss of NAS access while LDT operations are in active or suspended state:

- Application file operations (read/write, truncate, rename, etc.) on files undergoing rekey can be blocked and consequently affect subsequent LDT operations on the same files. Rekey operations will be delayed, or even not started, as the result of pending file IO operations by applications.
- Pending LDT rekey IO operations will not complete and consequently, block or prevent, subsequent rekey operations from starting as well as block applications attempting to access such files.
- Rotation of a key will block launching rekey on the affected GuardPoints.

LDT over NFS I/O monitoring system to detect loss of NAS connection

To avoid the ripple effect of loss of NAS connection across entire LDT GuardPoint Groups, LDT monitors LDT level operations that access LDT metadata, such as MDS and LDT rekey attributes, and reads/modifies cipher-text data inside files undergoing rekey. LDT monitors progress on LDT operations in-progress. If an operation fails to complete within 30 seconds, LDT declares the pending operation incomplete and takes action to recover from the operation.

LDT over NFS Monitoring Control Thread

LDT starts a special control thread on every CTE host to monitor LDT operations for potential timeouts due to NAS connection loss. The monitoring begins when the first LDT over NFS protected GuardPoint is enabled. This thread monitors LDT operations on all LDT protected GuardPoints on the CTE host.

The LDT over NFS IO monitoring system monitors only LDT level operations. The control thread does not monitor application file operations on the files in the same GuardPoints that LDT over NFS monitoring thread is monitoring. If an application file operation hangs due to loss of NAS connection, the LDT over NFS monitoring control thread will detect it when the LDT operation starts and then timeouts on the same file.

Managing loss of NAS connection to a GuardPoint on the PRIMARY host

LDT takes action to recover from the loss of the NAS connection for LDT GuardPoint Group with multiple CTE clients as members of those groups. The action depends on whether the loss of the connection is detected on the primary host, or other members of the LDT GuardPoint Group. LDT takes no action to recover the LDT GuardPoint Group consisting of one member, a single node. The member of such a group is the LDT primary host for the GuardPoint, and LDT operations are blocked in the event of loss of a NAS connection with those operations resuming after the NAS connection is restored. The recovery action for Groups multiple clients depends on the type of loss.

Managing Primary host losing NAS connection to a GuardPoint - Primary Demotion

As soon as the monitoring thread detects the loss of the NAS connection to a GuardPoint on the primary host, the control thread initiates Primary Self-Demotion to demote the primary host from the primary role and responsibility for the GuardPoint. In this scenario, LDT on the primary host will start the demotion process for the affected GuardPoint in order to elect another member of LDT GuardPoint Group for the primary role. Election of another member triggers the failover process of LDT operations from the demoted primary host to the newly elected primary host. The election and the failover process is transparent and enables LDT to continue rekey operations using the newly elected primary host for all healthy members of the LDT GuardPoint Group.

The detection and recovery action resumes LDT operations and is fully transparent. It does not involve administrator intervention except when finishing rekey operations that were in progress on the demoted primary host when the loss of the NAS connection was detected. From the perspective of the newly promoted primary host, those files are in LDT **INCOMPLETE** status and resuming rekey on LDT **INCOMPLETE** files requires administrator intervention.

When the failover from primary role occurs, the newly elected primary host identifies the files undergoing rekey and marks those files as LDT **INCOMPLETE** status. At this stage, the self-demoted primary host remains in the LDT GuardPoint Group as an active member but without access to the NAS server. Due to the loss of the NAS access, LDT on the self-demoted primary host blocks all new user attempts to access files in the GuardPoint. It then continues to participate in the transformation of the remaining files in the GuardPoint with the newly elected primary host.

Rekey Completion on GuardPoint with INCOMPLETE Files

Although the newly-elected primary host resumes rekey and transforms the remaining files in the GuardPoint, it does not resume transformation on INCOMPLETE files until the self-demoted primary host has been recovered through the manual administrator intervention. Files in **INCOMPLETE** rekey status are the last files in the GuardPoint after administrator intervention.

Recovering self-demoted primary host

The self-demoted primary host can be recovered manually by shutting down the host with the host membership

removed from the LDT GuardPoint Group. A successful shutdown process that halts the host automatically removes the host membership from the LDT GuardPoint Group. Therefore, it is critical for the self-demoted primary host to reach the halt state at the completion of the shutdown. However, the shutdown process may not reach the halt state due to pending IO operations as the result of the loss of NAS connection.

Shutdown failure on self-demoted primary host

If you are using LDT over NFS with GuardPoints across multiple NAS shares, and a primary node loses the connection with a NAS server but does not reach the halt state, then the other GuardPoints from the other NAS shares, that are also guarded on that self-demoted primary node, must be manually removed from the LDT GuardPoint Group for recovery.

When you must manually force the host to halt, this is referred to as an ungraceful failure. Remedy this issue from the newly promoted primary server:

1. Remove the self-demoted primary host from the GuardPoint. Type:

```
voradmin ldt group remove <hostname_of_self-demoted primary> <guardpoint_path>
```

Note

- When you run the `voradmin ldt group remove` command for other GuardPoints, from other NAS servers present on that node, and if the node is the primary for any of those GuardPoints, then primary failover is triggered.

2. Repeat the command on any other GuardPoints on other NAS servers that are guarded by the self-demoted primary host.
3. Run the recover command for the GuardPoints that were on the node that lost connection to the NAS server. Type:

```
# voradmin ldt demotion recover <guardpoint_pathname>
```

For more information, see the following two sections:

- [Failover for LDT GuardPoint Group](#)
- [Secondary Host Failure](#)

Self-demoted primary host reaches HALT state

If the shutdown process on the self-demoted primary does reach the halt state, then the self-demoted primary host has already been removed from LDT GuardPoint Group. Your next step in the recovery process depends on the status of NAS connection of the host.

If a loss of NAS connection persists, disable the GuardPoints on NAS servers that cannot be accessed on the self-demoted primary host:

- Change the guard status of the GuardPoints configured for Auto Guard to remain disabled on the self-demoted primary host
- Do not enable GuardPoints configured for Manual Guard if the self-demoted primary host has rebooted

You can then proceed with the following voradmin command to resume rekey operations on the files in INCOMPLETE status. This command must be executed on the newly elected primary host.

```
# voradmin ldt demotion recover <guardpoint_pathname>
```

If the loss of NAS connection has been resolved by the time the self-demoted primary host reboots, you can allow CTE start-up services to enable the GuardPoints configured for Auto-Guard on the host, or you can manually enable a GuardPoint configured for Manual Guard. After enabling the GuardPoints, you can perform the following command on the newly-elected primary host to resume rekey on files currently in INCOMPLETE status: use # voradmin ldt demotion recover

Upon completion of the recovery steps, the remaining files in INCOMPLETE status will be rekeyed and the GuardPoint itself will transition to rekeyed state.

Note

Self-demoted primary hosts must be rebooted after the promotion of a member to primary host.

Handling loss of the NAS connection to a GuardPoint on a non-PRIMARY host

In the event of a non-primary host losing NAS connection, the LDT over NFS IO monitoring thread on the non-primary host will detect the loss of the NAS connection and trigger self-isolation from LDT GuardPoint Group.

The outcome of self-isolation is that LDT on the non-primary host blocks all users' access to the affected GuardPoint and begins acknowledging all LDT requests from the primary host. Effectively, it does not perform subsequent operations requested by the primary host, but it sends positive responses to the primary host so that the primary host can continue rekey operations.

Recovery steps for recovery from a self-isolated secondary host are the same as those for the recovery of a self-demoted primary host.

LDT over NFS demotion-related Alarms to CipherTrust Manager

LDT sends the following alarms to CipherTrust Manager during primary host self-demotion, election of a new primary host after demotion, recovery of the self-demoted primary host, and recovery and transformation of the INCOMPLETE files on the new primary host:

[CGS3347i] LDT over NFS-ALERT: Primary host of GuardPoint [GuardPoint] demoting

LDT on the primary host sends this alarm to notify of the loss of the NAS connection on the primary host, for the specified GuardPoint, and the initiation of the self-demotion process.

[CGS3348i] LDT over NFS-ALERT: Primary host of GuardPoint [GuardPoint] demoted

LDT on the self-demoted primary host sends this alarm for the specified GuardPoint when the self-demotion process completes.

[CGS3349e] LDT over NFS-ALERT: Demotion of Primary host of GuardPoint [GuardPoint] failed, error [ErrorNumber]

LDT on the primary host sends this alarm if the self-demotion attempt fails for the specified GuardPoint. The error code included in the alarm indicates the reason for failure. Notify Thales Support in the event of this alarm.

[CGS3355i] LDT over NFS-ALERT: INCOMPLETE file. After DEMOTION, Admin intervention is required for full recovery, GuardPoint [GuardPoint] objID [InodeNumber] error [ErrorNumber]

LDT on the newly-elected primary host sends this alarm for each file detected in INCOMPLETE status.

[CGS3357i] LDT over NFS-ALERT: Manual recovery invoked to recover the DEMOTED GuardPoint[GuardPoint]

LDT sends this alarm from the newly-elected primary host when the administrator executes the `voradmin` command to begin the recovery process.

[CGS3358e] LDT over NFS-ALERT: DEMOTED GuardPoint recovered on the newly-elected primary host while the old primary host is still alive, objID [InodeNumber]

LDT sends this alarm from the self-demoted primary host before the recovery steps, if the self-demoted host receives a request for an LDT operation on a file in INCOMPLETE status from the newly-promoted host. This alarm indicates that the newly promoted host has begun recovery of files in INCOMPLETE status without first recovering the self-demoted primary host.

[CGS3354e] LDT over NFS-ALERT: Manual recovery failed on DEMOTED GuardPoint [GuardPoint] objID [InodeNumber] error [ErrorNumber]

LDT sends this alarm from the newly elected primary host, during recovery of an INCOMPLETE file, when it encounters any errors during LDT rekey related to the recovery of the file or during the resumption of rekey on the file.

[CGS3359i] LDT-NFS-ALERT: Secondary host DEMOTED due to loss of NAS connection, GuardPoint [GuardPoint]

LDT on a self-demoted secondary host sends this alarm for the specified GuardPoint when the self-demotion process completes on the self-demoted secondary.

Using LDT with CIFS/NFS shares

- [Introduction to LDT over CIFS](#)
 - [LDT over CIFS/NFS High-Level Overview](#)
-

-
- LDT Communication Groups and LDT GuardPoint Groups
 - Sharing LDT NFS/CIFS GuardPoints between Linux and Windows
 - Limitations
 - Prerequisites
 - Administrating LDT over CIFS/NFS with CipherTrust Manager
 - Upgrading CTE agent in an LDT Communication Group
 - Quality of Service for LDT CIFS/NFS GuardPoints
 - Alerts
 - Troubleshooting LDT CIFS

Introduction to LDT over CIFS

Live Data Transformation is now extended to network share deployments through a distributed architecture system, which allows users to encrypt data on CIFS/NFS shares without any application downtime. CTE agents can support encryption of data workloads for both direct-attached storage and network shares with zero encryption downtime and automated key rotation capabilities. This allows you to meet compliance requirements, without disrupting business applications.

The administration of LDT protected GuardPoints over NFS/CIFS shares is similar to the administration of GuardPoints in local file systems. The requirements related to policies, versioned keys, security and key rules, QoS, and file level rekey operations, for GuardPoints over local file systems, also apply to GuardPoints over NFS/CIFS shares.

The distributed aspect of LDT over NFS/CIFS shares extends the LDT administration across multiple hosts sharing access to the same GuardPoints. This section describes the extended administration of LDT across multiple hosts and how you can use LDT for data transformation across those multiple hosts.

LDT over CIFS/NFS High-Level Overview

As mentioned, the LDT operation for transformation of data over CIFS/NFS is almost the same as for GuardPoints in local file systems. LDT uses the same workflow for transforming data in files and GuardPoint management. The difference between local file systems and NFS/CIFS shares is the number of hosts involved in the transformation of GuardPoints. As multiple hosts can access the same GuardPoint over NFS/CIFS, LDT operations for transforming files in shared a GuardPoint must be coordinated across the CTE hosts enabling the GuardPoint. Coordination entails multiple file-level and LDT operations to ensure the data transformed from the previous key to the new key is not accessed by any other application on any hosts on which the GuardPoint is enabled.

Note

LDT support for NFS shares is restricted to Linux, and LDT support for CIFS shares is restricted to Windows. This means that LDT on Linux does not support LDT protected GuardPoints on CIFS shares,

and similarly, LDT On Windows does not support LDT protected GuardPoints on NFS shares.

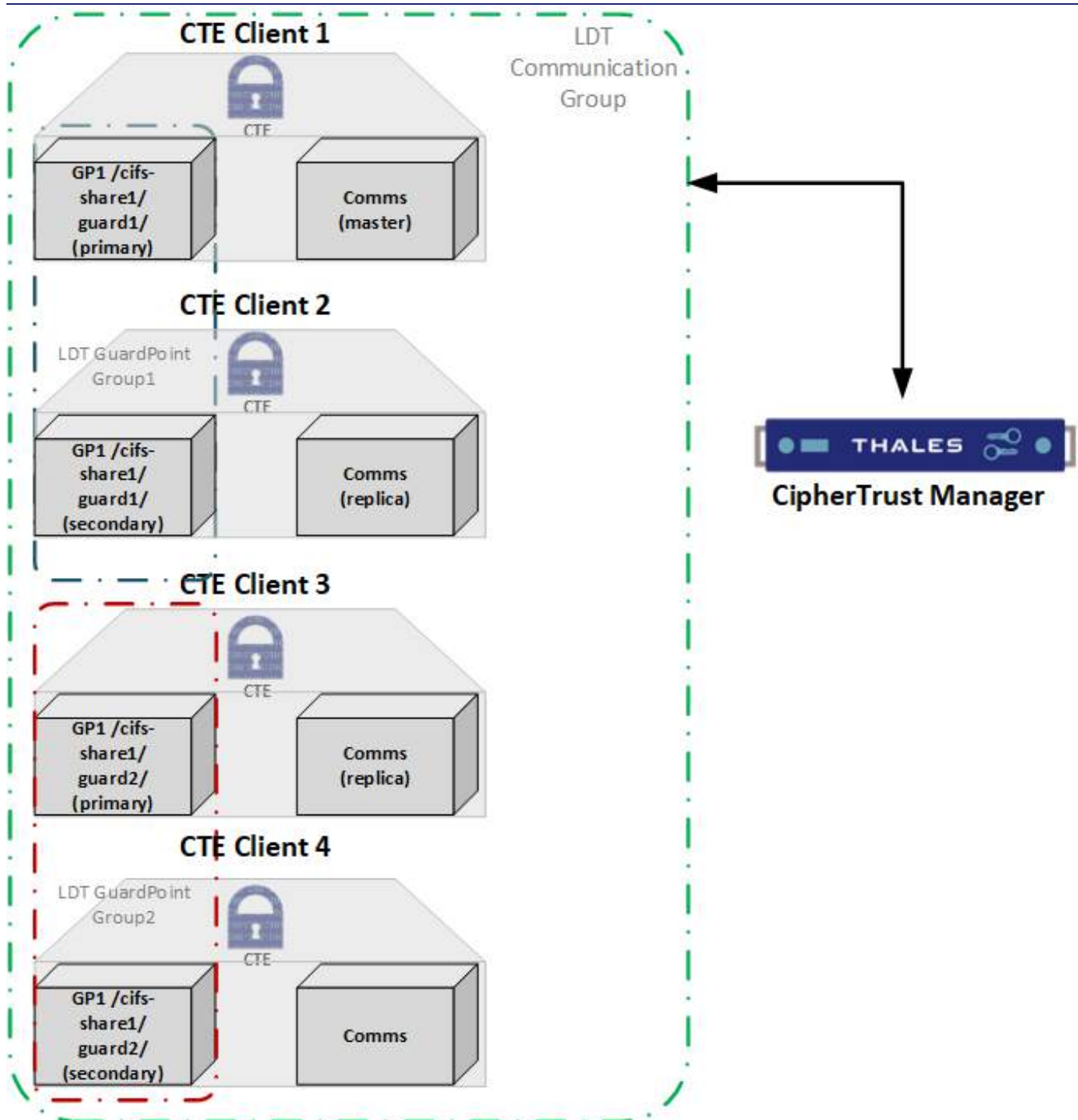
LDT architecture for supporting NFS/CIFS shares is based on a distributed architecture. In this architecture, a single CTE host is delegated the responsibility for transforming the entire dataset in a GuardPoint. Other CTE hosts, sharing access to the same GuardPoint, participate in the data transformation process by the transforming host. The transforming host is referred to as the **LDT GuardPoint Group primary host**, and the participating hosts in the data transformation process are **LDT GuardPoint Group secondary hosts**. In this architecture, an LDT GuardPoint Group is composed of at least four or more CTE hosts (all Linux or Windows) sharing access to the same LDT protected GuardPoint (over NFS or CIFS shares, respectively).

Within an LDT GuardPoint Group, the LDT primary host executes the same operations for data transformation as those executed on GuardPoints in a local file system. The extended architecture of LDT over NFS/CIFS involves the secondary hosts in the group for execution of LDT operations initiated by primary host. For example, when a file is selected and initialized for rekey, the selection and initialization process is not local to the primary host. The primary host performs an extended selection and initialization operation across the members of the group. Once the operation is successfully performed and acknowledged by each member, the primary host proceeds with the next step in the transformation process on the selected file. Below are other extended LDT operations performed by the primary host in conjunction with members of the LDT GuardPoint Group:

1. Locking/unlocking data for rekey.
2. Suspending/resuming LDT.
3. Applying a new key to the GuardPoint.
4. Launching LDT, or concluding LDT, on the GuardPoint associated with the LDT GuardPoint Group.
5. Certain file operations, initiated on a secondary host, that change LDT metadata. For such operations, the secondary host performing the file operation notifies the primary host to update and commit all metadata changes for the operation.

LDT Communication Groups and LDT GuardPoint Groups

The LDT Communication Group provides the services for management and monitoring for the members of the LDT GuardPoint Group, and supports the LDT Messaging Services. An LDT Communication Group contains a collection of LDT-enabled CTE clients that are all on the same network, managed by one CipherTrust Manager and can communicate with each other over that network. An LDT GuardPoint Group consists of CTE clients guarding a common NFS/CIFS share. An LDT Communication Group enables the primary host of an LDT GuardPoint Group to communicate with the secondary hosts that are members of that LDT GuardPoint Group.



LDT Communication Group

- An LDT Communication Group is mandatory when using LDT over NFS/CIFS across all CTE clients managed through CipherTrust Manager. CipherTrust Manager pushes the LDT Communication Group details to all of the CTE clients in a group.
- The first CTE client added to the group is initially designated as the master node. The remaining CTE clients are replicas. All active communications go through the master node.

- All CTE clients intending to guard NFS/CIFS shares with an LDT policy must be able to communicate with each other. In order for the CTE clients to communicate, they must be on the same network, in the same data center and in a single LDT Communication Group. The agents can specify the LDT Communication Group to join at the time of registration.

Note

Even if the CTE clients do not guard the same share, they must be in the same LDT Communication Group on CipherTrust Manager.

LDT Communication Group Limitations

1. You must create an LDT Communication Group on your CipherTrust Manager and manually add all of the CTE clients to it.
2. Minimum of **three CTE clients required** for membership to the LDT Communication Group for proper and continuous operations of LDT services across all LDT GuardPoint Groups. The three clients are called the **triad**.
3. The majority of the CTE clients must be fully operational for proper LDT operations across all LDT GuardPoint Groups.

The LDT Communication Group requires that the majority of CTE clients are active, in order for the LDT Communication Group to work properly. If 50% of the LDT Communication Group servers, or 2 out of 3 **triad** nodes fail, then the LDT Communication Group cannot recover from that situation. To fix this issue, you must either:

- Reboot all of the CTE clients in the entire LDT Communication Group.
 - In Windows, restart **secfsd** through the **Control Panel > Services** page on all of the CTE clients in the entire LDT Communication Group.
4. The name of the LDT Communication Group cannot contain special characters.
 5. If you are repurposing a CTE client that is currently being used for LDT over NFS/CIFS, but still runs CTE and is still registered to the same CM, then you must:
 - a. Remove all CIFS/NFS LDT GuardPoint Groups from the host prior to removing the host from the LDT Communication Group.
 - b. Reboot the host.
 6. Remove a host from the LDT Communication Group if the host is being decommissioned, meaning that you plan to power it down for the foreseeable future, or while CTE is being uninstalled.

LDT Communication Group Considerations

- The LDT Communication Group must be specified at the time of client registration.

Note

For upgrades, add the agents to the LDT Communication Group using the **Add Client** function on CM. See [Adding Clients to an LDT Communication Group](#) for more information.

- Do not shut down the entire LDT Communication Group at once. This is so that maintenance cycles can activate and run. Perform maintenance in a round robin fashion.
- Remove a host from the LDT Communication Group if the host is being decommissioned, meaning that you plan to power it down for the foreseeable future, or while CTE is being uninstalled.
- The CTE host that is the LDT Communication Group master is critical for proper operations of LDT across all LDT GuardPoint Groups. Thales recommends that you dedicate a separate host as your LDT Communication Group master, although it is not mandatory. This isolates the host from unexpected system failures, hence preventing failover of the LDT Communication service to another CTE client critical for your production workload.
- Thales recommends using a minimum of three nodes for optimal performance. All three nodes must be located in the same data center.
- Before rebooting a node, Thales recommends stopping the secfsd service:

For **Windows**:

- a. Go to **Control Panel > Services (local)**.
- b. Select **secfsd**.
- c. Select **Stop the Service**.

For **Linux**, type:

```
/etc/vormetric/secfs stop
```

To create and manage LDT Communication Group in the UI, see: [Managing LDT Communication Groups](#).

Multiple LDT Communication Groups Considerations

CipherTrust Transparent Encryption now supports multiple LDT Communication Groups. Be careful to not misconfigure the multiple LDT Communication Groups:

- You cannot use identical NFS/CIFS share paths in multiple LDT Communication Groups registered to a **single**

CipherTrust Manager. Each share path must be unique.

- You cannot use identical NFS/CIFS share paths in an LDT Communication Group with the same name on **multiple** CipherTrust Managers. LDT Communication Group names must be unique.

Moving Client Nodes from one LDT Communication Group to another LDT Communication Group

If you are repurposing a CTE client node that is currently used for LDT over NFS/CIFS in an LDT Communication Group, but still runs CipherTrust Transparent Encryption and is still registered to the same CipherTrust Manager, then you must **remove** all CIFS/NFS LDT GuardPoints from the host prior to removing the host from the LDT Communication Group. Then you can reboot the host and add that CTE client node to another LDT Communication Group.

LDT GuardPoint Group

As described, an LDT GuardPoint Group is a group of three or more CTE hosts sharing access to the same GuardPoint over NFS/CIFS. A CTE host with n number of GuardPoints has membership to n number of distinct LDT GuardPoint Group and is specific to the GuardPoint directory. A CTE host guarding multiple GuardPoints over NFS/CIFS is a member of multiple LDT GuardPoint Groups.

LDT GuardPoint Group Primary

One CTE host in each LDT GuardPoint Group assumes the **Primary** role for that group. The CTE host that enables a GuardPoint directory first is assigned the primary role for the group associated with the GuardPoint directory. Subsequent hosts enabling the same GuardPoint are assigned **Member** or **Secondary** status. A CTE host can be a primary for a group, or multiple groups, and a secondary for other groups.

LDT manages primary host departure from the group during transformation. Departure of a primary host can occur as the result of disabling a GuardPoint directory on the primary host, or an unexpected failure of a primary host. In the event of the primary host departure from the group, LDT elects and delegates the primary role to one of the members of the group.

For additional information, see:

- [Failover](#)
- [LDT GuardPoint Group Commands](#)
- [Responsibilities of the Primary host](#)
- [Designation of Primary role and Primary Set in an LDT GuardPoint Group](#)

LDT GuardPoint Group Capability Level

In CTE 7.6.0, LDT NFS introduces a feature called: Capability Level, which is for an LDT GuardPoint Group. The feature is based on the compatibility level for each member in the group. The Capability Level of a member determines what features that host can access and use, and allows the group to decide on a common capability level at which to run. This allows support for multiple versions of CTE in the same LDT GuardPoint Group as the group runs at the capability level of the least capable member. The capability level of the group is calculated when a member leaves the group, or a primary failover occurs. As lesser capable members depart the group, the overall capability level of the group increases. The capability level of a group cannot be decreased. As such, members at a lesser capability level cannot join once the capability level of the group has increased. New

members joining an existing group will attempt to join with the highest capability level supported by the host and, if rejected, retry with progressively lower capability levels until the group accepts the join request. If the group is running at a capability level that exceeds the joining member's highest capability, that host is not allowed to join the group.

When a new feature is introduced that is unavailable to, or incompatible with, older versions of CTE agents, the maximum capability level of the newer agents is increased to a value greater than the maximum capability level of the older agents. If there is a group with a mix of the new and old agents, the group runs at the capability level of the older agent. This means that no member of the group will be allowed to use the new feature, regardless of the actual version of CTE running on the member. Only after all of the members running the older agent have left the group will the group be upgraded to the new capability level and use of the new feature is enabled. Older agents will no longer be allowed to join the group as there are now features in use that are not available to, or compatible with, older agents. If the LDT GuardPoint Group needs to contain the older agent, then a member running that older agent must be present at all times to ensure that the compatibility level of the group is not upgraded to the level of the newer agents.

LDT GuardPoint Groups with Different CTE Versions (Linux Only)

LDT does not allow key rotation to begin in an LDT GuardPoint Group over NFS when hosts in that group are not homogenous, meaning they are running different versions of CTE. When an LDT GuardPoint Group containing a mix of CTE versions needs to rotate a key, the rekey is blocked and the GuardPoint is marked with the relaunch flag. This persists until the group only contains homogenous hosts; after which rekey automatically starts. If rekey is already in progress on a GuardPoint, disparate hosts are blocked from joining the group until rekey completes. This block on joining also includes when the GuardPoint is rekeyed but flagged for relaunch.

Note

Patch releases within the same major/minor version do not block rekey from starting; ex. 7.8.0.x and 7.8.0.y.

Scenario

For example, given an LDT GuardPoint Group over NFS with:

- One CTE 7.6.x host as the primary
- One CTE 7.6.x host as a member
- Two CTE 7.7.y hosts as members

When the key rotates, the GuardPoint transitions into the rekeyed/relaunch state and remains there until only CTE 7.6.x or CTE 7.7.y hosts remain.

While the GuardPoint is in the rekeyed/relaunch state, no disparate CTE hosts are allowed to guard. This remains true even if the CTE 7.6.x primary unguards, and one of the CTE 7.7.y members is promoted into the primary role. Only after all CTE 7.6.x hosts have unguarded will CTE 7.7.y hosts be allowed to guard, at which point rekey can begin. However, after all of the CTE 7.6.y hosts have unguarded, no CTE 7.6.y hosts will be able to guard moving forward, as the group is now running at the CTE 7.7.x level.

Note

- Thales recommends that you upgrade CTE on all hosts in an LDT GuardPoint Group group during the same maintenance window. If that is not possible, Thales recommends that subsequent maintenance windows for upgrades occur before the key is scheduled to rotate.
- It is possible that a host that was previously part of the group, could fail to rejoin after a reboot due to key rotation occurring and blocking hosts with mismatched versions from joining. Upgrade all hosts to the same version of CTE to ensure that key rotation does not block any host from joining.
- CTE 7.6.0 agents prior to 7.6.0.134 acting as primary will start rekey even if there are CTE 7.7.0 hosts in the group; CTE 7.7.0 hosts will log an alert in this case. Thales recommends all CTE 7.6.0 hosts using LDT NFS GuardPoints be upgraded to CTE 7.6.0.134 or a subsequent version.

CTE Version Capability Levels

- CTE 7.5.0 members are automatically assigned to a maximum capability level of **2**
- CTE 7.6.0 members can run at a maximum capability level of **3**

The difference in capability between CTE 7.5.0 and CTE 7.6.0 is due to the inclusion of sharing LDT NFS GuardPoints with Windows. See [Windows/Linux Compatibility](#) for more information on this feature.

- CTE 7.7.0 members can run at a maximum capability level of **4**

To find the capability level of an LDT GuardPoint Group, type:

```
voradmin ldt group capability <GuardPoint Path>
```

This command outputs the capability level that the current host is running at for the specified GuardPoint. If the host is the primary host, then the value also represents the capability level for the entire group.

Reference Information

- [Use Case for Setting up LDT Communication Group and LDT GuardPoint Group](#)

Designation of Primary role and Primary Set in an LDT GuardPoint Group

The first host that enables a GuardPoint over NFS/CIFS share is designated as the primary host for the LDT GuardPoint Group. The primary role designation persists until the GuardPoint is disabled on the primary host or the primary host crashes. Designation of another CTE host for the primary role is the result of the old primary crashing, or disabling the GuardPoint. Another member of the LDT GuardPoint Group will be elected to assume the primary role for the LDT GuardPoint Group.

A secondary host **is not** a proper candidate for promotion to primary role if any of the following conditions exist for the GuardPoint on the secondary host:

-
- The NAS share is mounted as read-only on the CTE host
 - The CTE host has not received the latest policy information from CipherTrust Manager
 - The latest key version available to the CTE host is not the most recent key version available to other members of the LDT GuardPoint Group

The read-only access to the GuardPoint directory restricts the designated host from performing LDT operations. LDT operations require read and write access to the NAS share.

The second and third conditions are most likely a transient communication failure between CipherTrust Manager and the designated CTE host. Once the communication issue between CipherTrust Manager and the CTE host is resolved, the CTE host will be updated with the most recent policy information, and it will accept subsequent designations for promotion to primary role.

In addition to the previous conditions, is usually the result of IO or networking issues between CTE host and the NAS share. If this occurs, disable the CTE host and remove it from the LDT GuardPoint Group. Removal of the CTE host triggers election of another CTE host for the primary role. If you are unable to disable the GuardPoint on the CTE host, you must reboot the host, and then remove the host from the LDT GuardPoint Group using the `voradmin ldt group remove` command.

The Designated Primary Set (DPS) contains a list of CTE hosts from which a primary role can be chosen by the LDT/LGS service. CipherTrust Manager administrators can create a DPS by choosing the hosts from the CTE client groups membership that can be promoted to the primary role. Thales recommends that CTE administrators inform the CipherTrust Manager administrator of their choice for DSP membership. The CipherTrust Manager administrator can update DPS as needed. The selected clients should be systems with sufficient resources that can sustain production workloads and the load from rekeying GuardPoints on the primary host. Note that the first CTE client enabling a GuardPoint assumes the primary role for that GuardPoint, regardless of the membership of the client to DPS. Election of another CTE host for promotion to primary role will be a member of the DPS, unless none of the members of the DPS has the GuardPoint enabled. In such a case, one of the members of the LDT GuardPoint Group on which the GuardPoint is enabled will be promoted to the primary role.

A Designated Primary Set (DPS) is created and assigned to a single LDT GuardPoint Group within a LDT GuardPoint Group. With the DPS assigned to a GuardPoint, the election of a new client for the primary role will be from the DPS.

In a Linux environment with a mix of clients from the client group and individual clients guarding the same NAS share, if you guard the NAS share on an individual client first, and later guard it through the client group, the individual client that guarded first is the primary client for the GuardPoint group.

Recommendations for selecting members for DPS

- A designated primary set (DPS) should contain at least two fully operational and highly available nodes with minimal risk of crashes, network issues, or reboots. Ideally, these nodes should be in the same subnet, or in closely connected subnets to ensure uninterrupted LDT operations.
- Only select server class systems capable of carrying out the rekey load without interruptions as the result of frequent reboots. Do not select transient hosts, such as a laptop.
- Avoid disabling GuardPoints on a primary host as much as possible. Disabling GuardPoints on the primary client triggers election of another member from DPS.
- Minimize selecting the same preferred primary for multiple GuardPoints for better load distribution unless the primary host can carry out the LDT load.

- When removing a host from the DPS, ensure that at least two eligible nodes remain. If only one remains, add another node to maintain high-availability. If all DPS nodes are removed, a non-DPS node is promoted to primary node during failover.
- To remove a node from an LDT Communication Group that is part of a DPS, first remove it from the DPS, then the client group, and finally LDT Communication Group.
- Do not include transient nodes in the DPS. They can cause GuardPoint failures.

Limitations

- A Designated Primary Set is fully enforced when all members the client group are DPS-capable.
- If a client group with DPS enabled has non-DPS capable members, the GuardPoints will not be pushed to the non-DPS capable clients.
- Insufficient systems could cause slower rekey rates.

Configuration

When configuring a Designated Primary Set:

- You can **only** choose clients from the client group membership as the designated primary client.
- You must guard the NAS share on the client group **first**.

This Designated Primary Set feature is supported with CipherTrust Manager and CTE agents installed with:

Software	Minimum Version
CipherTrust Transparent Encryption	7.7.0
CipherTrust Manager	2.17

Prerequisites

Be sure to have completed the following configuration steps for guarding a share on your clients before creating a Designated Primary Set:

1. Configure a [CIFS/SMB connection](#) if your CTE clients are Windows clients.
2. Create an LDT Communication Group. See [Managing LDT Communication Groups](#) to create LDT Communication Groups.
3. Create an LDT Client Group. See [Managing Client Groups](#) to create Client Groups.

Note

- Modifications made to a Designated Primary Set list are updated/pushed to the members of the client group associated with the DPS.
- A Designated Primary Set (DPS) is fully enforced when all members of the client group are DPS-capable CTE agents. This means that the clients must be agents installed with CTE 7.7.0 or subsequent versions. If any member of the client group enabled with DPS is a non-DPS capable client, the GuardPoint will not be pushed to non-DPS capable clients.

Creating a Designated Primary Set

1. In CipherTrust Manager, click **Transparent Encryption > Clients > Client Groups**.
2. Click the desired client group name.
3. Select the **Designated Primary Set** tab.

It displays the list of Designated Primary Sets. Expand the desired Designated Primary Set to see its details.

4. Click **Create Designated Primary Set**.
5. In the **General Info** screen, provide a name for the Designated Primary Set and select an LDT Communication Group. Click **Next**.
6. In the **Add Clients** screen, select, or search for, the clients for the primary set.

Note

- A Designated Primary Set **must** contain at least one client.
- Add two or more clients to the Designated Primary Set to have available clients in DPS for election to the primary role, in the case of LDT primary promotion.
- During the promotion process, if the corresponding GuardPoint is not enabled on any members of the DPS, another client in the LDT GuardPoint Group that is not a member of the DPS will be promoted to the primary role. As such, it is a best practice to select multiple clients for the Designated Primary Set for each GuardPoint.
- Select/un-select designated primaries **only** when guarding NFS/CIFS shares in a client group.

7. In the **Confirmation** screen, review the details of Designated Primary Set.

-
8. Click **Create**. The screen displays a message indicating whether the Designated Primary Set was created successfully.
 9. Click **Close** to close the screen. The Designated Primary Set displays in the **Designated Primary Set** tab.
 10. After you have created a Designated Primary Set for a client group, you can create a corresponding LDT GuardPoint for it.

Adding New Clients to a Designated Primary Set

To add new clients to an existing Designated Primary Set:

1. Under **Clients > Client Groups**, click the desired client group name.
2. Select the **Designated Primary Set** tab.
3. Expand the desired Designated Primary Set.
4. Click **Add Clients**.
5. Select the checkboxes for the desired client names.
6. Click **Add**.

Changing the Designated Primary Set Associated with a GuardPoint

You can modify the Designated Primary Set associated with a GuardPoint, after the GuardPoint is created.

To change the Designated Primary Set associated with a GuardPoint:

1. Open the **Transparent Encryption** application from the CipherTrust Manager console.
2. Click the client group name in the **Client Group Name** column.
3. On the **GuardPoints** tab, click the ellipsis corresponding to the desired GuardPoint.
4. Click **View/Edit**. The Edit GuardPoint dialog box is displayed.
5. In the **Designated Primary Set** drop-down list, select a different client.
6. Click **Save**.

The GuardPoint is updated successfully with the new Designated Primary Set.

Validating the Designated Primary Set

In CipherTrust Transparent Encryption, you can get the list of designated primary clients for the guard path if you have configured a Designated Primary Set.

- To get the list, type:

```
voradmin ldt group get_dp <guard path>
```

Example

```
voradmin ldt group get_dp /test/nov25
```

Response

```
LDT GuardPoint Primary: 192.68.34.54  
LDT GuardPoint Designated Primary List: 192.68.34.53,192.68.34.54
```

Note

If the DPS is not configured and you type the command to get the list, the command output shows N/A for the designated primary list:

```
LDT GuardPoint Primary: 192.168.34.54  
LDT GuardPoint Designated Primaries: N/A
```

Responsibilities of the Primary host

As described earlier, the primary host in the LDT GuardPoint Group is responsible for performing data transformation operations. In addition:

1. On Linux, the primary host drives execution of committing a new key version to all members of the LDT GuardPoint Group. During this process, the primary host sends a message to all members, inquiring if each member has received the new key version from CipherTrust Manager. If all members have received the new key, then the primary host, and the members, commit the new key version to their GuardPoints. If at least one member does not have the new key version, the primary host delays committing the new key version and retries the commit process in 30 seconds.

The delay in committing the new key version avoids applications accessing files encrypted with the new key version. Without the delay, the primary host would proceed to rekey the GuardPoint, and consequently, applications running on those member(s), without the latest key version, would be blocked when accessing files encrypted with the latest key version.

Note

The delay only affects rekey operations re-encrypting existing files to the new key version. It does not affect newly created files which inherit the latest key version, that may not have been committed across the entire LDT GuardPoint Group by the primary host. If newly created files are accessed on CTE hosts which do not have the latest key version, the process of accessing such files will be blocked until the latest key version becomes available on those CTE hosts.

2. On Linux, the primary host is also responsible for updating and committing LDT metadata for file operations in progress on the secondary hosts. For example, truncating a file while the primary host is rekeying the file requires changing the LDT metadata for that file. As the primary host is updating the LDT metadata during the rekey process, the member host truncating the file does not update the metadata that the primary host is changing. Instead, the secondary host sends a message to the primary host, requesting LDT metadata changes for the truncate operation, and the primary host provides the metadata updates for the truncate operation triggering the secondary to proceed. The host then commits or discards the metadata changes for the truncate operation after the secondary hosts completes it and notifies the primary host of their status. This process forces the primary host to engage with the hosts that perform truncate operations, strictly on those files that the primary host is rekeying.
3. Operations such as file or directory rename initiated on a member of the group also involves engagement of the primary host, if the primary host is actively rekeying the affected files or GuardPoints. Renaming a subdirectory on a secondary host engages the primary host to scan a list of files under the renamed subdirectory. The primary host performs the scan outside of the scope of the GuardPoint level rekey process and starts separate file level rekey operations for each file not undergoing rekey in the renamed subdirectory. The primary host conducts up to 8 concurrent file level operations, and the GuardPoint level rekey operation does not complete until every file in the renamed subdirectory is rekeyed. File level rekey operations are slow as compared to GuardPoint rekey operations, therefore, subdirectories with a large number of renamed files delay rekey completion time.

Responsibilities of non-primary hosts

When secondary hosts in the LDT GuardPoint Group perform file operations on files that the primary host is actively rekeying, it must notify the primary host of those operations. Truncating a file on secondary hosts, as described earlier, is an example of a secondary host notifying the primary host for updating LDT metadata.

Secondary hosts can also be selected for promotion to the primary role within an LDT GuardPoint Group. A host elected for promotion checks whether it's capable of assuming the primary role for the LDT GuardPoint Group, and if capable, it accepts and promotes itself to assume the primary role for the LDT GuardPoint Group.

Note

Ensure that at least one secondary host is always qualified to accept promotion to primary status.

Connectivity to CipherTrust Manager and mounting NFS shares with read and write access are critical for qualifying secondary hosts for promotion to the primary role.

GuardPoint Directories (Linux Only)

The pathname of a GuardPoint directory does not have to be fixed across all members of the group. For example, if host_1 mounts the share at `/nfs-host-1/gp-dir` and host_2 mounts the same share at `/nfs-host-2/gp-dir`, the LDT GuardPoint Group for the GuardPoint represents both pathnames.

GuardPoint Directories (Windows Only)

GuardPoints for Windows directories use the UNC format. See [Creating a GuardPoint on a CIFS Share Drive on CipherTrust Manager](#) for more information.

Overhead in LDT over NFS/CIFS

The primary host performs LDT operations across all members of an LDT GuardPoint Group. It sends a message, for each operation, to all members of the LDT GuardPoint Group and waits for acknowledgment from all members before executing the operation. A message holds information specific to an operation that the primary host wants to perform, such as file initialization for rekey, lock/unlock operations, LDT launch on GuardPoint, etc. Each member of the LDT GuardPoint Group validates each operation requested by the primary host before responding to the request. This coordination incurs significant overhead in execution of LDT operations on GuardPoints over NFS/CIFS shares in contrast to the same operations performed over GuardPoints in local file systems. It also increases network traffic across all members of LDT GuardPoint Group and potentially increasing overhead in your network infrastructure.

This overhead can pose challenges for LDT to achieve the desired rekey IO rate specified under QoS. Delays incurred in delivery of requests and responses can slow down LDT operations such that the expected rekey IO rate becomes difficult to achieve. Consider the bandwidth of your network infrastructures, number of GuardPoints on the primary host and number of members sharing access to those GuardPoints before setting the rekey IO rate. With multiple GuardPoints on the same primary host such that some of those GuardPoints are over NFS/CIFS and others on locally attached storage devices, rekey IO rate on GuardPoints over NFS/CIFS shares will likely be significantly lower.

Failover for the LDT Communication Group Master and the LDT GuardPoint Group

Failover for the LDT Communication Group Master

CTE clients in an LDT Communication Group have a master/replica relationship. The first client that joins the group is initially designated as the master node. The other clients are replica nodes. The master node must be functional in order for communications to persist. All communications happen through the master node.

A host can leave the LDT Communication Group in one of two ways:

Graceful Failover for the LDT Communication Group Master

There are two cases for graceful failover:

▪ Reboot

If the master node becomes unavailable because it's rebooted by the administrator or as part of a maintenance cycle, but there are other live CTE clients in the LDT Communication Group, then the LDT Communication Group automatically elects a replica CTE client to become the new master node and fails over to it.

▪ Power Off

When a master node powers off, a new master is automatically elected, but if the initial master node is being decommissioned, then you should remove it from the LDT Communication Group.

Note

Any CTE client that is being decommissioned, regardless of its role in the LDT Communication Group, needs to be removed from the LDT Communication Group See [Remove].

Ungraceful Shutdown/Failure for the LDT Communication Group Master

An ungraceful failure is when a CTE client fails abruptly due to a hardware or software failure. It means that the administrator did not trigger the client to either shutdown, reboot or become unreachable, but the client still transitioned into that state. This is applicable to the master node failing as well.

If an LDT Communication Group master node fails ungracefully, it is handled automatically. A new master is elected by the remaining nodes. Meanwhile, LDT operations may continue to fail for all LDT GuardPoints. Operations will resume once a new LDT Communication Group master node is functional.

In the event that all, or a majority of, the CTE clients in an LDT Communication Group fail (**ungraceful** shutdown):

Ensure that **all** of the CTE clients in the LDT Communication Group are active (rebooted, powered on and accessible through the network), to reestablish the cluster.

1. All LDT NFS/CIFS GuardPoints must be unguarded before you remove a CTE client from the LDT Communication Group.
2. Once a CTE client is removed from the LDT Communication Group, it must either be rebooted or shut down.
3. Whenever a graceful exit, or failover event, is in progress for the LDT Communication Group, LDT operations will be affected across the entire LDT Communication Group, which means that GuardPoints could be affected.

Failover for the LDT GuardPoint Group Primary

Gracefully

Graceful Failover occurs when the primary node exits cleanly or gracefully. Then the LDT GuardPoint Group automatically fails over to one of the available secondary hosts, and the secondary host is promoted to the new primary host for the LDT Communication Group.

- Triggered when the GuardPoint is disabled on the primary
- Triggered when the `secfs` service is manually stopped on the primary
- Triggered during a reboot if `secfs` stops cleanly before shutdown
- Triggered when the primary node is removed from the LDT Communication Group

All CTE clients guarding the share, or trying to guard the share, depend on the primary being available.

Graceful Failover

Graceful Failover occur when a node in the LDT GuardPoint Group:

- Performs a reboot
- Performs a Shutdown
- Disables a GuardPoint from CipherTrust Manager
- Unguards a GuardPoint

Note

Remember that if the primary client exits gracefully, then a new primary is elected through failover.

Ungraceful Failover

Ungraceful Failover occurs when the primary node fails, unexpectedly, or **ungracefully**. Then an administrator will need to manually remove the primary from the group so that a secondary member can become the primary host. This also enables the failed primary host to guard again and become a member of the group in the future.

- Triggered if the primary crashes, or reboots, without a clean `secfs shutdown`. A secondary node is promoted to primary after executing a `voradmin` command.

To identify the primary node, type:

```
voradmin ldt group list <absolute guardpoint> (Windows)
voradmin ldt group list <guardpoint> (Linux)
```

!!! note

You can only run this command on a host where the `#{gp}` is currently guarded.

To restore, or repair, the original node after an ungraceful failover, type the following on the LDT GuardPoint Group secondary node:

```
voradmin ldt group repair <failed host> <guard path>
```

Example: If nodes A, B, and C are part of the LDT GuardPoint Group protecting the network share `/test/path1`, and the primary node crashes and comes back online, run the following command on either node B or C:

```
# voradmin ldt group repair /<primary IP> <absolute GuardPoint> (Windows)

# voradmin ldt group repair /<primary ip> <${gp}> (Linux)
```

You can also use the repair command to remove a secondary node that is no longer guarding a GuardPoint but still shows in the Group Info list. This command repairs the host and keeps it in the group.

Example: If nodes A, B, and C are part of the LDT GuardPoint Group protecting the network share `/test/path1`, and the primary node crashes and does not come back online, run the following command on either node B or C to remove a primary host from the group and automatically select a secondary host as the primary, type:

```
voradmin ldt group remove A /test/path1
```

If a secondary host fails ungracefully, you can use the same command to remove that host.

Note

If you plan to reboot a primary node for maintenance or a software update, a graceful primary failover is typically triggered as part of the secfs service shutdown. However, if stopping the secfs service takes too long, and the system proceeds to reboot before the shutdown completes, it can result in an ungraceful failover. To ensure a graceful primary failover, Thales recommends manually stopping the secfs service before initiating the reboot. This allows the GuardPoint to be cleanly disabled and failover to proceed as expected.

Note

Do not use this command in the case of a temporary failure when the failed primary host crashes and then reboots.

Ungraceful Exits

Ungraceful exits occur when a node in the LDT GuardPoint Group:

- Is forced to power off | shutdown | reboot
- Suffers a hardware failure
- Power cycles
- Has a kernel crash

Note

Remember that if the primary host fails ungracefully, then an administrator must manually remove the primary.

Troubleshooting Ungraceful Exits

After the reboot, if you see the following logs in `secfsd.log`, and if `secfsd -status guard` displays the GuardPoint as unguarded, then the reboot did not happen gracefully and the present scenario is classified as an ungraceful exit.

```
lgs_joining: host(xyz_1.com) is already PRIMARY for GPID(060cd923-6026-4341-81e3-f8cc367df90d) in comm server. It seems like a crash+reboot scenario. Informing others about primary failure
```

If this occurs, follow the node repair steps in the previous section, [Failover for LDT GuardPoint Group](#) to recover the structure.

- **Linux** `secfsd.log`: `/var/log/vormetric/secfsd.log`
- **Windows** `secfsd.log`: `C:\ProgramData\Vormetric\DataSecurityExpert\agent\log\secfsd.log`

Secondary Host Failure

In the event that a secondary host crashes, you must first remove that failed secondary host from the entire LDT GuardPoint Group that the host was a member of before allowing that CTE host to rejoin that same LDT GuardPoint Group after the host is restored. The following steps must be performed in exact order for each GuardPoint that was enabled on the host prior to the crash. (You can get the list of GuardPoints from CipherTrust Manager.) For each GuardPoint:

1. On any CTE client that is a member of the LDT GuardPoint Group for that GuardPoint, run the `voradmin ldt group list` command to identify the failed host. The role of the failed host is UNRESPONSIVE within the group, type:

```
# voradmin ldt group list <GuardPoint Path>
```

Role	State	Hostname	GuardPoint Path
UNRESPONSIVE	N/A	Host-3	N/A
PRIMARY	JOINED	Host-1	/nfs/gp

2. On the primary CTE client for the GuardPoint, run the `voradmin ldt group remove` command to remove the failed host from the LDT GuardPoint Group, type:

```
# voradmin ldt group remove <hostname> <GuardPoint Path>
```

Failure Scenario Examples

Following are some basic failure scenarios and suggested recovery steps:

Secondary node crash (Non-Triad node)

Scenario

- Nodes A, B, C, D, E, and F are part of the LDT Communication Group.
- Nodes A, B, and C are the Triad nodes.
- An NFS/CIFS share is guarded on nodes D, E, and F, forming an LDT GuardPoint Group, where node D is the LDT primary.

After the LDT GuardPoint Group has been active for a while, node E, a secondary node, crashes.

Troubleshooting Scenario

If node E remains down:

- From the LDT primary (node D), verify the status of the LDT GuardPoint Group, type:

```
voradmin ldt group check <guard path>
```

- If node E displays as UNKNOWN, even after rebooting, check if the network share is mounted on E. If it's not mounted, fix the network connectivity. Once resolved, node E should rejoin the LDT GuardPoint Group as a secondary.
- If node E does not resume, remove the node from the LDT GuardPoint Group. On the LDT primary node D, type:

```
voradmin ldt group remove E <guard path>
```

Primary Node Crash(Non-Triad Node)

Scenario

Same setup as above, with node D acting as the LDT primary. After some time, node D crashes.

Troubleshooting Scenario

1. If node D does not resume, remove the node from the LDT GuardPoint Group. On any secondary nodes, type:

```
voradmin ldt group remove D <guard path>
```

2. If node D resumes, but fails to guard the share, repair the LDT GuardPoint Group from any of the secondary nodes (E or F), type:

```
voradmin ldt group repair D <guard path>
```

Communication Group in Inconsistent State

Scenario

- Nodes A, B, C, D, and E are part of the LDT Communication Group.
- A, B, and C are Triad nodes.
- An NFS/CIFS share is guarded on nodes C, D, and E, with D as the primary and C and E as secondaries.

Nodes A and B (both Triad nodes) fail at the same time (gracefully or ungracefully), the LDT Communication Group enters an inconsistent state.

Troubleshooting Scenario

Restart the secfsd service on all nodes to restore the LDT Communication Group.

For **Windows**:

1. Go to **Control Panel > Services (local)**.
2. Select **secfsd**.
3. Select **Stop the Service**.
4. Wait a few moments and select, **Start the service**.

For **Linux**:

1. Type:

```
/etc/vormetric/secfs stop
```

2. Type:

```
/etc/vormetric/secfs start
```

Primary Node Ungraceful Reboot (Triad Node)

Scenario

- Nodes A, B, C, and D are in the LDT Communication Group.

- Nodes A, B, and C are the Triad nodes.
- A NFS/CIFS share is guarded on all nodes
- Node A is the primary for the GuardPoint.

Node A undergoes maintenance or a software update, and is rebooted with the expectation of a graceful failover to one of the secondary nodes. However, failover does not occur, and once node A comes back up, it fails to guard the network share and in the output of `secfsd -status guard`, it displays: `Group Join Failed, needs LDT repair`

Explanation

During the shutdown, the `secfs` service is stopped, which disables all GuardPoints. A successful disable operation triggers failover to another secondary node. However, if the system proceeds with shutdown before the service is cleanly stopped, it results in an ungraceful shutdown, and the failover does not occur.

Troubleshooting Scenario

- Run the repair command from any active secondary node, type:

```
voradmin ldt group repair <failed hostname> <guard path>
```

LDT GuardPoint Group Commands

Prerequisites for CIFS Share drives

Prior to running the `voradmin ldt group` commands, you must:

1. Ensure that you have access and permission to read/write to/from the CIFS share.
2. Mount the CIFS share using the `net use` command, or login to the CIFS shares using Windows Explorer.

Group check

The `group check` command is used to send out an internal ping to all hosts that are registered with the master as part of the LDT Communication Group. Each functioning host responds. Then the host displays a message of the hosts in the LDT Communication Group that did not respond. This allows an administrator to easily find the problem.

Syntax

```
voradmin ldt group check <gp_path>
```

Example (Windows)

```
voradmin ldt group check \\192.168.1.160\share
```

Hostname	Role	State	GuardPoint Path

192.168.1.161	PRIMARY	JOINED	\\192.168.1.160\share
192.168.1.162	SECONDARY	JOINED	\\192.168.1.160\share

Example (Linux)

```
voradmin ldt group check /nfs1/gp
```

Role	State	Hostname	GuardPoint Path
PRIMARY	JOINED	host1.domain	/nfs1/gp1
SECONDARY	JOINED	host2.domain	/nfs1/gp1

Info

Use the `info` command to display information about the cluster.

Syntax

```
voradmin ldt group comm_info <gp_path>
```

Example (Windows)

```
voradmin ldt group comm_info \\192.168.1.160
```

```
LDT Communication Group Master IP:      10.171.34.111
LDT Communication Group Master Port:    7024
LDT Communication Group Name:           tanmay_windows
LDT Communication Group Servers:        10.171.34.111,10.171.34.120,10.171.34.11
9
```

Example (Linux)

```
voradmin ldt group comm_info /nfs1/gp1
```

```
LDT Communication Group Name:           tanmay-linux
LDT Communication Group Master IP:      10.171.47.121
LDT Communication Group Master Port:    7024
LDT Communication Group Servers:        10.171.47.241,10.171.47.121,10.171.47.75
```

Remove

This command allows a client to be manually removed from the group safely. Use the `Remove Host` command if a client dies without properly leaving the group.

Note

Only run this command on clients which will be powered off. Do not run it on a client which may simply have temporary network issues.

Syntax

```
voradmin ldt group remove <hostname> <GuardPoint pathname>
```

Example (Windows)

```
voradmin ldt group remove host42 \\server\share
```

WARNING: This command will forcibly remove host42 from the LDT group for gp_path. You should only perform this step if the host is guaranteed to be powered off, otherwise a loss of data may result. Do you wish to continue? (Y/N)

Example (Linux)

```
voradmin ldt group remove host2 /nfs-ldt
```

host2 has been removed from the group for GuardPoint /nfs-ldt

Repair

Run the following command to manually clean up the group and allow the primary to rejoin as a member. The Client will complete the guard operation once the group has been repaired.

```
voradmin ldt group repair /<primary IP> <absolute GuardPoint> (Windows)
```

```
voradmin ldt group repair /<primary IP> <${gp}> (Linux)
```

Sharing LDT NFS/CIFS GuardPoints between Linux and Windows

An LDT GuardPoint Group is used to organize clients guarding the same NFS or CIFS share. In CTE 7.5.0 or previous versions, each group could only contain Linux or Windows members, and not a mix of the two. Starting with CTE 7.6.0, it is now possible to have Windows clients as AccessOnly clients to guard a share that is part of a Linux LDT GuardPoint Group. Refer to [Configuring CTE Windows LDT AccessOnly nodes](#) for more information on AccessOnly clients.

Windows LDT is capable of mixing AccessOnly, and non-AccessOnly clients, in an LDT GuardPoint Group accessing a share through CIFS protocol. This capability is possible because of the CIFS protocol supporting exclusive access to a file from a remote node. Linux LDT does not support AccessOnly clients because the NFS protocol does not support exclusive file access capability. Therefore, an AccessOnly client is not privy to LDT messages between clients. The Windows client can only access a Linux based LDT GuardPoint Group while a GuardPoint is rekeyed. As such, Windows clients can only guard after the Linux primary client has completed rekey on the GuardPoint. Subsequently, the GuardPoint must be unguarded on Windows clients before any subsequent key rotation begins. Failure to do so will cause data corruption as any write operation from the Windows client may write without any coordination with the Linux primary client performing transformation.

The capability to allow Windows and Linux clients to guard the same GuardPoint is supported on GuardPoint directories which have been guarded for the first time, and completed the initial transformation, by a CTE 7.6.0 Linux client. This restriction is in place because there are metadata format changes in newly created GuardPoints to support sharing access between Linux and Windows clients.

Note

Access to shared GuardPoints is available through NFS on Linux and CIFS on Windows.

Windows clients are blocked from accessing files marked with a lazy_rekey flag. This is because the files marked with a lazy_rekey flag will launch the data transformation process the next time a Linux member of the LDT GuardPoint Group accesses the file without any awareness of Windows clients sharing access to the GuardPoint.

Although there is no communication between Windows and Linux clients for sharing access to GuardPoints, there is awareness of shared access across the clients because of the LDT metadata changes applied to the newly created GuardPoints for sharing on both platforms. Both platforms apply compatible LDT metadata when creating new files.

Finally, suspending rekey does not qualify Windows clients to guard and share access. Rekey must be completed before Windows clients can attempt to guard.

LDT Communication Group

All members of an LDT Communication Group must be Linux CTE clients. Windows clients do not belong to LDT Communication Groups because of AccessOnly mode configuration.

Limitations

- Only new GuardPoints are supported in v7.6.0.
- All existing CTE clients must be upgraded to CTE Agent v7.6.0, or a subsequent version.
- Guarding a GuardPoint for the first time on Windows disqualifies the GuardPoint for sharing between Windows and Linux, and subsequent attempts on a Linux client to guard.
- Windows AccessOnly client fails to guard the GuardPoint while rekey is suspended.
- All Windows clients must unguard before the key rotates on CipherTrust Manager.

Limitations

The following limitations exist for LDT over CIFS/NFS:

Windows

- Only supported for customers using unstructured data.
- LDT over CIFS is not supported on single processor systems.
- All nodes sharing a CIFS drive **must** have homogenous system drivers installed. You **cannot** have some nodes installed with the `vm\lfs.sys` driver and some installed with the `vm\filtr.sys` driver. That scenario is not supported.

Note

To determine which driver your node has installed, type: `fltmc` from the administrative command line.

Linux

- Although CTE supports GuardPoints over NFS shares using NFS v3 and v4 protocols, Thales strongly recommends using NFS v4 protocols, or a subsequent version, when using LDT policies.
- CTE **does not support** mixing NFS v3 and v4 protocols on different CTE hosts for accessing the same GuardPoint. All members of an LDT GuardPoint Group must access the same GuardPoint using the same NFS protocol version.
- When installing CTE patches, make sure that the new patch is compatible with CTE latest release. Follow instructions in the release note for a patch release, if any, for upgrading CTE hosts sharing access to the same GuardPoints across multiple hosts.
- Other current limitations will be removed over the next several patches. Refer to the release notes to determine which limitations, noted below, have been removed:
 - a. Applications will experience performance degradations on secondary hosts when targeting files undergoing rekey, even while LDT is suspended. LDT disables read-ahead on files undergoing rekey on secondary hosts resulting in lower IO throughput.
 - b. Loss of network connectivity to the NAS server from the primary host during active rekey can block access to files undergoing rekey across all members of LDT GuardPoint Groups for all GuardPoints on the NAS server.
 - c. If the secfsd daemon fails on a secondary host, it will require rebooting the host and removing the secondary host from each LDT GuardPoint Group on that secondary host prior to reboot. If the secfsd daemon fails on the primary host, it also requires rebooting the primary host and the delegation of the primary role to one of the secondary members of the LDT GuardPoint Group.

Key Guidelines for Configuration of an LDT Communication Group

1. You must create an LDT Communication Group on your CipherTrust Manager and manually add all of the CTE clients to it sequentially.
2. Minimum of three CTE clients required for membership to the LDT Communication Group for proper and continuous operations of LDT services across all LDT GuardPoint Groups. (Four is better, but three is required).
3. The first three nodes of the LDT Communication Group are critical and **cannot** be removed or shutdown/

reboot simultaneously.

4. All nodes, Windows and Linux, **must be running** CTE 7.5.0, or a subsequent version, in order for the nodes to communicate properly.
5. The majority of the CTE clients must be fully operational for proper LDT operations across all LDT GuardPoint Groups.

The LDT Communication Group requires that the majority of CTE clients are active, in order for the LDT Communication Group to work properly. If 50% of the LDT Communication Group servers, or 2 out of 3 **triad** nodes fail, then the LDT Communication Group cannot recover from that situation. To fix this issue, you must either:

- Reboot all of the CTE clients in the entire LDT Communication Group.
 - In Windows, restart **secfsd** through the **Control Panel > Services** page on all of the CTE clients in the entire LDT Communication Group.
6. The name of the LDT Communication Group cannot contain special characters.
 7. If you are repurposing a CTE client that is currently being used for LDT over NFS/CIFS, but still runs CTE and is still registered to the same CM, then you must:
 - a. Remove all CIFS/NFS LDT GuardPoint Groups from the host prior to removing the host from the LDT Communication Group.
 - b. Reboot the host.
 8. Remove a host from the LDT Communication Group if the host is being decommissioned, meaning that you plan to power it down for the foreseeable future, or while CTE is being uninstalled.
 9. Triad nodes must be on the same subnet with low-latency network connections to ensure stable failover.
 10. If a triad node is permanently down, remove it from CipherTrust Manager to allow a new node to join the triad. If 2 out of 3 triad nodes fail, the LDT Communication Group cannot recover automatically. Once the crashed nodes are back, restart **secfs** on all nodes in the group to restore communication.

Key Guidelines for Configuration of an LDT GuardPoint Group

- Failover, after an ungraceful failure, is manual. If a primary node becomes unavailable and LDT cannot automatically reassign the primary to another CTE client, the administrator must manually assign another CTE client as the primary node. See [Failover](#) for more information.

LDT Communication Group and LDT GuardPoint Group

- For continuous and seamless synchronization and control between all clients (excluding Windows AccessOnly clients) in an LDT Communication Group, in the LDT over CIFS/NFS environment, the **secfsd** service on each client must be continuous and uninterrupted. LDT support for NFS and CIFS depends on continuous
-

availability of the `secfsd` process for management and availability of LDT GuardPoint Groups and continuous flow of LDT messages from primary hosts to members of the LDT GuardPoint Groups during rekey.

In the event that the `secfsd` process abruptly fails and/or restarts for any reason, the LDT GuardPoint Groups will be erased on the CTE hosts and the LDT message flow to/from the CTE client to other members of the LDT GuardPoint Groups stops. The only method for recovering from this event is to reboot the CTE host. **Do not** terminate the `secfsd` process on the primary host, as this results in the election and promotion of another member of the LDT GuardPoint group to the primary role.

LDT Reverse Migration

- Converting LDT CIFS/NFS GuardPoints from Live Data Transformation policies to Standard CTE policies is not supported.
- LDT CIFS/NFS-protected GuardPoints cannot be migrated to `clear_key`.
- Reverse migration is **not** supported for network shares.
- LDT over CIFS/NFS **DOES NOT** support rolling back migrations.

Prerequisites

For LDT over CIFS/NFS to work properly, see Installation Prerequisites of the CipherTrust Quick Start Guide.

Space Required

The space requirements for share drives is the same as the requirements for local file systems. However, you must plan for additional space for metadata. Refer to [Planning for LDT Attribute Storage](#) for calculating space.

Network and Port requirements

- Ports 7024 and 7025 must be open on all triad nodes.
- Port 7024 is used for master-replica communication.
- Port 7025 is used for communication group monitor process.
- For optimized performance, put the triad nodes on the same subnet. Locate them close to each other with a low-latency network connections. High round-trip time (RTT), or unstable networks, can cause unnecessary master failovers and impact LDT GuardPoint Group health.

Supported Versions

Linux

Upgrade your CTE Agents to CTE v7.2.0 or later, and your CipherTrust Manager to version 2.7 or later, in order to

support LDT GuardPoints on NFS shares. It is not supported for earlier versions. You can use the standard upgrade procedure for both the CTE Agents and CipherTrust Manager. See the [CTE Agent for Linux Quick Start Guide](#) for more information.

Windows

On Windows, you must install the full version of CTE 7.2. Guarding CIFS/SMB shares with LDT GuardPoints is not supported in the upgrade version of CTE. Refer to the [CTE Agent for Windows Quick Start Guide](#) for more information. Requirements for GuardPoints

On Windows, the requirements for GuardPoints created on CIFS shares using LDT are different from those created on local directories or for those created on CIFS shares using standard CTE policies. You cannot mix the two on a single host. Instead, each host must contain either LDT CIFS share GuardPoints or local directory/standard policy GuardPoints.

If you want to use LDT on a CIFS share which contains GuardPoints on a host on which the CTE Agent is already installed, you must:

1. Remove any existing local directory GuardPoints.
2. Uninstall the current version of CTE Agent from the host.
3. Install CTE Agent version 7.5.0 or higher and respond **Yes** when prompted about guarding network shares.

If you do not see this prompt during installation, make sure that you have fully uninstalled the previous version of the CTE Agent.

Administering LDT over CIFS/NFS with CipherTrust Manager

The following sections contain information about the administration tasks required for using LDT over CIFS/NFS.

- [Adding a CIFS Connector for CipherTrust Manager](#)
- [Configuring CTE Windows LDT AccessOnly nodes](#)
- [Policy and GuardPoint Management](#)
- [Key Rotation Commitment](#)
- [LDT Metadata Management Over NFS/CIFS Shares](#)
- [Backup and Restore LDT on NFS GuardPoints](#)

Adding a CIFS Connector for CipherTrust Manager

In order to create GuardPoints on a CIFS share, you must obtain credentials for the CIFS share and add it as a connector in CipherTrust Manager.

CIFS Credentials

Prior to guarding data on the CIFS share, LDT needs permissions to access the share drive and its data and for

saving metadata to the CIFS share. CipherTrust Manager stores the CIFS Share credentials centrally. Credentials are protected similarly to the way CTE protect keys and policies. These credentials are associated with a GuardPoint. The CM pushes the credentials to the host and LDT uses them. Thales recommends customers create a new LDT account that contains a user name, password and domain, to access the CIFS share with read/write permissions. Users must not share their user accounts.

Adding the CIFS Share to CipherTrust Manager

In order for LDT to access that CIFS share and encrypt the data, you must provide the credential data when you add a CIFS share as a connector in CipherTrust Manager:

1. Log in to CipherTrust Manager as an administrator.
2. On the main screen, in the sidebar on the left, click **Access Management > Connections**.
3. Click **Add Connection**.
4. Click **File-Share**.
5. In the Select File-Share type field, select **CIFS/SMB** and click **Next**.
6. Enter a name and description for the connection and click **Next**.
7. Enter appropriate information for the fields:
 - **Host:** IP or FQDN of the CIFS share server
 - **Port:** Port where the CIFS service is running on the host
 - **Username:** Username to access the CIFS share
 - **Password:** Password to access the CIFS share
 - **Domain:** Domain under which the username is configured (Optional)
 - **Path:** Path to the CIFS file-share for which the credentials need to be tested (Optional)

Note

If you want to change a user name, domain or password of a CIFS credential in a CM connection, then you need to create a new connection on CM and change the GuardPoint to use the new connection.

Add Connection [X]

1 Select Connection Type 2 General Info 3 **Configure Connection** 4 Add Products

Host* 192.168.1.160 Port* 445

Username* ldfuser

Password* [masked]
☐ Show Password

Domain WinSrv

Test Path* \\192.168.1.160\share

Status: OK
 Tested: 19 November 2021 08:52

Back

8. Click **Next**.
9. In the Products list, select **CTE** and click **Save**.

LDT AccessOnly nodes

- Configuring CTE Windows Deployment for LDT AccessOnly nodes
- Configuring LDT for CIFS shares (with LDT AccessOnly nodes) Mapped to Multiple IP addresses

CTE Windows Deployment for LDT AccessOnly nodes

Currently, Windows clients that attempt to access CIFS paths must be part of an LDT Communication Group. The LDT Communication Group assigns the role of primary node to one of the clients, which performs LDT data rekeying. All of the other clients are assigned as secondary nodes, and they do not participate in rekeying data.

This is important to note because there are specific use cases which require that some of the nodes accessing a GuardPoint do not join the LDT Communication Group, such as when:

- All of the nodes accessing the GuardPoint are not able to communicate to other servers in the LDT Communication Group due to differences in security policies. Nodes with weaker security policies are left out of the LDT Communication Group to ensure the LDT Communication Group maintains a highest level of security.
- Certain nodes, which go through frequent network disconnects, should not participate in the LDT

Communication Group to again, ensure the highest level of security. For example, windows endpoint protection clients or laptop users.

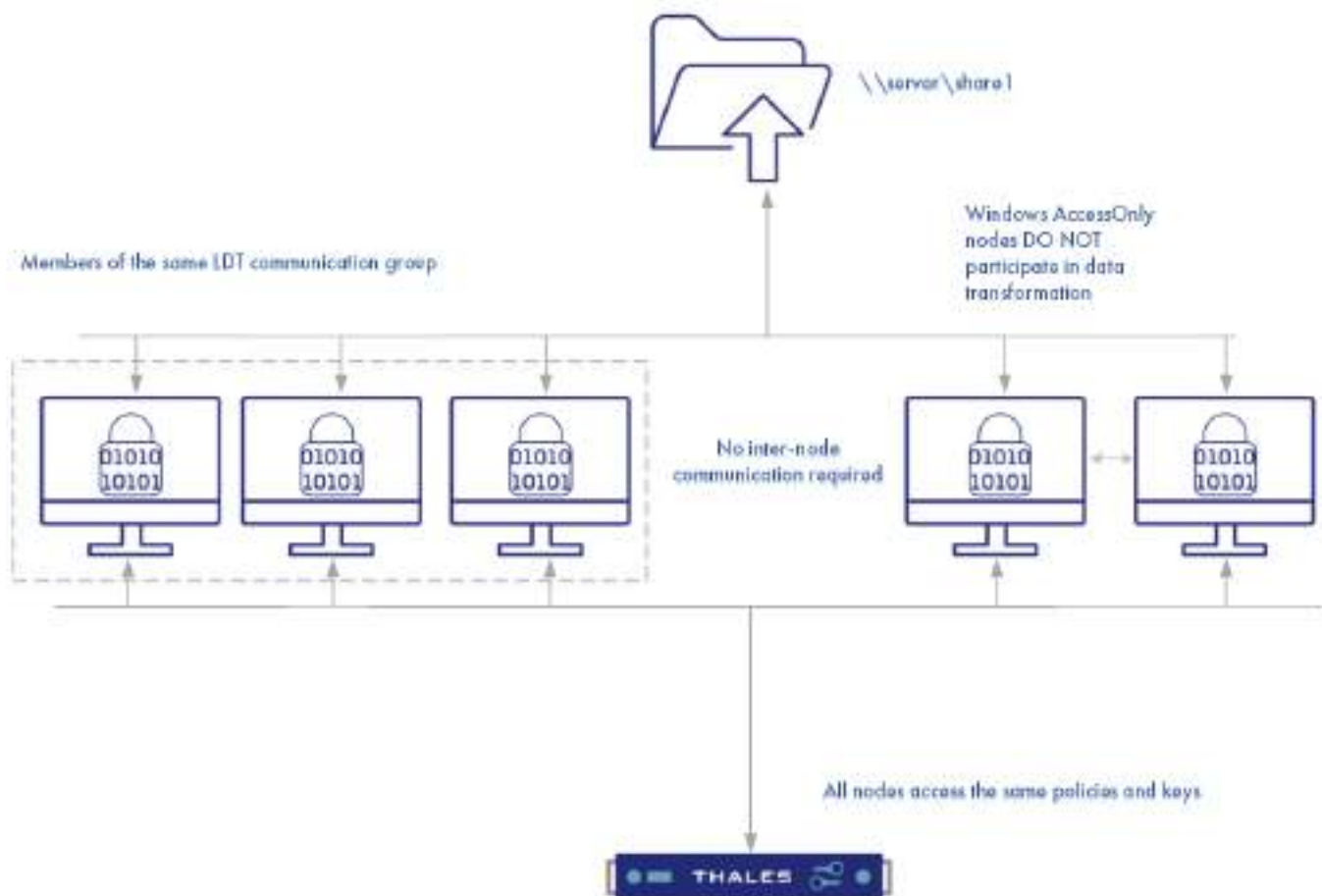
To overcome these limitations, CipherTrust Transparent Encryption has a new feature called **Windows AccessOnly**. AccessOnly clients:

- **Do not** participate in data transformation.
- **Cannot** become part of an LDT Communication Group
- **Have** the same CIFS GuardPoint applied on them as other LDT GuardPoint Group nodes

Best Practices with AccessOnly nodes

- Do not assign a primary or secondary role to them.
- Apply GuardPoints on CIFS paths from LDT GuardPoint Group nodes, BEFORE applying the same GuardPoints to Access Only nodes.

The following illustration shows a typical setup for a network with LDT clients and Windows AccessOnly clients:



Note

- An AccessOnly node can set a GuardPoint, however, a node in the LDT Communication Group will be the system to rekey the GuardPoint.
- When an LDT rekey is in-progress, AccessOnly nodes cannot access the files being rekeyed.

Warning

All CTE AccessOnly agents, in an LDT Communication Group, **must** have CTE v7.4.0 or subsequent versions, installed. Agents that contain a previous version **must be** upgraded.

Setup and Configure Windows AccessOnly Nodes for LDT CIFS

The new role, **LDT AccessOnly**, can be assigned to any CipherTrust Transparent Encryption Windows client in multiple ways.

1. Agent registration:

- During Agent registration, a new option **AccessOnly (No LDT Transformation)** displays. Select it to setup the client as a Windows AccessOnly client.

Note

If you enable it, then the option to specify an LDT Communication Group name is disabled.

2. On CipherTrust Manager:

- In the client details page, there is a checkbox to enable/disable LDT AccessOnly.

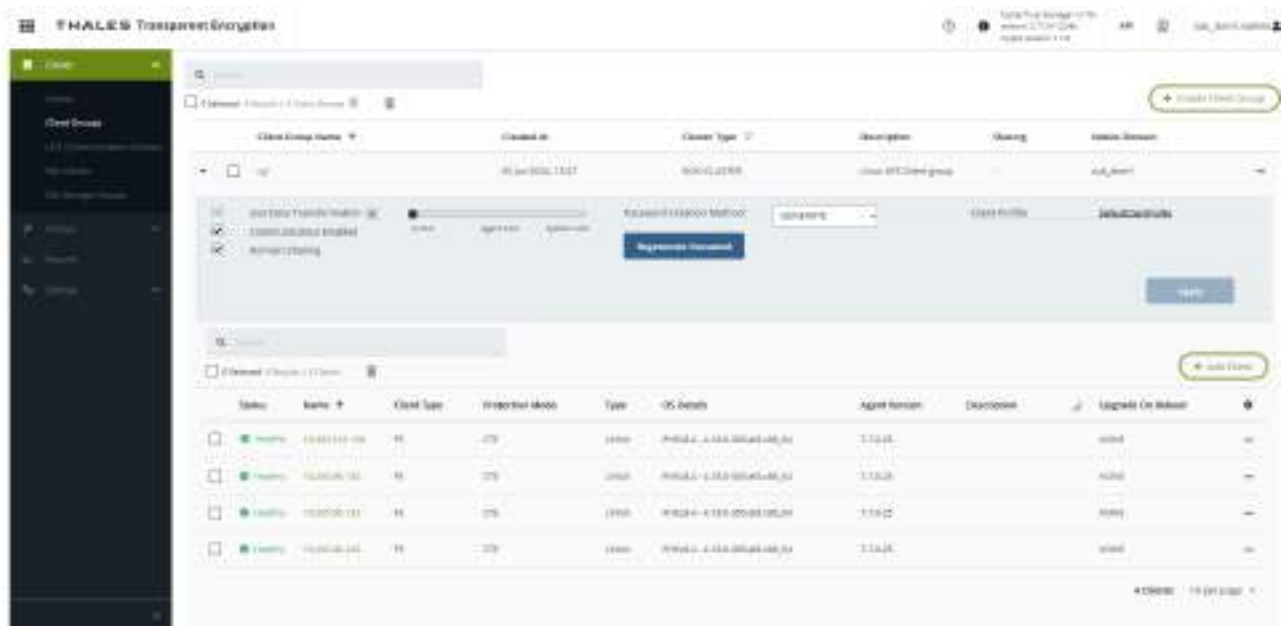


Note

You cannot assign a node to be Windows AccessOnly before removing it from an LDT Communication Group.

Creating the Setup

1. On CipherTrust Manager, create a Windows LDT AccessOnly Client Group.



2. Add the Windows LDT AccessOnly clients to the Windows Client Group.
3. Create the GuardPoint.
 - a. Select the same LDT policy that you used for the clients participating in initial transformation.
 - b. Mount **the same** path on **each** client to participate in the transformation of the GuardPoint, or in the client group containing those clients. Example path: `\\192.168.1.100\Share1\Data1`.
4. Once the has fully completed initial data transformation, and the status is REKEYED, then create the GuardPoint in the Windows Access-Only Client Group. All Windows LDT AccessOnly clients will now be able to guard and access the files.
 - a. Select the same LDT policy that you used for the clients participating in initial transformation.
 - b. Mount **the same** path on **each** client to participate in the transformation of the GuardPoint, or in the client group containing those clients. Example path: `\\192.168.1.100\Share1\Data1`.

Converting a Windows AccessOnly node to an LDT node

1. Unguard/Disable the GuardPoint from the Windows AccessOnly node.
2. Un-check the **LDT Access Only** option in the CipherTrust Manager Client Window.
3. Add the client to a relevant LDT Communication Group.
4. Enable/Apply the GuardPoint on the CIFS path from this converted LDT node.

Converting an LDT node into a Windows AccessOnly node

- You **must remove them** from the LDT Communication Group **before** enabling the **LDT Access Only** option.

Backup/Restore from Access-Only nodes when LDT is in progress

- While LDT is in progress, backup/restore from Windows AccessOnly nodes is not recommended. Backup/Restore must be performed from **Primary** or **Secondary** nodes in the LDT Communication Group. This is because while LDT is in progress, files under rekey may not be accessible from Windows AccessOnly nodes. This may cause the Backup/Restore process to fail as file access is denied.

Configuring LDT for CIFS shares Mapped to Multiple IP addresses

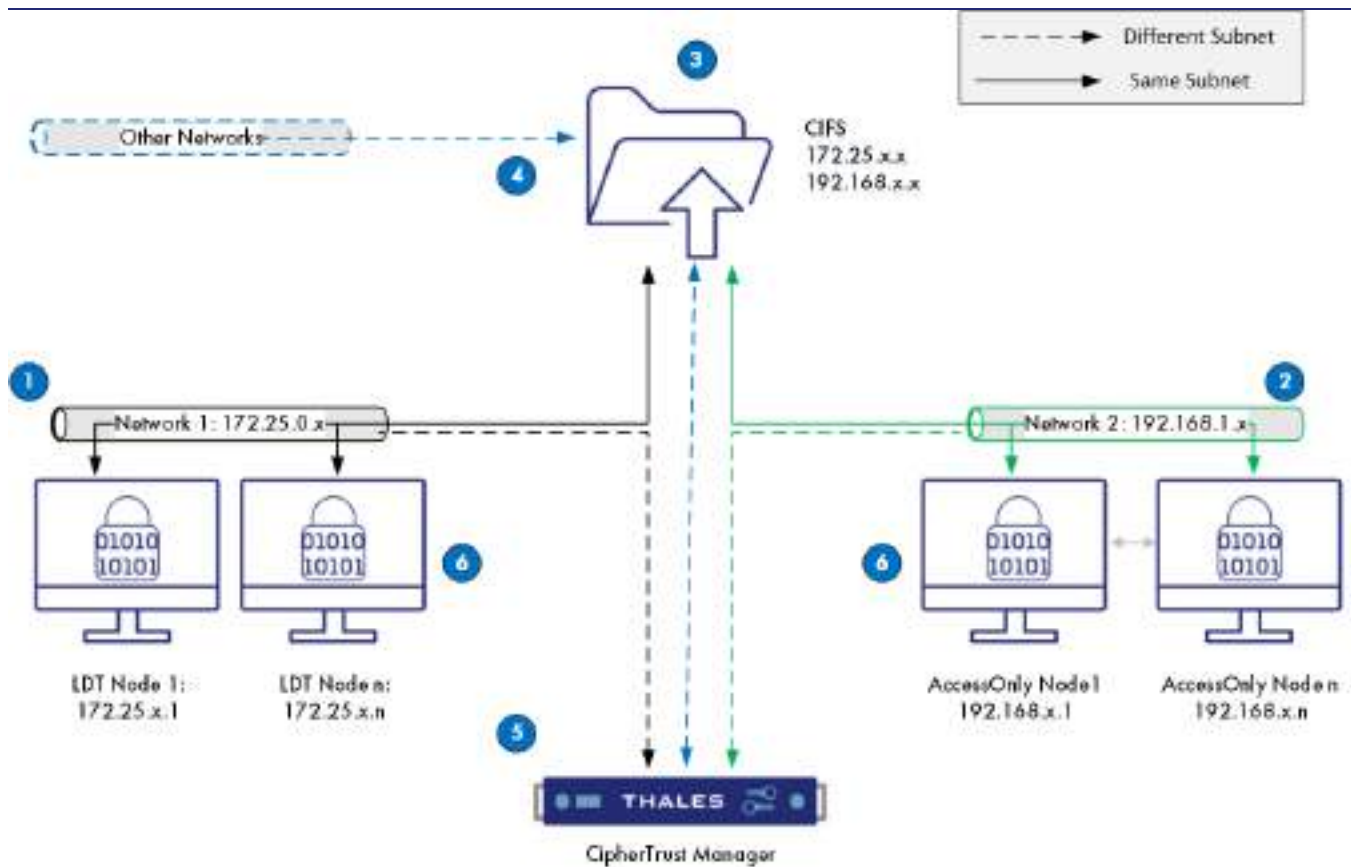
This feature allows you to apply the same GuardPoint to two IP addresses that point to the same CIFS share. This can be useful because different applications may use different IP addresses for accessing data.

Note

This feature is available only when using LDT AccessOnly nodes.

Network Setup for CIFS shares Mapped to Multiple IP addresses

The following illustration shows how to setup your network. The table below explains the setup in more detail:



In the above sample diagram:

#	Description
1	LDT nodes are connected to Network 1
2	LDT AccessOnly nodes are connected to Network 2
3	CIFS server is connected to both Network 1 and 2, and have one IP address corresponding to each network
4	CIFS server may also be connected to more networks, based on use case and requirement
5	CipherTrust Manager can be connected to Network 1, 2 or some other network
6	Network 1 and 2 nodes can reach CipherTrust Manager and vice versa

Creating the Setup

1. Register LDT nodes from Network 1 on CipherTrust Manager and add them to the LDT Communication Group.
2. Create a CIFS\SMB share connection on CipherTrust Manager, using one of the two IP addresses of the CIFS machine, preferably IP 1.

3. Register the Windows AccessOnly nodes from Network 2 to CipherTrust Manager.
4. Create two **Client Groups**: one for the LDT nodes and one for the Windows AccessOnly nodes
5. Apply **GuardPoints** in both client groups using the respective network IP addresses.
6. Access the protected CIFS path using the respective IP addresses.

Policy and GuardPoint Management

You can use the same LDT policies that you use for protecting GuardPoint directories in local file systems and NFS/CIFS shares. The only exception is that for LDT protected GuardPoints, it only supports backup/ restore of files that do not use Apply Key.

Security Rule Ordering for Policies

If you want to enforce restrictions when guarding NFS/CIFS shares using an LDT or standard policy with a **CBC-CS1** key, note the following:

CipherTrust Transparent Encryption embeds the LDT and/or IV (initialization vector) attributes in the first 4K of files for NFS/CIFS shares guarded with an LDT or standard policy with a **CBC-CS1** key. Embedding CipherTrust Transparent Encryption attributes increases the actual file size by 4K. CTE hides that extra 4K when reporting the file size to users, or processes, that access the file with the Apply Key effect.

If you need the actual file size, or read/write access on the embedded header, for backup/restore processes for example, then you need a rule that permits access without Apply Key.

LDT Policies

Example 1: Permits Backup and Restore

A policy that allows backup and restore of encrypted data, clear-text access to certain processes, and denies access to all others:

Order	Resource Set	User Set	Process Set	Action	Effect	Browsing	
1				Reg. Op	permit, applykey	No	
2			backup	all_ops	permit, audit	Yes	
3			authorized-processes	all_ops	permit, audit, applykey	Yes	
4				all_ops	deny, audit	Yes	

Rule	Purpose
1	Default LDT rule required for LDT policies.
2	Allows for processes in the backup Process Set to access the real file size and backup the CipherTrust Transparent Encryption attributes along with the encrypted file data.
3	Allows for processes in the authorized-processes

Rule	Purpose
	Process Set to access the clear-text data, but it hides the additional 4K from the CipherTrust Transparent Encryption attribute.
4	Denies all other processes access to the data.

Example 2: Permits access to certain Processes

A policy that only allows certain processes clear-text access but allows all others to see the OS file attributes.

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1				key_op	permit:applykey	No	
2			authorized-processes	all_ops	permit:audit,applykey	Yes	
3				f_read,f_read_dir	permit:audit	Yes	
4				all_ops	deny:audit	Yes	

Rule	Purpose
1	Default LDT rule required for LDT policies.
2	Allows for processes in the authorized-processes Process Set to access the clear-text data.
3	Allows for processes not in the authorized-processes Process Set to read the OS file and directory attributes. Note: Processes that match this rule obtain the file size with the 4K header. If a process that is not in the authorized-processes Process Set needs the file size without the header, then the Apply Key must be present in the Effect or you will need an additional rule granting Apply Key to that specific process. That rule must be defined before this rule.
4	Denies processes not in the authorized-processes Process Set from reading any data from the files.

Standard Policies

Example 1: Permits access to certain Processes

A policy that allows backup and restore of encrypted data, clear-text access to certain processes, and denies access to all others:

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1			backup	all_ops	permit:audit	Yes	
2			authorized-processes	all_ops	permit:audit,applykey	Yes	
3				all_ops	deny:audit	Yes	

Rule	Purpose
1	Allows for processes in the backup Process Set to access the real file size and backup the CipherTrust Transparent Encryption attributes along with the encrypted file data.
2	Allows for processes in the authorized-processes Process Set to access the clear-text data, but it hides the additional 4K from the CipherTrust Transparent Encryption attribute.
3	Denies all other processes access to the data.

Example 2: Permits access to certain Processes

A policy that only allows certain processes clear-text access but allows all others to see the OS file attributes.

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1			authorized-processes	all_ops	permit:audit,applykey	Yes	
2				file_audit_read_secu...	permit:audit	Yes	
3				all_ops	deny:audit	Yes	

Rule	Purpose
1	Allows for processes in the authorized-processes Process Set to access the clear-text data.
2	Allows for processes not in the authorized-processes Process Set to read the OS file and directory attributes. Note: Processes that match this rule obtain the file size with the 4K header. If a process that is not in the authorized-processes Process Set needs the file size without the header, then the Apply Key must be present in the Effect or you will need an additional rule granting Apply Key to that specific process. That rule must be defined before this rule.
3	Denies processes not in the authorized-processes Process Set from reading any data from the files.

For more information, see [Adding Security Rules](#) in the CipherTrust Manager documentation.

Creating a GuardPoint on a CIFS Share Drive on CipherTrust Manager

Creating GuardPoints on a CIFS share drive requires you to add the CIFS share drive to CM as a connector first, and then select it as a network drive.

To add the CIFS share in the CipherTrust Manager Connection Manager, see [Adding a CIFS Connector for CipherTrust Manager](#).

Note

For the host name, use the IP address if the host name does not work.

GuardPoint Naming

When creating GuardPoints in a CIFS share, you must use the UNC name. A Universal Naming Convention (UNC) format name defines the location of files and other resources that exist on a network. UNC provides a format so that each shared resource can be identified with a unique address.

UNC names must conform to the `\\SERVERNAME\SHARENAME` syntax, where **SERVERNAME** is the name of the Provisioning Server and **SHARENAME** is the name of the shared resource.

- UNC names can also include the directory path:

`\\SERVERNAME\SHARENAME\DIRECTORY\FILENAME`

- To define a folder that contains a configuration database file in:

`C:\Program Files\Oracle\customer_data`

- On the shared server, enter:

`\\server1\customer_data`

Selecting the CIFS Share Drive for Guarding

When you create a GuardPoint for CIFS shares, you will have more options when browsing for the file system to guard. You can select to guard a local path, or a network path.

To create the GuardPoint on the CIFS share:

1. In CTE, select **Clients**.
 2. Click on the Client to access it.
 3. Click **Create GuardPoint**.
 4. Select a **policy** and **type**.
 5. For Path, click **Browse**.
-

6. In the Browse Path dialog, select **Network Path**.

Browse Path

Path Type: *

☐ Local

☒ Network Path

User Name: *

Thales-Admin

Password: *

Domain

CPL_Internal

Search Network Path * ?

\\192.8.0.14\cifs_share1

Refresh


C:
D:

[Back](#) [Add](#)

7. Enter the **User Name** and **Password for the CIFS share drive.
8. Enter a **domain/IP address** for the CIFS share drive.
9. Enter the **UNC name** for the Network Path.
10. Click **Refresh** to test the connection.
11. Select the directories to guard.
12. Click **Add**.
13. In the Create GuardPoint window, select the **SMB** connection to use.
14. Click **Create**.

Create GuardPoint

×

Policy: *

Pol1-LDT-CIFS

Select

Type: *

Auto Directory

Path: *

☒ Enter/Browse Path
 ☐ Upload CSV

\\10.171.83.35\Gillian_CIFS_Share\Test-GP\

Browse

ⓘ To apply the same GuardPoint settings to multiple paths, type paths in the Path field or specify them using the Browse button. A maximum of 200 GuardPaths can be specified.

SMB Connection: *

Cifs-10.171.83.1

Preserve Sparse Region: ☒

Secure Start: ☐

Cancel

Create

Use the GuardPoint Settings on another GuardPoint

1. If you want to guard another GuardPoint on a different path, click **yes** to the question: **Would you like to use these GuardPoint settings on another guard point with a different path?**
2. Select the path for the GuardPoint and click **Create**.

Verifying the GuardPoint

- Before starting the application or accessing the data, you must ensure that the GuardPoints are guarded successfully. Check the status on CM or by running the `voradmin ldt stats` command.
- For Linux, LDT Communication Group member hosts cannot guard or unguard GuardPoints that have single file rekey jobs in progress. Attempts to guard or unguard result in a warning message and the operation is automatically retried until all single file rekey jobs are finished and the state of the GuardPoint can be changed.

Accessing the GuardPoint

If a GuardPoint is applied on a CIFS share on a CTE client, you can only access the data from a CTE client that has CTE installed on it. You cannot access the CTE client from an agent that does not have CTE installed.

Pausing and Resuming LDT per host and per GuardPoint

Rekey operations on a GuardPoint can only be paused or resumed by the primary host for that GuardPoint. You must run the `voradmin` command on the primary host for the GuardPoint. If multiple GuardPoints reside on the same CTE host, and the host is the primary for some of the GuardPoints and the secondary for other

GuardPoints, the `voradmin` command is applied only on the GuardPoints for which the CTE host holds the primary role.

The same applies if you pause or resume GuardPoints on a host using CipherTrust Manager. Pausing or resuming LDT on a host from CipherTrust Manager only applies to the GuardPoints for which the host holds the primary role.

Migrating GuardPoints over NFS from or to an LDT Policy

GuardPoints over NFS can be guarded using policies with key rules specifying a mix of CBC or CBC-CS1 keys.

You can migrate to an LDT policy from clear text (no existing policy) or from a standard CTE policy. If the standard policy uses:

- **CBC keys**

The CBC keys are transformed during the initial data transformation when LDT embeds the LDT metadata in the beginning of each file. LDT shifts the existing data in the files by 4096 bytes to make room for the LDT metadata.

- **CBC-CS1 keys**

The IV attribute is already embedded in the protected files. LDT transforms the files in those GuardPoints without shifting the existing data because the required IV attribute already exists.

Migration out of an LDT policy is only *partially* supported because of the shift to the existing data that was done to accommodate the LDT metadata. You can only migrate from a Live Data Transformation policy that uses CBC or CBC_CS1 keys to a different Live Data Transformation policy that uses CBC or CBC_CS1 keys. You cannot remove the Live Data Transformation policy from a guarded directory, and you cannot migrate from a Live Data Transformation policy to a standard CTE policy. The migration support matrix is shown in the following table.

Source Policy Type	Target Policy Type	Supported?
Live Data Transformation using CBC or CBC_CS1 keys	Live Data Transformation using CBC or CBC_CS1 keys	Yes
Live Data Transformation	No policy (unguarded directory)	No
Live Data Transformation	Standard CTE policy	No
Standard Policy using CBC or CBC_CS1 keys	Live Data Transformation using CBC or CBC_CS1 keys	Yes

The only method for migrating an NFS GuardPoint from LDT to clear-text or to a CTE standard policy that uses CBC or CBC_CS1 keys is the following:

1. Perform a full backup of files in the NFS GuardPoint in clear text. Make sure that you disable the security rule for the backup process in the LDT policy, if the security rule skips Apply Key as part of backup operation.
2. Upon completion of full backup, unguard the directory on the key manager and then remove the LDT Private Space directory (`ldtprivspace`) in the NFS GuardPoint using the `voradmin ldt rmltdt <GuardPoint>` command.
3. Remove the remaining files inside the NFS GuardPoint directory and restore the full backup of the files in clear-text over the NFS GuardPoint directory. If you are migrating to a standard CTE policy, you can now proceed with re-guarding the NFS GuardPoint directory using the standard policy.

Multiple GuardPoint Pathnames

If you have multiple LDT hosts guarding and sharing the same LDT GuardPoint directory with different local pathnames, the pathname that will be associated with LDT operations is the pathname used on the LDT host designated with primary status.

When you are entering `voradmin ldt` commands, you must use the primary host's local pathname for the GuardPoint when you specify the GuardPoint parameter. If another host is promoted to the primary status for the GuardPoint, and the GuardPoint directory pathname is different from the pathname on the previous primary host, then LDT changes the the pathname of the GuardPoint to the pathname of the new primary host.

For example, let's say you have two hosts (`LDT_Host_1` and `LDT_Host_2`) with the same directory in an NFS share mounted on different mount points on each host, and subsequently, you must enter the new primary host's local pathname for the GuardPoint:

- GuardPoint on `LDT_Host_1`: `/nfs-oxf-fs1-host1/gp`
- GuardPoint on `LDT_Host_2`: `/nfs-oxf-fs1-host2/gp`

When the GuardPoint is first added to `LDT_Host_1`, that starts the initial data transformation:

```
secfsd -guard /nfs-oxf-fs1-host1/gp
secfsd: Guardpoint initialization in progress
```

MDS has the GuardPoint configured for rekey at `/nfs-oxf-fs1-host1/gp`.

```
voradmin ldt list all

MDS_1:  type=file, nguards=0, name=/nfs-oxf-fs1-host1/gp/__vorm_mds__
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/nfs-oxf-fs
1-host1/gp
        File List: count 4
```

When the GuardPoint is enabled on `LDT_Host_2`, the host joins the LDT GuardPoint Group for the GuardPoint.

```
secfsd -guard /nfs-oxf-fs1-host2/gp
secfsd: Path is guarded
```

Unguard the GuardPoint on `LDT_Host_1` while rekey in progress:

Note

This operation triggers the promotion of `LDT_Host_2` to primary status:

```
secfsd -unguard /nfs-oxf-fs1-host1/gp secfsd: Path is not guarded
```

On `LDT_Host_2`, guard the same directory mounted at the different path:

```
voradmin ldt list all

secfsd -guard /nfs-oxf-fs1-host2/gp
secfsd: Path is guarded
```

MDS now has the GuardPoint configured for rekey at /nfs-oxf-fs1-host2/gp on LDT_Host_2.

```
voradmin ldt list all
MDS_1:  type=file, nguards=0, name=/nfs-oxf-fs1-host2/gp/___vorm_mds___
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING SUSPENDED (qos), flags=GP LOCKED, gp=/nfs-oxf-fs1-host2/gp
        File List: count 4
```

Key Rotation Commitment

The primary host drives the execution of the process for checking and committing a new key version across all members of LDT GuardPoint Groups associated with the affected GuardPoints. The primary host commits and launches LDT if all members have also received the same key version from CM. If a member has not received the new key version, the primary delays launching LDT and continues checking for the availability of the key versions with all of the members of the LDT GuardPoint Group.

The primary host triggers an ALARM on CM if a member of the LDT GuardPoint Group has not received the new key version. The message for this displays as:

LDT-NFS-ALERT: Some members of the LDT GuardPoint Group for [GuardPoint Pathname] have not received the latest key version.

After receiving this message, check the status of the connections between CTE hosts and CM to make sure each member is in an active state and in communication with CM, type:

```
voradmin ldt attr get /nfs-oxf-fs1/gp1

LDT stats: version=5, rekey_status=rekeyed
  Number of times rekeyed:      1 time
  Rekey start time:             2022/01/08 09:12:14
  Last rekey completion time:   2022/01/08 09:12:15
  Estimated rekey completion time: N/A
  Policy key version:           3627
  Pushed Policy key version:    3627
  Policy ID:                    18729
  Data stats:
    total=0.0MB, rekeyed=0.0MB
    truncated=0.0MB, sparse=0.0MB
  File stats:
    total=0, rekeyed=0, failed=0
    passed=0, skipped=0, created=0, removed=0, excluded=0
```

LDT Metadata Management Over NFS/CIFS Shares

CTE manages LDT metadata as extended attributes in local file systems for each file and GuardPoint directory. Because the NFS/CIFS protocol does not support extended attributes, CTE embeds LDT metadata into each file

to be encrypted inside the GuardPoint, over NFS/CIFS shares, during the initial data transformation. The size of the LDT metadata is 4096 bytes, so the size of each file in the NFS/CIFS share is increased by 4096 bytes. The presence of LDT metadata and larger file sizes is not visible to users and applications as long as the GuardPoint remains enabled. The same file stored in an LDT protected GuardPoint, over NFS/CIFS and a non-protected directory, is identical to other users and applications despite the presence of the embedded LDT attribute and the additional 4096 bytes.

As the Linux example below illustrates, the presence of the attributes embedded during the initial transformation of the file is invisible to users and applications. Note that the size of the file after transformation appears unchanged until the GuardPoint is disabled.

```
ls /nfs-oxf-fs1/gp1

cp /etc/hosts /nfs-oxf-fs1/gp2

ls -l /nfs-oxf-fs1/gp2/hosts
-rw-r--r--. 1 root root 241 Jan  3 16:14 hosts

secfsd -guard /nfs-oxf-fs1/gp2
secfsd: Guard point initialization in progress

voradmin ldt attr get /nfs-oxf-fs1/gp2/hosts
LDT attributes: rekeyed_size=0, rekey_status=none
Key:      clear_key

ls -l /nfs-oxf-fs1/gp2/hosts
-rw-r--r--. 1 root root 241 Jan  3 16:15 /nfs-oxf-fs1/gp2/hosts

secfsd -unguard /nfs-oxf-fs1/gp2
secfsd: Path is not guarded

ls -l /nfs-oxf-fs1/gp2/hosts
-rw-r--r--. 1 root root 4337 Jan  3 16:15 /nfs-oxf-fs1/gp2/hosts

voradmin ldt attr get /nfs-oxf-fs1/gp2/hosts
LDT attributes: rekeyed_size=4096, rekey_status=none
Key:      name=LDTNFS_KEY_1, version=1482
```

As noted, CTE also manages the LDT attribute for each GuardPoint directory as an extended attribute. For GuardPoints over NFS/CIFS shares, LDT stores the LDT metadata for each GuardPoint in the LDT Attribute File associated with the directory. In general, there are multiple metadata files that LDT manages for GuardPoints over NFS. Those metadata files are stored in the LDT Private Space Directory inside each GuardPoint directory. The directory name of LDT Private Space is `vorm_ldtprivspace`. The directory is created inside the GuardPoint directory at the time of initial transformation. The LDT metadata file for a GuardPoint is also created in the `vorm_ldtprivspace` directory of the GuardPoint at the time of initial transformation. The name of the file is `::vorm:ldtxattr::`, similar to the MDS file which is also protected against user modification or deletion. The size of the LDT metadata file is 4096 bytes. For example:

```
ls -l /nfs-oxf-fs1/gp1/vorm_ldtprivspace/
total 4
-rwxr-xr-x. 1 root root 4096 Jan  4 12:13 __vorm:ldtxattr__
```

Note

The LDT Attribute file is protected, and it can only be manually removed using `voradmin ldt rmldt <GuardPoint Path>`. For details, see [Deleting LDT Metadata \(Linux\)](#).

Backup and Restore LDT on NFS GuardPoints

Native backup capabilities in an NAS server is the recommended method for backing up and restoring GuardPoints on a NAS share. You may also backup or restore GuardPoints on NAS shares on the host designated as the primary host for an LDT GuardPoint Group, as described earlier.

Backup LDT on NFS GuardPoint

Backups of the NAS servers are remote from an LDT perspective.

It is extremely important that while you are backing up the NAS server:

- LDT is **not** performing data transformation in the GuardPoint
- No client is modifying data in the GuardPoint

This rule applies for:

- Initial data transformation
- Automatic or manual key rotation
- Backups of an entire GuardPoint, or any subset of files within a GuardPoint namespace.

Restore LDT on NFS GuardPoints

All clients must have their GuardPoints disabled prior to **restoring** the backup on the NAS server. GuardPoints is required because LDT over NFS clients are unaware of changes being performed to the files, and LDT metadata for the files, on the NAS server.

Upgrading CTE agent in an LDT Communication Group

Upgrading from 7.2.0. to 7.3.0

- [Upgrading CTE Agents from 7.2.0 to 7.3.0](#)

Upgrading to 7.4.0

You can [Upgrade CTE](#) from previous versions to 7.4.0 with no special considerations.

Warning

For CTE Agents using LDT over CFS/NFS, you **MUST** upgrade to v7.4.0 **BEFORE** you can upgrade to 7.5.0. You cannot upgrade to 7.5.0 from versions previous to 7.4.0.

Upgrading to 7.5.0 and Post 7.5.0

Note

CipherTrust Transparent Encryption 7.5.0, and subsequent versions, have architectural design changes which require all nodes, Windows and Linux, to run CTE 7.5.0 in order for the LDT Communication Group nodes to communicate properly. The architecture design changes introduces [New Terminologies](#). It is critical to understand these new terms.

- Upgrading CTE Agents in an LDT Communication Group from 7.4.0 to 7.5.0 and post 7.5.0

Best Practices for Upgrading

Only perform an upgrade when LDT is **NOT** in progress or is in a SUSPENDED state.

Triad Nodes

- Upgrade the LDT Communication Group replica nodes one at a time, before upgrading the LDT Communication Group primary node. When the LDT Communication Group primary is upgraded, the primary fails over to one of the secondary nodes, which becomes the new primary node.

LDT GuardPoint Group

- Upgrade the secondary nodes first, followed by the primary node.

To check the current node role and status of the LDT Communication Group, type:

```
voradmin ldt group list <guard path>
```

Upgrading the LDT Agents in an LDT Communication Group from 7.2.0 to 7.3.0

Note

This is applicable for Linux **and** Windows.

When upgrading from CTE 7.2.0, all nodes in an LDT Communication Group **must be** upgraded together to 7.3.0. Rolling upgrades **do not work** because CTE 7.3.0 introduces security improvements and authentication features that involve the LDT Communication Group. All nodes must contain CTE 7.3.0 in order to be able to communicate.

For example, if an LDT Communication Group contains 10 nodes, then, with 7.2.0, you could upgrade them individually and still expect secfsd communication services to operate as expected. Note that the 10 nodes in the LDT Communication Group may or may not guard the same CIFS/NFS share, but they use the same LDT Communication Group master for communicating. With 7.2.0, if node1 were to be upgraded from 7.2.0.xxx to 7.2.0.yyy, then this does not affect the progress of LDT. Also, node1 is able to use all services correctly because it is admitted to the group by the upgraded communication master. So in this case, a rolling upgrade is possible.

With 7.3.0, Thales is introducing authentication for the LDT communication group nodes. Therefore, only nodes that have the capability to authenticate themselves can be part of the LDT Communication Group. As a result, for an upgrade operation, the entire set of 10 nodes in the LDT Communication Group have to be scheduled for maintenance at the same time. In the maintenance window, you must upgrade all nodes to 7.3.0. After a successful upgrade, the administrator should verify that all GuardPoints are green and working as expected. Any node with 7.2.0 will not be able to authenticate to the LDT Communication Group and, therefore, will not be admitted into the LDT Communication Group.

Procedure

1. Start a maintenance window by removing all nodes, in the LDT Communication Group, from production.
2. Upgrade all nodes to 7.3.0.
3. Verify that all GuardPoints are guarded on all nodes as expected, type:

```
voradmin ldt group check <gp path>
```

4. Verify that the LCG communications master is up and running, in **Windows**, by typing: `voradmin ldt group comm_info`

Note

Linux is adding support for this command in a subsequent version.

5. When finished upgrading, add the nodes back into production.

New Terminology

The architecture design changes introduces new terminologies. It is critical to understand these new terms.

New LDT Communication Group Terms

- **Triad nodes**

The triad nodes are the first three servers in the LDT Communication Group.

- **Subordinate nodes**

The subordinate nodes are the remaining nodes in the LDT Communication Group.

GuardPoint Terms

- **Primary node**

The node that performs LDT rekeying of data.

- **Secondary node**

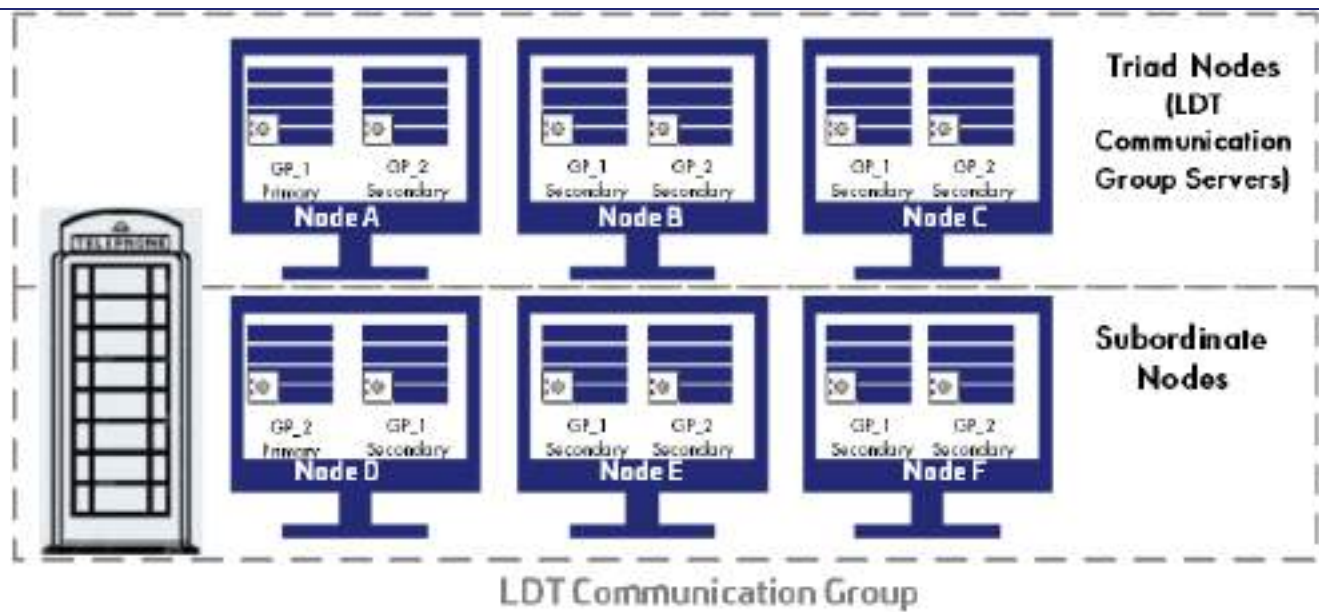
All of the other clients in the LDT GuardPoint Group are assigned as secondary nodes.

Note

They do not participate in rekeying data. Secondary nodes can be promoted to primary nodes if a primary node fails.

- **LDT GuardPoint Group**

An LDT GuardPoint Group contains a collection of LDT-enabled CTE clients that are all on the same network, managed by one CipherTrust Manager, guarding a common NFS/CIFS share and can communicate with each other over that network. An LDT GuardPoint Group enables the primary host of an LDT GuardPoint Group to communicate with the secondary hosts that are members of that LDT GuardPoint Group.



CTE Terminology

Following is a complete list of CTE terms which includes the new LDT terms.

The guide uses the following terminology:

Term	Description	OS Applies to
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. Notes • This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". • For example, the default installation directory is /opt/vormetric/DataSecurityExpert/agent/ for Linux and AIX, and C:\Program Files\Vormetric\DataSecurityExpert\agent\ for Windows.	Windows/Linux/AIX
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.	Windows/Linux/AIX

Term	Description	OS Applies to
CTE Capabilities	CipherTrust Transparent Encryption agent version-specific features like Multi-Factor Authentication.	Linux
CTE-K8s	CipherTrust Transparent Encryption for Kubernetes. Policy-based encryption of data stored on persistent volumes	Linux
CTE-RWP or RWP	CipherTrust Transparent Encryption with Ransomware Protection. Ransomware protection for volume-level (Windows)/GuardPoint (Linux) data storage through process behavior monitoring and analytics.	Windows/Linux
CTE UserSpace (CTE-U)	CipherTrust Transparent Encryption (formerly known as ProtectFile FUSE). File system level encryption and access control solution for Linux servers.	Linux
Data Transformation	Encrypting or decrypting data.	Windows/Linux/AIX
Domain Sharing	This allows Clients in one domain to get cross-domain resources, specifically GPs.	Windows/Linux/AIX
GuardPath	A directory to which a CTE Kubernetes data protection and encryption policy has been applied. CTEK8s will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.	Linux
GuardPoint	A device, or directory, to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.	Windows/Linux/AIX
Host /Client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.	Windows/Linux/AIX
In-place Data transformation	Encryption mechanism for block devices.	Linux
Key Manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers CipherTrust Manager, a key manager for use with CTE.	Windows/Linux/AIX

Term	Description	OS Applies to
LDT (Live Data Transformation)	After initial GuardPoint enablement, LDT performs initial encryption, or rekeying, in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block applications and user access to data during encryption or rekey operations, which can inconvenience users and affect operational efficiency.	Windows/Linux
LDT Communication (Comm) Group	A group of LDT clients who communicate with each other, and are responsible for, initial data transformation and future key rotation of CIFS/NFS GuardPoints.	Windows/Linux
LDT GuardPoint Group	An LDT GuardPoint Group contains a collection of LDT-enabled CTE clients that are all on the same network, managed by one CipherTrust Manager, guarding a common NFS/CIFS share and can communicate with each other over that network. An LDT GuardPoint Group enables the primary host of an LDT GuardPoint Group to communicate with the secondary hosts that are members of that LDT GuardPoint Group.	Windows/Linux
LDT Primary node	The LDT GuardPoint Group node that performs LDT rekeying of data.	Windows/Linux
LDT Secondary node	All of the other clients in the LDT GuardPoint Group are assigned as secondary nodes. Note: Secondary nodes do not participate in rekeying data, however, they can be promoted to primary nodes if a primary node fails.	Windows/Linux
LDT Subordinate nodes	The subordinate nodes are the remaining nodes in the LDT Communication Group.	Windows/Linux
LDT Triad nodes	The triad nodes are the first three servers in the LDT Communication Group.	
Learn Mode	Logging mode for audit logs to help generate security policies. Learn Mode allows access to guarded paths while logging access details. Users can analyze the content users and processes are accessing, the data used, and	Windows/Linux

Term	Description	OS Applies to
	define GuardPoint policies accordingly.	
MFA	Multifactor authorization ensures that the access credentials presented belong to the actual person. After logging in to the system, when a user tries to access a CipherTrust Transparent Encryption GuardPoint, it triggers a second factor authorization to verify the user with a second form of authentication, like sending a passcode to the users's registered cell phone, that they then have to input into the application.	Windows/Linux
Profile	Shared configuration resource for Client logging, Quality of Service, Multi-Factor Authentication, Ransomware Protection and key manager communication settings.	Windows/Linux/AIX
Signature	The hash of an entity. Where Entity can be the process or the docker image.	Windows/Linux/AIX
Versioned key and Key versions	Keys whose name remains the same but keybytes are different for each different version.	Windows/Linux/AIX

Upgrading CTE agents in an LDT Communication Group from 7.4.0 to 7.5.0 and post 7.5.0

When upgrading the CTE agent version on all nodes of an LDT Communication Group, you must stop CTE on all of the nodes to be upgraded before upgrading them.

1. Unguard the GuardPoints on the nodes to be upgraded:
 - a. Go to the CipherTrust Manager UI.
 - b. In the GuardPoint window, click the ellipsis on the right side of a GuardPoint and select disable to disable the GuardPoint.
 - c. Repeat the steps for all of the GuardPoints on the nodes to be upgraded.
2. Stop the CTE service on all of the nodes to ensure that all of the GuardPoints are unguarded.

For **Windows**:

- a. Go to **Control Panel > Services (local)**.
- b. Select **secfsd**.

- c. Select **Stop the Service**.

For **Linux**, type:

```
/etc/vormetric/secfs stop
```

3. Upgrade **CTE** on all of the nodes.
4. If your setup contains **manual directory** type GuardPoints, then you must run `secfsd -guard <gp>` to guard the GuardPoints again after the upgrade.
5. Verify that the GuardPoints are guarded on all of the nodes. Type:

```
# secfsd -status guard
```

Quality of Service for LDT CIFS/NFS GuardPoints

You can perform QoS administrative functions on the current primary CTE host. If the same CTE host is acting as a primary and secondary for multiple GuardPoint, the LDT schedule and/or Pause/Resume administrative options target those GuardPoint for which the host has assumed the primary role. This restriction is enforced through QoS functions available on CipherTrust Manager and the voradmin command.

Note

- The current pause/resume state of LDT at the host/client level, is contained in the `/var/vormetric/vorm-prs` file. This file is not protected. If it is accidentally removed or changed, it will be re-created and updated to reflect the correct pause/resume status within 30 seconds or less.
- Be sure to pause or resume LDT on the primary host only.

Suspending LDT from the CTE Agent CLI and CipherTrust Manager GUI

Promotion of a secondary host, to the primary role, can alter the current pause/resume state of the GuardPoint on the newly promoted host. The new state of the GuardPoint depends on the pause/resume state and how the pause/resume was initiated on the primary host prior to promotion. The following bullet points outline two ways to initiate pause/resume and the limitation of pause/resume on an LDT NFS GuardPoint:

Pause/Resume using CTE Agent CLI

- The voradmin command to suspend the GuardPoint is a persistent state that will be retained even after a system reboot.
- The suspended state enforced by the new primary after a promotion process.

- Suspend/resume on an LDT NFs GuardPoint through a voradmin command can only be executed on the primary host.

Pause/resume using CipherTrust Manager GUI

- Pressing the pause button on a specific client, on the CipherTrust Manager client tab, only suspends the GuardPoint(s) on that host.

In the event of a promotion, the GuardPoint resumes rekey on the new primary host, if the host tab on the CipherTrust Manager, for the newly promoted primary, is not set to suspend state.

- When using a client group, pressing the pause button sets the pause setting on all of the client that are members of that client group.

In the event of a promotion, the GuardPoint remains in the suspended state on the newly promoted primary host, until the pause button is pressed to resume rekey.

Alerts

This section lists the alerts for LDT over NFS and describes what to do in each case. LDT generates alerts when issues arise that require attention from the Administrator. Without prompt attention, alerts can delay the rekey process or cause the process to remain incomplete.

Linux Alerts

Guard/Unguard alerts

Label	Alert	Description
I_LDT_NFS_PTS_ACCESS_FAILURE	Failed to preserve time stamps: GuardPoint [GuardPoint] objID [objID] error [error]	Primary host sends this alert to notify of the failed attempt to preserve time stamps on the specified inode number in the GuardPoint. The reason for the failure is reported using the error code.
E_LDT_NFS_REKEY_OP_FAILED	Failed to start or stop rekey on GuardPoint [%s] over NAS share, error [error]	Primary host sends this alert if it fails to start or stop rekey on a specified GuardPoint. The error code in the alert provides the error code associated with the failed attempt.

LDT Communications Group alerts

Label	Alert	Description
W_LDT_COMMGRP_MASTER_DOWN	LDT Communication Master is down	Each member of an LDT GuardPoint Group sends this warning reporting that the LDT Communication Group Master

Label	Alert	Description
		associated with the group is down.
I_LDT_COMMGRP_MASTER_UP	LDT Communication Master is up	Each member of LDT GuardPoint Group sends this notice reporting that the LDT Communication Group Master associated with the group is no longer down.
W_LDTGRP_PRIMARY_LEFT	LDT Group Primary host left the group for GuardPoint [%s]	This warning reports that the specified GuardPoint has been disabled on the host designated as the primary host for the GuardPoint. LDT immediately designates another member in the LDT GuardPoint Group as the primary host for the group.
I_LDTGRP_PRIMARY_ELECTED	LDT Group Primary host has been elected for GuardPoint [GuardPoint]	Every member of an LDT GuardPoint Group for a specific GuardPoint sends this notice to report the election of a member of the group as the primary host for the GuardPoint.
I_LDTGRP_PRIMARY_PROMOTED	Host has been promoted to LDT Group Primary role for GuardPoint [GuardPoint]	The host promoted to the primary role for the GuardPoint sends this notice.
W_LDTGRP_PRIMARY_REFUSED	Host cannot be promoted to LDT Group Primary role for GuardPoint [GuardPoint]	This warning reports that the host sending the alert was elected for promotion to the primary role for the GuardPoint, and the host rejected the request. Read-only access to a GuardPoint or the host not having the latest policy key version are common reasons for a host to reject the promotion.
E_LDTGRP_PRIMARY_EFAILED	Election of this host for LDT Group Primary role has failed for GuardPoint [GuardPoint]	The host elected and accepted the primary role for the GuardPoint sends this error message if the host fails to perform the operations required for promotion to the primary role for the GuardPoint.
E_LDTNFS_FOVER_FOP	File operation recovery failed on new primary host after primary election, GuardPoint [%s] objID [%llu] error [%d] source [%d]	This error message reports that the host promoted to primary status was unable to complete the file operation that was initiated prior to the unexpected failure and departure of the previous primary host from the group. The file inode number is the objID in the message. The error code indicates the reason for the failure. The source identifies the operation that the new primary host failed to complete.

Label	Alert	Description
E_LDTNFS_RECOVERY_FAILED	LDT recovery failed on new primary host after primary election, GuardPoint [%s] objID [%llu] error [%d]	This error message reports that the host promoted to primary status was unable to recover incomplete rekey operation on the specified file inode number in the specified GuardPoint after unexpected failure and departure of the previous primary host from the group. The error code indicates the reason for the failure. The error code indicates the reason for the failure.
W_LDTNFS_PROMOTION_TOOLONG	Promotion too long	Promotion process taking too long, causing a delay in file operations, GuardPoint [%s] objID [%llu]. This warning occurs when a request to the primary host is delayed for a long time because a new primary has not been promoted.
E_LDTNFS_FOP_FAILED	File operation failed on secondary host, GuardPoint [%s] objID [%llu] error [%d] source [%d]	This alert from the primary host reports primary host failure to update LDT related metadata on behalf of a member performing a file operation that requires making changes to LDT metadata. File operations performed on secondary hosts to files undergoing rekey, such as truncate or rename, involves the primary host to intervene for updating LDT metadata.
W_LDTNFS_KEY_ROTATE_ENOKEY	Some members of LDT GuardPoint Group for [%s] have not received latest key version	This warning is initiated by the primary host when at least one member of the group for the specified GuardPoint Group has not received the latest policy key version that the primary host is committing. Make sure that all member of the LDT GuardPoint Group are connected to the CM.
W_LDTNFS_LAZY_RK_FAILURE	Lazy rekey operation failed to rekey <file name>, error <error code>	This alert reports failure to rekey the specified file name. The error code provides the reason for the error.

Windows Alerts

Guard/Unguard alerts

Label	Alert	Description
E_LDT_GUARD_FAILED	Failed to enable/apply GuardPoint	Guard operation failed

Label	Alert	Description
E_LDT_UNGUARD_FAILED	Failed to disable/delete GuardPoint	Unguard operation failed

Credentials alert

Label	Alert	Description
E_LDT_CIFS_INVALID_CRED	Failed to enumerate GuardPoint <.. \GP0>, Verify the provided CIFS credentials.	CIFS credentials may be expired or may not have permission to access.
E_LDT_CIFS_LOGIN_FAILED	Failed to authenticate a user	Failed to authenticate user using given credential.
[CGA] [ERROR] [4] [CGA3142E]	Not guarding path; Reason: Resource not available	If the agent logs display this message during CIFS GuardPoint creation, you can safely disregard. The GuardPoint will be created after the credentials are authorized. It may take a few minutes.

LDT Communication Group alerts

Label	Alert	Description
E_LDT_LGS_JOINING_FAILED	Failed to join GuardPoint group	CTE client was unable to join the LDTGuardPoint group
E_LDT_LGS_LEAVING_FAILED	Failed to leave GuardPoint group	CTE client was unable to leave the LDT GuardPoint group

Troubleshooting LDT CIFS

The majority of the CTE clients must be fully operational for proper LDT operations across all LDT GuardPoint Groups.

If 50% or more CTE clients fail, LDT Communication Group cannot recover from that situation. To fix this issue, you must reboot all of the CTE clients in the entire LDT Communication Group.

The LDT Communication Group requires that the majority of CTE clients are active in order to work properly. If 50% or more CTE clients fail, LDT Communication Group cannot recover from that situation. To fix this issue, you must either:

- Reboot all of the CTE clients in the entire LDT Communication Group.
- In Windows, restart **secfsd** through the **Control Panel > Services** page all of the CTE clients in the entire LDT Communication Group.

Troubleshooting LDT

- [Monitoring and Statistics](#)
- [Protecting LDT GuardPoints against Failure in Underlying File Systems \(Linux\)](#)

- Alerts Playbook
- Error Messages
- Warning and Info Messages
- Recommendations and Considerations
- Troubleshooting LDT CIFS
- Troubleshooting LDT Encryption Failures

Monitoring and Statistics

This section describes how to find the runtime status of LDT and how to get statistics about its operation.

Note

When you check GuardPoint status on the CipherTrust Manager, be aware that the status is not relayed in real time. There can be a delay of several minutes before the CipherTrust Manager becomes aware of events on the host. When you configure the host and CipherTrust Manager for one-way communication, the delay is longer, up to an hour, because LDT sends statistics to the CipherTrust Manager only once per hour.

To find out when the CipherTrust Manager last received a status update from the host, check the Last Status Update timestamp in the GuardPoint Health dialog (for information about how to display this dialog, see [Obtaining Statistics with GuardPoint Status](#)). For the most up-to-date statistics, inspect the host/client. Run the `voradmin` command on the managed hosts to retrieve status and statistics pertaining to GuardPoints.

Obtaining Statistics with GuardPoint Status

During and after data transformation, you can view statistics about any GuardPoint on any client in your system. Either use the CipherTrust Manager, as described in this section, or use the `voradmin` command, as described in [Obtaining LDT Statistics at the Command Line](#).

To display the GuardPoint status in CipherTrust Manager:

1. Open the **CTE** application and click **Clients** in the left-hand menu bar.
2. Click on the name of the client whose GuardPoint you want to view.
3. Click the Status of the GuardPoint you want to view in the GuardPoints table.
4. CipherTrust Manager displays the GuardPoint Health dialog box with various statistics about the GuardPoint.

Obtaining LDT Statistics at the Command Line

You can obtain LDT statistics from the command line using the following command:

```
voradmin ldt stats <guard path> [interval]
```

This command displays transformation statistics for a GuardPoint, or for all GuardPoints, if none are specified. If you specify an interval (in units of seconds), the command continually updates the statistics on the given interval. If no GuardPoint is specified, the command returns the aggregate statistics at the host level, including specific statistics related to QoS. If a GuardPoint is specified, statistics include:

- Current rekey status
- Rekey Start time
- Last rekey completion time
- Estimated Rekey completion time
- Data Statistics including the amount of data transformed
- File statistics including:
 - Number of files transformed
 - Number of files skipped
 - Number of files remaining for rekey

Obtaining a Rekey Report

LDT generates a report automatically after completion of a key rotation. The report lists the files in the GuardPoint and the key and version of the key applied to each file. This kind of report may be a common compliance requirement.

The administrator can also request a rekey report during rekey, if the need to see the partial transformation results so far.

About the rekey report

On Linux hosts, LDT writes rekey reports to a local file on the agent host in `/var/log/vormetric/`. The file name begins with `ldtaudit-log-`. It is followed by the file system directory name, GuardPoint directory name, and a timestamp. For example, for a GuardPoint at `/oxf-fs2/gp2` with rekey completed on November 19, 2016, just after 2:00 p.m. (hour 14), the rekey report file name would be `ldtaudit-log-_oxf-fs2_gp2-2016111914917`.

The report includes:

- Total number of files in the GuardPoint
- Number of files transformed
- Rekey start and end times
- List of all files transformed

- Applied key and key version for each file (for example, files in different resource sets might have used different keys)

Manually generating a rekey report

To generate a rekey report manually, use the following command:

```
voradmin ldt rekey report <GuardPoint> [<logfile>]
```

In **<GuardPoint>**, type the GuardPoint path. In **<logfile>**, you can optionally direct the output to a file. If no logfile is specified, the report displays on **stdout**.

Monitoring Ongoing LDT Operations at the Command Line (Windows only)

Use the following syntax to monitor LDT progress. If an interval is specified (in units of seconds), it continually updates the monitoring output at the specified interval.

```
C:\> voradmin ldt monitor [interval]
```

For an overview of **voradmin ldt**, see [LDT Command-Line Administration: voradmin command](#).

Protecting LDT GuardPoints against Failure in Underlying File Systems (Linux)

LDT Recovery Challenges

The main challenge with LDT recovery is a failure to access files or specific blocks in files inside a GuardPoint. Before LDT runs the recovery process on a GuardPoint, the underlying file system was recovered before file system was mounted. File system recovery may create orphan files in the **lost+found** directory inside the mount point. If an orphan file belongs to the GuardPoint, LDT cannot recover the file as the file is no longer in the same directory as it was prior to the crash while it was undergoing rekey.

LDT Recovery Enhancement

LDT has been improved for handling inconsistencies in the underlying file system during execution of LDT recovery. When enabling a GuardPoint after a system crash, LDT performs consistency checks on the files undergoing rekey at the time of crash before enabling GuardPoint. If the LDT recovery process is unable to recover any of the affected files, the GuardPoint will not be enabled and LDT will send the following alert to the CipherTrust Manager:

```
[CGS3266E] LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in underlying file system encountered during LDT recovery.
```

You can check the status of a GuardPoint and the reason for failing to enable a GuardPoint using the **secfsd -status guard** command. For example, the GuardPoint/**mnt/gp** failed to guard because **Guard point needs LDT recovery** as reported in the **Reason** column for the following example GuardPoint.

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	-----	-----	-----	-----
/mnt/gp	LDT220	manual	guarded	not guarded	Guard point needs LDT recovery

Details on the specific issues encountered, including any files that could not be recovered, are reported to a log file in the `/var/log/vormetric` directory. The log file name is in the format:

```
ldt_recovery_log:<guardpoint_name>:<timestamp>.txt
```

The log file name starts with `ldt_recovery_log`, followed by the GuardPoint pathname and the date and time of the recovery attempt. The GuardPoint pathname and date and time are separated with “.”. For example:

```
/var/log/vormetric/ldt_recovery_log:_mnt_gp:2018-12-08-14:6:12.txt
```

Refer to the issues listed in the log file, and resolve those issues before enabling the GuardPoint again. A GuardPoint cannot be enabled in subsequent guard attempts until those issues are resolved. Each attempt generates a new log file. Check the LDT log file for missing files whose inode numbers match inode numbers of orphan files in `lost+found`. If there is a match, restore the file from `lost+found` to the pathname specified in the LDT recovery log file. Be sure to run the `mv` command to restore the file to the original location, do not run the `cp` command. After resolving all or some of the reported issues, you must run the command `voradmin ldt recover <GuardPoint>` to repeat the recovery process.

```
voradmin ldt recover <GuardPoint>
```

Running this command resolves the problems that can be corrected and clears the failed recovery status on the GuardPoint, allowing the GuardPoint to enable automatically within 30 seconds. If the GuardPoint does not enable, you can enable it using `secfsd -guard` command, if manual guard, or enable it on the CipherTrust Manager, if auto-guard. Note that if you are unable to resolve all of the reported issues, you accept the loss of some data or files, as reported in the latest recovery log file for the GuardPoint, when you run the command `voradmin ldt recover <GuardPoint>`.

Recovery Alerts

LDT sends two alerts to CipherTrust Manager if LDT fails to resolve the issues encountered during recovery.

The alert below is an error report sent to the CipherTrust Manager whenever LDT encounters failure during recovery prior to enabling GuardPoint. This alert also reports the GuardPoint specified in the message is not enabled:

```
[CGS3266E] LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in underlying file system encountered during LDT recovery.
```

The alert below is a warning report sent to the CipherTrust Manager only if `voradmin ldt recover` encounters errors and continues anyway. This alert reports the GuardPoint specified in the message has been enabled with some files in error status.

```
[CGS3267W] LDT-ALERT: LDT manual recovery on guard point [GuardPoint] completed with [#] errors.
```

The full message body does not currently appear in the logs on the CipherTrust Manager. At this time, the

CipherTrust Manager shows the message ID without the message body.

Alerts Playbook

This section lists the LDT alerts and describes what to do in each case. LDT generates alerts when issues arise that require attention from the Administrator. Without prompt attention, alerts can delay the rekey process or cause the process to remain incomplete.

The alerts are grouped into the following categories:

- Failure to Enable GuardPoints
- Failure to Suspend or Resume LDT Operation
- Insufficient Resources
- Failed to Update LDT Attribute
- Rekey Stopped
- Incomplete Key Rotation
- Skipped Key Rotation
- Failed to Update LDT Metadata During Scan Phase
- File system inconsistencies after system crash

Failure to Enable GuardPoints

The following alerts trigger when LDT fails to enable a GuardPoint:

- **LDT-ALERT: Cannot enable GuardPoint due to wrong policy applied to [GuardPoint]**

This message indicates that there was an attempt to apply an LDT policy to a GuardPoint that was previously guarded with a different LDT policy:

The GuardPoint status changes to **Incorrect policy** .

Solution

Unguard the GuardPoint and re-guard with the correct policy or, if you want to change the policy associated with the GuardPoint, clean up the LDT metadata and the re-guard. For details on cleaning up the GuardPoint, see [Deleting LDT Metadata \(Linux\)](#).

- **LDT-ALERT: Failed to update LDT attribute (Linux only)**

LDT failed to create or update an LDT extended attribute of a file in a GuardPoint.

Solution

An I/O error is the most common cause of failure when updating an LDT extended attribute. For I/O errors, fix the problem at the host OS or storage level.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

- **LDT-ALERT: Failure to Enable GuardPoint Due to Mismatched Policy or Key** (Linux only)

The following status indicates that a node has attempted to apply an LDT policy to a GuardPoint that uses a policy or key version that is different than the primary host.

- The GuardPoint status changes to **Stale Policy**.

Solution

Wait for the CipherTrust Manager to send the new policy to all members of the LDT group. If left in this state, the GuardPoint will automatically be guarded once the policy version matches the primary version. If the GuardPoint does not guard, make sure network connection between CipherTrust Manager and CipherTrust Transparent Encryption host is active and running, and the policy applied to the GuardPoint on the CTE host matches the policy applied across all members of LDT GuardPoint Group.

- **LDT-ALERT: Failure to Enable GuardPoint due to Unavailability of LDT Communication Group** (Linux only)

The following status indicates that the LDT Communication Group is not yet running on the host.

- The GuardPoint status changes to **LDT Group Services is not initialized**.

Solution

Wait for the LDT Communication Group to start up. This can occur if the attempt to guard the GuardPoint occurs immediately after LDT start up. The GuardPoint will automatically complete the guard operation once the LDT Communication Group completes initialization.

Note

The LDT Communication Group may require up to a minute to start up after rebooting the CTE host.

- **LDT-ALERT: Failure to Enable or Disable GuardPoint due to Single File Rekey** (Linux only)

The following status indicates that a GuardPoint is busy with single file rekey jobs and cannot be interrupted to allow a member to join or leave the group.

- When guarding, the status changes to **Single file rekey in progress, retrying**.
- When unguarding the status changes to **Busy, will continue to retry**.

Solution

Wait for the single file rekey to finished so that the group allows members to join or leave. The status of a single file rekey can be found by running `voradmin ldt list all` on the primary host. This command lists all of the single file rekey jobs as `type=FILE`. The GuardPoint will automatically complete the guard or unguard operation once all single file rekey jobs are completed.

▪ LDT-ALERT: Failure to Enable GuardPoint on Primary Host after Crash

The following status indicates that the primary host failed to leave the group correctly, and is now attempting to re-join the group.

- The GuardPoint status changes to, **Group join failed, GuardPoint needs LDT repair**

Solution

Run the following commands to manually clean up the group and allow the primary to rejoin as a member. Client will complete the guard operation once the group has been repaired.

```
voradmin ldt group repair /<primary IP> <absolute GuardPoint> (Windows)
voradmin ldt group repair /<primary IP> <${gp}> (Linux)
```

▪ LDT-ALERT: Failure to Enable GuardPoint due to mismatched NFS Version (Linux only)

The following status indicates that a member is attempting to guard an NFS share mounted with a different version than what the primary uses.

- The GuardPoint status changes to, **NFS version mismatch with primary**

Solution

Unguard on the member, unmount the NFS share, and remount it with the same NFS version as the primary.

▪ LDT-ALERT: Failure to Enable GuardPoint due to mismatched LDT Message Versions (Linux only)

The following status indicates that the member is using a message version that is incompatible with the primary.

- The GuardPoint status changes to, **LDT message version mismatch with primary.**

Solution

Unguard and verify that the member is running the same version of CipherTrust Transparent Encryption as the primary. If this problem persists, contact Thales Support for further troubleshooting. Note that the LDT message service in CipherTrust Transparent Encryption v7.2 and CipherTrust Transparent Encryption v7.3 are incompatible. When members of an LDT GuardPoint Group consist of CTE 7.2 and 7.3 hosts, this failure is expected and the solution is to upgrade those members running CipherTrust Transparent Encryption 7.2 to

CipherTrust Transparent Encryption 7.3 or a subsequent version. All members of the LDT GuardPoint Group must be running the same version of CipherTrust Transparent Encryption.

Failure to Suspend or Resume LDT Operation

- **LDT-ALERT: Failed to suspend rekey on GuardPoint [GuardPoint]**

Solution: An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, you must fix the problem at the host OS or storage level.

The appropriate corrective action depends on when this problem occurs and the reason for the suspension. If the suspend request was at the host level as part of a QoS schedule, or it was initiated by a user on the CipherTrust Manager, the failure occurred at the host level rather than the specified GuardPoint.

Otherwise, the source is probably the initiation of a suspension on a specific GuardPoint before backup. If the backup operation is in progress when this alert message occurs, you must fix the cause of the suspension failure and then restart the backup. If the backup has already completed when the alert message occurs, the backup image on the GuardPoint may have inconsistent data and LDT metadata. Discard this backup image and do a fresh backup.

If you cannot find and fix the host OS or storage issue, contact Thales Support for troubleshooting and recovery.

- **LDT-ALERT: Failed to resume rekey on GuardPoint [GuardPoint]**

- **LDT-ALERT: Failed to resume rekey on all GuardPoints**

Solution: An I/O error is the most common cause of failure when updating persistent state of a GuardPoint. For I/O errors, you must fix the problem at the host OS or storage level.

The appropriate corrective action depends on when this problem occurs and the source of the problem. If the resume request was at the host level as part of a QoS schedule, or the resume request was initiated by a user on the CipherTrust Manager, the failure occurred at the host level rather than the specified GuardPoint.

Otherwise, the source is probably initiation of a resume operation on a specific GuardPoint after a backup is completed.

If you cannot find and fix the host OS or storage issue, contact Thales Support for troubleshooting and recovery.

Insufficient Resources

The following alerts trigger when there are not enough resources for LDT operations.

- **LDT-ALERT: Aborting rekey of file [FileName] due to insufficient disk space**

The key rotation process was stopped on a GuardPoint because there was not enough available disk space.

Solution: Resize or free up space in the file system where the PathName resides. Key rotation automatically starts again when sufficient free space becomes available.

- **LDT-ALERT: Failed to launch transformation on [GuardPoint]**

LDT failed to launch the data transformation process on the specified GuardPoint.

Solution: The most common causes of this failure are:

- Low amount of system resources, such as free disk space.
- Check the system logs for insufficient free space in underlying file systems. You can free up space by removing older files or resizing your underlying file system. You may resize the file system on-line or off-line.

For other issues, contact Customer Support.

- **LDT-ALERT: QoS failed to start**

The Quality of Service subsystem failed to launch QoS services due to lack of system resources.

Solution: A low amount of available memory is the most common cause of this failure.

Contact Customer Support.

- **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint] due to insufficient disk space**

- **LDT-ALERT: MDS file [PathName] exceeded diskspace quota on gp [GuardPoint]**

There was not enough storage space in one or more file systems containing GuardPoints undergoing rekey.

Solution: Check the file systems where your GuardPoints reside to see how much space it is using. Add more storage space as needed. After the condition is corrected and disk space is available, LDT operations resume automatically.

- **LDT-ALERT: Low space on guard point [GuardPoint], increase free space or LDT will be suspended.**

Available storage space in the file system containing the GuardPoint is nearing the threshold below which LDT rekeying cannot continue. If available space does drop below that threshold, rekeying will be automatically suspended.

Solution: Check the file system where your GuardPoint resides to see how much space is available. Make more free space available if necessary. After the condition is corrected and storage space is available, rekeying resumes automatically.

Failed to Update LDT Attribute

The following alerts trigger when LDT extended attributes are not properly updated.

- **LDT-ALERT: Failed to update LDT attribute on GuardPoint [GuardPoint]. Error: [ErrorNumber]**

Solution

I/O error is the most common cause of failure when updating LDT extended attributes. For I/O errors, fix the problems at the host OS or storage level. In Linux, if you experience an I/O error, identify the file that had the error, and restore it from backup. See [Backing Up and Restoring LDT GuardPoints](#).

In Windows, you can recover a file that has corrupt metadata as follows:

- If the file is fully encrypted, remove the metadata. Type:

```
voradmin ldt attr delete <file name path>
```

Then apply the same policy that was used to encrypt the data.

- If the file was only partially rekeyed, restore the file from a backup.

If you cannot find and fix the underlying host OS or storage issue that is causing corrupt metadata, contact Customer Support for troubleshooting and recovery.

Rekey Stopped

The following alert is specific to Windows and is triggered when rekey is stopped before it completes normally.

LDT-ALERT: Suspending rekey of binary file [PathName] during its execution

LDT operations encountered an executable file that is running.

LDT cannot rekey a running executable file until the execution of the binary file stops.

Solution (Windows)

1. Obtain the name of the executable file from the alert message.
2. Stop execution of the binary file.

Incomplete Key Rotation

- **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint]. Another rekey operation is already in progress (Windows only)**
- **LDT-ALERT: Key rotation failed on GuardPoint [GuardPoint]**

LDT failed to complete the key rotation process on the specified GuardPoint. On Windows, this may occur if a key rotation process is already in progress on the GuardPoint. This pre-existing rekey operation could be active, or it could be in a suspended state, either because of the QoS schedule or a manual pause initiated by the administrator. See [Suspending and Resuming Rekey and/or Scan Phase](#).

Solution

1. On Linux, you can run the following command to see whether key rotation is in progress on the GuardPoint.

```
voradmin ldt list all
```

2. On Linux or Windows, check the rekey status of GuardPoints in the CipherTrust Manager Console.
3. If key rotation is already in progress on a Windows GuardPoint, wait for the key rotation to complete.

Contact Customer Support if this error occurs on Linux or if the cause of key rotation failure on Windows is not a key rotation in progress.

Skipped Key Rotation

The following alerts trigger when LDT skips key rotation.

- **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint]. It is on a read-only file system**

Key rotation is skipped on a specified GuardPoint because the mount point where the GuardPoint resides does not permit write operations.

Solution:

Remount the file system where the GuardPoint resides, and change the mount option to read/write.

- **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint] during pre-commit**
- **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint] during commit**
- **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint]. Error: [ErrorNumber]**
- **LDT-ALERT: Failed to update LDT attribute on GuardPoint [GuardPoint]. Error: [ErrorNumber]**

LDT failed to start a key rotation process on a GuardPoint during a guard operation or when processing a key rotation notification from the CipherTrust Manager. For [ErrorNumber], a Linux error number is substituted, such as `errorcode 17`.

Solution: The host returns error code 17 during LDT key rotation if it cannot perform the key rotation because there is already a rekey in progress. This pre-existing rekey operation could be active, or it could be in a suspended state, either because of the QoS schedule or a manual pause initiated by the administrator. See [Suspending and Resuming Rekey and/or Scan Phase](#).

An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, fix the problem at the host OS or storage level.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

Failed to Update LDT Metadata During Scan Phase

LDT triggers the following alerts when LDT cannot properly update metadata during the scan phase. (See [LDT Runtime Flow](#) for information about the scan phase.)

- **LDT-ALERT: Scan error on [GuardPoint] removing MDS guard for relaunching dataxform**

LDT failed to update metadata when restarting a scan on the specified GuardPoint.

Solution: An I/O error is the most common cause of failure when updating LDT metadata. For I/O errors, fix the problem at the host OS or storage level and then restart operations.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Thales Support for troubleshooting and recovery.

- **LDT-ALERT: Online Dataxform failed during post scan stage on [GuardPoint]**

LDT failed to update metadata when transitioning from scan to rekey phase on the specified GuardPoint.

Solution: An I/O error is the most common cause of failure when updating LDT metadata. For I/O errors, the problem must be fixed at the host OS or storage level and the operation restarted.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

File system inconsistencies after system crash

LDT sends two alerts to the CipherTrust Manager if LDT fails to resolve the issues encountered during recovery.

The alert below is an error report sent to the CipherTrust Manager whenever LDT encounters failure during recovery prior to enabling GuardPoint. This alert also reports the GuardPoint specified in the message is not enabled:

- **LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in underlying file system encountered during LDT recovery**

The alert below is a warning report sent to the CipherTrust Manager only if `voradmin ldt recover` encounters errors and continues anyway. This alert reports the GuardPoint specified in the message has been enabled with some files in error status.

- **LDT-ALERT: LDT manual recovery on guard point [GuardPoint] completed with [#] errors.**

Solution: See [Protecting LDT GuardPoints against Failure in Underlying File Systems \(Linux\)](#).

Error Messages

This section describes runtime error messages. For information about other types of runtime messages, see [Alerts Playbook](#) and [Warning and Info Messages](#).

Failed to Transform File During Rekey

LDT could not complete transformation on a file.

Related Messages:

-
- **LDT: Rekey failed for file [PathName] on GuardPoint [GuardPoint]**
 - **LDT: Extended attribute of inode [InodeNumber] is corrupted under GuardPoint [GuardPoint]**

Solution

An I/O error is the most common cause of failure when updating LDT metadata. For I/O errors, fix the problem at the host OS or storage level, and then restore the file from a backup.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

Failure to Suspend LDT

A request to stop LDT processing did not succeed. The suspend request was at the host level as part of a QoS schedule, or the suspend request was initiated by a user on the CipherTrust Manager.

Related Messages:

- **LDT: Failed to suspend rekey on all GuardPoints**
- **LDT operations could not be suspended on the host**

Solution: An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, fix the problem at the host OS or storage level.

If a backup operation is in progress when this message occurs, you must fix the cause of the suspend failure and then restart the backup. If the backup has already completed when the alert message occurs, the backup image on the GuardPoint may have inconsistent data and LDT metadata. Discard this backup image and do a fresh backup.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

Failure to Start or Stop Transformation

The following general messages are recorded when there are errors attempting to start or stop LDT:

- **LDT: Failed to abort key rotation on GuardPoint [GuardPoint]**
- **LDT: Failed to start**
- **LDT: Failed to stop**
- **LDT: Failed to exit**

Solution

Examine system logs for additional information as to the cause. If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

Failure to Restart Transformation

The following message is recorded when an attempt to restart transformation after a system reboot fails because the file system is mounted as read-only. Transformation on the specified GuardPoint cannot continue until the file system is mounted with write permission.

- **LDT: Skipped LDT recovery on read-only file system [GuardPoint]**

Solution

Re-mount the file system with write permissions.

Failure to Schedule Relaunch

The following message indicates that a rekey request was sent to a Linux GuardPoint that was already undergoing data transformation, and an error was encountered when LDT attempted to defer the rekey request until after the current data transformation completes:

- **LDT: Failed to flag GuardPoint [GuardPoint] for deferred key rotation, error [Error]**

Solution

Contact [Thales Tech Support](#) for help.

Temporary Failure to Start Transformation on a File

The following messages are recorded when there are communication issues or lack of resources on the host. Once the condition is corrected, transformation of the file continues automatically:

- **LDT: Insufficient memory condition encountered during LDT on GuardPoint [GuardPoint]**
- **LDT: Encryption key for file [PathName] unavailable for LDT, possibly due to loss of communication to CipherTrust Manager**
- **LDT: Aborting rekey of file [PathName] due to lack of free memory. Try closing other application to resolve the issue**

Solution

Resolve the communication issues or increase the available resources, then verify that LDT has resumed processing.

Transient Condition while enabling GuardPoint

The following messages are recorded when a request is made to guard an LDT GuardPoint when GuardPoint initialization is already in progress. During the GuardPoint initialization, the system initializes MDS file associated with the GuardPoint in preparation for LDT. Initialization of the MDS file can take a few minutes. During this time, if the system retries the guard operation, one of the following messages displays.

Related Messages:

-
- **Not re-guarding path `[path]` (Reason: GuardPoint initialization already in progress)**
 - **Not re-guarding path `[path]` from container `[container]` (Reason: GuardPoint initialization already in progress)**

Solution

Wait for the current GuardPoint initialization to complete and then resubmit the new GuardPoint initialization request if desired.

Transient Failure to Read LDT Attributes from NFS

NFS may incorrectly return 0's when reading LDT metadata from files in NFS shares. As LDT doesn't expect 0's returned for LDT attributes, it retries the read operation, and the second operation succeeds and returns valid LDT attribute.

The first read attempt returning 0's results in the first warning message logged in the system log file as LDT attribute validation fails. However, the second read attempt succeeds and reads valid LDT attribute data, resulting in the second message logged in response to the first message. You can ignore the first warning message if both messages appear together in system log.

Failed to transform passthrough files for AD database files (Windows Only)

LDT skipped the transformation of passthrough files for all AD database files. The problem occurs when the AD database remains in the default folder location.

Related Messages:

- **Skipping transformation of passthrough file `[filename]`. The file resides in the boot directory. CTE cannot encrypt boot directory files.**
- **Skipping transformation of passthrough file `[filename]`. CTE cannot encrypt these files. They are already encrypted using NTFS encryption or compressed.**
- **Skipping transformation of passthrough file `[filename]`. File is not in a GuardPoint directory.**

Solution

To fix this issue, move the AD database to any folder other than `c:\windows` or `c:\program files`.

Warning and Info Messages

This section describes runtime warning messages. For information about other types of runtime messages, see [Alerts Playbook](#) and [Error Messages](#).

Stopping Transformation of a File on Volume Dismount (Windows only)

The following warning message is recorded when transformation of a file is stopped because the containing volume is dismounted.

-
- **LDT: Volume dismounted. Aborting transformation at file [PathName]**

Issues with Policy or System Configuration

The following warning messages are recorded when CTE cannot perform LDT on the GuardPoint, because there are errors in the policy associated with the GuardPoint, or the file system containing the GuardPoint is not supported by LDT. Files in the GuardPoint can still be accessed, but no LDT encryption occurs.

- **LDT: The GuardPoint [GuardPoint] does not have a valid transformation policy, there is no new key rule**
- **LDT: The GuardPoint [GuardPoint] does not have a valid transformation policy, there is no key_op rule**
- **LDT: The GuardPoint [GuardPoint] does not support online rekey, only file operations from the offline data transform process will be allowed**

Failure to Enable GuardPoint During Cleanup

LDT records the following informational message when a user attempts to enable a newly added GuardPoint. This message displays if the GuardPoint directory was previously guarded with an LDT policy and the LDT metadata cleanup is in progress when user is guarding under the new policy.

- **LDT: Cannot enable GuardPoint [GuardPoint] during LDT clean-up process**

Solution

Retry the operation once the cleanup completes.

General LDT Operations

The following informational messages are recorded during various LDT operations. No action is required.

- **LDT: Successfully suspended rekey on GuardPoint [GuardPoint]**
- **LDT: Successfully suspended rekey on all GuardPoints**
- **LDT: Successfully resumed rekey on GuardPoint [GuardPoint]**
- **LDT: Successfully resumed rekey on all GuardPoints**
- **LDT: Rekey operation completed on GuardPoint [GuardPoint]**

Missing LDT extended attribute

The following warning message reports that the file with the specified inode number in the specified GuardPoint directory does not have an LDT extended attribute, therefore, access to the file is denied.

- **LDT: Extended attribute of inode [InodeNumber] is missing under GuardPoint [GuardPoint]**

Solution

LDT cannot determine the encryption key associated with the data in the file, therefore, you can only remove the file.

Locking Contention

The following messages are recorded during the rekey process on a file. When user access to the file is very high, it causes a high degree of locking contention between the rekey process and user access. The second message reports when the contention is no longer in effect and the rekey process has resumed accessing file to rekey.

- LDT: Exclusive access for rekey delayed on inode [*InodeNumber*]
- LDT: Exclusive access for rekey granted after delay on inode [*InodeNumber*]

Initiation and completion of LDT metadata cleanup

The following messages are recorded at the beginning and completion of LDT metadata cleanup through voradmin command.

- LDT: Metadata will start getting removed from all files in GuardPoint [*GuardPoint*]
- LDT: Metadata has been removed from all files in GuardPoint [*GuardPoint*]

The secfs component doesn't support data transform on the GuardPoint

The following warning messages displays when offline dataxform command was accidentally executed on an active LDT GuardPoint.

```
Checking if <guardpoint> is a guard point with a rekey policy applied
The secfs component doesn't support data transform on <guardpoint>
Verify this is a guardpoint with valid data transformation policy, and check the
system log files for any other problems. It may be
due to one or more of following reasons; 1.policy has no valid key rule(s), and/o
r 2. policy has no key_op rule, and/or 3. policy
has valid permit rule(s), and/or 4. policy rule that contains key_op in the actio
n field also specifies other actions.
```

This action results in an input/output error when creating new files in the GuardPoint.

Solution

For auto GuardPoint:

1. Disable the GuardPoint on CipherTrust Manager.
2. Delete the `dataxform_auto_lock` file in the GuardPoint.
3. Enable the GuardPoint on CipherTrust Manager.

For a manual GuardPoint:

1. Unguard using `secfsd -unguard <guardpoint>`.

2. Delete the `dataxform_auto_lock` file in the GuardPoint.
3. Enable the GuardPoint using `secfsd -guard <guardpoint>`.

Dataxform command fails with file `<GuardPoint>` Invalid xf mode

The following warning message displays when offline dataxform command was executed on an unguarded LDT GuardPoint.

```
dataxform command fails with file "<gp>" invalid xf mode
```

This action creates the `dataxform_auto_lock` file in the GuardPoint which causes the write error when creating new files in the GuardPoint, if the GuardPoint was enabled prior to deleting the file.

Solution

Before enabling the GuardPoint, delete the `dataxform_auto_lock` file in the GuardPoint.

Recommendations and Considerations

The following information provides guidance for a better user experience.

- [All Platform Recommendations and Considerations](#)
- [Windows Recommendations and Considerations](#)

All Platform Recommendations and Considerations

- [Binary Re-signing](#)
- [Check for available disk space for LDT metadata](#)
- [LDT Requirements for Backup](#)
- [Learn Mode](#)
- [Quality of Service \(QoS\)](#)
- [Upgrade to CTE 7.2.0.128](#)

Binary Re-signing

Any executable that is part of either a Signature set or a Host setting, and that resides in a GuardPoint that uses an LDT policy, will use different signatures for an LDT key rotation. The result is that the Host Settings binaries will no longer be authenticated, or that the Signature Set policy rules will no longer trigger for those binaries.

To prevent these issues, the Security Administrator must manually re-sign each affected binary after each key rotation.

Alternatively, CTE can generate unencrypted signatures of binaries inside GuardPoints to avoid these problems. For details, see the CipherTrust Manager documentation.

Check for available disk space for LDT metadata

Before launching LDT on a GuardPoint:

1. Check the available free disk space in the file system where your GuardPoint resides.
2. Type the following command to check the disk space requirement of LDT on a target GuardPoint:

```
voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 1501 files without LDT extended attributes
LDT disk space requirements: total 169MB (LDT attributes=6MB, MDS=163MB)
```

In this example, the output shows that LDT requires 169MB of available disk space to launch and execute LDT on `/oxf-fs1/gp1`.

Note

Make sure that the free space in your file system exceeds the disk space requirement for LDT.

LDT Requirements for Backup

CTE offers the option to backup encrypted data from files through a security rule, which skips the Apply Key function when reading encrypted files by backup applications or processes. Such files can also be restored from backup streams, to the same or a different GuardPoint, without Apply Key. If you choose to restore to another GuardPoint, the target GuardPoint must be protected with the same key and security rules as the source GuardPoint.

If you backup encrypted data from files inside GuardPoints with LDT policies, LDT imposes a hard requirement on the backup application, or process, to backup or restore LDT metadata. The LDT metadata is stored as an extended attribute on Linux and as alternate data streams on files on Windows platforms. If the backup process cannot backup the metadata, then LDT protected GuardPoints must be backed up in clear key.

Customers are required to verify their backup application, or process, to ensure extended attributes (on Linux) or alternate data streams (on Windows) are backed up and restored through their backup/restore processes.

Note

Make sure that you suspend LDT operations before you start the backup process, and resume them after the backup process completes.

Learn Mode

Learn Mode provides a temporary method for disabling the blocking behavior of regular CTE or LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set.

Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption.

Note

Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.

Quality of Service (QoS)

By default, the QoS component of LDT does not monitor live transformation operations unless you enable QoS on your host by entering QoS parameters in the CipherTrust Manager profile associated with the client. To avoid overhead of LDT on your production system, you must select QoS parameters suitable to your production environment. For information on tuning QoS, see [Quality of Service](#). It is critical that you understand the impact of LDT on your system and how to manage this impact using QoS.

Upgrade to CTE 7.2.0.128

Since the first release of the LDT feature, Thales has made several improvements in the areas of error handling, interoperability with applications, and Quality of Service (QoS). Thales strongly recommends that new deployments use version 7.2.0.128 (or later) of CTE. Thales further recommends that customers who have already deployed the LDT feature upgrade to version 7.2.0.128.

Windows Recommendations and Considerations

- File Handling
- File Modification
- Logical Sector Size

File Handling

The CTE-LDT process is subjected to all of the File System policies and attributes set on the files. In some cases, this prevents CTE-LDT from encrypting a file. If users or applications are accessing files while CTE-LDT is in progress, CTE-LDT cannot change the attributes of the files and encrypt the file. It is critical that you understand how CTE-LDT handles various types of files:

- NTFS Encryption and Compression

If NTFS encryption or compression is enabled on a file or folder, the CTE-LDT process cannot encrypt these

files. To maintain the data coherency, CTE-LDT skips the encryption of these files. These files display as “passthrough” files in the CTE-LDT statistics.

- **Read-Only Files**

As the CTE-LDT process performs a read-encrypt-write operation on a file, it cannot encrypt read-only files. The CTE-LDT process skips these files and changes to the INCOMPLETE state.

- **Exclusively Locked Files**

If an executable file is running, or if files are exclusively locked by the application, the LDT process **cannot** encrypt those files, as it is unable to acquire the required locks on the files. LDT skips these files and changes to the INCOMPLETE state.

File Modification

The CTE-LDT process performs a read-encrypt-write operation on the files that need to be encrypted, (also known as rekeying). Previously, file modification and access dates were changed when CTE-LDT was processing. In order to maintain compatibility for applications, we addressed this issue by saving a copy of the original access and modification times, and restoring them after the encryption completed. Preserved timestamps are updated during the rekey process, if an application/user accesses the files during rekey.

Logical Sector Size

CTE-LDT Windows transformation is supported if the **logical sector size** is more than 512 Bytes. (A logical sector size of 4K is supported.) To find the logical sector size of the file system, type:

```
> fsutil fsinfo ntfsInfo <volume pathname>
```

For example:

```
> fsutil fsinfo ntfsInfo C:
NTFS Volume Serial Number :      0x5092568a92567506
NTFS Version      :              3.1
LFS Version       :              2.0
Number Sectors    :              0x000000001c004eeb
Total Clusters    :              0x00000000038009dd
Free Clusters     :              0x00000000008bb274
Total Reserved    :              0x0000000000001864
Bytes Per Sector   :              512
.
.
.
```

Troubleshooting LDT Encryption Failures

If you use Windows quotas, which allow you to limit the amount of storage space a user account can use on a drive, you may not be allowing enough space for LDT. LDT uses an extra 4K per file for an LDT policy. If the extra space is not considered, and the space permitted by quotas is exceeded in a directory, then LDT may not be able to transform files or rekey those files later.

LDT also requires space for temporary recovery metadata that exists during transform or rekey of a file. If the file metadata exists, but the recovery metadata cannot be created and written to, then rekey of that file fails.

So make sure to allocate enough space for LDT transformation, rekeying, and recovery of metadata when setting quotas.



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

CTE Agent Windows Advanced Configuration Guide	4
Overview of CTE	4
Getting Started with CTE for Windows	8
Installation Workflow	9
Installing CTE with No Key Manager Registration	9
Configuring CTE for Windows with CipherTrust Manager	10
Interactive Installation on Windows	11
Silent Installation on Windows	12
Silent Installation Using the exe File	12
Silent Installation Using the MSI File	17
Validating CM and CTE with a Local CA Certificate	21
Using external certificates for communication between CTE Agent and CipherTrust Manager ...	23
Registering CTE After Installation is Complete	25
Setting the CM log for Ransomware Protection	28
Guarding a Device with CipherTrust Manager	29
Installation Prerequisites	37
Multifactor Authentication for CTE GuardPoints	39
Introduction to Multifactor Authentication	39
Compatible MFA Providers	41
Using STA for Multifactor Authentication for CTE GuardPoints	41
Using Okta for Multifactor Authentication for CTE GuardPoints	43
Using Keycloak for Multifactor Authentication for CTE GuardPoints	44
Using Cisco DUO for Multifactor Authentication for CTE GuardPoints	47
Using Microsoft Azure Entra ID Multifactor Authentication for CTE GuardPoints	48
Use Cases for MFA on CTE	50
Exempting some users or processes from authentication with a Whitelist	54
Remote Authentication for Multifactor Authentication	55
Administrator Tasks for Multifactor Authentication	58
Troubleshooting Multifactor Authentication	65
Choosing a Login Name Type	66
Ransomware Protection	66
Ransomware Protection Overview	67
Creating GuardPoints for Ransomware Protection	69
Guarding Data on CIFS Servers and Clients	72
Special Cases for CTE Policies	75
Enhanced Encryption Mode	78
Compatibility	79
Disk Space	80
Encryption Migration	80
File Systems Compatibility	80
FileTable Support on Windows	82
Using the AES-CBC-CS1 Encryption Mode in CM	82

Exceptions and Caveats	82
Best Practices for AES-CBC-CS1 Keys and Host Groups	82
Utilities for CTE Management.	82
Agent Health Return Codes	83
agentinfo Utility	84
Backup Utility.	85
voradmin secfs Commands.	87
vmsec Utility	89
vmutil.	90
Upgrading CTE on Windows	91
Silent Upgrade	91
CTE Scheduled Upgrade	92
Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades	95
Uninstalling CTE from Windows	96
Troubleshooting and Best Practices	98

CTE Agent Windows Advanced Configuration Guide

This document covers the following information:

- Overview of CTE
- Getting Started with CTE for Windows
- Special Cases for CTE Policies
- Enhanced Encryption Mode
- Utilities for CTE Management
- Upgrading CTE on Windows
- Uninstalling CTE from Windows
- Troubleshooting and Best Practices

Overview of CTE

For very large data sets, initial encryption deployments can affect data availability, require unacceptable maintenance windows or require cloning and synchronizing data. Encrypting millions of files can span hours or even days, which can delay encryption, or require extra disk space and data synchronization, which can be labor-intensive. Rekeying large data sets can demand significant processing time and lengthy maintenance windows. Security and IT teams face tough tradeoffs, having to choose between security and availability.

CipherTrust Transparent Encryption operates with minimal disruption, effort, and cost. Its transparent approach enables security organizations to implement encryption without changing application, networking, or storage architectures. CipherTrust Live Data Transformation builds on these advantages, offering patented capabilities that deliver breakthroughs in availability, resiliency and efficiency.

CTE includes several unique utilities to help you encrypt and manage your data. It also integrates with several third-party platforms such as Oracle, Microsoft SQL, and Quantum StorNext.

This document describes the installation and advanced configuration options for CTE, as well as detailed information about how to integrate CTE with the supported third-party products.

CTE Terminology

The guide uses the following terminology:

The guide uses the following terminology:

Term	Description	OS Applies to
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is	Windows/Linux/AIX

Term	Description	OS Applies to
	the CTE Agent, which must be installed on every host whose devices you want to protect. Notes • This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". • For example, the default installation directory is <code>/opt/vormetric/DataSecurityExpert/agent/</code> for Linux and AIX, and <code>C:\Program Files\Vormetric\DataSecurityExpert\agent\</code> for Windows.	
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.	Windows/Linux/AIX
CTE Capabilities	CipherTrust Transparent Encryption agent version-specific features like Multi-Factor Authentication.	Linux
CTE-K8s	CipherTrust Transparent Encryption for Kubernetes. Policy-based encryption of data stored on persistent volumes	Linux
CTE-RWP or RWP	CipherTrust Transparent Encryption with Ransomware Protection. Ransomware protection for volume-level (Windows)/GuardPoint (Linux) data storage through process behavior monitoring and analytics.	Windows/Linux
CTE UserSpace (CTE-U)	CipherTrust Transparent Encryption (formerly known as ProtectFile FUSE). File system level encryption and access control solution for Linux servers.	Linux
Data Transformation	Encrypting or decrypting data.	Windows/Linux/AIX
Domain Sharing	This allows Clients in one domain to get cross-domain resources, specifically GPs.	Windows/Linux/AIX
GuardPath	A directory to which a CTE Kubernetes data protection and encryption policy has been applied. CTEK8s will control access to, and monitor changes in, this device and directory, encrypting new or	Linux

Term	Description	OS Applies to
	changed information as needed.	
GuardPoint	A device, or directory, to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.	Windows/Linux/AIX
Host /Client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.	Windows/Linux/AIX
In-place Data transformation	Encryption mechanism for block devices.	Linux
Key Manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers CipherTrust Manager, a key manager for use with CTE.	Windows/Linux/AIX
LDT (Live Data Transformation)	After initial GuardPoint enablement, LDT performs initial encryption, or rekeying, in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block applications and user access to data during encryption or rekey operations, which can inconvenience users and affect operational efficiency.	Windows/Linux
LDT Communication (Comm) Group	A group of LDT clients who communicate with each other, and are responsible for, initial data transformation and future key rotation of CIFS/NFS GuardPoints.	Windows/Linux
LDT GuardPoint Group	An LDT GuardPoint Group contains a collection of LDT-enabled CTE clients that are all on the same network, managed by one CipherTrust Manager, guarding a common NFS/CIFS share and can communicate with each other over that network. An LDT GuardPoint Group enables the primary host of an LDT GuardPoint Group to communicate with the secondary hosts that are members of that LDT GuardPoint Group.	Windows/Linux
LDT Primary node	The LDT GuardPoint Group node	Windows/Linux

Term	Description	OS Applies to
	that performs LDT rekeying of data.	
LDT Secondary node	All of the other clients in the LDT GuardPoint Group are assigned as secondary nodes. Note: Secondary nodes do not participate in rekeying data, however, they can be promoted to primary nodes if a primary node fails.	Windows/Linux
LDT Subordinate nodes	The subordinate nodes are the remaining nodes in the LDT Communication Group.	Windows/Linux
LDT Triad nodes	The triad nodes are the first three servers in the LDT Communication Group.	
Learn Mode	Logging mode for audit logs to help generate security policies. Learn Mode allows access to guarded paths while logging access details. Users can analyze the content users and processes are accessing, the data used, and define GuardPoint policies accordingly.	Windows/Linux
MFA	Multifactor authorization ensures that the access credentials presented belong to the actual person. After logging in to the system, when a user tries to access a CipherTrust Transparent Encryption GuardPoint, it triggers a second factor authorization to verify the user with a second form of authentication, like sending a passcode to the users's registered cell phone, that they then have to input into the application.	Windows/Linux
Profile	Shared configuration resource for Client logging, Quality of Service, Multi-Factor Authentication, Ransomware Protection and key manager communication settings.	Windows/Linux/AIX
Signature	The hash of an entity. Where Entity can be the process or the docker image.	Windows/Linux/AIX
Versioned key and Key versions	Keys whose name remains the same but keybytes are different for each different version.	Windows/Linux/AIX

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.

After the CTE Agent has encrypted a device on a host, that device is called a GuardPoint. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.

- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Note

For a list of CTE versions and supported operating systems, see the [CTE Compatibility Portal](#).

How to Protect Data with CTE

CTE uses policies created in the associated key manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your protected hosts. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of GuardPoints.

Policies specify:

- Whether or not the resting files are encrypted.
- Who can access decrypted files.
- What level of file access auditing is applied when generating fine-grained audit trails.

A Security Administrator accesses key manager through a web browser. You must have administrator privileges to create policies using key Manager. The CTE Agent then implements the policies once they are pushed to the protected host.

CTE can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

Getting Started with CTE for Windows

This section describes how to install CTE for Windows, register it with your selected key manager, and then create a simple GuardPoint on the protected host. It contains the following topics:

-
- [Installation Workflow](#)
 - [Installing CTE with No Key Manager Registration](#)
 - [Configuring CTE for Windows with CipherTrust Manager](#)
 - [Multifactor Authentication for CTE GuardPoints](#)
 - [Choosing a Login Name Type](#)
 - [Ransomware Protection](#)
 - [Guarding Data on CIFS Servers and Clients](#)

Installation Workflow

In order to install and configure CTE, you need to perform the following high-level tasks: 1. Select which key manager you want to use. The Vormetric Data Security Manager and the CipherTrust Manager have different requirements and support different features, so you must make this decision first. For details, see [CTE Components](#).

1. If you want to install the CTE Agent without registering with a key manager, see [Installing CTE with No Key Manager Registration](#). However, you cannot protect any data on the host until it has been registered.

Otherwise, set up your systems according to the requirements of the selected key manager. For details, see [Configuring CTE for Windows with CipherTrust Manager](#).

2. Create your policies, encryption keys, and GuardPoints using the selected key manager. For details, see [Guarding a Device with CipherTrust Manager](#).

Installing CTE with No Key Manager Registration

The following procedure installs the CTE Agent on the host but does not register it with a key manager. You cannot protect any data on the host until the CTE Agent is registered with one of the supported key managers. For a comparison of the available key managers, see [CTE Components](#).

If you want to register the CTE Agent immediately after installing it, see [Configuring CTE for Windows with CipherTrust Manager](#).

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the *License Agreement* page, accept the License Agreement and click **Next**.
6. Click **Next** to accept the default folder. When you are done, click **Next**.

Note

- Thales recommends that you install CTE in the default installation directory, `C:\Program Files\Vormetric\DataSecurityExpert\agent\`
- You must install the CTE Agent on the same drive as Windows. For example, if Windows is installed on the `C:` drive, you must install the CTE Agent on the `C:` drive.

7. On the *Ready to Install* page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
8. To tell the installer that you want to register later, clear the check box for **Register CipherTrust File System now**, then click **Finish**.
9. Reboot the host system to complete the installation.

Configuring CTE for Windows with CipherTrust Manager

This section describes how to install and configure CTE on Windows systems that you plan to register with a CipherTrust Manager.

The installation and configuration process consists of three basic steps:

1. [Installation Prerequisites](#)

Gather the information needed for the installation and set up your network.

2. [Interactive Installation on Windows](#)

Install CTE interactively on a protected host and register the protected host with CipherTrust Manager.

[Silent Installation on Windows](#)

Install CTE silently (non-interactive) on a protected host and register the protected host with CipherTrust Manager.

3. [Registration](#)

Register the protected host with CipherTrust Manager and make sure that CipherTrust Manager and CipherTrust Transparent Encryption can communicate with each other. This can be done as part of the initial installation or at any point after the CTE Agent has been installed.

4. [External Certificates](#)

Use for communication between CTE and CM. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

5. Validating CipherTrust Manager and CipherTrust Transparent Encryption with a Local CA Certificate

Ensure that registration by the CTE agent is serviced only by the expected key manager by providing a copy of the CA certificate that will be used to authenticate the TLS communications with the key manager.

6. Setting the CM log for Ransomware Protection

Configure the logging level for CipherTrust Manager for Ransomware Protection.

Interactive Installation on Windows

The Windows interactive install uses a standard InstallShield wizard that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see [Silent Installation on Windows](#)).

After you install CTE, you are prompted to register it immediately with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

The following procedure describes how to install the CTE Agent on the host and then register the CTE Agent with a CipherTrust Manager..

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the **License Agreement** page, accept the License Agreement and click **Next**.
6. Click **Next** to accept the default folder. When you are done, click **Next**.

Note

- Thales recommends that you install CTE in the default installation directory, `C:\Program Files\Vormetric\DataSecurityExpert\agent\`
- You **must** install the CTE Agent on the same drive as Windows. For example, if Windows is installed on the `C:` drive, you must install the CTE Agent on the `C:` drive.

7. On the **Ready to Install** page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
 8. On the **InstallShield Wizard Completed** page, make sure the **Register CipherTrust Transparent Encryption now** option is selected and click **Finish**. The installer opens the [Register CipherTrust Transparent Encryption](#) wizard.
-

Silent Installation on Windows

Silent install refers to using the command line to install CTE in a non-interactive session. Use silent install to roll out CTE installations or upgrades to large numbers of hosts or to reduce your time and interaction as an administrator. Thales provides two types of installation binaries for silent installation:

- Self-extracting `.exe`
- Windows Inst

Note

Thales supports installing or upgrading CTE with Microsoft System Center Configuration Manager (SCCM) using MSI installation binaries. For details, see your SCCM documentation.

For details, see one of the following procedures:

- [Silent Installation Using the exe File](#)
- [Silent Installation Using the MSI File](#)

Silent Installation Using the exe File

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a CipherTrust Manager using the exe file. To install silently using the MSI file or using the Microsoft System Center Configuration Manager (SCCM), see [Silent Installation Using the MSI File](#).

Prerequisites

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group that you want this client to be a member.
- CipherTrust Manager must contain an LDT Communication Group if you will use CTE to guard data over CIFS/ NFS shares using LDT policies. See [Managing LDT Communication Groups](#) for more information.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `exe` file onto the Windows system.

3. Run the installation file using the following syntax:

```
"<Installation_executable>" /s /v" /qn INSTALLDIR=\"install-dir\" REGISTERHOST
OPTS=\"Options\""
```

Example

```
"C:\installer\vee-fs-7.8.0-45-win64.exe" /s /v" /qn INSTALLDIR=\"C:\Program
Files\Vormetric\DataSecurityExpert\" REGISTERHOSTOPTS=\"192.168.13.249 -enable
ldt -useip -usehwsig -
token=123456789. ...123456789 -domain=domain1 -description=\"\"EXE silent inst
all example\"\"\""
```

Note

If you want to enter an option with spaces in any value, it must be surrounded by two double-quotes with an escape character () before each double-quote. If the syntax is incorrect, the installation fails.

where:

- **Installation_executable** is the name of the executable, example: vee-fs-7.8.0.75-win64.exe
- **/s** (required) specifies that this is a silent install.
- **/v** (required) specifies that you want to pass command line options and values of public properties through to the installer.
- **ENABLE_LDT_CIFS=Yes** is an optional parameter that indicates you plan to use CTE-LDT with CIFS share GuardPoints on this host with a CipherTrust Manager. If you specify this option, you will *not* be able to guard any local directories on this host, even if those directories use a Standard CTE policy. Only CTE-LDT GuardPoints on CIFS shares will be supported for this host.
- **/qn** (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- **INSTALLDIR=\"install-dir\"** is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory C:\Program Files\Vormetric\DataSecurityExpert\agent\

Note

Thales recommends that you install CTE in the default directory if at all possible.

- **REGISTERHOSTOPTS=**"Options\" (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

Parameter	Description
CipherTrust Manager host name	Required if you want to register CTE with a CipherTrust Manager.
-accessonly	Enables access-only mode for LDT. (Default is full access mode.) In access-only mode, nodes are not be allowed to become part of an LDT Communication Group or participate in data transformation, but they will continue to access a protected LDT CIFS GuardPoint.
-agent=your.agent.name.com	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
-description	Specifies a description for the host. This description is displayed in the CipherTrust Manager. If an entry for this host already exists, and the host already has a description, CipherTrust Manager does not overwrite the existing description, even if this option is specified.
-enableldt	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.
-enable_host_check/-disable_host_check	When using CipherTrust Data Security Platform Services (CDSPaaS), set this value to 1 to enable SSL certificate host name checks. Set to 0 to disable. Default: 0. This also forces CTE to enable the verify peer feature during registration. Use only when the CDSPaaS web server certificates contain the target DNS name or IP address.
-hostgroup	Specifies the optional host/client group with which this host/client will be associated.

Parameter	Description
-log <log_file_path_&_name>	Record installation steps in a log file.
-port <port#>	Specifies the port number this CTE Agent should use.
-profile	Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.
-rwp	Enables Ransomware Protection.
-silent	Make this a silent installation.
-token	The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.
-usehwsig	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
-useip	Use the IP address of the protected host instead of host name. Used when -agent is not supplied.
-vmd	Defines what kind of agent is being installed.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- The CTE Agent will be installed in the custom directory `C:\cte\custom dir`.
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The CipherTrust Manager registration token is `12345` (-token parameter).
- The host will be registered using the host name `my-host.example.com` (-agent parameter).
- The host will be registered with the description `This host was silently installed` (-description parameter). Again, the spaces in the description require the same syntax as in the installation directory name. For example: `-description=\"\"This host was silently installed\"\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
vee-fs-7.8.0.75-win64.exe /s /v" /qn
INSTALLDIR=\"\"C:\cte\custom dir\" registerhostopts=\"my-key-mgr.example.com
agent=my-host.example.com -token=12345
description=\"\"This host was silently installed\"\""
```

Example: LDT, LDT AccessOnly and Hardware Acceleration

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), LDT AccessOnly (`-accessonly`), and hardware association (`-usehwsig` parameter) features are enabled.

```
vee-fs-7.8.0.75-win64.exe /s /v" /qn
registerhostopts=\"my-key-mgr.example.com -token=12345 -useip -enableldt -acces
sonly -usehwsig\""
```

Example: LDT over CIFS/NFS

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter) and LDT Group (`-ldtgroup` parameter) features are enabled.

```
vee-fs-7.8.0.75-win64.exe /s /v" /qn
registerhostopts=\"my-key-mgr.example.com -token=12345 -useip -enablel
dt -ldtgroup=\"\"LDT-CG1\"\""
```

Silent Installation Using the MSI File

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a CipherTrust Manager using the MSI file. To install silently using the exe file, see [Silent Installation Using the exe File](#).

Prerequisites

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.
- CipherTrust Manager must contain an LDT Communication Group if you will use CTE to guard data over CIFS/ NFS shares using LDT policies. See [Managing LDT Communication Groups](#) for more information.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `msi` file onto the Windows system.
3. Run the installation file using the following syntax:

```
msiexec.exe /i "<Installation_executable>" /qn INSTALLDIR="install-dir" REGISTERHOSTOPTS="REGISTERHOSTOPTS_Options"
```

Example: IP method

```
msiexec.exe /i "C:\installer\vee-fs-7.8.0-87-win64.msi" /qn INSTALLDIR="C:\cte\custom dir" REGISTERHOSTOPTS="10.171.63.222 -enableldt -useip -usehwsig -token=123456789...123456789 -domain=domain1 -description=""testsilentinstallation""
msiexec /i "<Installation_executable>" /qn INSTALLDIR="install-dir\" REGISTERHOSTOPTS="REGISTERHOSTOPTS_Options" -token
```

Example: IP method

```
msiexec.exe --% /i "C:\Users\Administrator\Desktop\vee-fs-7.8.0.75-win64.msi" /qn REGISTERHOSTOPTS="10.171.63.222 -enableldt -useip -token=wrkzr8836034m2PC"
```

```
PBqW1fQk -description=testslientinstallation" -log="C:\install.log" /norestart
```

Example: FQDN method

```
msiexec.exe --% /i "C:\Users\Administrator\Desktop\vee-fs-7.8.0.75-win64.msi"
/qn REGISTERHOSTPTS="10.171.63.222 -enableldt -agent=w2k22x64-61119.sj-clab.c
om -token=wrkzr8836034m2PCPBqW1fQk -description=testslientinstallation" -lo
g="C:\install.log" /norestart
```

where:

- **Installation_executable** is the name of the executable, example: **vee-fs-7.8.0-87.66-win64.msi**
- **/i** (required) enables CTE installation.
- **ENABLE_LDT_CIFS=Yes** is an optional parameter that indicates you plan to use CTE-LDT with CIFS share GuardPoints on this host with a CipherTrust Manager. If you specify this option, you will not be able to guard any local directories on this host, even if those directories use a Standard CTE policy. Only CTE-LDT GuardPoints on CIFS shares will be supported for this host.
- **/qn** (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- **/norestart** Prevents the agent from rebooting after installation.
- **INSTALLDIR="install-dir\"** is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory **C:\Program Files\Vormetric\DataSecurityExpert\agent**

Note

Thales recommends that you install CTE in the default directory if at all possible.

- **REGISTERHOSTPTS="\Options\"** (required if you want to register CTE to a CipherTrust Manager). It is a list of options that you want the installer to use. The common options are:

Parameter	Description
CipherTrust Manager host name	Required if you want to register CTE with a CipherTrust Manager.
-accessonly	Enables access-only mode for LDT. (Default is full access mode.) In access-only mode, nodes are not

Parameter	Description
	be allowed to become part of an LDT Communication Group or participate in data transformation, but they will continue to access a protected LDT CIFS GuardPoint.
-agent=your.agent.name.com	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
-description	Specifies a description for the host. This description is displayed in the CipherTrust Manager. If an entry for this host already exists, and the host already has a description, CipherTrust Manager does not overwrite the existing description, even if this option is specified.
-enableldt	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.
-enable_host_check/-disable_host_check	When using CipherTrust Data Security Platform Services (CDSPaaS), set this value to 1 to enable SSL certificate host name checks. Set to 0 to disable. Default: 0. This also forces CTE to enable the verify peer feature during registration. Use only when the CDSPaaS web server certificates contain the target DNS name or IP address.
-hostgroup	Specifies the optional host/client group with which this host/client will be associated.
-log <log_file_path_&_name>	Record installation steps in a log file.
-port <port#>	Specifies the port number this CTE Agent should use.
-profile	Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.
-rwp	Enables Ransomware Protection.
-silent	Make this a silent installation.
-token	The registration token for the CipherTrust Manager with which you plan to register this client. Required

Parameter	Description
	for registration.
-usehwsig	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
-useip	Use the IP address of the protected host instead of host name. Used when -agent is not supplied.
-vmd	Defines what kind of agent is being installed.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- The CTE Agent will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be in double-quotes. For example: `INSTALLDIR="C:\cte\custom dir"`.
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The CipherTrust Manager registration token is `12345` (`-token` parameter).
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The host will be registered with the description `This host was silently installed` (`-description` parameter). Because description is inside a double-quoted string, you must escape the double-quotes `-description=\"This host was silently installed\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
msiexec /i vee-fs-7.8.0-87-87-win64.msi /qn
INSTALLDIR="C:\cte\custom dir" registerhostopts="my-key-mgr.example.com
-agent=my-host.example.com -token=12345 -description=Description_without_spaces_and_no_double_quotes"
```

To pass arguments successfully, you must use a hyphen and the equal sign.

Warning

Once the above command is executed, the server reboots automatically. To avoid automatic reboot (i.e. restarting manually), use the `msiexec /norestart` parameter. An example below:

```
msiexec /i vee-fs-7.8.0-87-win64.msi /qn /norestart INSTALLDIR="C:\cte\custom dir" registerhostopts="my-key-mgr.example.com -agent=my-host.example.com -token=12345 -description=Description_without_spaces_no_double_quotes"
```

Example: CTE-LDT, LDT AccessOnly and Hardware Acceleration

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), LDT AccessOnly (`-accessonly`), and hardware association (`-usehwsig` parameter) features are enabled.

```
msiexec /i vee-fs-7.8.0-87-win64.msi /qn registerhostopts="my-key-mgr.example.com -token=12345 -useip -enableldt -accessonly -usehwsig"
```

Validating CM and CTE with a Local CA Certificate**Note**

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

To ensure that registration by the CTE agent is serviced only by the expected key manager, you can provide a copy of the root CA certificate that will be used to authenticate the TLS communications with the key manager, during the registration process.

Note

You can only download the CA certificate when you are a root user in the root domain. You cannot

download the certificate from a subdomain. It will not work.

Prerequisite

Make sure that you have previously [created the client](#) in CipherTrust Manager.

Using a Local CA Certificate

1. Extract the root CA certificate from the CipherTrust Manager.
 - a. Log on to CipherTrust Manager as an administrator.
 - b. In the left navigation pane, click **CA > Local**. The list of available CAs displays.
 - c. Click the ellipsis icon corresponding to the CA.
 - d. Click **Download** to download the CA.
 - e. Copy the certificate to a directory on the agent system.
2. To install the root CA certificate into the CTE client, add it to the registration command line:

Note

You must have administrator privilege to complete this step.

```
C:\Windows\system32> C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\
register_host.exe -silent -log= -vmd -agent= -token= -cafile=
```

Example

```
C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.e
xe -silent -log=c:\vte_reg_log.txt -vmd 10.171.36.175 -agent=ani-vm-217-3519
0.sjcicd.com -token=mMEz3Y60b9D4L7QuvK5S0mhulRm8DYI8odV5j30dvuHqk6LhZqE0FeIZHI
LYTmDiE9 -cafile=C:\tmp\Austin175.pem
```

3. Confirm in CipherTrust Manager that the client is registered and healthy.

Using external certificates for communication between CTE Agent and CipherTrust Manager

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Note

This feature is not compatible when using CipherTrust Transparent Encryption with CipherTrust Data Security Platform Services (CDSPaaS).

Overview

Use for communication between CTE and CipherTrust Manager. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

Prerequisites

The external certificate must be:

- On the file system
- In PEM format

A key pair must already exist for the client:

- Must have Encryption type of either:
 - sha256WithRSAEncryption
 - ecdsa-with-SHA384
- Must be Encrypted with a pass phrase

Initial setup

1. Obtain your external CA certificate.
2. Create a certificate using the external CA certificate and key.

CipherTrust Manager Setup

To setup CipherTrust Manager to communicate through an external certificate:

1. Import the CA certificate into the CipherTrust Manager, click **CA > External > Add External CA**.

Note

In the Add External CA dialog, copy and paste the `<ca_certificate_name>.pem` file content from the UI page and provide a user-friendly name.

For more information, see [Using an Externally Generated Server Certificate for an Interface](#)

2. Add the CA certificate to the list of trusted sources for the web interface, click **Admin Settings > Interfaces > web > Edit > External Trusted CAs**.
3. Restart the web server, click **Admin Settings > Services > web > Restart**.
4. [Create a Registration Token](#) for the CTE agent.

CTE Agent setup

1. Create a directory on the system to hold the required files, for example:
 - `/root/cert_files` (**Linux/AIX**)
 - `c:\temp\cert_files` (**Windows**)
2. Copy or create the following files in this directory:
 - `client_cert.pem`
 - `client_key.pem`
 - `passphrase` - this is currently expected as plain text
3. For **Linux/AIX** systems, to add the directory path to the environment, type:

```
$ export EXTERNAL_CERT_DIR=/root/cert_files
```

4. For **Windows** system, invoke `registerhost.exe` from the command line and add this argument:

```
c:\> register_host.exe -extcertdir=c:\temp\cert_files
```

5. Register the CTE client with the CM server as normal. If this is being done as part of an installation, then the above steps should be done before the installation, or, on windows, added to the registration parameters passed to the installer.

Post Registration

During registration, the certificate file is uploaded to the CipherTrust Manager, and the certificate and key files are imported into the CTE pem store. The key is decoded using the provided passphrase, then re-encoded using a random key using the normal CTE key security mechanisms for TLS keys. There is no need to keep the input files after registration is successful, so for security reasons they should be removed / shredded.

Certificate Renewal

The location of the external certificate files (i.e. the `EXTERNAL_CERT_DIR` or `-extcertdir` parameters) will be recorded in the CTE agent configuration file, `agent.conf`. When the current certificate is approaching expiration date (i.e. approx. 60 days prior to expiration) the CTE agent will look in this directory for an updated set of files.

If a new certificate file is present, then the file will be read and pushed to the CM, and if accepted, then the certificate and key will be imported into the CTE pem store, and the VMD process restarted to use the new certificate.

If no new certificate is present, a WARNING level message will be written to the logs and/or uploaded to the CM as per the logging settings, and the CTE agent will check again after 24 hours.

If the user wishes to change the directory path to store the new certificates, then the entry in the `agent.conf` file should be updated and the vmd service restarted. Alternatively, the user can update the external certificate set using the following command (this will not update the saved path):

```
# vmutil -a vmd -d <ext_cert_Dir> updatecerts
```

If the user fails to update the certificate set prior to expiration then communication with the CM may be blocked, and re-registration will be required.

Note

Any renewed certificates must have exactly the same common name field as the original certificate, or the CipherTrust Manager will reject the update.

Registering CTE After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete.

Use the `register_host` utility to create certificate requests, exchange certificates between the CipherTrust Manager and the host, to enable ransomware detection, and to register CTE on the CipherTrust Manager. After the host is registered, if you selected to enable file system encryption, you can configure CTE, apply GuardPoints, or perform database backups. If you selected ransomware protection, you can apply the protection to volumes. Run the `register_host` utility in text mode on a terminal window.

Caution

The default host registration timeout is 10 minutes. If the host is unable to reach the CipherTrust Manager within the allotted period because of an extremely slow network connection, set the **REGISTER_HOST_TIMEOUT** environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

1. Log on to the host as a Windows user with administrative privileges.
2. Launch the CTE Registration Wizard using one of the following methods:
 - In the system tray, right click the CipherTrust Lock icon and select **Register Host**.
 - Run `...\register_host.exe -vmd -silent`.
3. Reboot the system. CTE automatically displays the registration wizard if CTE is not already registered.
4. In the Register Host dialog box, verify the host's machine name and click **Next**.

Note

For CipherTrust Data Security Platform Services, the host names of the services are:

- **Europe:** `ciphertrust.dpondemand.io`
- **North America:** `us1.ciphertrust.dpondemand.io`

5. On the **Gathering agent information** page, select one or both of the following options and click **Next**.
 - **File System:** Allows you to protect and encrypt CTE files with policies
 - **Ransomware Protection:** Protects volumes from ransomware
6. On the **Gathering Key Manager information** page, enter the FQDN or IP address of the primary CipherTrust Manager.

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: **<hostName>:<port#>**. For example: `10.3.200.141:8445`

When you are done, click **Next**. CTE communicates with the selected CipherTrust Manager to validate what features have been licensed and are available to the CTE Agent.

7. On the **Gathering host information** page:

File System

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see [Hardware Association Feature](#).
- If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the client, select **Enable LDT Feature**. For details on LDT, [CTE Agent Live Data Transformation](#).
- If you want the node to be an [Windows AccessOnly](#) node, select **Enable LDT AccessOnly Feature**.

Ransomware

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see [Hardware Association Feature](#).

When you are done, click **Next**.

8. On the **Gathering registration information** page, enter the following:

File System

- **Registration token:** The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name:** The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.
- **LDT Communication Group:** If you are planning on using LDT over CIFS/NFS on a CipherTrust Manager, enter the name of the LDT Communications Group that this node will join. See [Adding Clients to an LDT Communication Group](#) for more information.

Ransomware

- **Registration token:** The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name:** The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.

- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.

Warning

The registration information is case-sensitive. If any of it is entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

When you are done, click **Register**. CTE contacts the CipherTrust Manager and attempts to register the client with the specified options. The Register Host dialog box displays a message with the results of the registration request.

If the registration completed successfully, click **Finish**.

- Restart the client to complete the installation process on the client.
- After the host has rebooted, you can verify the installation by checking CTE processes:
 - In the system tray of the protected host, right-click the CipherTrust Lock icon.
 - Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.
 - If you are using CipherTrust Manager version 2.2 or later, you can now use CipherTrust Manager to administer CTE on the client.

If you are using CipherTrust Manager version 2.1 or earlier, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Setting the CM log for Ransomware Protection

Setting the CipherTrust Manager log for Ransomware Protection

You need to configure the logging level on CipherTrust Manager to INFO instead of the default, which is ERROR.

To define client log configurations for a profile:

- Open the **Transparent Encryption** application.
- In the left pane, click **Settings > Profiles**.

3. Click on the name of the relevant profile.
4. Click **CLIENT LOGGING CONFIGURATION** to expand it.
5. Set the **Log Level** to **INFO**.
6. Click **Update**. The changes are effective immediately and apply to the clients linked with the profile.

The CTE client logs can be seen on the **Records > Client Records** page of the CipherTrust Manager GUI. Filter the records by **Client Type** and look for the **CTE** records.

Guarding a Device with CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many standard GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

Note

For guarding using LDT on a local drive, or on a CIFS/Share drive, refer to [CTE-Live Data Transformation with CipherTrust Manager guide](#).

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

1. [Access the CipherTrust Manager domain](#) in which the client is registered.
2. Identify or [create an encryption key](#) that CTE will use to encrypt the data on the device or directory.
3. Identify or [create a policy](#) for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. [Assign a GuardPoint](#) to the device or directory.

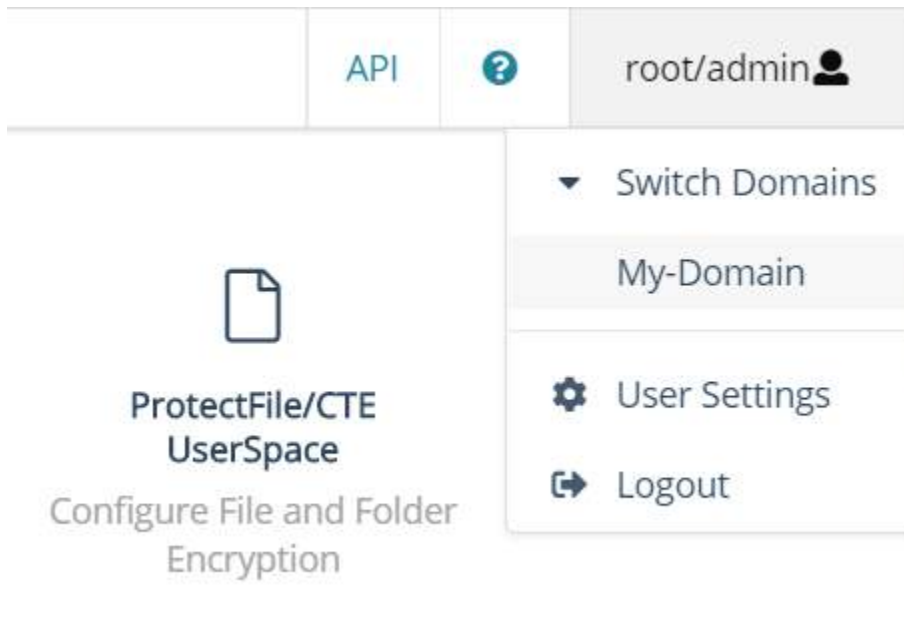
The following example creates a simple policy and uses it to guard a directory on a registered client. For all of the following procedures, you must be logged into the CipherTrust Manager Console as a CipherTrust Manager Administrator, and you must be in the domain with which the client is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the CipherTrust Manager documentation.

Access the CipherTrust Manager Domain

1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to [Create an Encryption Key](#). If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the user name **root/admin** on the right-hand side.

- b. Select **Switch Domains**, then select the domain in which the client is registered.
- c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

Note

The following procedure is based on CipherTrust Manager version 2.2. If you are using a different version, see the CipherTrust Manager documentation for the version that you are using.

1. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.

Tip

To navigate to the Products page from anywhere in the CipherTrust Manager Console, click the App Switcher icon in the top left corner.

2. Above the Key table, click **Create a New Key**.
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
4. In the **Key Usage** section, make sure **Encrypt** and **Decrypt** are selected.
5. Click **Create**. CipherTrust Manager displays the properties for the new key.

6. In the general options area, enable the **Exportable** option.

You can also enable the **Deletable** option in this section if you want a CipherTrust Manager Administrator to be able to delete the key.

ID	2e58c582...61136313	Owner	Global	Object Type	Symmetric Key
UUID	e3ad9c3e...7f047711	Created	05 Mar 2021, 05:13	Algorithm	AES
MUID	e3ad9c3e...7b333c9f	Last Modified	05 Mar 2021, 05:13	Size	256
KeyID	N/A	Exportable	☒	Deletable	☐

7. In the **Key Access** section, do the following:

- a. In the Search Groups box, type "cte".

If no groups are displayed, make sure the **Added Only** option is *disabled*.

- b. Click the **All** check box for both the CTE Admins and CTE Clients groups.

KEY ACCESS								
Key Owner								
Q cte								
2 Results 2 groups								
Group	Read	Use	Decrypt	Encrypt	Sign	Sign/Verify	Export	All
CTE Admins	☒	☒	☒	☒	☒	☒	☒	☒
CTE Clients	☒	☒	☒	☒	☒	☒	☒	☒

- c. When you are done, click **Update**.

8. Click the **CTE** tab and set the following properties:

- **CTE Versioned:** Specify whether the key is versioned. By default, the key is set as versioned.

For a standard policy, you should clear this check box. If you do not, the key will *not* appear in the keys list when you add the key rule to the standard policy.

- **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.

When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.

When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.

- **Encryption Mode:** Encryption mode of the key. The options are:

- CBC
- CBC-CS1
- XTS

Encryption using the XTS and CBC-CS1 keys is known as enhanced encryption.

When you are done, click **Update**.

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **Transparent Encryption** application.
2. In the sidebar on the Clients page, click **Policies**.
3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
4. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a Standard policy.
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints.
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data

Field	Description
	corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.
Data Transformation	If you select Standard as the policy type, also select the the Data Transformation option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

When you are done, click **Next**.

- On the Security Rules page, define the security rules that you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of **key_op** and the effects **Permit** and **Apply Key**. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version.

To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

When you are done, click **Next**.

- On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one. If the data has not yet been encrypted, select clear_key . Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select clear_key .
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one.

Field	Description
	CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

When you are done, click **Next**.

- On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click Select to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in Create an Encryption Key.

When you are done, click **Next**.

- Click **Next**.
- On the confirmation page, review the information for the policy and click **Save**.

Create Policy



- 1 General Info 2 Security Rules 3 Key Rules 4 Data Transformation 5 Confirmation

Review the provided policy details.

1 General Info

Name: Simple-Policy
Policy Type: Standard
Description: Standard policy for new GuardPoints

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*			key_op	permit:applykey	Yes
*					Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	Simple-Key

[Back](#)
[Save](#)

Create a GuardPoint

Caveats

- You cannot have a symlink reside inside of a GuardPoint that is pointing to another location in that same GuardPoint
- You cannot have a symlink reside inside of a GuardPoint that points to the root of that same GuardPoint

Prerequisites

- Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key.
 - C:\HR Files\
 - C:\Accounting Files\
 - C:\Shared Resources\HR\
 - C:\Shared Resources\Accounting\

Tip

If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

Procedure

1. In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
2. In the Clients table, click on the name of the client you want to protect.
3. Above the GuardPoints table, click **Create GuardPoint**.
4. In the Create GuardPoint page:
 - a. In the **Policy** field, select the policy you created earlier.
 - b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a explorer window.

If you want to enter multiple paths, put each path on its own line. For example:

Create GuardPoint [X]

Policy: *
Simple-Policy [Select]

Type: *
Auto Directory [v]

Path: *
C:\HR Files\
C:\Accounting Files\
C:\Shared Resources\HR\
C:\Shared Resources\Accounting\ [Browse]

- d. Click **Create**.
- e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted.

Otherwise, click **No**. For this example, click No.

The CTE clients pull the GuardPoint configuration information from the CipherTrust Manager.

5. Type the following to transform the data:

```
dataxform --rekey --print_stat --preserve_modified_time --gp <pathToGP>
```

When the data transformation has finished, applications can resume accessing the now-protected data. (See the [CTE Data Transformation Guide](#) for more information.)

Installation Prerequisites

This section lists the installation requirements and options you should consider before installing CTE.

Installation Method Options

Requirements

There are two methods for installing CTE:

- **Interactive installation:** This is the most common and recommended type of installation. Use this for installing CTE on one host at a time using a standard InstallShield installation and registration wizard. See [Interactive Installation on Windows](#).
- **Silent installation:** Create pre-packaged installations by providing information and answers to the installation questions. Use silent installations when installing on a large number of hosts. See [Silent Installation on Windows](#).

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the Windows system on which you plan to install CTE to the CipherTrust Manager. After the Windows system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.
- It must also allow for connectivity of the CipherTrust Manager to all clients where you install CTE as well as communication between different CTE clients that plan to enable LDT over NFS/CIFS.
- If the system is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

The following port information applies to both Windows and Linux systems.

Communication through a Firewall

If a protected client must communicate with CipherTrust Manager through a firewall, see the CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

Communication with CipherTrust Manager

The default port for http communication between CipherTrust Manager and the CTE Agent is **443**. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

Communication for LDT over CIFS/NFS

All nodes that intend to use **LDT over CIFS/NFS** GuardPoint must have the following ports open:

- 7024
- 7025

Note

When you are registering a CipherTrust Transparent Encryption client with CipherTrust Manager, you can manually include a destination port number, (Default: 443). If you enter a port value, using the syntax `<hostname or IP address>:<port number>` then CipherTrust Transparent Encryption **does not** perform a port scan. CipherTrust Transparent Encryption uses the port number provided to verify the target server type using a TLS operation.

If you do not enter a port number, CipherTrust Transparent Encryption performs a port scan to check which ports are listening, including port 443.

Hardware Association Feature

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware clients.

You can enable hardware association during CTE registration process. You can disable hardware association by re-running the registration program.

To verify if hardware association (cloning prevention) is enabled on the protected client, access the Windows command line and run the `vmsec.exe hwok` command. The default location of `vmsec.exe` is `C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin`.

To change the status from enable to disable or vice versa:

1. Open the system tray and right-click on the CipherTrust Lock icon.
2. Select **Register Host**.
3. Follow the prompts to re-register CTE with the CipherTrust Manager.

-
4. Select **Enable hardware association** in the wizard.

Multifactor Authentication for CTE GuardPoints

CipherTrust Transparent Encryption is supporting Multifactor Authentication through integration with various MFA providers. CipherTrust Transparent Encryption will continue to integrate with additional providers.

- [Introduction to Multifactor Authentication](#)
- [Current Compatible Multifactor Authentication Providers](#)
- [Use Cases for Multifactor Authentication](#)
- [Exempting some users from authentication with a Whitelist](#)
- [Remote Authentication for Multifactor Authentication](#)
- [Administration for Multifactor Authentication](#)
- [Troubleshooting Multifactor Authentication](#)

Introduction to Multifactor Authentication

Why do companies need Multifactor Authentication

Every day, the threat of ransomware attacks increase in frequency, sophistication, and effectiveness. Victims of ransomware attacks can be blocked from data, applications, and systems – making an organization unable to function.

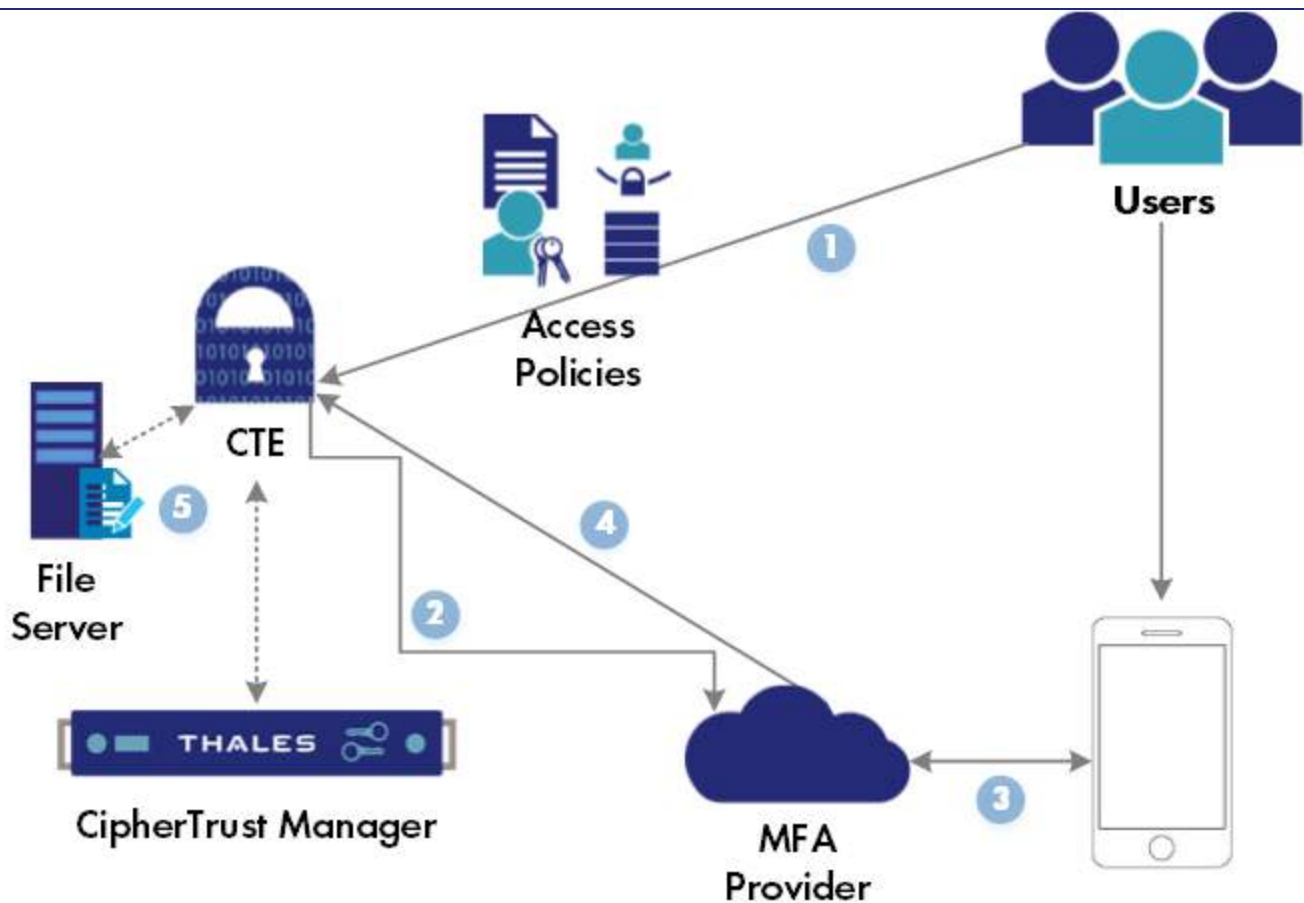
Credential compromise is the leading cause of ransomware attacks, because credentials give hackers the access they need to hold your systems hostage. Unfortunately, credentials can be stolen, shared, bought or hacked. Once the hackers gain entry, the threat actors will often look to compromise privileged access credentials to further infiltrate your network and steal sensitive data.

What is Multifactor Authentication

Multifactor authorization ensures that the access credentials presented belong to the actual person. After logging in to the system, when a user tries to access a CipherTrust Transparent Encryption GuardPoint, it triggers a second factor authorization to verify the user with a second form of authentication, like sending a passcode to the user's registered cell phone, that they then have to input into the application.

How does Multifactor Authentication work

The following diagram explains how Multifactor Authentication operates in a CipherTrust Transparent Encryption environment.



Step	Description
1	Multifactor Authentication is performed when a user tries to access a file in a GuardPoint. NOTE: Multifactor Authentication is only enforced when a file, in a GuardPoint, is first accessed by the user. Multifactor Authentication is not enforced during IO activity, (read/write requests). Therefore, if the file has already been opened by a user/application, Multifactor Authentication will not be enforced on that file.
2	CipherTrust Transparent Encryption sends a message to the Multifactor Authentication provider to verify the user.
3	Multifactor Authentication provider sends a verification request to the user's registered device. NOTE: If Multifactor Authentication is using Password Authentication, this step is not required.
4	Multifactor Authentication provider confirms/denies user access.
5	If authenticated, user has access to the MFA-enabled GuardPoint based on the CipherTrust Transparent

Step	Description
	Encryption access policy. If denied, user does not gain access to the GuardPoint.

For more information on Multifactor Authentication, see [Multifactor Authentication](#).

Compatible MFA Providers

Thales will be continually adding new MFA providers to CipherTrust Transparent Encryption. When the MFA providers pass compatibility testing, they will be added to this page. Select the MFA provider that you are using and follow the instructions below to set up CipherTrust Transparent Encryption for the MFA.

- [Safenet Trusted Authentication](#)
- [OKTA](#)
- [KeyCloak](#)
- [Cisco DUO](#)
- [Microsoft Azure Entra ID Support](#)

Using STA for Multifactor Authentication for CTE GuardPoints

Prerequisites

- Have a CipherTrust Manager set up with:
 - [Client Profile enabled for Multifactor Authentication](#)
 - [Registration token](#)
- Integrate with SafeNet Trusted Access by creating and managing your access controls in [SafeNet Trusted Access](#).

Selecting the Proper Template

Note

Make sure that, in SafeNet Trusted Access, you choose the custom template: **CTE_OIDC**.

If the **CTE_OIDC** template is not available in your account:

1. Create an app using the **Generic Template**.
2. For the Integration Protocol, select **OIDC**.

3. Configure **VALID REDIRECT URL** as: `http://127.0.0.1:5560/auth/callback`.

Note

Port 5560 is the default CTE OIDC login port. If the CTE admin changes it through the `voradmin mfa` command, you must change that value in the redirect URL.

Create an OIDC Connection with CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management > Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values for the configuration information.

Note

Refer to your Multifactor Authentication provider profile for the values:

- URL of OIDC provider:

Linux

- For KeyCloak, select the URL of the OIDC provider

Windows

- For Thales SafeNet Trusted Access, select **Well Known Configuration URL**
- For all other providers, select the URL of the OIDC provider
- Client-ID as configured for the OIDC client
- Client-Secret as shown for the OIDC client

7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

For more on the SafeNet Trusted Access OIDC template, see [OIDC applications](#).

Using Okta for Multifactor Authentication for CTE GuardPoints

Integration with Okta requires creating an OIDC connection in CipherTrust Manager, after you create an OIDC template in Okta.

Prerequisites

- Have a CipherTrust Manager set up with:
 - Client Profile enabled for Multifactor Authentication
 - Registration token

On the Okta platform

1. Create an admin user.
2. Create one or more Okta users. **Note** that Okta requires the username to be in email format.
 - Create **domain users** in the format: `<username>@<domain>.com`
 - Create **host specific users** in the format: `<username>@<hostname>.com`
 - Create **non-domain users** in the format: `<username>@localhost.com`.

Non-domain users map to system users with implicit host domain access on each host.

3. Create an OIDC application (“App Integration”) with the following settings:
 - **Application type:** Web Application
 - **Client Authentication:** Client Secret
 - **Grant type:** Authorization Code
 - **Login/Sign-in Redirect URIs:** `http://127.0.0.1:<CTE-OIDC-Login-Port>/auth/callback`
 - **Default value of CTE-OIDC-Login-Port:** 5560, if CTE admin changes this port, they must provide the updated value.
4. Note the OIDC parameters:
 - Client-ID as configured for the OIDC client
 - Client-Secret as shown for the OIDC client

On CipherTrust Manager

The Provider Url for the Okta account is in the following format:

<https://<okta-account>.okta.com/.well-known/openid-configuration>

Create an OIDC connection on CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management > Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values for the configuration information.

Note

Refer to your Multifactor Authentication provider profile for the values:

- URL of OIDC provider:

Linux

- For KeyCloak, select the URL of the OIDC provider

Windows

- For Thales SafeNet Trusted Access, select **Well Known Configuration URL**
- For all other providers, select the URL of the OIDC provider
- Client-ID as configured for the OIDC client
- Client-Secret as shown for the OIDC client

7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

Using Keycloak for Multifactor Authentication for CTE GuardPoints

Integration with Keycloak requires creating an OIDC connection in CipherTrust Manager, after you create an OIDC template in Keycloak.

Prerequisites

- Have a CipherTrust Manager set up with:
 - [Client Profile enabled for Multifactor Authentication](#)

- Registration token
- CipherTrust Transparent Encryption host and Keycloak server must have their time's synchronized. If they are not time-synced, then Multifactor Authentication login fails with the following error:

Failed to verify ID Token: oidc: token is expired (Token Expiry: 2022-11-08 22:42:20 -0800 PST)

On the Keycloak platform

1. Create an admin user.
2. Login to the realm and create one or more users.
3. Create a password for the user.
4. Create an OIDC client in realm with the following settings enabled:
 - **Valid Redirect URIs:** Configure in the format:
`http://127.0.0.1:<CTE-OIDC-Login-Port>/auth/callback`
 - **Default value of CTE-OIDC-Login-Port:** 5560, if CTE admin changes this port, they must provide the updated value.
 - **General Settings:**
 - **Client Type:** OpenID Connect
 - **Client ID:** Client name
 - **Capability Config:**
 - **Client Authentication:** On
 - **Authorization:** On
 - **Authentication Flow:** Standard Flow
5. Note three OIDC parameters:
 - Provider URL format:
 - For **non-TLS**: `http://<keycloak-ip>:<keycloak-port>/realms/<realm-name>/.well-known/openid-configuration`
 - For **TLS**: `https://<keycloak-ip>:<keycloak-port>/realms/<realm-name>/.well-known/openid-configuration`

Note

If KeyCloak is configured for TLS, the KeyCloak certificate (if self-signed), or certificate chain, including the root CA, and any intermediate CAs, must be imported into the CipherTrust Transparent Encryption client machine. Import the self-signed certificate as a root CA. CipherTrust Transparent Encryption will fail to connect to the provider if certificates are not imported. To import a certificate: see [Importing Certificates Using MMC](#)

- Client-ID as configured for the OIDC client
- Client-Secret as shown for the OIDC client

Create an OIDC connection on CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management > Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values for the configuration information.

Note

Refer to your Multifactor Authentication provider profile for the values:

- URL of OIDC provider:

Linux

- For KeyCloak, select the URL of the OIDC provider

Windows

- For Thales SafeNet Trusted Access, select **Well Known Configuration URL**
- For all other providers, select the URL of the OIDC provider
- Client-ID as configured for the OIDC client
- Client-Secret as shown for the OIDC client

7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

Using Cisco DUO for Multifactor Authentication for CTE GuardPoints

Integration with Cisco DUO requires creating an OIDC connection in CipherTrust Manager, after creating a DUO account.

On the DUO platform:

1. [Create an account on Cisco Duo](#).
2. Login to your Cisco DUO account as an admin and click **Users** in the left navbar to create/add one or more users.
3. While creating a user, set the **Status** as **Active**
4. Click **Applications** in the left navbar.
5. Click **Protect an Application**.
6. In the search field, type **Web SDK**.
7. In the Web SDK field, click **Protect**.
8. In the application created, note the values for:
 - **Client ID**
 - **Client Secret**
 - **API hostname**

Note

https:// is the value for the URL of the OIDC Provider.

Create an OIDC Connection with CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management > Connections**.
3. In the Connections, click **Add Connection**.

4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values for the configuration information.

Note

Refer to your Multifactor Authentication provider profile for the values:

- URL of OIDC provider:

Linux

- For KeyCloak, select the URL of the OIDC provider

Windows

- For Thales SafeNet Trusted Access, select **Well Known Configuration URL**
- For all other providers, select the URL of the OIDC provider
- Client-ID as configured for the OIDC client
- Client-Secret as shown for the OIDC client

7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

Using Microsoft Azure Entra ID Multifactor Authentication for CTE GuardPoints

Create an OIDC Application in Entra ID

1. Select **Microsoft Entra ID** from your Azure Homepage.
2. Click **App Registration**.
3. Create a **New Registration**.
4. Record the client ID. You will need it when you create an OIDC connection on CipherTrust Manager.
5. Click **Certificates and Secrets** in the left Nav bar.
6. Create a new **Client Secret**. This is the Client Secret value that you will enter in CipherTrust Manager.
7. For the Redirect URI, select **Web**.
8. Enter redirect URL with your local host name: `http://<localhost>:5560/auth/callback` and save

it.

- Click on the name of your registration and click **Endpoints**.
- Copy the value for the Endpoint for **OpenID Connect metadata document**. This is the OIDC Provider value that you will enter in CipherTrust Manager.

Create an OIDC Connection in CipherTrust Manager

- Log on to the CipherTrust Manager as an administrator.
- In the left pane, click **Access Management > Connections**.
- In the Connections, click **Add Connection**.
- Click **OIDC** and then click **Next**.
- Provide a name for the connection and click **Next**.
- Enter values collected in the previous section for the configuration information.
 - OIDC Provider: <value for the Endpoint for OpenID Connect metadata document>
 - Client ID
 - Client Secret
- Click **Next** and in the Add Products window, select **CTE** for product.
- Click **Add Connection**.

Set Client Profile in CipherTrust Manager

- In CipherTrust Manager, open the Transparent Encryption application.
- In the left pane, click **Settings > Profiles**.
- Select the desired client profile.
- Expand **MULTIFACTOR AUTHENTICATION**.
- Select the OIDC Connection that you created for Entra ID.
- Select **MFA Exempted User Set** from the drop-down list. This user set will be exempted from MFA so MFA will not be enforced on the users of this set. See [Exempting some users from authentication with a Whitelist](#) for more information.

Domain Mapping

Domain mapping is required for Entra ID. If you try to log in prior to mapping the domain, CTE generates an error.

You must map the domain **from** the Entra ID domain **to** the domain of the existing CTE host. Ask your System Administrator for the domain information.

1. To set the domain, type:

```
voradmin mfa domains-map set <domain1>:<domain2>
```

Example

```
voradmin mfa domains-map set thalesgroup.com:qa.com
```

Response

```
Restart secfsd service to affect changes.
```

Note

You can map multiple domains using a comma in between domain names. For example:

```
voradmin mfa domains-map set <domain-1-onMFA-provider>:<domain-1-onHost>,<domain-2-onMFA-provider>:<domain-2-onHost>
```

2. To stop secfsd, type:

```
net stop secfsd
```

3. To restart secfsd, type:

```
net start secfsd
```

Use Cases for MFA on CTE

When using Multifactor Authentication with CipherTrust Transparent Encryption, after successfully completing the [MFA provider](#), you can enable it on a:

- Client
- GuardPoint

- GuardPoint, while exempting certain users/applications/processes from authentication

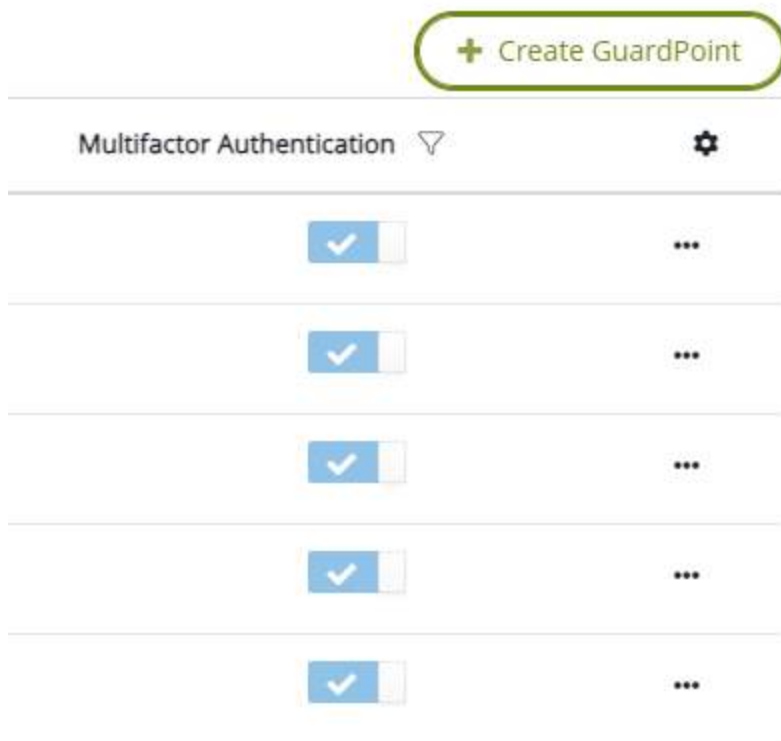
Enable Multifactor Authentication on a client

You can enable Multifactor Authentication for all of the GuardPoints on a client. When Multifactor Authentication is enabled at the client level, CTE enforces the configuration for all GuardPoints configured on the client. It overrides any MFA configuration set for individual GuardPoints.

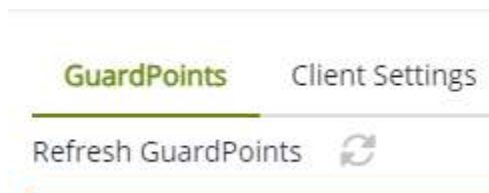
1. Open **CipherTrust Manager > Transparent Encryption** application.
2. Select the relevant client.
3. In the upper pane, select **Multifactor Authentication**.



4. Select **Apply**. All of the Multifactor Authentication switches are toggled to the **on** position.



5. If the MFA column doesn't display with all switches set to on, click **Refresh GuardPoints** to display the Multifactor Authentication column.



Note

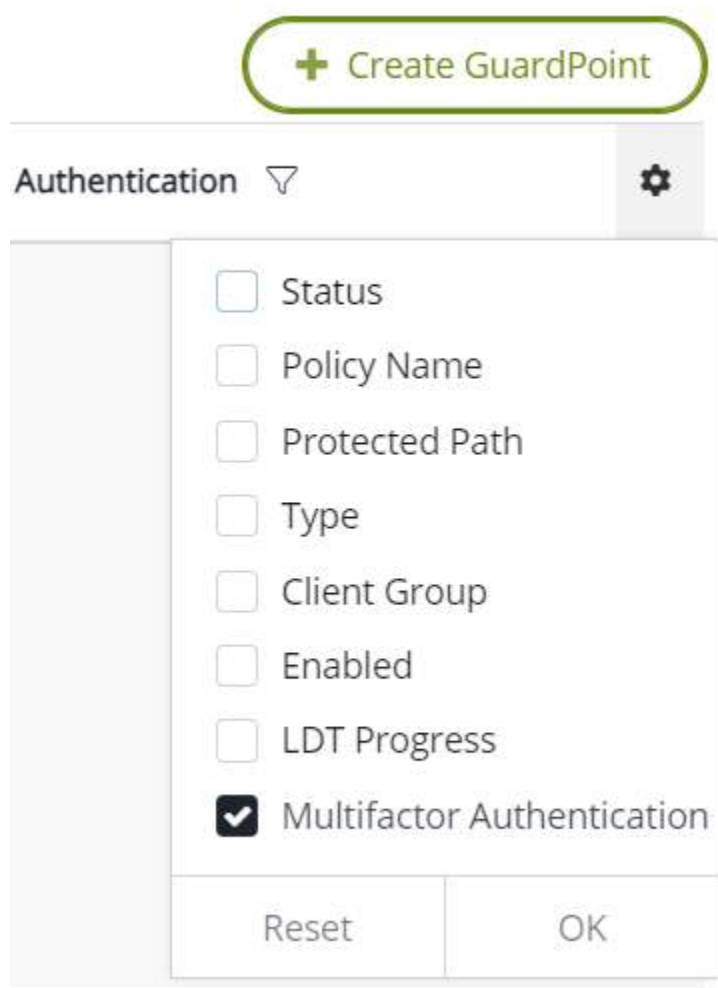
To disable Multifactor Authentication on a GuardPoint, deselect Multifactor Authentication in the upper pane and click **Apply**.

Enable Multifactor Authentication on a GuardPoint

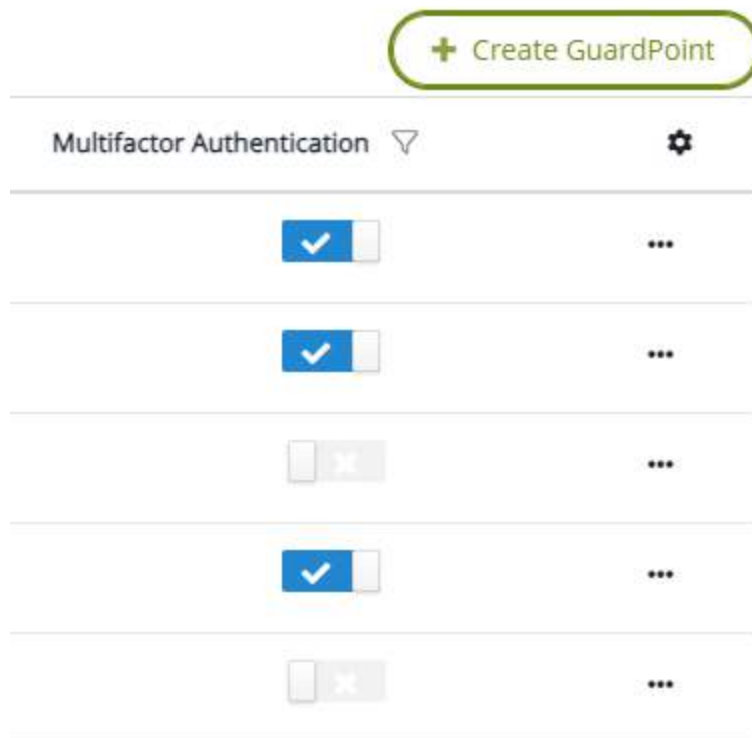
You can enable Multifactor Authentication for individual GuardPoints on clients.

1. Open **CipherTrust Manager > Transparent Encryption** application.
2. Select the relevant client.
3. Select the **GuardPoints** tab.

4. Click the settings icon.
5. Select **Multifactor Authentication** to enable Multifactor Authentication for the GuardPoints.



6. Click **OK**. The Multifactor Authentication column displays.



7. Toggle the Multifactor Authentication switch to enable Multifactor Authentication for the selected GuardPoints.

Note

To disable Multifactor Authentication on a GuardPoint, deselect the Multifactor Authentication toggle switches.

Enable Multifactor Authentication for Client Groups

Multifactor authentication cannot be enabled at the client group level. However, you can enable Multifactor Authentication for individual GuardPoints on client groups.

While propagating the Multifactor Authentication-enabled GuardPoints to the member clients, CipherTrust Transparent Encryption checks the Multifactor Authentication capability of the member clients. If a client is Multifactor Authentication-capable, the GuardPoints are added to the client. If a client is not Multifactor Authentication-capable, the GuardPoints are skipped.

Exempting some users or processes from authentication with a Whitelist

When you activate CTE Multifactor Authentication, all users attempting to log in to the CTE client must successfully pass through CTE Multifactor Authentication to gain entry to the MFA-enabled GuardPoints. However, there are specific exemptions to this rule. Users whose system services, or applications, initiate automatically during system boot-up cannot undergo authentication through CTE Multifactor Authentication, as Multifactor Authentication necessitates user interaction. To accommodate such cases, exempt these users from Multifactor Authentication enforcement within the Client Profile by including them in the user set exemption list.

Typically, only system users responsible for running system services are included in this list. However, since many system applications operate under the root user, or even under normal application user accounts, you must also add these system administrator/application users to the list. These users form part of the user set, commonly referred to as a whitelist.

Caution

Be careful when adding a user to the whitelist. The exemption applies for the entire client. Users on this list can bypass Multifactor Authentication and access all MFA-enabled GuardPoints. If a system service, or application, accesses only one GuardPoint among multiple GuardPoints, Thales advises you to leave that specific GuardPoint without Multifactor Authentication enforcement.

Note

You **cannot** share the whitelist between Windows and Linux operating systems. Each client profile must contain a unique Multifactor Authentication whitelist. Therefore, the User Set contains different users in Windows and Linux platforms. A CTE Windows client and a CTE Linux client **cannot** share the same client profile when Multifactor Authentication is enabled.

Creating a User Set

See [Creating User Sets](#) for information on creating a User Set in a Policy Element.

Adding the User Set to the Client Profile

To add an Multifactor Authentication whitelist to the client profile:

1. Create your [Client Profile](#) if it is not already created.
2. Click on your client profile to open it.
3. Click **Multifactor Authentication**.
4. In the **Select OIDC connection** field, select the OIDC connection that you created.
5. In the **Select the MFA exempted User Set** field, select the User Set that contains the people/applications that are exempted from authorization.
6. Click **Update**.

Remote Authentication for Multifactor Authentication

By default, CipherTrust Transparent Encryption works with a local Multifactor Authentication login. In CipherTrust Transparent Encryption v7.6 and subsequent versions, you can configure remote authentication for Multifactor Authentication. This allows a user to log into Multifactor Authentication through a machine other than a CTE client. This allows you to enable authentication from remote endpoints accessing CIFS shares, exported by a CTE

agent.

Note

- Your Windows remote access system logon account name, and your Multifactor Authentication account name, **MUST** be the same.
- The MFA username, including the domain-name, in the format domain\username or username@hostname, must exist on the MFA provider.

Remote Authentication configuration requires a non-encrypted private key and certificate. The CipherTrust Transparent Encryption OIDC service uses the key and certificate for TLS communication. CTE stores encrypted keys and certificates internally.

Prerequisites

- Create a firewall rule on a CTE agent to allow all incoming TCP traffic on the Multifactor Authentication login port.
- Generate a private key and certificate. You must know the name and location of these files.
- In the Keycloak setup, set the **redirect-url** parameter for OIDC configuration using the following format: `https://<cte-hostname>:<mfa login port>/auth/callback`.

Note

- The Administrator can choose to use a wildcard ('*'), if the same configuration is reused across many CTE agents.

- You must have administrator access so that you can restart secfsd service:
 - a. To stop secfsd service, type:

```
net stop secfsd
```
 - b. To start secfsd service, type:

```
net start secfsd
```

Starting Remote Authentication for Multifactor Authentication

To configure remote authentication:

1. In a command line, type:

```
voradmin mfa remote-config set [<privateKeyFile> <certificateFile>]
```

Example

```
voradmin mfa remote-config set private-key.pem cert.pem
```

Response

```
voradmin mfa remote-config set  
Restart secfsd service to affect changes.
```

2. Restart the secfsd service.

Disabling Remote Authentication for Multifactor Authentication

To disable remote authentication:

1. In a command line, type:

```
voradmin mfa remote-config unset
```

Response

```
Restart secfsd service to affect changes.
```

2. Restart the secfsd service.

Validating Certificate and Private files information

To validate the two certificates:

- In a command line, type:

```
voradmin mfa remote-config get [<privateKeyFile> <certificateFile>]
```

Example

```
voradmin mfa remote-config get private-key.pem cert.pem
```

Response

```

sha256 of key file:
dcb8eXXXXa92ac5dff34aXXXXab3811245aXXXXc204733bbeat43f4846274674

sha256 of certificate file:
3e2eec5bXXd357d14f5c0047d36aXXXXXXXXfc87f2a74ca3b5c2c2627XXxe6db4

certificate:
-----BEGIN CERTIFICATE-----
MIIFuTCCA6GgAwIBAgIUR+Gh3z7J8TzQr6buZGDcK9h/8MQwDQYJKoZIhvcNAQEL
BQAwbDELMAkGA1UEBhMCSU4xCzAJBgNVBAGMALVQMqswCQYDVQQHDAJOTzEMMAoG
A1UECgwDQ1BMMQwwCgYDVQQQLDANESVMxCzAJBgNVBAMMALRIMRowGAYJKoZIhvcN
.
.
.
/31kjs/Kms582KTKFKFqzuZHJ4L6odL6JB0mbvv4UZGB2t99ah0R9BAutivru/0M
ZFvotV9Xsxs49PtOggj1vkwFdlWUR7VtcdF0tiIoSvuXhMjCvTq8KtPIXiJJjFFkN
3xD4ZmG7M14u1hzmaXqHfZ02YZ0ISFltq2PUWqQ=
-----END CERTIFICATE-----

```

Using Remote Authentication for Multifactor Authentication

To login and use Multifactor Authentication from a remote endpoint:

- User must open a browser and enter a valid URL with the format: `https://<cte-hostname>:<mfa login port>/login`.

Note

When launched from the Etray application on a CTE agent, the browser is launched with the required URL automatically in the URL field.

Administrator Tasks for Multifactor Authentication

Using the Proper Filter

Note

The Multifactor Authentication feature **requires** the CTE VMLFS driver. This driver **must** be running in order for Multifactor Authentication to work.

- All new installations of 7.3.0.x contain this driver. Type `fltmc` to verify. A table displays listing all current drivers.

Filter Name	Num	Instances	Altitude	Frame
WdFilter		4	328010	0
storqosflt		0	244000	0
wcifs		0	189900	0
vmifs		4	142900	0
FileCrypt		0	141100	0
luafv		1	135000	0
npsvctrig		1	46000	0
Wof		1	40700	0

- Agents upgraded from 7.2.0, and previous versions, may be using the vmfiltr driver. If the agent ran the vmfiltr driver, then when you upgrade to 7.3.0, it will start with the vmfiltr driver. If the previous agent ran the vmifs driver, then when you upgrade to 7.3.0, it will start the vmifs driver. Type the following to switch to the vmifs driver:

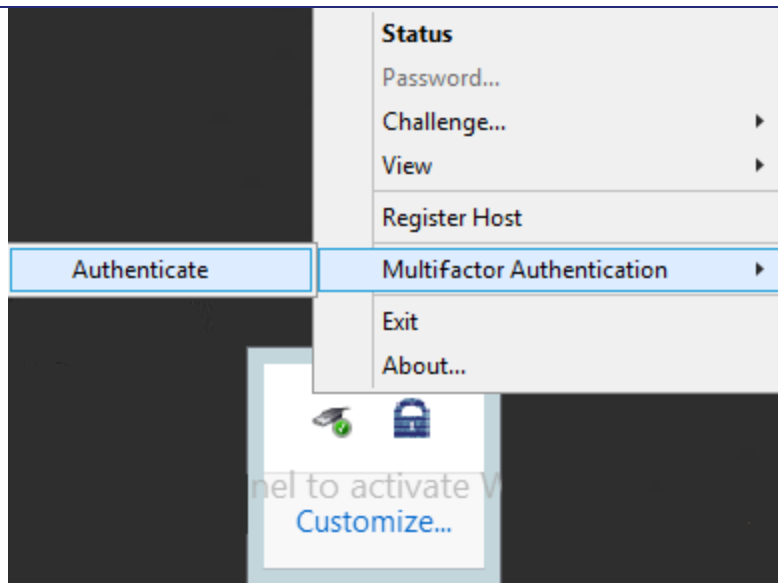
```
voradmin config enable vmifs
```

User Authentication

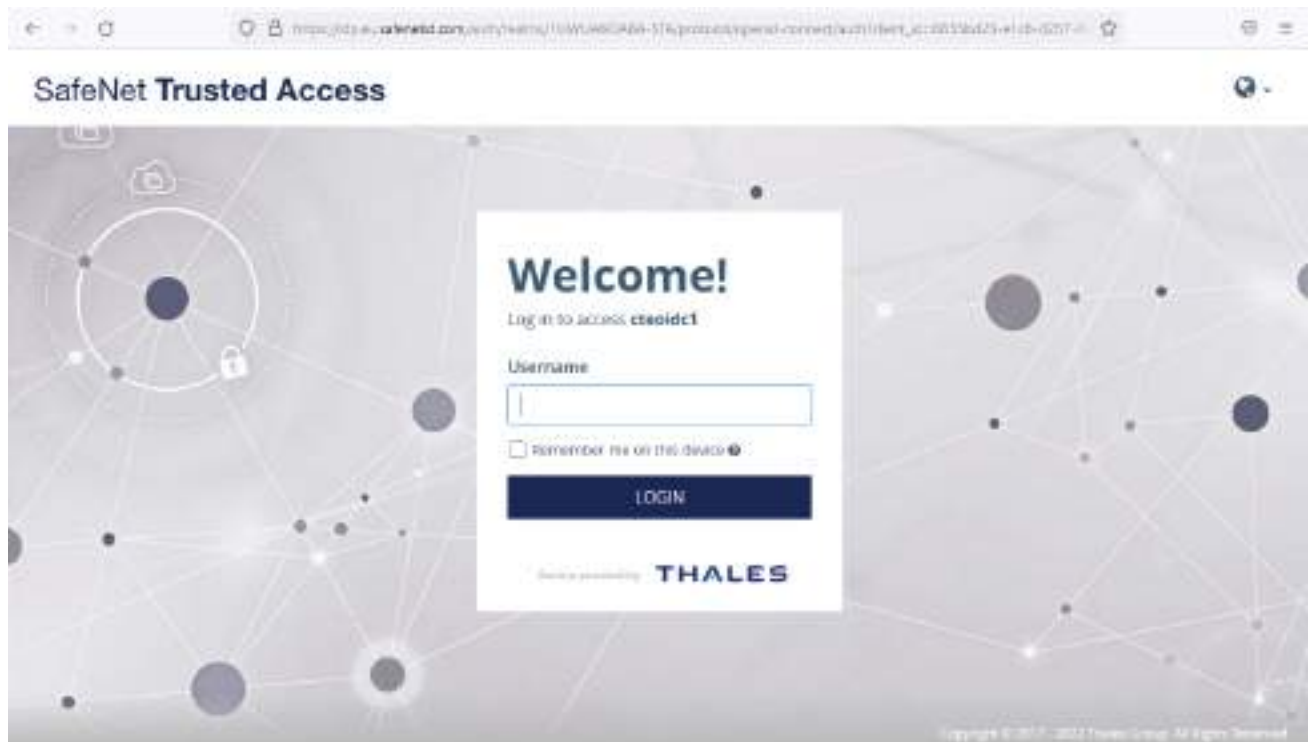
Authentication is provided for the entire client and is enforced the first time a user opens a file. After the initial file opening, the user can perform read/writes to the file.

To authenticate, a user can login to MFA from the Windows system tray:

1. Click on the CTE icon in the System Tray.
2. Select **Multi-Factor Authentication > Authenticate**.



3. Login in to access the STA OIDC template.



After you log in, a message displays confirming your authentication and your access to the GuardPoint.

4. Close the Window to continue.

Note

If you logout, you disable your access to the GuardPoint.

Voradmin Commands

voradmin mfa status

Displays the MFA information for a user.

Syntax

```
voradmin mfa status
```

Example

```
C:\Windows\system32>voradmin mfa status
```

Response

```
User \dram is allowed access.  
MFA enabled guardpath(s) (Number of paths: 2):  
C:\cm\gp2  
C:\cm\gp1
```

voradmin mfa config

Displays configuration information.

Syntax

```
voradmin mfa config
```

Response

```
HostMfaEnable is set.  
MFA enabled guardpath(s) (Number of paths: 2):  
C:\cm\gp2  
C:\cm\gp1  
MFA access allowed users(s) (Number of users: 2):  
  Users\dram  
  NT AUTHORITY\SYSTEM  
MFA Exempt-List: (Number of entries: 1)  
  user: "system", group: "", domain(s): "NT AUTHORITY"  
OIDC configuration:  
  login-port : 5560  
  notification-port : 5562  
  client-id : 6653gd25-e1c7-4257-6034-46c77ffc8cb6  
  url : https://idp.eu.safenetid.com/auth/realms/1UWUA52A8A-STA
```

voradmin mfa check-connection

Allows the admin user to check the connection to the OIDC provider.

Syntax

```
voradmin mfa check-connection <name_of_OIDC-configuration-url>
```

Example

```
C:\Windows\system32>voradmin mfa check-connection https://idp.eu.safenetid.com/auth/realms/1UWUA60A8A-STA/.well-known/openid-configuration
```

Response 1: Success

```
Connection ok to https://idp.eu.safenetid.com/auth/realms/1UWUA60A8A-STA/.well-known/openid-configuration
```

Response 2: Failure

```
Connection failed to https://idp.eu.safenetid.com/auth/realms/1UWUA60A8A-STA/.well-known/openid-configuration-bad
```

voradmin mfa update-ports

Allows the administrator to update the OIDC ports.

- Updating the ports restarts the CipherTrust Transparent Encryption Multifactor Authentication application. Users must login to Multifactor Authentication again after the ports are updated.

Warning

If the OIDC-login-port is changed, then the redirect-URI for the OIDC application at the Multifactor Authentication provider must also be changed. It is specified in the format: `http://127.0.0.1:<oidc-login-port>/auth/callback`. If redirect-URI is not changed, CipherTrust Transparent Encryption may fail to connect to the provider.

Syntax

```
voradmin mfa update-ports <oidc-login-port> <oidc-notification-port>
```

Example

```
C:\Windows\system32> voradmin mfa update-ports 8000 8075
```

Response

```
Updated OIDC ports
```

voradmin mfa set-auth-expiry

Allows the admin to set an authentication expiry time.

Note

Changing authentication expiry clears all existing MFA logins. Users must login again.

Syntax

```
voradmin mfa set-auth-expiry <time interval in minutes (specify 0 to disable expiry time)>
```

Example

```
C:\Windows\system32> voradmin mfa set-auth-expiry 5
```

Response

```
Authentication will expire every 5 minute(s).  
Re-authenticate for new settings.
```

voradmin mfa localhost-redirect-uri

You do not need to manually set a parameter for this command. If you use **set** it automatically uses `http://localhost:5590/auth/callback` as the redirect URI. If you use **unset** it automatically uses the default redirect URI for the MFA provider. This command is useful if an MFA provider does not allow 127.0.0.1 as the redirect URI.

Syntax

```
voradmin mfa localhost-redirect-uri <get|set|unset>
```

voradmin mfa domains-map

Domain mapping is generally applicable for use with all providers, though it is only required for Entra ID.

Syntax

```
voradmin mfa domains-map <get|set|unset> <domain1>:<domain2>
```

Example

```
voradmin mfa domains-map set thalesgroup.com:<localhost>.com
```

Response

```
Restart secfsd service to affect changes.
```

Note

You can map multiple domains using a comma in between domain names. For example:

```
voradmin mfa domains-map set <domain-1-onMFA-provider>:<domain-1-onHost>,<domain-2-onMFA-provider>:<domain-2-onHost>
```

voradmin mfa remote-config

Remote authentication allows a user to log into Multifactor Authentication through a machine other than a CTE client. This allows you to enable authentication from remote endpoints accessing CIFS shares, exported by a CTE agent.

Syntax

```
voradmin mfa remote-config [<get|set|unset>] [<privateKeyFile> <certificateFile>]
```

Options	Description
certificateFile	Presented to web browser during TLS communication to the web browser.
get	Displays the 'sha256' encryption for keys and certificates. It allows the customer to check for a valid key and certificate that they imported using the set option.
privateKeyFile	Used by the OIDC service for TLS communication with the web browser.
set	Imports the key and certificate in use by CTE.
unset	Disables the remote authentication for Multifactor Authentication and reverts back to local Multifactor Authentication authentication.

See [Remote Authentication for Multifactor Authentication](#) for more information.

Restarting SecFSD

Many Multifactor Authentication commands require restarting SecFSD to enable.

1. To stop secfsd, type:

```
net stop secfsd
```

2. To restart secfsd, type:

```
net start secfsd
```

Troubleshooting Multifactor Authentication

Error Message: Failed to exchange token

This error message occurs when there are multiple failed login attempts for MFA due to incorrect username or credentials.

Solution

Contact an administrator who controls access to the MFA provider. The administrator needs to unlock the user's account(s) to fix the problem.

User denied access to Multifactor Authentication

User is blocked from accessing Multifactor Authentication.

Solution

- Your Windows remote access system logon account name, and your Multifactor Authentication account name, **MUST** be the same.
- The MFA username, including the domain-name, (if provided, in the format domain\username), must exist on the MFA provider. If no domain is provided, CTE infers it as hostname\username.

"Unknown Certificate" warning from browser

When a remote user launches the browser for remote Multifactor Authentication, it generates a TLS handshake error for unknown certificate in the agent system log directory.

Solution

To prevent the **Unknown Certificate** warning from a browser when accessing a remote endpoint, an administrator must import the certificate configured for remote Multifactor Authentication, to the CTE agent in the endpoint and in the browser configuration.

Multifactor Authentication Client Profile Failed on CipherTrust Manager enrollment**

Switching existing Multifactor Authentication Client Profile using `register_host` failed on CipherTrust Manager enrollment.*

Work-around

- In CipherTrust Manager, change the existing Multifactor Authentication **Select MFA Exempted User Set** parameter to your new target user set

Choosing a Login Name Type

Currently, CipherTrust Transparent Encryption authenticates users with a User Principal Name (UPN). In Windows Active Directory, a UPN is the name of a system user. It is written in an email address format, for example: john.doe@domain.com.

The Security Account Manager (SAM) is a Windows database that stores user accounts and security descriptors for users on the local computer. The SAM Account Name is used to support clients and servers running earlier versions of the operating system, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager.

Previously, CipherTrust Transparent Encryption only supported the UPN. Now, you can choose which login name you want your users to use. However, you must choose SAM Account Name or UPN. You cannot use both. By default UPN support is enabled on a host.

CipherTrust Transparent Encryption provides the following **voradmin** commands to change the Windows registry entries.

To enable SAM support:

1. Type the following command:

```
voradmin config usernamesupport samAccountName
```

2. Reboot the system for the changes to take affect.

To enable UPN support:

1. Type the following command:

```
voradmin config usernamesupport userPrincipalName
```

2. Reboot the system for the changes to take affect.

To get a status of the current support:

1. Type the following command:

```
voradmin config usernamesupport getCurrentNameSupport
```

2. Reboot the system for the changes to take affect.

Ransomware Protection

- [Setting up Ransomware Protection during Registration](#)
- [Use Cases for Ransomware Protection](#)

Ransomware Protection Overview

Compatibility

Operating System	CipherTrust Manager version
Ransomware Protection for Windows	v2.12 and subsequent versions
Ransomware Protection for Linux	v2.17 and subsequent versions

Overview

Ransomware is a type of malicious software that is designed to block access to a computer system until a sum of money is paid. CTE for supports detection of Ransomware and protection of sensitive data from Ransomware.

CTE Agent monitors volumes and looks for processes that perform suspicious behavior such as processes that try to encrypt files or open thousands of files. If a process displays suspicious behavior, then it is either audited, which means it is flagged in a log file, or it is blocked. The action taken is preconfigured by the user in the profile linked to the client.

Licensing

Ransomware Protection is supported with RWP-enabled CTE clients. A CTE for Ransomware Protection license must be activated on the CipherTrust Manager to register an RWP-enabled CTE client. Refer to [CTE Licensing Model](#) for details.

Protecting Non-Sensitive Data

Use the Ransomware Protection mode to protect systems that do not contain sensitive data, but have access to your network.

A use case of this scenario is when you have users with laptops who frequently use your network and access servers on it, but they do not have any sensitive data locally on their laptops. A system like this might belong to a salesperson who travels and frequently uses other networks to access the internet. When such users log on to your network, they access the sales network server and upload data to it. They could easily pick up a Ransomware from another network and accidentally upload it to your company's network. Using the Ransomware Protection mode would protect the data on the local volumes, mounted volumes, and the network servers from being infected with Ransomware.

Protecting Sensitive Data

The Ransomware Protection mode protects data on servers and endpoints from Ransomware attacks by auditing and blocking malicious IPs. Users can strengthen the security posture with CTE access and encryption policies and Ransomware protection for complete control on their data.

To protect sensitive data against Ransomware:

1. Ensure that the CTE Ransomware Protection license is activated and available on the CipherTrust Manager. Refer to [CTE Licensing Model](#) for details.
2. Install the CTE Agent with the Ransomware Protection capability enabled. The Ransomware Protection

support uses the same registration process as CTE clients. Refer to [Configuring CTE with CipherTrust Manager](#) for information on installing and configuring CTE Agents.

3. Configure the Ransomware Protection settings in the linked client profile. Refer to [Setting Ransomware Protection Configuration](#) for details.
4. Create a Ransomware Protection GuardPoint on a volume (Windows)|directory (Linux) and on the directory for Linux to be protected. Refer to the [Creating Ransomware GuardPoints](#) for details.

CTE Registration

During CTE registration with CipherTrust Manager, the following question displays:

```
If you are planning to use Ransomware Protection, type Y.
Do you want this host to have Ransomware protection support enabled on the server? (Y/N) [N]
```

CTE Ransomware Protection can support the following protection modes:

- **Filesystem protection (CTE)**

Allows you to protect and encrypt files with policies **without** Ransomware Protection.

- **Ransomware Protection (RWP)**

CTE is deployed to monitor volumes (Windows)|GuardPoints (Linux), for suspicious behavior from processes, and supports auditing or blocking of the processes.

- **Filesystem and Ransomware Protection (CTE-RWP)**

Protects GuardPoints from Ransomware and allows you to protect and encrypt CTE files with policies.

Use Ransomware Protection GuardPoints to monitor or block Ransomware access attempts to a protected GuardPoints on the CTE clients. Note that if the GuardPoint type is "Ransomware Protection Only", Ransomware Protection GuardPoint does not require any policy.

Locking the System after a Ransomware Attack

After enabling Ransomware Protection during installation, turn on the agent lock and the system lock in CipherTrust Manager. The Agent lock protects the CTE Agent files from modification and deletion. The System lock protects a system files from modification and deletion. Agent Lock automatically enables when System Lock enables. You can manually enable or disable the Agent Lock only when the System Lock is disabled.

Make sure that no one is currently accessing the Agent installation directories while applying the locks.

To apply the locks:

1. In CipherTrust Manager, open the **Transparent Encryption** application.
2. Click on the **Client Name** or **Client Group Name**.

3. On the lock bar, click **Agent Lock**.



4. Click **System Lock**.



5. Click **Apply**.

Windows Volume Shadow Copies

Ransomware Protection now detects and prevents deletion of Windows Volume Shadow Copies. The Volume Shadow Copy service is a built-in Windows feature that allows for the creation of backup snapshots of computer files, or disks, and often facilitates other commercial backup solutions. Most ransomware threats normally try to delete the volume shadow copies in order to prevent a healthy recovery from a Ransomware-infected system. Starting from CTE 7.7, deletion of volume shadow copies is prevented if CTE flags the presence of one or more malicious processes on the entire system. This will allow customers to recover their systems if infected by ransomware.

Reference Information

- [Setting Client Locks](#)

Disabling Ransomware Protection

To disable Ransomware Protection for all GuardPoints on the clients linked with a profile.

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **RANSOMWARE PROTECTION CONFIGURATION**.
5. Select the **Operation** to **Disable**.
6. Click **Update**.

Creating GuardPoints for Ransomware Protection

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

To create a Ransomware Protection GuardPoint:

1. In CipherTrust Manager, open the **Transparent Encryption** application.
2. Select the client or client group on which you want to create a GuardPoint.
 - Click an Ransomware Protection-enabled client under the **Client Name** column (**Clients > Clients**). These are the clients with either Ransomware Protection, or CTE Ransomware Protection, protection mode.
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click **Create GuardPoint**:

Note

Once Ransomware Protection is enabled during CTE registration, Ransomware Protection is applied to all GuardPoints.

Ransomware Protection is supported in 2 Protection Modes:

- **RWP**: In CipherTrust Manager, when creating a GuardPoint, you cannot assign a policy and type is automatically set to Ransomware Protection Only.
- **CTE-RWP**: On clients with **CTE RWP** mode, you can create a Ransomware Protection GuardPoint set to Ransomware Protection Only, as well as other types of GuardPoints that use policies as shown below. In Linux, Ransomware Protection is also available for other GuardPoints if the GuardPoints are set on a directory.



Status	Policy Name	Protected Path	Type	Client Group	Enabled	LEP Progress	Multistep Authentication
	ctm_rwp	\\mybookworms\c:\	Anti-Corruption		Yes	100%	
	ctm_rwp	\\mybookworms\c:\	Ransomware Protection Only		Yes	100%	

4. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:
 - **Enter/Browse Path**: Select this option, and enter the path by either typing or clicking the **Browse** button.

Note

- For **CTE Windows**, Ransomware Protection GuardPoints are applied at the volume level. Even if you specify the path of a folder or a file, the GuardPoint will be applied at the volume level.

- For **CTE Linux**, Ransomware Protection is applied at GuardPoint level.
- If you specify a network share, all of the network shares to be mounted subsequently will be protected.
- A CTE client administrator can configure protection of all existing GuardPoints, and those to be added to the client subsequently.
- A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

Browse Method

- a. Click **Browse** to select the path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths. Note that the client must be registered with CipherTrust Manager in order to browse its file system.
- b. In the **Enter Path** field, specify the path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.
- c. Click **Add**.

Manual Method

Alternatively, if you know the path, manually enter path in the given text box. Enter one path per line.

- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more paths. This is the recommended method to specify a large number of paths in one step.

Note

If a manually entered path does not yet exist, check that you entered the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.

5. Click **Create**. A message appears prompting to confirm the reuse of these GuardPoint settings on another path.
 - Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:
 - a. In the **Enter Path** field, specify the path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.
 - b. Click **Add Path**. The newly added path appears under the Paths list on the left. Similarly, add as many

paths as required.

c. Click **OK**.

- Click **No** if you do not want to use the same settings on another path.

6. Check the GuardPoint status, type:

```
secfsd -status guard
```

Guarding Data on CIFS Servers and Clients

The Common Internet File System (CIFS) is a well-known and widely-deployed distributed file sharing protocol for Windows. *NIX (Unix/Linux-like operating systems) offer support, to share a directory with Windows, via SAMBA.

Note

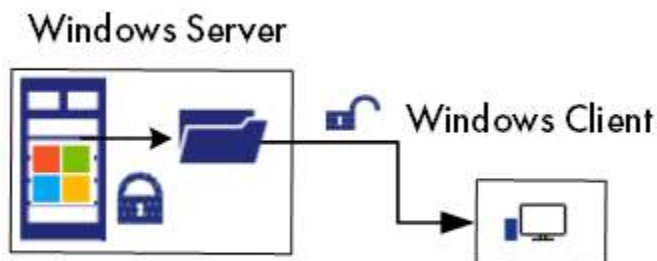
This topic is **not** about CTE Live Data Transformation.

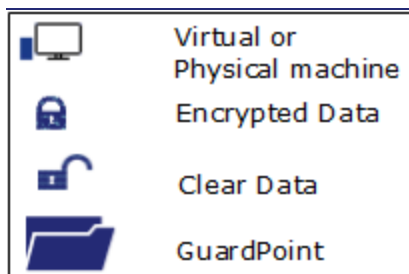
You can guard data on a CIFS share:

- On the Server side of the share (WIN and *NIX)
- On the client side (WIN client only)

Guarding on the Windows SERVER side of a share

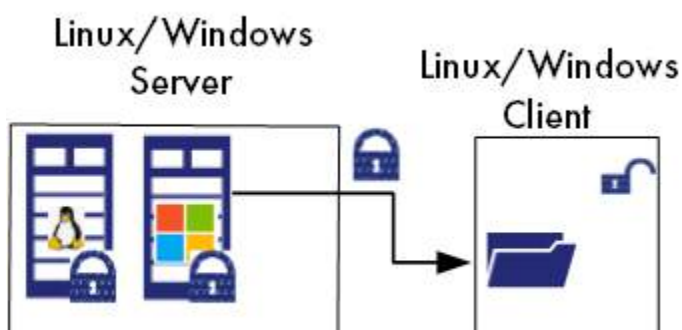
Guarding on the server side is supported for a local Windows volume drive (i.e. E: or local directory (i.e. E:\gp)). After which you can share the CIFS share out to another Windows server or client. **Do not** guard the share on the server side and then also on the client side. This will lead to double encryption and other problems.





Guarding on the Windows CLIENT side of a Share

You can guard server share on the client side, independent of the server side. The server side can be Windows or *NIX. For either the server or client side OS, the GuardPoint must be a File System that CipherTrust Transparent Encryption supports guarding, which is most typically a native FS.



PROS

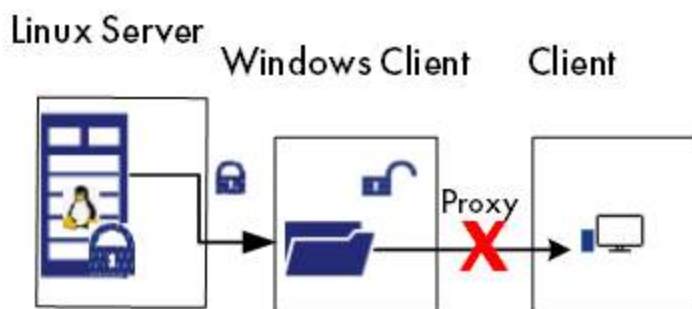
- Data sent over the channel is encrypted by the agent, above any channel protocol encryption.
- GuardPoint policy sees the processes on the host accessing files.

CONS

- More agents required, one per client, than guarding on the server side.

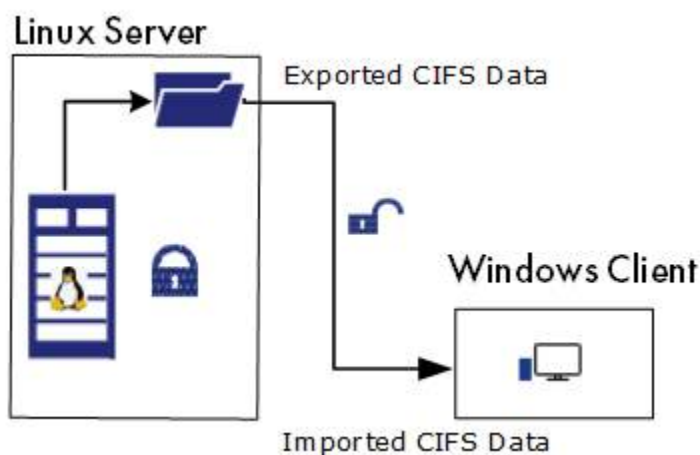
Proxy GuardPoint

Guarding on a client, and then exporting that client to another server, is not supported.



Guarding on the *NIX Server side of a Samba share

Guarding on a mounted CIFS/SAMBA share on *NIX is not supported. Use NFS to guard on the client side.



Whenever you are creating a GuardPoint on a CIFS share, you have two options.

1. Install CipherTrust Transparent Encryption agent on the CIFS server. Then create a GuardPoint on the network share. Have users connect remotely from their systems to the network share.
2. Install the CipherTrust Transparent Encryption agent on all remote user computers and again create a GuardPoint on the network share.

Note

- When creating a GuardPoint, do not use the share mount point `\<serverName>\share$`. You must create the GuardPoint on a sub-folder of the mount point `\<serverName>\share$\folder1`
- In the policy, you must create a **UserSet** for remote users accessing the network share. This UserSet must be linked to the ProcessSet for `ntoskrnl.exe` (Windows Only). Then grant the user Permit and Apply_key permissions.

- If a user that is logging in with `UserPrincipalName` (xyzuser@thales.com) is accessing the share folder, then the `UserSet` must contain the UPN. If the remote user logs on with a `sAMAccountName`(jharriman), then the `UserSet` must contain the `sAMAccountName`.

Special Cases for CTE Policies

This following section describes a CTE-specific configuration task related to configuring policies in the key manager.

Behavior of Hard Links Inside and Outside of GuardPoints (Windows)

When using hard links on Windows, all the hard links to a file must be within the boundary of a GuardPoint and must use the same key. The following scenarios provide additional details:

- If hard links to the same file are inside a GuardPoint and outside a GuardPoint, the effect on the file depends on what process accesses which hard link first. If the hard link within the GuardPoint is opened first, the file is transformed. If the hard link outside the GuardPoint is opened first, the file won't be transformed.
- If hard links to the same file exist in different GuardPoints with different keys, the file will be corrupted.
- If hard links to the same file exist in the same GuardPoint but with different keys, such as if folder-based rules are used, there will be a conflict in the key.

Security Rule Ordering for Policies

If you want to enforce restrictions when guarding NFS/CIFS shares using an LDT or standard policy with a **CBC-CS1** key, note the following:

CipherTrust Transparent Encryption embeds the LDT and/or IV (initialization vector) attributes in the first 4K of files for NFS/CIFS shares guarded with an LDT or standard policy with a **CBC-CS1** key. Embedding CipherTrust Transparent Encryption attributes increases the actual file size by 4K. CTE hides that extra 4K when reporting the file size to users, or processes, that access the file with the Apply Key effect.

If you need the actual file size, or read/write access on the embedded header, for backup/restore processes for example, then you need a rule that permits access without Apply Key.

LDT Policies

Example 1: Permits Backup and Restore

A policy that allows backup and restore of encrypted data, clear-text access to certain processes, and denies access to all others:

Order	Resource Set	User Set	Process Set	Action	Effect	Browsing	
1				key_op	permit:applykey	No	
2			backup	all_ops	permit:audit	Yes	
3			authorized-processes	all_ops	permit:audit:applykey	Yes	
4				all_ops	deny:audit	Yes	

Rule	Purpose
1	Default LDT rule required for LDT policies.
2	Allows for processes in the backup Process Set to access the real file size and backup the CipherTrust Transparent Encryption attributes along with the encrypted file data.
3	Allows for processes in the authorized-processes Process Set to access the clear-text data, but it hides the additional 4K from the CipherTrust Transparent Encryption attribute.
4	Denies all other processes access to the data.

Example 2: Permits access to certain Processes

A policy that only allows certain processes clear-text access but allows all others to see the OS file attributes.

Order	Resource Set	User Set	Process Set	Action	Effect	Browsing	
1				key_op	permit:applykey	No	
2			authorized-processes	all_ops	permit:audit:applykey	Yes	
3				f_md_audit_md_read_r...	permit:audit	Yes	
4				all_ops	deny:audit	Yes	

Rule	Purpose
1	Default LDT rule required for LDT policies.
2	Allows for processes in the authorized-processes Process Set to access the clear-text data.
3	Allows for processes not in the authorized-processes Process Set to read the OS file and directory attributes. Note: Processes that match this rule obtain the file size with the 4K header. If a process that is not in the authorized-processes Process Set needs the file size without the header, then the Apply Key must be present in the Effect or you will need an additional rule granting Apply Key to that specific process. That rule must be defined before this rule.
4	Denies processes not in the authorized-processes

Rule	Purpose
	Process Set from reading any data from the files.

Standard Policies

Example 1: Permits access to certain Processes

A policy that allows backup and restore of encrypted data, clear-text access to certain processes, and denies access to all others:

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1			backup	all_ops	permit,audit	Yes	...
2			authorized-processes	all_ops	permit,audit,applykey	Yes	...
3				all_ops	deny,audit	Yes	...

Rule	Purpose
1	Allows for processes in the backup Process Set to access the real file size and backup the CipherTrust Transparent Encryption attributes along with the encrypted file data.
2	Allows for processes in the authorized-processes Process Set to access the clear-text data, but it hides the additional 4K from the CipherTrust Transparent Encryption attribute.
3	Denies all other processes access to the data.

Example 2: Permits access to certain Processes

A policy that only allows certain processes clear-text access but allows all others to see the OS file attributes.

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
1			authorized-processes	all_ops	permit,audit,applykey	Yes	...
2				f_rd_attr_rd_sec,d_r...	permit,audit	Yes	...
3				all_ops	deny,audit	Yes	...

Rule	Purpose
1	Allows for processes in the authorized-processes Process Set to access the clear-text data.
2	Allows for processes not in the authorized-processes Process Set to read the OS file and directory attributes. Note: Processes that match this rule obtain the file

Rule	Purpose
	size with the 4K header. If a process that is not in the authorized-processes Process Set needs the file size without the header, then the Apply Key must be present in the Effect or you will need an additional rule granting Apply Key to that specific process. That rule must be defined before this rule.
3	Denies processes not in the authorized-processes Process Set from reading any data from the files.

For more information, see [Adding Security Rules](#) in the CipherTrust Manager documentation.

Enhanced Encryption Mode

This section describes the enhanced AES-CBC-CS1 encryption mode for keys. It contains the following topics:

- [Compatibility](#)
- [Disk Space](#)
- [Encryption Migration](#)
- [File Systems Compatibility](#)
- [FileTable Support on Windows](#)
- [Using the AES-CBC-CS1 Encryption Mode in CM](#)
- [Exceptions and Caveats](#)
- [Best Practices for AES-CBC-CS1 Keys and Host Groups](#)

The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

Note

AES-CBC-CS1 encryption does not require any additional license.

Security Improvements

	AES-CBC	AES-CBC-CS1
Unique IV per-file	No	Yes
IV predictability	Yes	No

File System Support

	AES-CBC	AES-CBC-CS1
Local FS	NTFS/ReFS	NTFS/ReFS
Remote FS	CIFS	No support
Block Device Support (secdm)	Fully supported	No. When a policy contains a key with CBC-CS1 encryption mode, the guarding fails on the CipherTrust Manager, and an error message displays.

Compatibility

- Starting with VTE for Windows version 6.1.0, CTE is backward compatible with, and fully supports, the existing AES-CBC mode for both new and existing datasets.
- Starting with VTE for Windows version 6.1.0, CTE fully supports AES-CBC-CS1 encryption for LDT and offline data transformation on CTE Windows environments.

Versions of VTE prior to version 6.1.0 are not backwards compatible with AES-CBC-CS1 encryption. On these earlier versions, attempting to guard a device using a policy containing an AES-CBC-CS1 key will fail.

- Protected hosts supporting AES-CBC-CS1 encryption can be added to host groups.

Difference between AES-CBC and AES-CBC-CS1

The two encryption modes are completely different from a file format standpoint.

- AES-CBC-CS1 encryption only applies to file system directories; AES-CBC encryption applies to both files and block devices.

Note

- If you attempt to use an AES-CBC-CS1 key to guard a block device or partition, the guarding fails with an error reported on the CipherTrust Manager, similar to: Raw or Block Device (Manual and Auto Guard) GuardPoints are incompatible with Policy "policy-xxx" that contains a key that uses the CBC-CS1 encryption mode."
- While AES-CBC-CS1 encryption is supported on both Linux and Windows environments, the file formats are incompatible. An encrypted file created with a specific AES-CBC-CS1 key on Windows cannot be read on Linux, even if that specific key were to be used and vice versa.

- AES-CBC-CS1 uses cipher-text stealing to encrypt the last partial block of a file whose size is not aligned with 16 bytes.
- Each file encrypted with an AES-CBC-CS1 key is associated with a unique and random base IV.

- AES-CBC-CS1 implements a secure algorithm to tweak the IV used for each segment (512 bytes) of a file.

Disk Space

Files encrypted with AES-CBC-CS1 keys consume additional disk space in contrast to files encrypted with AES-CBC keys. This is because AES-CBC-CS1 encryption requires file IVs to be created and persistently stored in contrast to AES-CBC encryption which does not consume any additional disk storage.

Therefore, administrators need to plan and provision additional disk capacity prior to deploying AES-CBC-CS1 encryption.

	AES-CBC	AES-CBC-CS1
Local Windows FS	No change to file size. No ADS allocation.	Extra 4KB allocation (at minimum) in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.

Encryption Migration

You can use either LDT or offline dataxform to:

- Transform data encrypted by AES-CBC to AES-CBC-CS1 and vice versa.
- Transform AES-CBC-CS1 encrypted data to clear contents and vice versa.

File Systems Compatibility

On Windows, you can use AES-CBC-CS1 keys to guard currently supported file systems.

Note

The remote file system must have enough extra space to store the extra 4K bytes of the embedded header.

Storing Metadata

AES-CBC-CS1 encrypted files on Windows store the base IV (initialization vector) of a file in a Windows ADS (Alternate Data Streams) associated with the file. The size required for saving the CS1 key depends on the allocation size of the file system. If the allocation size is set to 4k, then the new IV will require 4K of extra space on the disk. You can run the `fsutil fsinfo` tool to find out the allocation size of the file system.

The AES-CBC-CS1 key is supported on the following file systems:

- **NTFS:** Supported on all Windows platforms that are supported by CTE.
- **REFS:** Supported on Windows 2012 R2 and later.

- **CIFS:** Supported if the backend storage for the CIFS share is Windows-based storage.

Note

Some network storage servers do not support multiple ADS associated with a file.

Compatibility

	AES-CBC	AES-CBC-CS1
Local FS (Windows)	No change	Alternate Data Streams
NTFS file system	Supported	Supported
Azure File Share	Supported	Not supported with a standard policy on a system with a VMFILTR driver.

Note

AES-CBC-CS1 encrypted files on CTE Windows are not compatible with AES-CBC-CS1 encrypted files on CTE Linux. Do not create a policy on Linux that uses AES-CBC-CS1 keys if access to the same NFS GuardPoint is required by both Windows and Linux LAN clients.

Base IV file

To get the value of the base IV, type:

```
voradmin secfs iv get <file-name>
```

Note

The base IV of a file is protected. It cannot be set/modified/removed by commands and applications. However, if a GuardPoint is unguarded, the files in the GuardPoint are no longer protected. An adversary can then corrupt the content of the files, as well as the IVs.

AES-CBC-CS1 depends on the physical file system's support for extended attributes in a manner similar to the CipherTrust Transparent Encryption Live Data Transformation feature.

Missing IV file

If the IV for a file is missing, or CTE is unable to read the IV, then CTE denies access to the file. This access

denied message may trigger an application to display an error message. This message may vary from application to application.

FileTable Support on Windows

The CBC-CS1 key does not support FileTables. This is because FileTables do not support alternate data streams. The CS1 key requires the ability to write the per-file IV into an alternate data stream on each file.

Using the AES-CBC-CS1 Encryption Mode in CM

When you create a key in CTE, you enable Encryption Mode by selecting CTE Key Properties. See *Creating a New Key* in the [Managing Policies](#) chapter in the [CTE Administrator Guide](#).

Exceptions and Caveats

Note the following when using AES-CBC-CS1 keys.

Guarding Existing Files Without Data Transformation

You must convert an existing file with clear text through offline data transformation or LDT. If you do not transform the file, then after you guard using an AES-CBC key, the file displays garbled characters.

If you use an AES-CBC-CS1 key, access to the file is blocked with an I/O error.

Best Practices for AES-CBC-CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC-CS1 keys unless all hosts are running VTE for Windows version 6.1.0 or CTE version 7.0.0 or later.

Utilities for CTE Management

Thales provides a variety of utilities that augment the standard Windows utilities. This combination of tools helps administrators manage CTE. The following utilities are described in this section:

- [Agent Health Return Codes](#)
- [agentinfo \(Java version\)](#)
- [Backup](#)
- [voradmin secfs Commands](#)
- [vmsec](#)
- [vmutil](#)

Agent Health Return Codes

The `agenthealth.ps` utility validates:

- Super-user privilege
- CTE Agent installation
- CTE registration to key manager
- CTE processes/modules that are running
- Available disk resources:
- Current GuardPoints: Tests if the agent can reach the GuardPoints
- CTE log directory resource status

This directory contains pending CTE log files for upload. This utility reports the size and number of pending files for upload. These text files are logs that contain vmd/SecFS information. They are regenerated whenever secfs restarts. If the number of files is unexpectedly large, this can indicate a problem.

Agent Health Check Script

The Agent health check script (`agenthealth.ps1`) is located in `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\`

To run the `Agenthealth` check script:

1. Run the power shell command to enable self-signing for the system.

Before running agent-health script make sure power shell command has enough privileges to execute the Powershell script. Some Windows operating systems have default execution policy set as `restricted`.

Use the Powershell command `Set- Execution-policy Remote Signed` to change the execution policy if needed.

2. Open the `Power shell` prompt as administrator.
3. Type:

```
.\agenthealth.ps1
```

System Response

```
Log file is at log\agent_health.log
Checking super user privilege..... OK
Vormetric Agent installation..... OK
```

```

Vormetric policy directory..... OK
Registration to server..... OK
Kernel drivers are loaded..... OK
VMD is running..... OK
SECFSD is running..... OK
rhat26130.qa1.com is resolvable.....K.....OK
rhat26130.qa1.com port 8446 is reachable..... OK
rhat26130.qa1.com port 8447 is reachable..... OK
Can communicate to at least one server..... OK
VMD is listening on port 7024..... OK
Time of last update from server      2016-12-01      14:39:49.038
Checking available disk space..... OK
Checking logging space ..... OK
    Log directory is ""
    File system for log data is "/", 32G free (17% full)
    Log directory contains 2 of maximum 200 files (1% full)
    Log directory contains 1 of maximum 100 Mbytes used (1% fu
ll)
Testing access to C:\GP2..... OK

```

agentinfo Utility

The **agentinfo** utility collects system logs, CTE agent logs, CTE agent trace information, and system information for diagnostic purposes. All this information is saved in the destination path and compressed into a zip file. The **agentinfo** utility is available as an **agentinfo.js** Java command and as an **agentinfo.ps1** PowerShell command.

agentinfo Utility (Java version)

The **agentinfo.js** utility is a JavaScript file. You can open it in a text editor to see specific functions.

The **agentinfo.js** support collection scripts reside in the following path on systems where the CTE agent is installed.

To run the **agentinfo** script on Windows, navigate to one of the following folders:

```

C:\Program
Files\Vormetric\DataSecurityExpert\agent\vmd\bin
or
C:\Program
Files\Vormetric\DataSecurityExpert\agent\shared\bin

```

Then run the following script:

```
agentinfo.js
```

agentinfo Utility (PowerShell version)

The PowerShell version of `agentinfo` supports several parameters.

PowerShell version agentinfo parameters

- **Directory** - Specify the directory where all the collection information is saved. By default, this information is saved in the current directory.
- **ZipFile** - Specify the name of the compressed file, where all the collected information will be archived. By default, this information is saved in the current directory.
- **LogFile** - Specify the name of the files where verbose logs will be saved. By default, this information is saved in the current directory.

Examples for using agentinfo utility (PowerShell version)

To save all the collection information in `"c:\AgentLogs"` folder, run the following command:

```
.\agentinfo.ps1 -Directory 'C:\AgentLogs'
```

To save all the collected information in `"c:\AgentLogs"` folder and verbose logs in `"c:\temp\AgentInfo.log"`, run the following command:

```
.\agentinfo.ps1 -Directory 'C:\AgentLogs' -LogFile 'c:\temp\AgentInfo.log'
```

To save all the collected information in `"c:\AgentLogs"` folder, verbose logs in `"c:\temp\AgentInfo.log"`, and create the `"AgentInfo.zip"` archive file, run the following command:

```
.\agentinfo.ps1 -Directory 'c:\AgentLogs' -LogFile 'c:\temp\AgentInfo.log' -ZipFile 'C:\temp\AgentInfo.zip'
```

Note

PowerShell 5.1 or later is required. Use the `$PSVersionTable.PSVersion` command to confirm which PowerShell version you are using.

Backup Utility

When a backup is performed, certain files and directories may be protected against access. Therefore, those files and directories are not written to the backup repository. These include files located in Data Transformation GuardPoints or files in GuardPoints with appropriate policies. Additionally, the following files are locked by default by CTE agent:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/.access
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/etc/*
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem/*
```

The following describes how to bypass the issue for multiple scenarios:

Agent is installed in the default location

1. Stop SecFS, type:

```
/etc/vormetric/secfs stop           //Linux

/etc/rc.d/rc2.d/S99secfs stop      //AIX
```

2. Run the backup application with the desired arguments.
3. Restart SecFS, type:

```
/etc/vormetric/ start
```

Using a backup image to install to other agents or restore to a different system

Note

When the image is used to reinstall the system, the agent will automatically start at system boot and will attempt to connect to the key manager to which it was originally registered.

To prevent multiple systems with the same agent ID, you must uninstall CTE from the system before running the backup application. The restore/install from the backup will not have an agent running.

1. Uninstall the agent, type

```
/opt/vormetric/DataSecurityExpert/agent/secfs/bin/uninstallsfs
```

2. Run the backup application with the desired arguments.
3. Re-install CTE agent.

Performing a backup while the agent is running

Before running the backup application, add the files that are protected by the agent to the exclusion rules to

exclude them from the backup:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/.access
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/etc/*
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem/*
```

The GuardPoint policy may implement access restrictions which would also cause the backup application to generate error messages. These GuardPoint/directories will also need to be added to the exclusion rule method to exclude them from the backup. Alternatively, you can temporarily unguard them while the backup application is running.

If the CTE agent reports a status of incomplete in the backup application and does not start properly, or partially starts but generates error messages at system boot time, then uninstall and reinstall the agent. The restore/clone image contains everything needed to uninstall the agent. Use the following command to perform this operation:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/bin/uninstallsf
```

Backing up Databases after Encryption

After encrypting a database, CipherTrust Transparent Encryption cannot make a backup of the database. Both scheduled and manual backup fail. The problem was the user's policy. A policy used in this scenario must follow a few rules.

With a CBC_CS1 key, a guarded file is modified to have a 4096 byte header holding key information. When an **Apply Key** effect is specified, the CipherTrust Transparent Encryption code adjusts the length and file offset for this header. Without an **Apply Key** effect, the size and access of the offset include the CBC_CS1 header.

Thales recommends that you modify the first rule of your policy. Remove the action entry for `f_rd_att` from the first rule and add a new rule before it:

```
**action**: f_rd_att

**effect**: Permit, Apply Key
```

Policy processing starts with the first rule and continues until a matching rule is found. The effect for the matching rule is then applied.

For the `f_rd_att` action, this results in the secfs code including the CBC_CS1 key header and adjusts the file size value. Without the Apply Key effect, the file size includes the CBC_CS1 header size and the file appears as 4096 bytes larger than its real size.

voradmin secfs Commands

The `voradmin secfs list` and `voradmin secfs status` commands display GuardPoint and policy information on the host.

voradmin secfs List Commands

The `voradmin secfs list` command has the following options:

voradmin secfs list Options

Guardpoints	Displays all the GuardPoints on the host.
Policy	Displays all the policies used on the host.
logger	Displays the logging details on the host.
Status	Displays the authentication settings on the host.

For example, to view all the GuardPoints on the host, type:

```
voradmin secfs list guardpoints
Guard Point:      1
Policy ID:        16553
Policy name:      ES-Standard-Policy
Directory:        esg-disk1-demo
Type:             rawdevice
Status:           guarded

Guard Point:      2
Policy ID:        18857
Policy name:      Accounting-IT-Access-Policy
Directory:        G:\Data
Type:             local
Status:           guarded

Guard Point:      3
Policy ID:        18985
Policy name:      LDT-Policy
Directory:        C:\LDT-Folder
Type:             local
Status:           guarded
```

To view just the policies in use on the host, you would enter:

```
voradmin secfs list policy
Policy:           1
Policy name:      LDT-Policy
Type:             LDT

Policy:           2
Policy name:      ES-Standard-Policy
Type:             ONLINE

Policy:           3
Policy name:      Accounting-IT-Access-Policy
Type:             ONLINE
```

voradmin secfs status Commands

The `voradmin secfs status` command has the following options:

voradmin secfs status Options

keys	Displays the current status of the keys on the host.
lock	Displays the status of any system or agent locks on the host.
crypto	Displays the encryption modes that are supported.

For example:

```
voradmin secfs status keys
```

Encryption keys are available

```
voradmin secfs status lock
```

FS Agent Lock: Disabled System Lock: Disabled

```
voradmin secfs status crypto
```

AES CBC, CBC_CS1, XTS modes are supported

Encryption key protection is supported

vmsec Utility

The `vmsec` utility allows you to manage the security aspect of the CTE Agent on the host. On Windows the `vmsec` utility is `<windows-agent-install-dir>\vmd\bin\vmsec.exe`. The default path is:

```
C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmsec.exe
```

vmsec Syntax

check_install	Verifies that the kernel component is running. This command checks CTE services and reports if any of the services are not running.
challenge	Initiates challenge-response on the host. This command displays a CTE Agent password challenge string and enter the response string when the key manager is not network accessible.
status	Displays kernel configuration.
vmdconfig	Displays the vmd configuration.
check_hwenc	Determines whether this system supports hardware crypto.
hwok	Reports status of hardware signature.

<code>passwd [-p passwd]</code>	Enters the host password when the key manager is not network accessible. User can unlock the GuardPoints with this password.
<code>version</code>	Displays the CTE version.

Displaying the CTE Challenge String

In addition to using `vmsec challenge` on Windows, you can also right-click the tray icon and select **Challenge...-> Response**. The *CTE Challenge/Response* window opens.

If no challenge string is displayed, the host password is static. If a challenge string displays, contact a Administrator for the response string.

Using the CTE Challenge String

When communication with the CipherTrust Manager is unavailable, the agent pauses on access to guarded directories. The agent waits for communication to be restored or a challenge/response to be issued and completed. The agent notifies the user of this condition and requests the challenge/response with log messages in `dmesg` and `vmd.log` in five minute intervals.

vmutil

Usage

```
vmutil <options> <operations>
```

Options

Option	Function	Description
<code>-a</code>	<code>--agent <name></code>	Specify agent type (vmd or pkcs11)
<code>-d</code>	<code>--extdir <string></code>	Specify location of external certificate and key set
<code>-e</code>	<code>--error <string></code>	Specify one or more errors for state report
<code>-h</code>	<code>--help</code>	Display help and exit
<code>-l</code>	<code>--loglevel <level></code>	Specify log output level (debug, info, warn, error or fatal)
<code>-f</code>	<code>--force enabled</code>	Force option for delete host operation
<code>-v</code>	<code>--version</code>	Display program version and exit

Operations

Operation	Description
certexpiry	Report the certificate expiration date for this agent
deletehost	Delete this client from the server
renewcerts	Renew certificate set for this agent
reportstate	Report agent state and error conditions to server
unregister	Unregister this agent/client from the server
updatecerts	Update external certificate and key set for this agent/client

Upgrading CTE on Windows

This chapter describes how to upgrade an existing VTE for Windows host to CipherTrust Transparent Encryption (CTE) for Windows and contains the following sections:

- To Upgrade in Windows Silently
- CTE Scheduled Upgrade
- Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades
- Upgrading CTE Agents in an LDT Communication Group from 7.4.0 to 7.5.0 and post 7.5.0

Silent Upgrade

If you have already installed CTE on a Windows computer and want to upgrade it silently, use the appropriate command below for the type of installation binary that you are using.

Note

The protected host must be able to connect to the CipherTrust Manager that it is registered to or the upgrade will fail.

Upgrade using self-extracting .exe

```
vee-fs-7.8.0.75-win64.exe /s /v" /qn"
```

Upgrade using MSI

```
msiexec.exe /i vee-fs-7.8.0.75-win64.msi /qn REINSTALLMODE=voums REINSTALL=ALL
```

Before upgrading using MSI, you must rename the installation file to the name of the previously used MSI installation file. See [Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades](#) for more information.

Note

For all types of upgrades, including interactive (GUI-based) and scheduled upgrades, the protected host must be able to connect to the CipherTrust Manager that it is registered to or the upgrade will fail.

Verify the Windows Installation

After running a silent install, verify the installation by checking CTE processes.

1. In the system tray, right-click the CipherTrust Lock icon.
2. Select **Status**. Review the information in the Status window to confirm the correct CTE are installed and registered.

Resolving Problems that Prevent Silent Install

If you encounter problems using MSI or self-extracting `.exe` silent install commands, first check the syntax of the command. To further investigate installation issues, you can use Microsoft diagnostics software:

- For desktop versions of Windows: [Microsoft Diagnostics Troubleshooting Wizard](#)
- For server versions of Windows: [Microsoft Automatic Troubleshooting Services \(MATS\)](#)

Refer to the Microsoft documentation on the linked pages for more information. See the *Compatibility Matrix for CTE Agent with Data Security Manager* for a list of versions of Windows that are supported for use with CTE.

CTE Scheduled Upgrade

Scheduled upgrade allows you schedule an upgrade of the CTE agent to occur after the next time the server hosting the agent reboots normally. Scheduled upgrade can minimize CTE service interruptions. Also, scheduled upgrade can reduce coordination issues in organizations where the security roles are separated.

Prerequisites

The following prerequisites are mandatory for a successful upgrade of a CTE agent node:

1. Install all Microsoft update patches before scheduling a CTE Agent upgrade.
2. Make sure that your Windows version is Windows Server 2008 R2 and subsequent versions. The CTE scheduled upgrade feature is not compatible with previous versions.
3. For all types of upgrades, including interactive (GUI-based) and scheduled upgrades, the CTE client must be able to connect to the CipherTrust Manager to which it is registered.

4. When upgrading from a CipherTrust Transparent Encryption version that is prior to v7.1, you must **first** upgrade to v7.1 before scheduling an upgrade to subsequent versions from v7.1.

If you are upgrading CTE agents in an LDT Communication Group, the following prerequisites are also mandatory for a successful upgrade:

1. Disable the GuardPoints on the nodes to be upgraded:
 - a. Go to the CipherTrust Manager UI.
 - b. In the GuardPoint window, click the ellipsis on the right side of a GuardPoint and select **disable** to disable the GuardPoint.
 - c. Repeat the steps for all of the GuardPoints on the nodes to be upgraded.
2. Stop CTE Services on the nodes to be upgraded:
 - a. Go to **Control Panel > Services (local)**.
 - b. Select **secfsd**.
 - c. Select **Stop the Service**.

Scheduling a CTE Upgrade on the Command Line

To schedule CTE to upgrade the next time the system reboots, type:

```
voradmin upgrade schedule <CTE setup executable path> UPGRADE_NO_CIFSGP=Yes
```

Note

You must set the **UPGRADE_NO_CIFSGP** variable to **yes** after ensuring that all CIFS GuardPoints are disabled. This is mandatory. The upgrade fails if any CIFS GuardPoints are enabled. The **UPGRADE_NO_CIFSGP** variable checks that LDT CIFS GuardPoints are disabled, or not present, in v7.5.0 and subsequent versions. For v7.4.0 and previous versions, it cannot verify the GuardPoint status.

Self-extracting .exe Example

```
voradmin upgrade schedule C:\<Release.build-number>\vee-fs-7.8.0.75-win64.exe UPGRADE_NO_CIFSGP=Yes
```

Minor MSI Upgrades Only (Patches)

1. Before running `voradmin upgrade schedule`, check and remove any existing MSI packages from `C:\ProgramData\Vormetric`.

2. Type:

```
voradmin upgrade schedule C:\<Release.build-number>\vee-fs-7.8.0.75-win64.msi  
MINOR_UPGRADE=Yes REINSTALL=ALL REINSTALLMODE=vomus UPGRADE_NO_CIFSGP=Yes
```

System Response

```
Creating and installing service to upgrade. CTE agent will be upgraded on next  
reboot.
```

Alternative MSI Method

1. Rename the package named: `vee-fs-7.8.0.75-win64.msi` to the previous install package name, ex: `vee-fs-7.8.0.75-win64.msi`
2. Type:

```
voradmin upgrade schedule C:\vee-fs-7.8.0.75-win64.msi REINSTALL=ALL REINSTALL  
MODE=vomus UPGRADE_NO_CIFSGP=Yes
```

Major MSI Installations

For a major MSI upgrade, the command is the same as that for the `.exe` file.

- Type:

```
voradmin upgrade schedule <CTE MSI installer path> UPGRADE_NO_CIFSGP=Yes
```

Example

```
voradmin upgrade schedule C:\vee-fs-7.8.0.75-win64.msi UPGRADE_NO_CIFSGP=Yes
```

Warning

If you have scheduled an upgrade on reboot and the system crashes or is not shutdown gracefully, you must restart the system again to upgrade the agent.

Scheduling a CTE Upgrade Interactively (self-extracting .exe only)

When you open the self-extracting .exe CTE installation binary and a version of CTE is already installed, you have the option of upgrading immediately or initiating a scheduled upgrade. See the procedure below for details. This is an alternative to scheduling an update on the command line using `voradmin` (see [Scheduling a CTE](#)

Upgrade on the Command Line).

1. Move the self extracting `.exe` CTE installation binary to the computer on which you want to initiate the scheduled upgrade.
2. Double-click the self extracting `.exe` CTE installation binary to run it.
3. Click through the standard initial dialog boxes like the license dialog box.
4. On the **UPGRADE - Install now or Later** dialog box, click **Schedule Upgrade on next reboot** and then click **Next**.
5. Click **Schedule** on the confirmation dialog box.

The next time the computer reboots, the upgrade will occur.

This interactive method of scheduling an update is not available for MSI CTE installation binaries. You must use the `voradmin` command line scheduled upgrade method.

Show Scheduled CTE Upgrades

To display all scheduled CTE agent upgrades, type:

```
voradmin upgrade show
```

System Response

```
Current version:      6.0.3.12
Target upgrade version: 6.0.3.15
Upgrade on reboot:    Enabled
```

Cancel a Scheduled CTE Upgrade

To cancel/cleanup a scheduled CTE agent upgrade, type:

```
voradmin upgrade cancel
```

System Response

```
CTE agent upgrade canceled successfully.
```

Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades

When performing an upgrade, Windows Installer Package (MSI) expects the name of the installation binary to be the same as the binary that you used to install CTE. Because Thales includes the software version and build number in the binary file name, you must rename the installation binary to the name of the previously used MSI installation binary before upgrading using MSI. This applies to any MSI CTE upgrade method: typical (interactive), silent upgrade, and scheduled upgrade. If the name does not match the previous binary file name, the upgrade

will fail with error code 1316.

For example, let's say that you installed the CTE Agent using the following installation file:

```
vee-fs-7.8.0.75.47-win64.msi
```

If you used this binary to install or upgrade CTE, the next time you want to upgrade CTE the installation binary that you download from Thales might have the following file name:

```
vee-fs-7.8.0.75.66-win64.msi
```

To upgrade successfully using MSI, you would need to rename the new installation binary to the previous file name of `vee-fs-7.8.0.75.47-win64.msi` before upgrading.

Finding The Name Used For A Previous MSI Installation or Upgrade

If you want to upgrade CTE using an MSI installation binary but don't know the file name that you used during the previous installation or upgrade, you can look it up by using one of the following methods on the computer where you installed CTE:

MSI File Name Lookup Method 1: PowerShell

Run the following command in PowerShell:

```
(Get-WmiObject Win32_Product | where { $_.Name -match "CipherTrust Transparent Encryption" }).PackageName
```

Rename the new CTE setup installation binary to the file name output from the PowerShell command and proceed with the upgrade.

MSI File Name Lookup Method 2: Windows Registry

Find the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Product\  
905CB36BF7940894995701C86901D14F
```

Rename the new CTE installation binary to the file name in the registry and proceed with the upgrade.

Uninstalling CTE from Windows

Considerations

- The CTE Agent must be removed from the Windows host before the host is removed from the key manager with which it is registered.

- Database applications like DB2 and Oracle can lock the user space while they run. If the uninstall fails because a GuardPoint is in use, determine which applications are using the files in the GuardPoint and stop them. Then uninstall again.

Procedure

1. Stop any application from accessing files in the GuardPoint.
2. In the key manager with which this host is registered, do the following:
 - Decrypt any data you want to use after uninstall. After the CTE Agent software is removed, access to data is no longer controlled. If data was encrypted, it will remain encrypted. If decrypted or copied out of the GuardPoint, the data is visible as clear text.

This decryption must be done on every GuardPoint on the host if you want to access all existing data on the host.

- Make sure the Agent and System locks have been disabled for the host.
- Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.

Do not remove the host from the key manager yet.

3. Log on to the host as with system administrator privileges.
4. Use one of the following methods to uninstall the CTE Agent:
 - Use the standard Windows Add/Remove program utility from the Control Panel to remove the CTE software.
 - If you installed the CTE Agent using the MSI file, you can uninstall it using the command line with:

```
msiexec.exe /x <Installation_executable> /qn` command.
```

For example:

```
:::yaml
msiexec.exe /x vee-fs-7.8.0.75-win64.msi /qn
```

5. Reboot the system when prompted.
6. Remove the host record from the key manager.

Troubleshooting and Best Practices

Windows Systems

CTE will not register with the CipherTrust Manager

- If there is a firewall between the CipherTrust Manager and CTE, configure **vmd.exe** as a firewall exception on CipherTrust Manager for Windows. Otherwise, the CipherTrust Manager is unable to browse CTE.
- If using a Windows XP or Windows 2003 system Firewall, select ****Control Panel > Windows Firewall > Exceptions > Add Program... **** and browse for **vmd.exe**. The default location is

```
C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmd.exe
```

- If using a Windows 7 system Firewall, select **Control Panel > System and Security > Windows Firewall > Allowed Programs...** click **Change settings**, click **Allow another program** and browse for **vmd.exe**. The default location is

```
C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmd.exe
```

CTE with NFSv4: Permission denied error

You may see a permission denied error if you try to access files on an NFSv4 file system that is guarded by CTE.

CTE imposes a restriction on NFSv4 file systems to prevent write-only permissions from being set on individual files. You can work around this restriction by configuring read and write permissions on the same files.

You can also add a policy that allows write permissions.

This restriction applies only in the case of files resident in guarded NFSv4 file systems.

McAfee VirusScan Enterprise + Antispyware Enterprise

You must install McAfee AV software **before** installing CTE agent. If CTE is installed first, McAfee cannot initialize and all attempts to scan fail.



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

CTE Agent Windows Integration Guides	4
Using CTE with Microsoft SQL AlwaysOn and SQL File Tables	4
Boot Order for MSSQL with CTE for Windows	4
Using CTE with Microsoft SQL	5
Using CTE with SQL	6
Using CTE with SQL FileTables	6
Supported FileTables Use Cases	7
Unsupported FileTables Use Cases	8
Installing CTE on Microsoft SQL AlwaysOn	9
Data Transformation (Encryption in place)	13
Copy/Restore	13
SQL Server Policy Tuning	13
Using LDT with Microsoft SQL	14
Using LDT with SQL AlwaysOn	14
Using LDT with SQL FILESTREAM	14
Guarding SQL Server FileTable databases with LDT	22
Integrating Imperva File Activity Monitoring (FAM) with CTE Windows	26
CTE with Microsoft DFSR	30
Overview	31
Terminology and Topology	33
Configure DFS(R)	36
CTE Configuration Workflow	43
Creating Required DFS(R) Policy Components	44
Using the Standard Encryption Method	46
Creating Standard Policies for DFS(R)	47
Creating Standard GuardPoints with the DFS(R) Hub and Spoke Topology	51
Creating Standard GuardPoints with the DFS(R) Full Mesh Topology	56
Using the LDT Encryption Method	57
Creating an LDT Policy for DFS(R)	58
Creating a LDT GuardPoint for DFS(R)	60
CTE QoS Throttling and Rekey Scheduling	61
Troubleshooting	62
CTE Client Groups	65
Encrypt Active Directory Database with Secure Start	66
Secure Start Overview	66
Prerequisites	67
Encrypt by Moving the AD Service into a Guarded Directory	68
Encrypt Data in Place with Offline Transformation	70
Encrypt with an LDT Transformation Policy	70
Configure the Time Out Failure	71
Recover a Server After it Loses Connection to the Key Manager	72
Other Use Cases	72

Best Practices for Encrypting and Protecting the AD Service	73
Exchange DAG	76
Exchange DAG Overview	76
CTE Policies for Exchange DAG	77
Creating a Policy for LDT Encryption with CipherTrust Manager	78
Creating Policies for Standard Encryption with CipherTrust Manager	79
Encrypting with LDT in an Exchange DAG Environment	82
Encrypting with a Standard CTE Policy in the Exchange DAG Environment	84
Decrypting with LDT in an Exchange DAG Environment	87
Storage Spaces Direct	88
Using CTE with Quantum StorNext	90
Overview of using CTE with Quantum StorNext	90
CTE and Quantum StorNext Compatibility	91
Setting up CTE and Quantum StorNext Integration	92
Setting up Microsoft DPM with CTE	94

CTE Agent Windows Integration Guides

You can integrate CTE with the following applications:

- [Integrating Imperva File Activity Monitoring \(FAM\) with CTE Windows](#)
- [Using CTE with Microsoft SQL](#)
- [CTE with Microsoft DFS\(R\)](#)
- [Secure Start](#)
- [Exchange DAG](#)
- [Storage Spaces Direct](#)
- [Using CTE with Quantum StorNext](#)
- [Setting up Microsoft DPM with CTE](#)

Solutions Guides

Solutions guides have been moved to the [Use Cases](#) section.

Using CTE with Microsoft SQL AlwaysOn and SQL File Tables

This section discusses using CTE with Microsoft SQL with standard and LDT policies. It contains the following topics:

- [Boot Order for MSSQL with CTE for Windows](#)
- [Using CTE \(Standard Policy\) with Microsoft SQL](#)
- [Using CTE \(LDT Policy\) with Microsoft SQL](#)

Boot Order for MSSQL with CTE for Windows

Prerequisite

Setting the Proper Boot Order for SQL Server

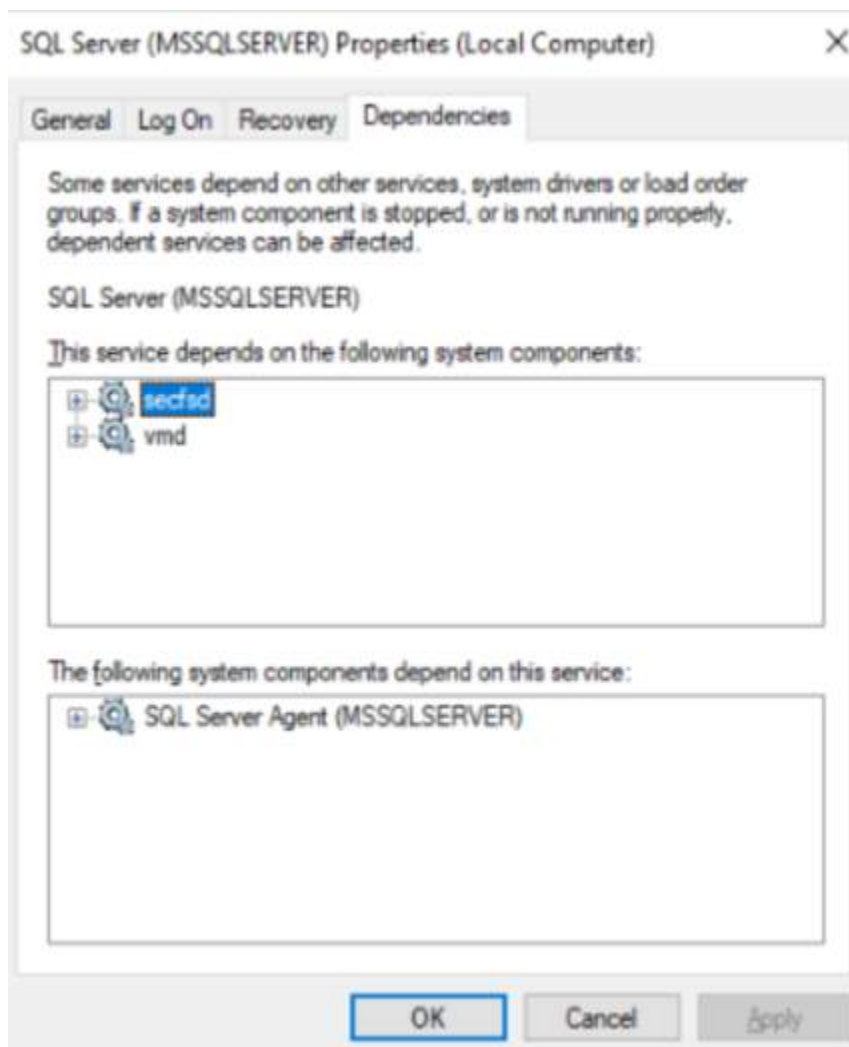
CipherTrust Transparent Encryption **must** always boot up **prior** to Microsoft SQL starting. If MSSQL starts prior to CTE starting, it does not function properly. You can set this as a dependency in the Windows services. To set this dependency:

1. Open the command prompt and run it as an Administrator.
2. Modify the value of the service entry, type:

```
sc config MSSQLSERVER depend=secfsd/vmd
```

To validate the dependency:

1. Open the Services.
2. Navigate to MSSQLSERVER service.
3. Click **Properties** > **Dependencies**. Under dependencies, it lists the two CTE services on which MSSQLSERVER is dependent.



Using CTE with Microsoft SQL

- Using CTE with SQL

- Using CTE with SQL FileTables
- Installing CTE on Microsoft SQL AlwaysOn
- Data Transformation (Encryption in place)
- Copy/Restore
- SQL Server Policy Tuning

Using CTE with SQL

You must stop the SQL service before guarding the SQL DB. When this occurs, the SQL Server replication may become unsynchronized. When restarting, it may take a brief period of time for the SQL Server replication to resynchronize with the other node. The SQL Server issues a warning against any attempted failovers during that brief period.

Note

Minimizing the duration for which the SQL Server service is stopped is beneficial for reducing the resynchronization period.

Using CTE with SQL FileTables

SQL FileTables allows you to store files and documents in special tables in the SQL Server called FileTables, but access them from Windows applications as if they were stored in the file system, without making any changes to your client applications. For some of the use cases, you can use FileTables with CTE.

Considerations

- The CTE Agent must be installed on the same server where the FileTables reside. If the FileTables reside on your SQL server, then you should install the CTE Agent on your SQL server.
- If multiple servers access the SQL FileTables:
 - Install CTE agent on all of the servers.
 - Protect all of the FileTable folders with the same CTE policy.

Caution

Accessing the FileTable without CTE may corrupt the data.

- When you create a new FileTable, alter, or drop FileTables, this may require applying a new GuardPoint.

-
- Every FileTable has a separate FileTable Folder so you must apply separate GuardPoints for each FileTable.
 - You must apply a unique GuardPoint to each VNN path.

For example, if you configure two FileTables on an SQL Server, then the remote SQL administrator system must apply one GuardPoint to each configured VNN name.

- Guarding on a VNN name is similar to guarding a network path with CTE.
- If you want to access the FileTables from multiple remote systems, you must install CTE agent on those systems and apply the GuardPoints.
- In the scenario where all remote systems guard the file tables of a Virtual Network Name (VNN) path with CTE LDT over CIFS, and no such GuardPoints exist on the file tables server, then **do not** make any SQL Server backups of the file tables database during Live Data Transformation. If an SQL Server backup is made during LDT rekey, then it is possible that a file in the File Tables directory could be backed up in an incorrect state.

Advantages

- System administrator cannot see the data locally on the SQL server because no CTE Agent is installed on the SQL server.
- The data transferring between servers is also encrypted.

Supported FileTables Use Cases

CTE supports the following FileTables use cases:

CTE Data Transformation of existing files in FileTables

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the FileTable folder for the existing FileTable.
3. Create an offline Data Transformation policy and apply to the GuardPoint on the FileTable folder.
4. Run the Dataxform utility to transform the data.

Protect files in SQL FileTables with CTE

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the FileTable folder for the existing FileTable.

3. Create a production policy and apply the GuardPoint on the FileTable folder.
4. Once the GuardPoint is active, you can use the file table to load and access files.

Protect files with SQL AlwaysOn Availability Groups with CTE

When the database that contains the FILESTREAM, or FileTable data, belongs to an AlwaysOn availability group, the FILESTREAM and FileTable functions accept or return virtual network names (VNNs) instead of computer names.

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the virtual network names (VNNs) for the existing FileTable.
3. Create a production policy and apply the GuardPoint to the VNN name
4. Once the GuardPoint is active, you can use the FileTable to load and access files.
5. When you enable FILESTREAM on an instance of SQL Server, it creates an instance-level share to provide access to the FILESTREAM data. Access this share by using the computer name in the following format:

```
\\<computer_name>\<filestream_share_name>
```

6. In an AlwaysOn availability group, the computer name is virtualized by using a Virtual Network Name, (VNN). When the computer is the primary replica in an availability group, and databases in the availability group contain FILESTREAM data, then SQL creates a VNN-scoped share to provide access to the FILESTREAM data. Applications that use the file system APIs have to use the VNN-scoped share, which has a path in the following format:

```
\\<VNN>\<filestream_share_name>
```

Install CTE on remote systems and guard the SQL Server VNN names

In this use case, CTE is installed on the SQL administrator system (a separate system from where the SQL Server resides) and a GuardPoint is applied to the VNN name.

Unsupported FileTables Use Cases

CTE does not support the following use cases:

1. Install CTE agent on the SQL Server and locally apply the GuardPoint on the SQL Server storage.
2. Access FileTables with Transact-SQL.

3. Access FileTables with File I/O APIs on the SQL server. Perform all file I/O on the remote system running the CTE agent.

Installing CTE on Microsoft SQL AlwaysOn

This section describes how to implement CTE with Microsoft SQL AlwaysOn in a variety of configurations for primary and secondary replica servers, and assumes that you have a basic understanding of Microsoft SQL database.

You may want to keep the primary server decrypted to serve all users, and use the secondary database for running reports or backups.

- If the database is encrypted, then the Volume Shadow copy-related backups will snapshot and backup encrypted protected data.
- Administrators with the `apply_key` permission can run a query and pull down reports from the secondary database server without affecting the performance of the primary database server.
- The secondary server could be in a remote Data Recovery location. You may want to secure it with encryption.
- LDT is supported with SQL AlwaysOn. See [Using LDT with SQL AlwaysOn](#) for more information.

Methods for Initial Encryption

There are multiple methods for performing the initial encryption of the databases. Decide on which of the following methods best fits your environment. For more information on transforming data, see the *CTE-Live Data Transformation with Data Security Manager*.

- Data Transformation – Encrypt data in place
- Backup and Restore to a GuardPoint
- Copy and paste the data into a GuardPoint

Configuration 1

- Databases on primary server and secondary replica servers require encryption
- Database name and location of secondary replica server are the same as the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Change the primary database to offline mode.
3. Confirm the creation of a data transformation and/or standard policy.
4. Guard the folder containing the primary database files with that policy:
 - a. If using 'Encrypt data in place' as the selected method of encryption, execute the data transformation and

then apply the standard policy.

- b. If using the 'Copy/Restore ' method of encryption, apply the standard policy on an empty folder/device.
5. On the secondary server, create a new folder to store the replicated database.

Note

The folder name and the path must be the same as the primary server.

6. Guard the folder with the standard policy.
7. Perform step 4 above for additional secondary server(s).
8. Put the primary database back into online mode.
9. Setup SQL AlwaysOn High Availability group to perform FULL Data Synchronization.

This copies the primary database and replicates it to secondary replica servers.

10. Verify that the databases in the secondary server are in "Synchronized" mode.

Configuration 2

- Database on the primary server does not require encryption, but the secondary replica database requires it
- Database names and locations for the secondary replica servers are the same as the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Confirm the creation of a data transformation and/or standard policy.
3. On the secondary server, create a new folder to store the replicated database.

Note

The folder name and the path must be the same as the primary server.

4. Guard the folder with the standard policy.
5. Perform step 3 & 4 above for additional secondary server(s).

6. Setup SQL AlwaysOn High Availability group to perform **FULL Data Synchronization**.

This copies the primary database and replicates it to secondary replica servers.

7. Verify that the databases in the secondary server are in “Synchronized” mode.

Configuration 3

- Databases on the primary and secondary replica servers require encryption
- Database name is the same, but the location of the secondary replica server is in a different location from that of the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Change the primary database to offline mode.
3. Confirm the creation of a data transformation and/or standard policy.
4. Guard the folder containing the primary database files with that policy:
 - a. If using 'Encrypt data in place' as the selected method of encryption, execute the data transformation and then apply the standard policy.
 - b. If using the 'Copy/Restore ' method of encryption, apply the standard policy on an empty folder/device.
5. On the secondary server, create a new folder to store the replicated database.

Note

The folder name and the path must be the same as the primary server.

6. Guard the folder with the encryption policy.
7. From secondary server, perform the restore to the primary database.
 - a. Select the options **Restore with norecovery** and **Relocate all files to folder**.
 - b. Specify the path of the new folder from step 5.
8. Repeat steps 4 & 5 above for any additional secondary server(s).
9. Setup SQL AlwaysOn High Availability group to perform **JOIN ONLY Data Synchronization**.

This joins the secondary database to the SQL Always High Availability Group. It also establishes replication of

new data and logs from the primary to the secondary replicated server.

10. Verify that the databases in the secondary server are in **Synchronized** mode.

Configuration 4

- Database on the primary server does not require encryption, but the secondary replica database requires encryption
- Database name is the same, but the location on the secondary replica server is in a different location than that of the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Confirm the creation of a data transformation and/or standard policy.
3. On the secondary server, create new folder to store the replicated database.
4. Guard the folder with the standard policy.
5. From secondary server, perform restore the primary database:
 - a. Select the options **Restore with norecovery** and **Relocate all files to folder**.
 - b. Specify the path of the new folder from step.
6. Setup SQL AlwaysOn High Availability group to perform **JOIN ONLY Data Synchronization**.

Joins the secondary database to the SQL Always HA Group. It also establishes replication of new data and logs from the primary to the secondary replicated server.

7. Verify that the databases in the secondary server are in **Synchronized** mode.

Configuration 5

Following is an alternative method for protecting data in a MS SQL Server AlwaysON environment.

To perform the procedure:

1. Shut down SQL services completely, on the secondary node.

Note

It is important to shut down the secondary node first, in order to keep the assignments the same.

2. Shut down SQL services completely on the primary node.
3. Create GuardPoints, using Data Transformation policies, on the directories containing the databases to be encrypted in the primary node.

Note

Perform encrypt-in-place encryption on each directory.

4. Create GuardPoints, using Data Transformation policies, on the directories containing the databases to be encrypted in the secondary node.

Note

Perform encrypt-in-place encryption on each directory.

5. Delete the GuardPoints, using Data Transformation policies, from the primary node.
6. Create GuardPoints, using operational policies, on the four directories in the primary node.
7. Delete GuardPoints, using Data Transformation policies, from the secondary node.
8. Create GuardPoints, using operational policies, on the four directories in the secondary node.
9. Activate SQL services on the primary node.
10. Activate SQL services on the secondary node.

Data Transformation (Encryption in place)

For more information on transforming and encrypting data-in-place, see the [CTE Agent: Data Transformation Guide](#).

Copy/Restore

For more information on transforming data using the copy and replace method, see the [CTE Agent: Data Transformation Guide](#).

SQL Server Policy Tuning

In this section, you created and defined a process set for SQL Server that grants certain executables, in this case, `sqlservr.exe`, unrestricted access to the database files. The need may arise to allow other executables, and/or users, access to the files.

You can grant this access by:

- Adding to the existing process set
- Creating a new one

The best option depends on the access requirements. The key decision is whether or not to select the **Apply Key** effect along with **Permit** or not. Omitting **Apply Key** on a security rule that still contains **Permit** allows the specified user or process to access to the data, but does not apply the encryption key, so therefore only shows them the data in its encrypted, cypher-text format. This is useful for anti-virus or backup software that may need to scan or copy the file, but does not necessarily need to see the contents.

Using LDT with Microsoft SQL

- Using LDT with SQL AlwaysOn
- Using LDT with SQL FILESTREAM
- Guarding SQL Server FileTable databases with LDT

Using LDT with SQL AlwaysOn

To guard a directory with an LDT (Live Data Transformation) policy, you must temporarily close all of the files in that directory. In an SQL Server AlwaysOn environment, this may entail temporarily stopping the SQL Server service on the node that is being guarded. Once the directory is guarded, then you can start the SQL Server service immediately.

It is important to remember that the SQL Server AlwaysOn replication standard operating procedures.

- If one SQL Server service is taken offline for any reason, then once it is brought back on line, it takes the SQL Server a moment to re-synchronize the database nodes.
- The longer that secondary service was down, and the more inserts/updates and deletes that occurred on the still active node during that downtime, then the longer the synchronization period takes.
- During that synchronization period, any attempted fail over results in the SQL Server warning that data loss may occur if the fail over continues. However, once the SQL Server has completed re-synchronizing that secondary node, then any fail over is safe and does not result in loss of data.

Using LDT with SQL FILESTREAM

The following section is for guarding an SQL Server FileStream database with an LDT policy. If the database contains FileTables directories instead, then follow the instructions in [Using CTE with SQL FileTables](#).

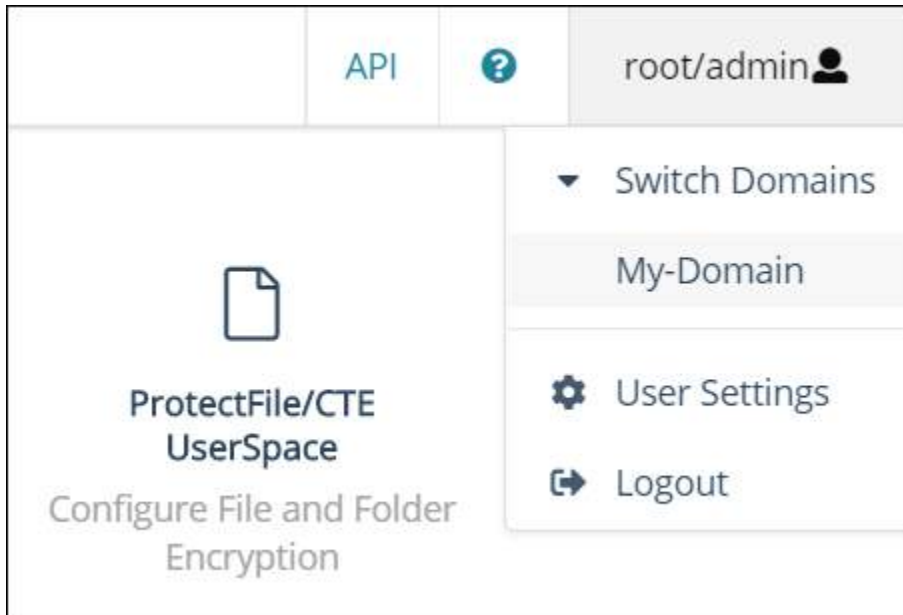
Creating a policy for LDT

To guard an SQL Server FileStream Database with an LDT policy, create an appropriate policy on CipherTrust Manager.

1. In a web browser, navigate to the URL of the CipherTrust Manager you want to use and log in with

CipherTrust Manager Administrator credentials.

2. If the client you want to protect is registered to the default domain (root), proceed to the next step. If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the domain/user name (default: **root/admin**) on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.
 - c. The logged in user now shows the new domain name/user name.



3. In the CipherTrust Manager Applications Page, open the **CTE** application.
4. In the left-hand menu bar on the Clients page, click **Policies**.
5. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
6. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. For example: LDT-Policy-West
Policy Type	Select Live Data Transformation.
Description	A user-defined description to help you identify the policy later. For example: LDT policy for the West Coast

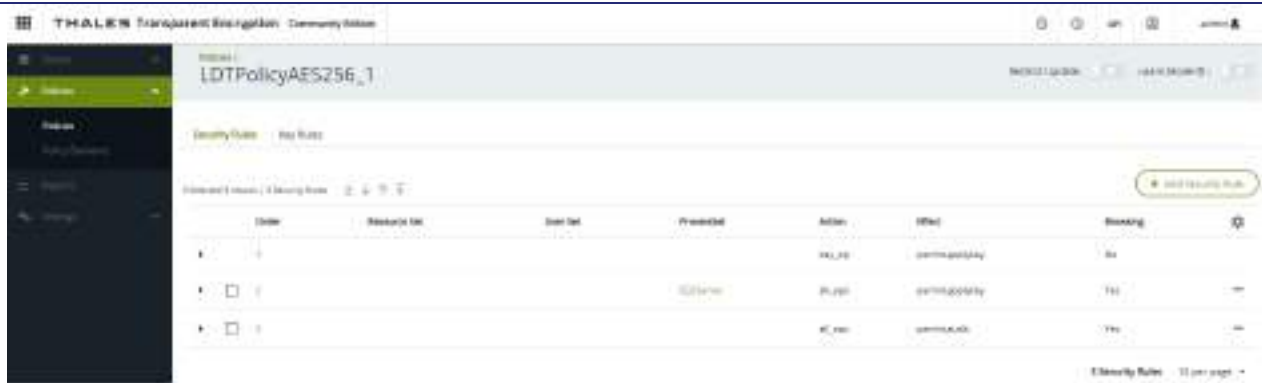
Field	Description
	Datcenter.
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.

7. Click **Next**.
8. On the Security Rules page, define the security rules you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of **key_op** and the effects **Permit** and **Apply Key**. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version. This rule is required by LDT, so you cannot edit it, move it, or delete it.

- a. If no process other than SQL Server's process needs access to clear data, then after the default security rule, create a security rule with:

Policy Element	Value
Process set	<code>path-to-sqlservr.exe</code>
Action	<code>all_ops</code>
Effect	<code>permit,apply key</code>



- b. The SQL Server process set for the second security rule should specify the path to `sqlservr.exe`, and optionally, select to sign that process when adding that process to the process set.

Create Process Set - Add Process



1 General Info 2 Add Processes 3 Confirmation

Add Process > Create Process

Add processes to the process set.

Directory

C:\Program Files\Git

Select

File

Git-cmd.exe

Signature

signsqlservr

Select

RWP Exempted Resource

RWP Exempted Resource

Select

Back

Add

- a. Create a third security rule:

Rule	Value	Note
Action	All_ops	
Effect	Permit, audit	Needed if each operation occurring on the database outside of <code>sqlservr.exe</code> will be audited.

9. On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one.

Field	Description
	If the data has not yet been encrypted, select clear_key . Otherwise select the name of the non-versioned key that is currently being used to encrypt the data.
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

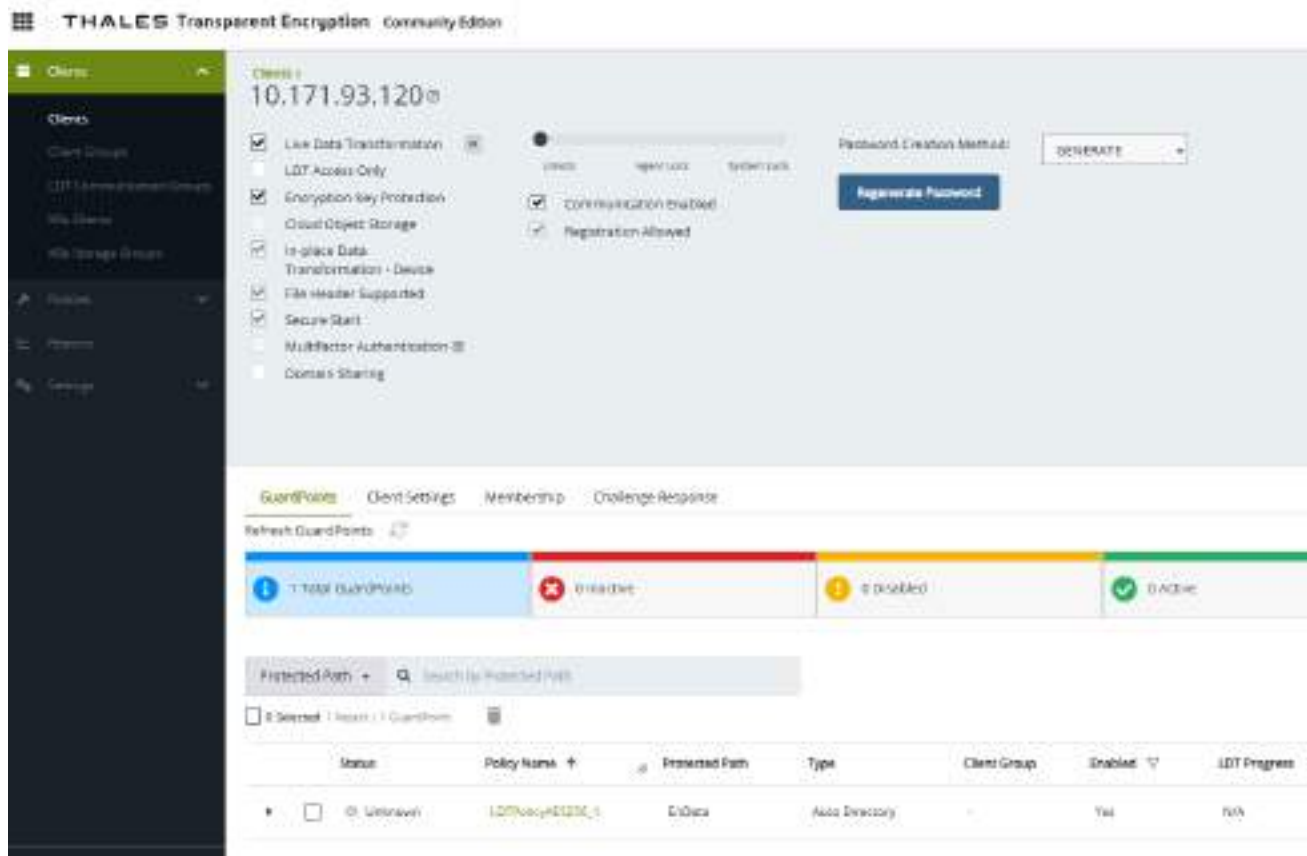
Note

LDT now supports dynamic resource sets. This means that you can alter the resource set, and the policy will pick up the changed resource set and apply it. However, make sure that you **do not** mix encryption keys in your edited resource set. This will cause corruption.

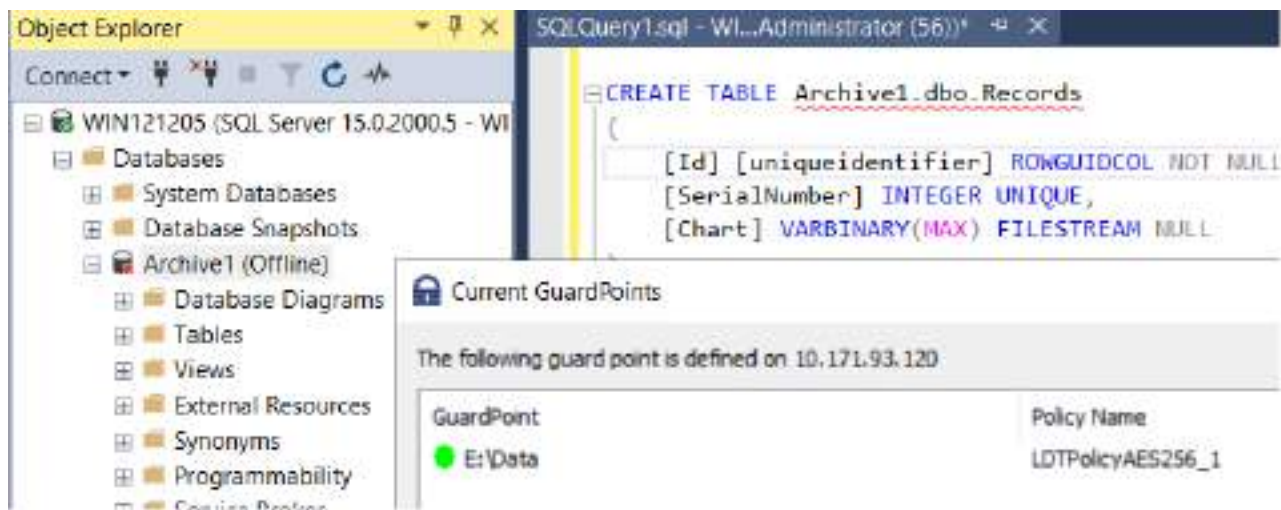
When you are done specifying key rules, click **Next**.

Create a GuardPoint

1. Navigate to and select the directory containing *.mdf, *.ndf and *.ldf database files to guard.



- On the SQL Server, take the database offline so that CTE Agent can guard the database.



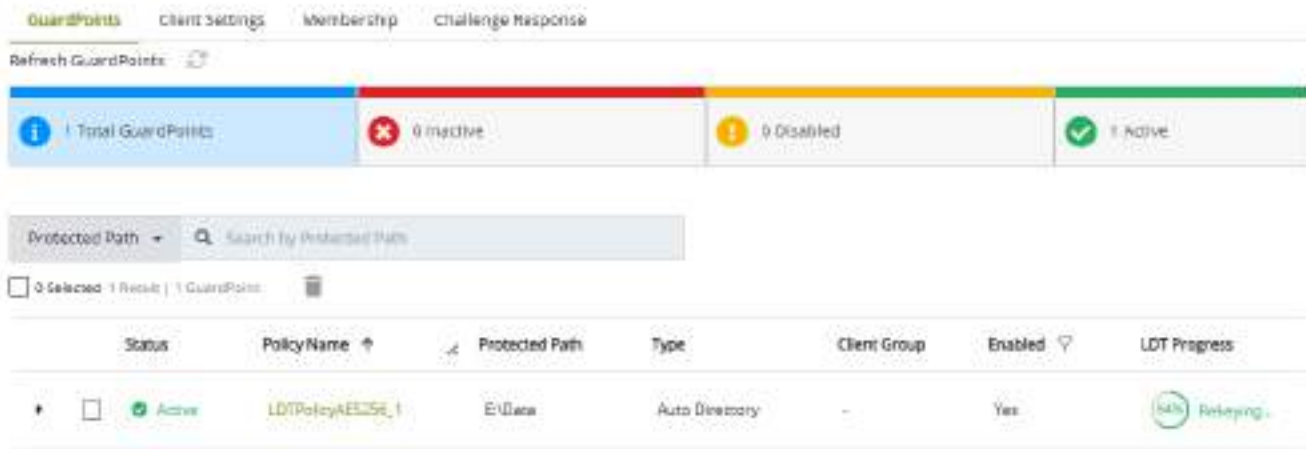
When the CTE Etray on the agent turns green, that indicates that the directory is now guarded. You can now bring the database back online.

- On the Confirmation page, review the information you entered and click **Save** when you are ready to save the policy.

Within a minute after the directory is guarded, either before or after the database is brought back online, LDT begins encrypting the files in the directory, including the database files (*.mdf, *.ndf and *.ldf), and any

other files in that directory or subdirectory. This LDT encryption activity includes all of the files in the the FileStream subdirectories in that guarded parent directory.

As the LDT activity is transparent, the database can be brought back online before or after this activity occurs. CipherTrust Manager will periodically update with the LDT percentage progress:



Verify Successful Encryption

To verify that the FileStream files are encrypted on a disk, open a file outside of SQL Server, using notepad or any desired application. Issue an SQL query to verify if `sqlservr.exe` is reading the decrypted data:

The screenshot shows a SQL query being executed in SQL Server Enterprise Manager. The query is `select * from Archive1.dbo.Records`. The results are displayed in a table with columns Id, SerialNumber, and Chert. The file explorer shows a directory containing several files with names like `0000002c-0000012c-0002`. A Notepad window is open, showing the decrypted content of one of the files, which is `new E=8w|`.

Id	SerialNumber	Chert
1	1	0x536569736D69632044617465
2	2	0x536569736D69632044617465
3	3	0x536569736D69632044617465
4	4	0x536569736D69632044617465

Once LDT completes, the status on CipherTrust Manager for that GuardPoint changes to **rekeyed**.

Backup an SQL FileStream Database

To backup a FileStream database using SQL, use SQL normally, however, if the backup file target location is outside of the guarded database directory, then that backup target location should be guarded as well. When utilizing SQL to backup a database, since `sqlservr.exe` is the process that creates the backup file and performs all of the database backups, the backup is encrypted inline and on disk for those writes when writing to that guarded backup directory. The backup includes the FileStream files in that backup.

Restore an SQL FileStream Database

To restore a FileStream database, restore the database as usual from a backup that was created either before, or after, the database was guarded by a LDT policy. (This is possible because LDT stores file metadata on each file, indicating if it is encrypted or not.) This is not supported though when guarding with a standard policy since no file metadata is stored on files for a standard policy. For a standard policy, any backup being restored, from within a guarded directory, needs to have been created after that directory was guarded with that standard policy. Otherwise, any older, unencrypted clear backup file needs to be outside of the guarded directory.

Conclusion

As `sqlservr.exe` is the only process that reads the decrypted data, avoid mixing accesses to SQL Server database backups across guarded directories and non-guarded directories. For example: If you use SQL to backup a database to a guarded directory, then outside of SQL Server, use explorer to copy that backup from the guarded directory to a non-guarded directory. Then using SQL to restore that backup results in undecipherable data being returned to `sqlservr.exe`. No corruption would occur, as the `sqlservr.exe` process would simply recognize that the file is not in SQL Server backup format and thus immediately fail to restore it. Copying the file back into a GuardPoint and then restoring it it would resolve the issue.

Guarding SQL Server FileTable databases with LDT

There are specific steps for guarding an SQL FileTables database which **must not** be deviated from to correctly and safely guard the FileTables directory.

The following steps are for the scenario where all of the remote systems, installed with CTE, are guarding the FileTables Virtual Network Name (VNN) directory, as well as the FileTables server.

Note

The remote agent, the LDT primary, encrypts the files in the VNN, but it does not encrypt the actual database. As well, all remote agents perform transparent encryption/decryption on the VNN. But the agent running on the SQL Server does not perform any encryption at all, not for LDT, or for the transparent encryption/decryption. It strictly provides access control.

The benefit of this scenario is access to the files in the VNN path are transmitted across the encrypted LAN, and the files on the FileTables server cannot be decrypted.

Even though the FileTables server does not decrypt the files, it must still have CTE installed and guarding the real path to prevent the SQL Server from backing up the FileTables files during LDT transformation.

Prerequisite

Create a CIFS connection with CIFS credentials that LDT will use:

1. Log on to CipherTrust Manager.
2. In the left nav-bar, click **Access Management > Connections**.
3. Select **+ Add Connection**.
4. In the **Select Connection Type**, click **More**.
5. From the **Select Connection** dropdown, select **CIFS/SMB** and click **Next**.
6. In the **General Info** section, enter the **Name** and **Description** for the connection and click **Next**.
7. In the Configure Connection page, enter valid values for:
 - **Host**: IP or FQDN of the SMB share server.
 - **Port**: The port where the SMB service is running on the host.

Note

The *Host* and *Port* fields must be specified together. If *Host* and *Port* are not specified while creating a connection, these fields cannot be added later.

- **Username**: Username to access the SMB share.
- **Password**: Password to access the SMB share.
- **Domain**: Workgroup or domain under which the username is configured. It is an optional field.
- (Optional) Click **Test Credentials** to validate the connection. If the test is successful, the status is **OK**, else the status is **Fail**.

Note

The *Host*, *Port*, and *Test Credentials* fields are mandatory for testing the connection credentials.

8. Click **Add Connection**.

Setup

1. Install [CTE agent for Windows](#) on the FileTables server and register the CTE clients to the CipherTrust Manager.
2. During registration, you **must** select Access Only to prevent this system's LDT from rekeying the files unsynchronized with the other systems.
3. Configure the FileTables server to treat all local GuardPoints as header-based. This is required because SQL Server FileTables technology does not support NTFS Alternate Data Streams (ADS), therefore, each file must contain a header for that file's LDT metadata for storage. Open the CLI with administrator privileges and type:

```
voradmin ldt header add 1 <path-to-GP>
```

Where

- Path is case sensitive
- Path only needs to be a partial matching substring of any part of that path

Example

```
voradmin ldt header add 1 FileTables
```

- This would match `e:\GPFileTables2`, but not `e:\GPfiletables2`
4. Use the following commands to list or delete the header information:

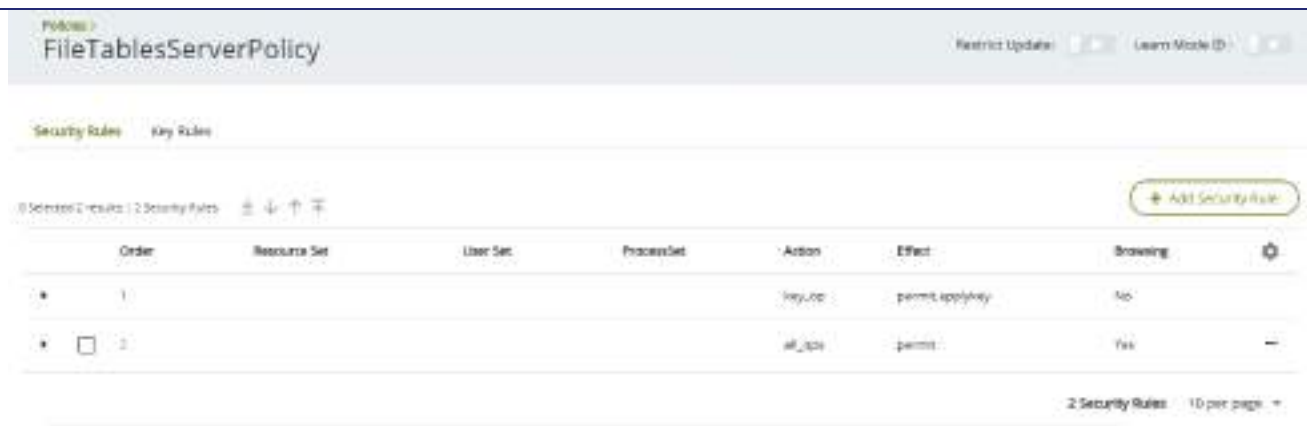
```
voradmin ldt header list
voradmin ldt header delete 1
```

5. Create a **DESKTOP_PRESENCE** file in the virtual network path. Type the following in the command line:

```
mkdir <VNN FileTable directory path>\.vorm_lgs

echo desktop > <VNN FileTable directory path>\.vorm_lgs\DESKTOP_PRESENCE
```

6. Create a policy for the FileTables server that prevents any local user, or any SQL Server, from accessing the clear data once it is encrypted.
 - For this scenario, no security rule can have apply key.
 - You **must** use the same encryption key for the policy used to guard the SQL FileTable Server, and the policy used to guard the VNN/FileTable directory from the ClientGroup.



7. Guard the real path that the SQL Server uses with that policy:

Example: If the database `.mdf` file is located at `e:\db4filetable`, then guard `E:\db4filetable`

8. Right-click on the database and take it offline. Select to drop the connections.
9. If necessary, restart the SQL Server instance to ensure all files are closed in each path to be guarded.
10. Once guarded successfully on the FileTables server, bring the SQL Server database back online.
11. Install CTE on each remote server that will access the VNN. During registration, **select the same Client Group** and **the same Communication Group** for each remote server.
12. You can also install CTE and register it as access-only on some systems. Those systems will not be able to access files that are actively being rekeyed, but they will reduce LDT cross-system communication traffic during rekey.
 - See [Configuring LDT for CIFS shares \(with LDT AccessOnly nodes\) Mapped to Multiple IP addresses](#) for more information.
13. Create a policy that each remote CTE agent will use:
 - a. Set up the security rules per customer's required access control for the Virtual Network Path (VNN). Grant users access to clear data

User set/Process Set Action: permit, apply key

- b. In the Client Group, guard the `Virtual_Network_Name/FileTable_directory` with that policy, and select the CIFS connection created as a prerequisite. Example:

```
VNN: \\192.168.93.89\FileTableShared\FileTableDB8\FileTableTb_Dir8_2
```

At this point, the Virtual Network Name paths should be accessible and return clear data from each remote system. Additionally, Live Data Transform should begin transforming the files accessed through the VNN on a remote primary agent automatically selected to perform LDT.

Accessing the files directly on the FileTables server itself, or querying the FileTables files through SQL, will return

the raw data of the file. This will include the LDT header followed by encrypted data.

SQL Server backups will backup the encrypted FileTables files with the database.

1. Once LDT has completed transforming the data, create a new database backup. Any restore operation should be performed from that new backup. If an older backup needs to be restored, then you must unguard and regard the VNN/FileTable directory GuardPoint from the client group once the older backup is restored, to recreate CTE metadata files in the GuardPoint.
2. LDT should be completed, or paused, before performing any restore of the database.

Unsupported FileTables Use Cases

CTE does not support the following use cases:

1. Install CTE agent on the SQL Server and locally apply the GuardPoint on the SQL Server storage.
2. Access FileTables with Transact-SQL.
3. Access FileTables with File I/O APIs on the SQL server. Perform all file I/O on the remote system running the CTE agent.

Integrating Imperva File Activity Monitoring (FAM) with CTE Windows

Software Requirements

Software	Minimum Version Required
CipherTrust Transparent Encryption	7.8.0.75
CipherTrust Manager	2.19 or subsequent versions

Overview of FAM on CTE agents

File Activity Monitoring (FAM) catalogs, monitors, and secures unstructured data (files). Unstructured data refers to any data that is not stored in databases. You can find these files locally, on the network, or in the cloud. FAM provides insights into data location, ownership, access history, permissions, protection, sharing, and sensitivity, enabling informed decisions about data protection.

For more information on FAM, see the [Introduction to the File Activity Monitoring User Guide](#)

CTE agents enabled with both File System Encryption and FAM capabilities can perform file system monitoring and audit file operations, as per the requirements of the Data Security Fabric (DSF) policies.

Scope of FAM on CTE host

Enabling FAM will also monitor activity on files outside of CTE GuardPoints.

Note

FAM will **not** monitor activity on RWP-enhanced files with CTE Ransomware Protection feature enabled

File Monitoring

The CTE agents monitor and audit user and application access to all files. Monitoring is not limited to files inside of CTE GuardPoints. Files outside of CTE GuardPoints are also monitored, except for those in the following directories:

Linux

```
/dev
/roc
/sys
/media
/opt/vormetric
/CTE-custom-install-location
```

Windows

```
\BOOT
\Windows
\Program Files*
\Users\*\APPDATA\ROAMING\MICROSOFT\WINDOWSAPPDATA\ROAMING\MICROSOFT\WINDOWS*
\Users\*\APPDATA\LOCAL\MICROSOFT\*
\Users\*\APPDATA\LOCAL\TEMP\*
\Users\*\APPDATA\LOCAL\PACKAGES\*
\Users\*\APPDATA\LOCAL\GOOGLE\CHROME\*
\PROGRAMDATA\MICROSOFT\*
\PROGRAMDATA\DELL\*
```

Also excluded from monitoring:

- VSS volumes
- DFSR private folders
- CSV volumes
- File operations performed by:
 - CTE internal processes
 - Thales Data Discovery and Classification processes
 - CTE-managed internal system operations
 - Metadata files

FAM Policies vs CTE Policies

FAM policies, which are similar to CTE policies with respect to security rules, allow you to monitor activity on specific data locations and/or by specific users. FAM policies only allow audit rules to specify/filter the content to be monitored. They do not impact access to the file.

Note

FAM policies are associated with the entire client, as compared to CTE policies which are limited to a particular GuardPoint path.

Performance Impact of FAM on CTE

File activity monitoring and audits consume system resources. This can potentially affect the performance of system and critical applications running on CTE agents. You can reduce the performance impact on the DSF management console by modifying the monitoring rules of the FAM policy applied to the CTE agent. For example:

- File operations, such as reading file attributes, are operations that are performed very frequently by applications and system utilities.
- If the CTE GuardPoint has policy rules with audit enabled, then with FAM also enabled, there may be additional overhead/performance impact due to the additional FAM policy evaluation and logging. However, the policy has no impact on file access/permissions.

Adjustments in the FAM policy to reduce, or eliminate highly frequent operations, can decrease the impact of FAM. Consult the FAM documentation for information on adjusting the FAM policy.

Enabling FAM on CTE Agent

You can enable FAM on CTE agent during CTE registration, or through the API.

Enable during Registration

After installing CTE, you enable FAM when registering, or re-registering, to CipherTrust Manager. During registration, you are prompted with the following two questions:

```
Do you want this host to have Filesystem encryption support enabled on the server? (Y/N) [Y]: Y
```

```
Do you want this host to have File Activity Monitoring support enabled? (Y/N) [N]: Y
```

Make sure that you answer **Y** to both questions.

Restart Secfs

For CipherTrust Manager v2.19 on **Linux**, post registration, you **must** restart **secfs**. This is **not** required for

CipherTrust Manager v2.20 and subsequent versions. To restart secfs:

1. Type:

```
/etc/vormetric/secfs stop
```

2. Type:

```
/etc/vormetric/secfs start
```

Enable through the CM API

You can enable FAM on CTE, post registration:

- As part of the CTE upgrade on reboot process.
- Through the CM API available for CM 2.20 and subsequent versions. See the API documentation available through the CipherTrust Manager software.
- Through the DSF management console. Refer to DSF documentation for more information.

Disabling FAM on CTE

- For CipherTrust Manager v2.19, you cannot completely disable FAM once enabled. However, you can remove the FAM policy associated with the client to temporarily disable FAM audit logging/monitoring.
- For CipherTrust Manager v2.20, you can disable FAM on CTE agent through the DSF management console or through the CM API. Refer to DSF documentation for disabling FAM on CTE agents.

Voradmin Support for FAM

The **voradmin** utility allows you to gather statistics and administer CTE on a host/client. It has slightly different syntax and command capabilities depending on whether the host/client is running in Linux or Windows. The voradmin command provides minimal support for FAM administration on CTE agents. You can check the state of FAM and the FAM policy name applied to the CTE host.

The following command reports the state of FAM, the FAM policy name applied to the CTE host, and the DSF GW configuration for forwarding FAM audits to the DSF GWs.

```
voradmin fam show config
```

FAM Output when policy not applied

Example

```
# voradmin fam show config
```

Response

```
FAM_STATE   : DISABLED
FAM_POLICY  : Not Applied
```

FAM Output when policy applied

Example

```
# voradmin fam show config
```

Response

```
FAM_STATE   : ACTIVE
FAM_POLICY  : fam-all-ops-policy
```

Limitation

- File path names included in the FAM audits that are generated from file operations performed inside Linux containers, or namespaces, under **chroot** enforcement, are relative to the directory created by the **chroot**, or container, as the root directory.
- CTE enforces a limit of 128 characters in the FAM policy names. FAM audits resulting from policies exceeding this limit, will have the policy name trimmed to the this limit.

CTE with Microsoft DFSR

The Microsoft Distributed File System Replication (DFSR) service is a multi-master replication engine used to keep folders synchronized on multiple servers. Using CTE with DFS(R) requires a unique configuration to make sure that all folders within a GuardPoint are only encrypted once, and that all sources to which those folders are replicated can access the proper encryption key to read the encrypted data.

This section contains the following topics:

- [Overview](#)
- [Terms and Topology](#)
- [Configure DFS\(R\)](#)
- [CTE Configuration Workflow](#)
- [Creating Required DFS\(R\) Policy Components](#)
- [Using the Standard/Offline Encryption Method](#)
- [Using the LDT Encryption Method](#)

- [Troubleshooting](#)

For more information about DFS(R), see the Microsoft DFS(R) documentation at [Distributed File System Replication](#).

Overview

This section details the CipherTrust software suite and will act as an operational (run book) guide for managing the CipherTrust security environment. It contains the steps to configure CTE agent on a Windows Server host running Microsoft Distributed File System (DFS) with Replication.

Microsoft introduced the Distributed File System in Server 2003 as a value-add for customers seeking low-cost data resiliency across high-latency, low-bandwidth WAN links. DFS is a free feature included with all subsequent versions of Windows Server software. DFS uses a namespace architecture where nested data folders use a replication service to synchronize similar data directories on 2 or more servers. Architects choose this model to ensure fault tolerance, preserve active uptime and to improve access performance by spreading the workload across many servers: client requests are routed to the nearest DFS folder for a given namespace. CTE began supporting DFS(R) starting with Windows 2012 R2 and continues to do so through Windows 2022 and subsequent versions.

Use this document for guidance on encrypting DFS data depending on how it is currently deployed. It contains a number of scenarios, often highlighting important configuration considerations applicable for the project. Before encrypting any DFS data, however, Thales Support assumes that the customer has made a backup of the latest production data, has a good understanding of their own DFS(R) deployment and has a fully-developed encryption plan.

The information listed here details best practices and tool sets when using encryption for DFS data. It starts by defining the terms and layouts for this technology and ends by reviewing common problems that may compound DFS(R) encryption and troubleshooting tips.

CTE Encryption Methods

CTE supports two encryption methods:

- **Standard offline data transformation**

Where the data is **unavailable** while it is being encrypted or rekeyed.

- **Live Data Transformation**

Where the data is encrypted and rekeyed in the background while it remains **accessible to users**. This method requires a separate license for the LDT feature.

While DFS(R) policies have some unique required components, the basic policy and GuardPoint creation process is identical to non-DFS(R) environments. For details about offline data transformation, see the [CTE Data Transformation Guide](#). For details about LDT, see the [CTE Live Data Transformation with CipherTrust Manager](#).

Considerations with DFS(R)

If you are using CTE in a DFS(R) environment, keep in mind the following:

- You should always back up your data prior to beginning the encryption process and you should have a full backup of the data in the hub server before you restore a spoke.

- You cannot place a GuardPoint *anywhere* on the boot drive, so if your DFS(R) replication point is currently `C:\`, or a directory under `C:\` such as `C:\data\`, you need to move that data and its replication point to a new volume on the server before you can encrypt it.

Note

Make sure that all GuardPoints are at, or above, the level of the DFS(R) replication point. For example:

- If the replication point is `D:\`, the CTE GuardPoint must also be at `D:\`. Adding a GuardPoint on a directory in `D:\`, such as `D:\data\`, fails.
- If the replication point is `D:\data\`, you can add a GuardPoint at `D:\data\` or `D:\`, but you *cannot* add a GuardPoint on a subdirectory of `D:\data\` such as `D:\data\HR-files\`.
- If you are backing up your DFS data, make sure that your backup software is not backing up the archive bit. File replication is triggered by file version change or a modified time stamp. As such, there is a chance that updating the archive bit may cause issues that trigger a replication storm, which will then put a heavy encryption load on the servers.
- When you set a replication point, Microsoft automatically creates a private directory called `<dir name>\DfsrPrivate` that resides with that replication point. For example, if the replication point is set on `D:\`, the private directory would be `D:\DfsrPrivate`. If the replication point is set on `D:\data\`, the private directory would be `D:\data\DfsrPrivate`.

How this private directory must be handled depends on the the encryption method that you are using.

- For **Standard** encryption, you must guard the private directory with the same policy that you use for the main GuardPoint. If the GuardPoint is at the root of the volume (for example, `D:\`), this happens automatically. But if you are guarding a specific directory, such as `D:\data\`, you need to create a second GuardPoint using the same policy on `D:\data\DfsrPrivate`.
- For **LDT**, you must guard the private directory with the same policy that you use for the main GuardPoint, even if the GuardPoint is at the root level. (For example, you must have a GuardPoint for both `D:\` and `D:\DfsrPrivate\`.) In addition, you must exclude this directory from LDT processing.
- The policy you specify for a DFS(R) GuardPoint **cannot** contain a resource set in any of the key rules included in the policy. All files in the guarded directory, and its subdirectories, must be encrypted with the same encryption key **without exception**. Additionally, if you rekey the GuardPoint, all files must be rekeyed with the same encryption key.
- If you want to change from one encryption key to an entirely different encryption key (as opposed to rekeying the data with a new version of the existing key), you must decrypt the data and remove all existing GuardPoints so that you have a clean environment. Then you can start the CTE encryption process over from the beginning.

Caution

You cannot change from one encryption key to another if any of the existing data is still encrypted with the old key. If you attempt to do so, you may encounter data replication errors and you may need to delete the entire volume and recreate it.

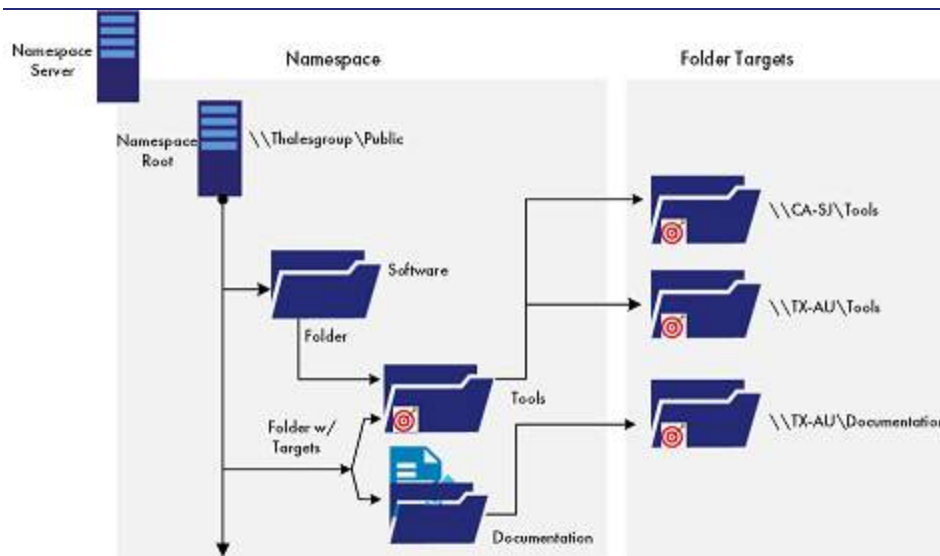
- When CTE encrypts data on a node, the encrypted data must be replicated to other nodes in the configuration. This may result in increased replication activity on the network.

Terminology and Topology

DFS(R) uses a compression algorithm known as remote differential compression (RDC). RDC detects changes to the data in a file and enables DFS Replication to replicate only the changed file blocks instead of the entire file. DFS(R) uses a database engine that keeps track of all file deltas and is used when reconciling replicated data across servers.

Term	Definition
DFS Namespace	A central namespace through which you can see a unified view of the shared folders that are included in the DFS.
DFS Namespace Server	The server that hosts the DFS Namespace. DFS Namespace Root is the top level of the DFS namespace. The namespace root and the DFS namespace use the same name.
DFS Folder	A folder presented to a client within the DFS namespace, but below the DFS root. A DFS folder can exist on the same server that is hosting the DFS root, but it is not required. DFS folders commonly represent file system resources located on other servers.
DFS Tree	A DFS tree is a reference to the DFS hierarchy. The tree starts with the DFS root, and contains all of the DFS folders defined within the root.
Replicated folder	A folder that stays synchronized on each member. As the data changes in each of the replicated folders, the changes replicate across connections between all members of the replication group.

In order to use DFS(R), administrators designate a namespace on a namespace server. Folders nested within the namespace contain all of the data that is distributed across many servers.



The **Tools** folder, in the preceding graphic, is part of a replication group composed of two servers, known as members, which participate in the replication of one or more replicated folders.

Creating multiple replicated folders in a single replication group simplifies the process of deploying replicated folders because the topology, schedule, and bandwidth throttling for the replication group are applied to each replicated folder. You can administer DFS(R) by using DFS Management, the DFS(R) Admin and DFS(R) diag commands, or scripts that call WMI. The connections between all members form the replication topology.

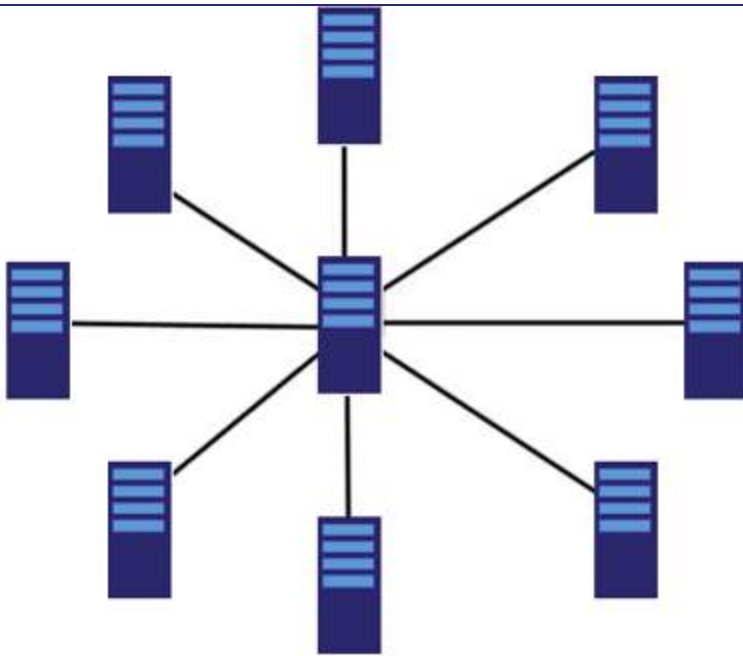
DFS(R) Topology

How you deploy CTE in a DFS(R) environment depends on the topology you have chosen for your DFS(R) configuration. Microsoft offers several topology options for DFS(R):

Hub and Spoke

In this configuration, there is a central server (an explicitly-designated hub) whose content is replicated on multiple satellite servers (the spokes). While each spoke server has a two-way communication channel with the hub server, none of the spoke servers can communicate with each other. If the data changes on one spoke server, that server communicates the changes back to the hub server and the hub server initiates the data replication on all of the other spoke servers.

This configuration allows you to encrypt servers one at a time, starting with the hub and then moving outwards to the spokes. This type of topology tends to be very efficient, but the problem with it is that if the initial master fails, then all replication ceases to function until it is online again. This topology is typically used for WANs that consist of faster network connections between major computing hubs and slower links connecting branch offices.

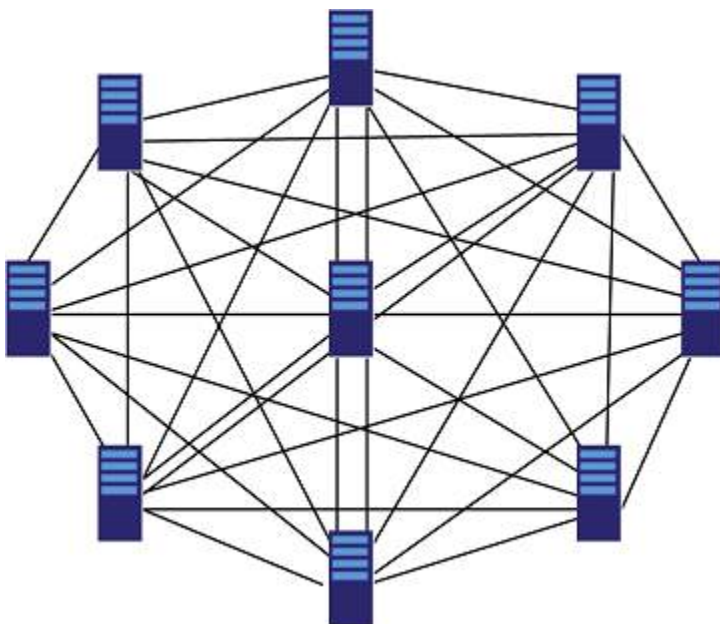


Full Mesh

A full mesh topology allows every replica to replicate with every other replica. In this configuration, data replication can be initiated by any server on all of the other servers. The advantage of using this topology is that replication continues functioning even if a server drops off-line. Users see no interruption in service. Deploying this model is useful for maintenance operations and satisfies data resiliency. The disadvantage to using this method is that it can result in an excessive amount of replication traffic.

As of Windows 2012, Microsoft added support for more than 5 replicas in a set. In addition, DFS(R) now supports multiple Namespaces: good for encrypting different namespaces with different AES keys (when required for “fencing” requirements).

In this configuration, you must stop the replication service while you encrypt the data on all servers in the mesh. You cannot restart the replication service until the initial encryption has completed on all servers.



No Topology

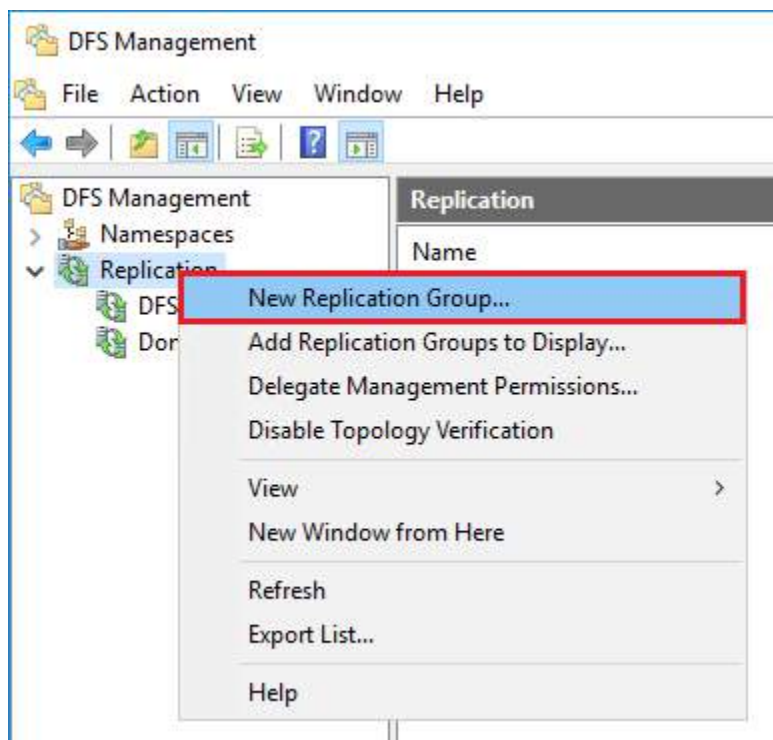
This option allows for creating a replication group without defining any replication topology. This means administrators may create their own custom replication topology later on.

Configure DFS(R)

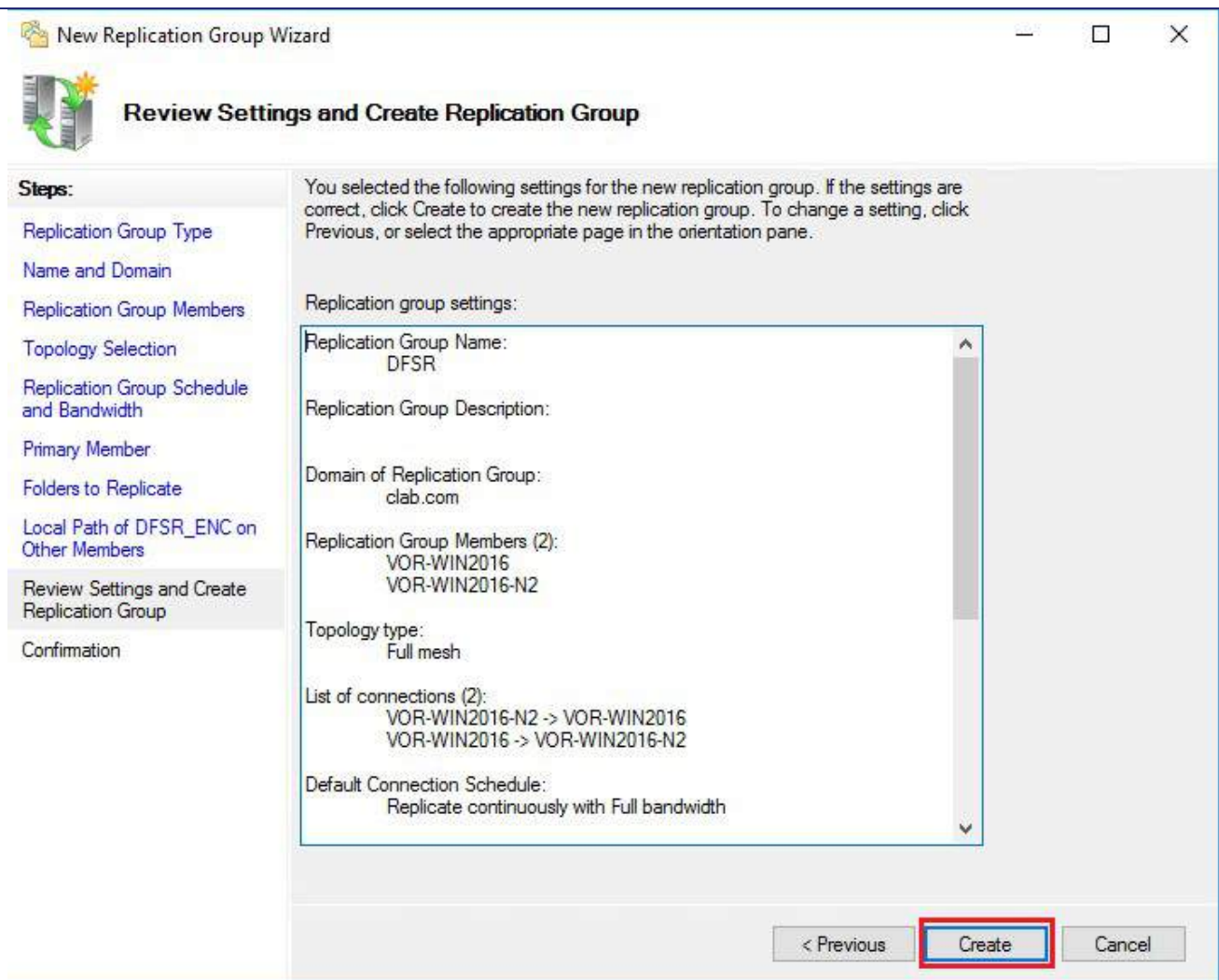
Note

The following instructions were written for Windows 2016. If you are using a subsequent version, steps may differ slightly. See [Distributed File System Replication](#) for more information.

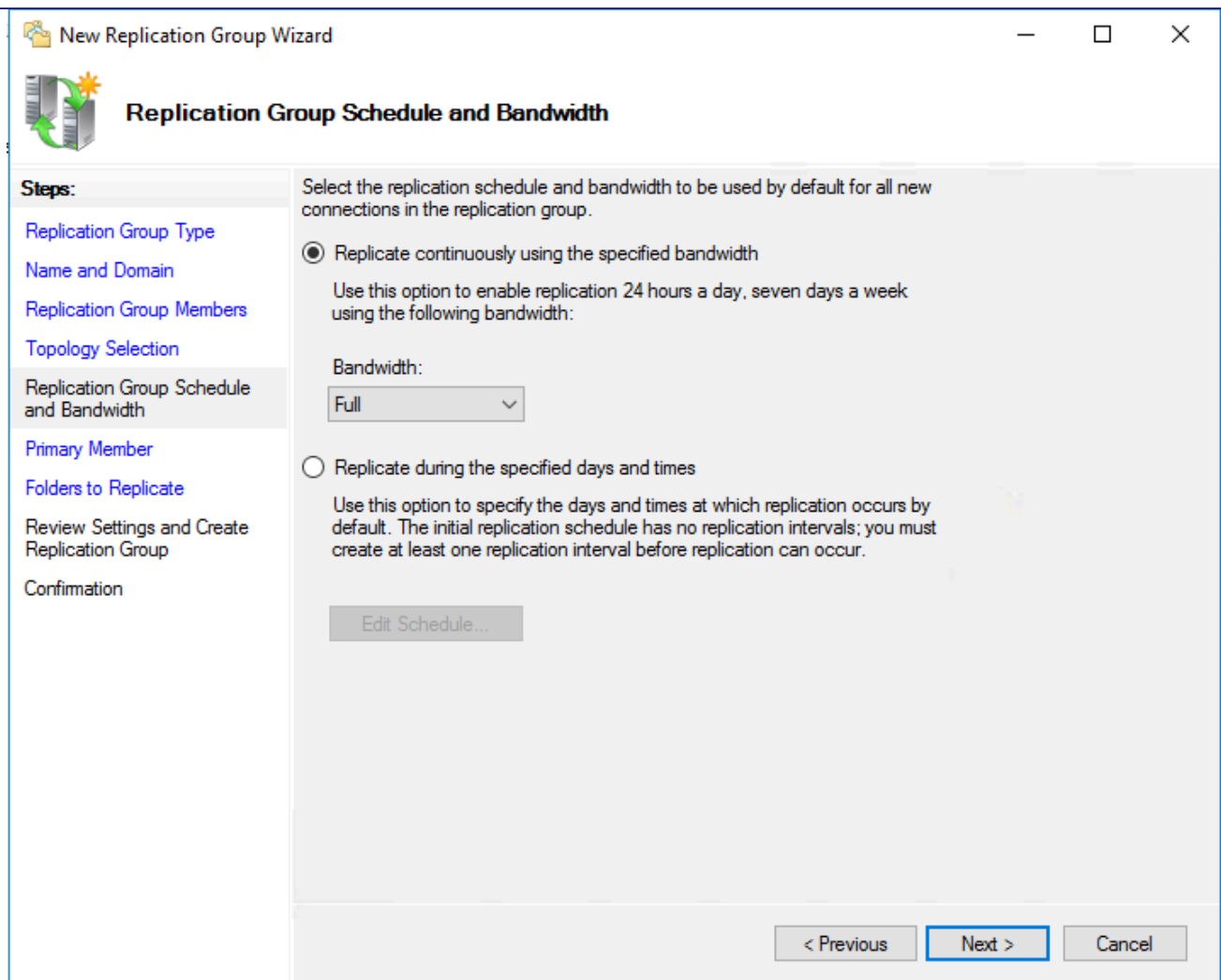
1. Launch the Server Manager applet.
2. Select **Tools > DFS Management**.
3. Right-click on Replication and select **New Replication Group ...**



4. For replication group, select **Multipurpose Replication Group**. Then click **Next**.
5. Enter a Replication Group name and the Domain name. Click **Browse** to select the domain. Then click **Next**.
6. In the Replication Group Members window, click **Add** and enter all of the DFS(R) replication group member servers. Then click **Next**.



7. Select the replication topology. Then click **Next**.
8. Set the replication schedule. Then click **Next**.



9. In the Primary Member section, select the Primary DFS(R) node. Then click **Next**.
10. In Folders to Replicate, click **Add**.
11. Click **Browse** and navigate to the folder on the primary node to place under DFS(R) replication.
12. Once the path is set, click **Permissions**.

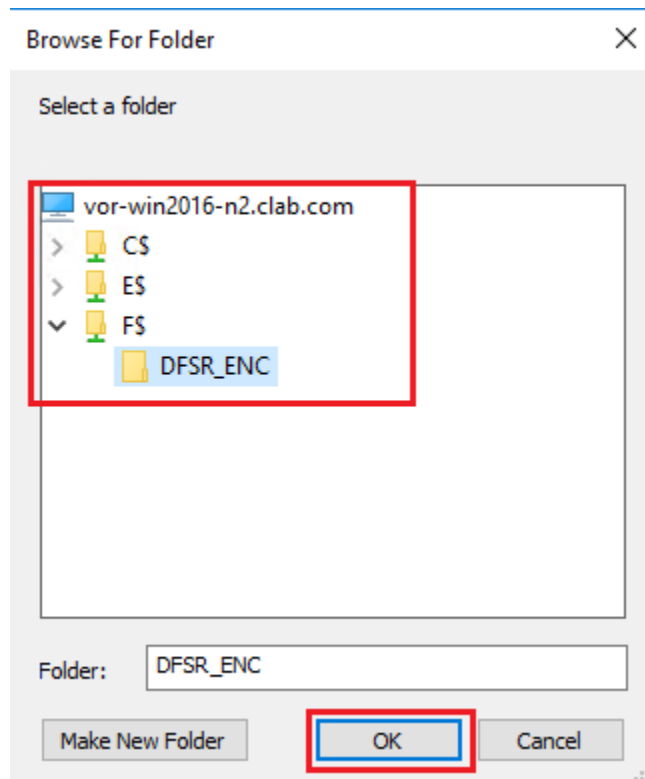


13. Change the permissions or keep the existing folder permissions. Click **OK**.
14. On the local path for other members, click **Edit**.
15. Click **Browse** and select the target replication folder on the replication group member.

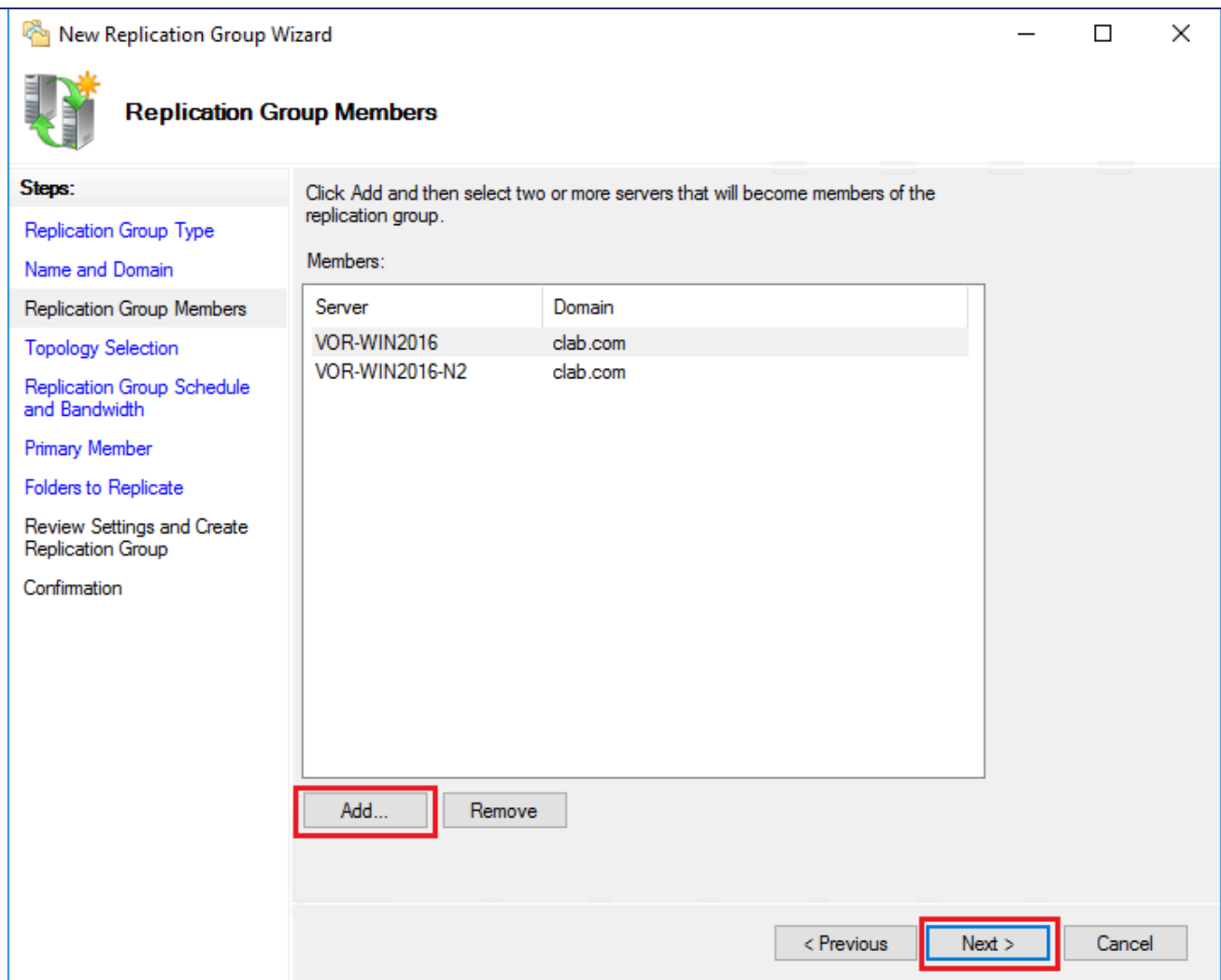
Note

If the path is different from the Primary member, then you cannot use CipherTrust Client Groups. You must set GuardPoints separately on individual member nodes.

16. Browse the folder structure for the member node and select the target replication folder. Click **OK**.



17. If the target replication folder displays correctly, click **OK** to continue. If it does not, click **Browse** and reset the folder.
18. Review the configuration and click **Create** if it all looks correct.

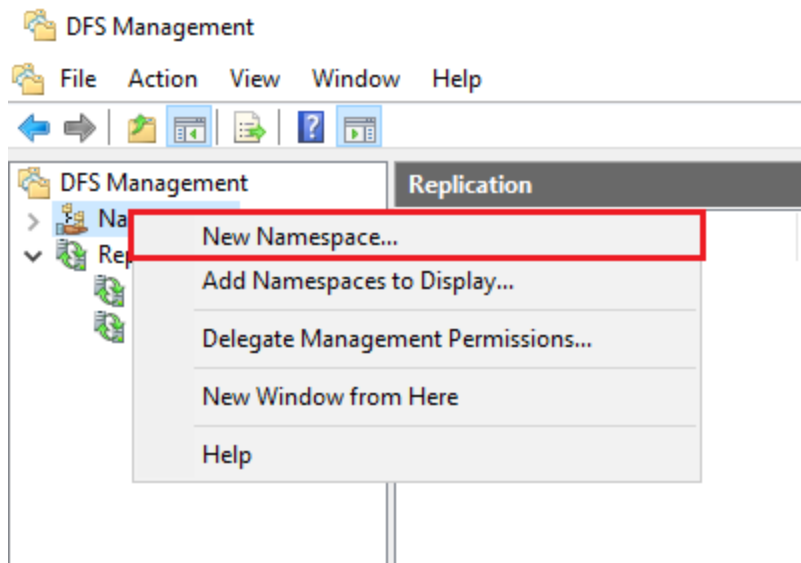


19. Click **Close** for a successful DFS(R) deployment.

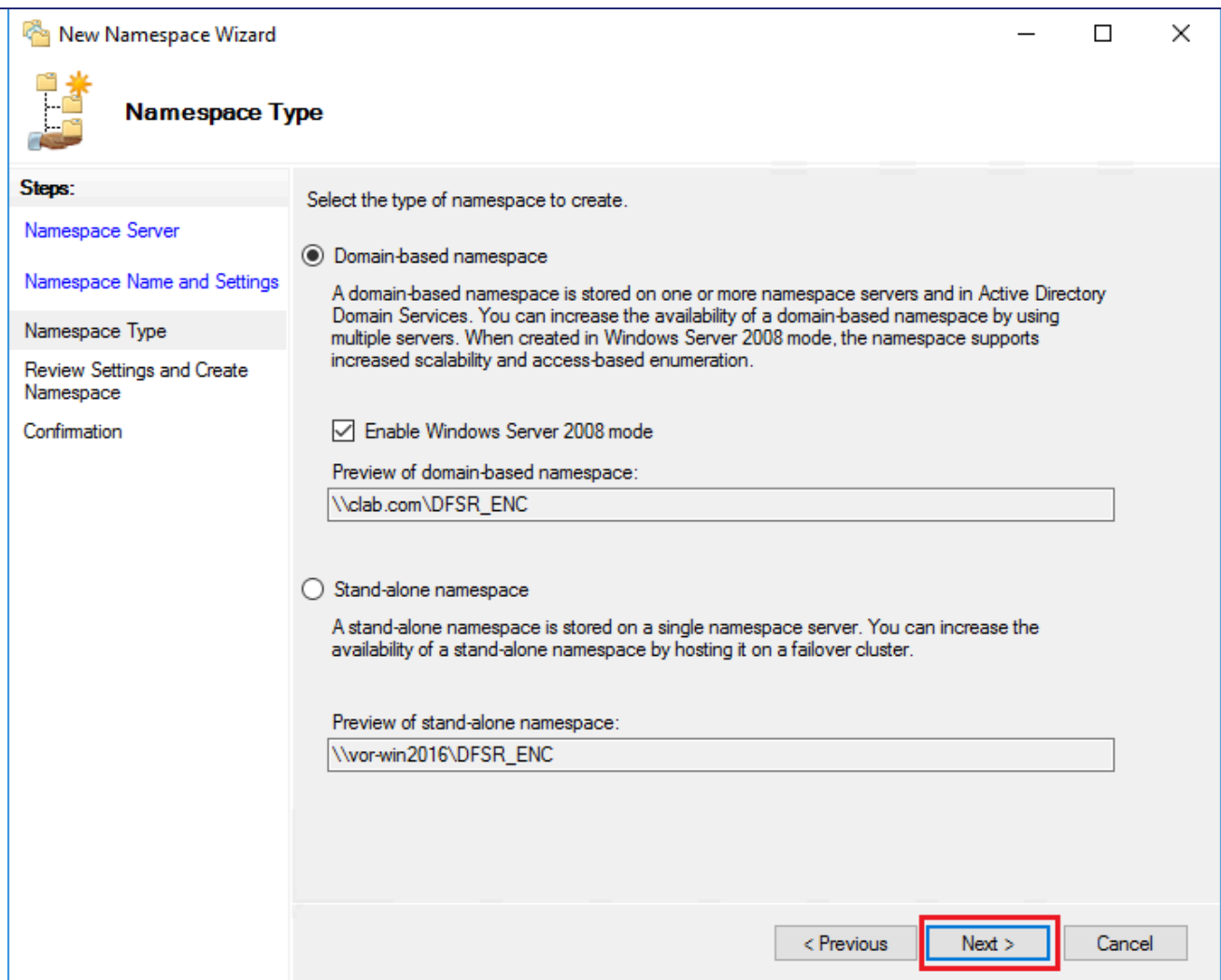
Configure Namespace

DFS(R) namespace allows you to access the data remotely, through a network share path. For CipherTrust Transparent Encryption, it must have a policy that has a security rule that contains a user set. The user set must include privileged users linked to the process `ntoskrnl.exe`. This provides additional security for sensitive data protected on a DFS(R) folder.

1. In the DFS management tool, right-click on Namespace and select **New Namespace...**



2. Click **Browse** and search for the replication group member to host the namespace.
3. Select the node that will host the DFS(R) Namespace. Click **OK** and **Next**.
4. Enter a name for the Namespace and click Next.
5. Accept the default for the Domain-based namespace and click **Next**.



6. Review the settings and click **Create** to create the Namespace.

7. After a successful outcome, click **Close**.

Install the DFS(R) Role and Features

Consult the Microsoft documentation to install DFS by using Server Manager

Stopping and Starting the DFS Services

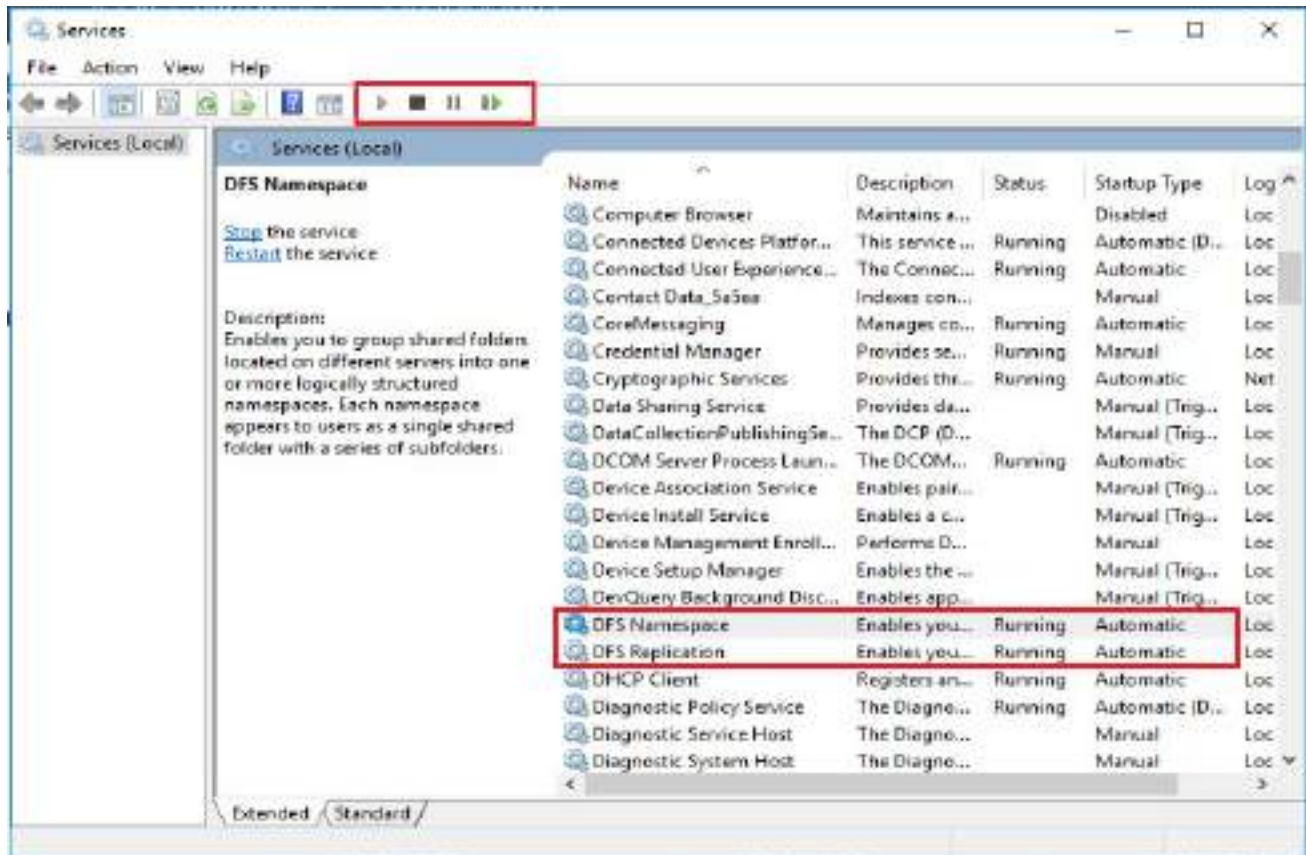
When setting up the topology, you will have to start and stop the DFS services. Following are the steps to stop and start the DFS services on a DFS management node. On all the nodes in a DFS(R) topology, there are two services running:

- DFS Namespace Service
- DFS Replication Service

Both of these services must be stopped before you can apply a CTE GuardPoint successfully:

1. Right-click on the start menu and click **Run**.

2. Type `services.msc` and hit enter. This launches the Services Management Console.
3. Locate the DFS Namespace and DFS Replication Services.
4. Select each one individually and click Stop.



CTE Configuration Workflow

In order to configure CTE with DFS(R), you must complete the following tasks:

1. Make sure you have a valid backup of the data you intend to encrypt.
2. Identify the volumes or folders you intend to encrypt.
3. Select an encryption method and make sure you understand how to create and deploy CTE GuardPoints using that encryption method. For details, see one of the following documents:
 - [CTE Data Transformation Guide](#)
 - [CTE-Live Data Transformation with CipherTrust Manager](#)
4. Create a DFS(R) Process Set and User Set for the policy. For details, see [Creating Required DFS\(R\) Policy Components](#).
5. Create the policies and GuardPoints you need to protect your data, using the process appropriate to the

selected encryption method. For details, see one of the following:

- [Using the Standard Encryption Method](#)
- [Using the LDT Encryption Method](#)

6. Consider configuring all nodes within a DFS topology under a single [CipherTrust Client Group](#)

Creating Required DFS(R) Policy Components

DFS(R) uses two services to for the replication process, `dfsrs.exe` and `ntoskrnl.exe` that must be associated with the NT AUTHORITY user. In order to do this, you need to create a process set and a user set that must then be combined into a security rule in the policy.

Note

Once you create these components, you can use them in any number of policies for both standard and LDT GuardPoints.

1. Log into the CipherTrust Manager Console and switch to the correct domain.
2. Launch the **Transparent Encryption** application.
3. In the left-hand menu bar, expand **Policies** and select **Policy Elements**.
4. Create a process set for the required DFS(R) processes:
 - a. Click **Process Sets**.
 - b. Click **Create Process Set**.
 - c. In the **Name** field, enter a name for this process set. In this example, we will use DFS(R)-Processes.
 - d. Click **Next**.
 - e. Enter the first DFS(R) process:
 - In the **Directory** field, enter `C:\Windows\System32\`.
 - In the **File** field, enter `dfsrs.exe`.
 - f. Click **Next**.
 - g. Below the table, click **Add Another Process**:
 - In the **Directory** field, enter `\SystemRoot\System32\`.
 - In the **File** field, enter `ntoskrnl.exe`.

h. Click **Next**. The process set should look like this:

Directory	File	Signature	
C:\Windows\System32\	dfsrs.exe		...
\SystemRoot\System32\	ntoskrnl.exe		...

Back Add Another Process Save

i. Click **Save** to save the process set.

5. Create the user set for the required **NT AUTHORITY** user:

a. Click **User Sets** tab.

b. Click **Create User Set**.

c. In the **Name** field, enter a name for the user set. In this example we will use **Local_NT_AUTHORITY**.

d. Click **Next**.

e. Click the **Manually Add Users** tab.

f. In the **uname** field, enter **SYSTEM**.

g. In the **OS domain** field, enter **NT AUTHORITY**.

h. Click **Next**. The user set should look like this:

uname	UID	gname	GID	OS domain	
SYSTEM				NT AUTHORITY	Remove

i. Click **Save** to save the user set.

j. Optionally, create another user set for other authorized users in the namespace. For example, you may want to add the "Administrator" user in each of the domains that are part of the namespace. You can create as many separate user sets as required.

6. Create the mandatory security rule for DFS(R):

The first security rule in a standard policy is for the DFS(R) process set (created in the previous section). This rule allows the DFS(R) processes to access the data and manage the replication under **DfsrPrivate** folder. The minimum permissions must be:

Rule	Permissions	Description
Process Set	DFS(R)_service	Contains the process <code>dfsrs.exe</code> and <code>ntoskrnl.exe</code>
Action	all_ops	Allows all read/write operations
Effect	Permit	Allows data to be copied/moved/replaced as encrypted

- When you have finished created the required components, you can use the components to create the appropriate policy for your chosen encryption method.

Using the Standard Encryption Method

If you want to encrypt your data using the standard (offline) encryption method, you need to create two different policies. The first policy is the initial encryption policy that specifies the symmetric key that you want to use to encrypt the data for the first time. The second is the production policy that you want to use for day-to-day operations on the encrypted data.

The initial encryption must be done while the volume or directory is offline, and users and applications must be prevented from accessing the data until the entire encryption process has finished. Once this initial encryption has been completed, any new or changed data in the GuardPoint will be automatically encrypted as it is added.

Note

If you want to encrypt the data without restricting access during the encryption process, you can use the LDT feature. For details, see [Using the LDT Encryption Method](#).

To use the standard encryption method:

- Make sure that you have created the required policy components for DFS(R) as described in [Creating Required DFS\(R\) Policy Components](#).
- Create the initial encryption and production policies as described in [Creating Standard Policies for DFS\(R\)](#).
- Create the GuardPoints that you want to use. The GuardPoint creation method depends on your DFS(R) topology. For details, see one of the following:
 - [Creating Standard GuardPoints with the DFS\(R\) Hub and Spoke Topology](#)
 - [Creating Standard GuardPoints with the DFS\(R\) Full Mesh Topology](#)

Creating Standard Policies for DFS(R)

If you are using the standard (offline) data encryption option, you need to create two policies, a data transformation policy that is used for the initial encryption and a standard policy that is used for day-to-day access of the encrypted data. The initial encryption policy is identical to the one you use for any standard GuardPoint. It is the standard policy that has DFS(R)-specific requirements.

How you create policies for DFS(R) depends on the key manager that you are using.

Procedure Using CipherTrust Manager

1. Log into the CipherTrust Manager Console and switch to the correct domain, if required.
2. Select **Keys** and select a symmetric key to use to encrypt the data, or create a new key to use for the DFS(R) namespace.
3. Launch the **Transparent Encryption** application.
4. In the left-hand menu bar, click **Policies**.
5. To create the **initial data encryption** policy, click **Create Policy** and enter the following information.

Note

The following example assumes you are using **dataxform** to encrypt the data in place. If you are using the copy or restore encryption method, create your initial data transformation policy as described in the [CTE Data Transformation Guide](#)

- a. In the **Name** field, enter a name for the policy. This example uses **DFS(R)-Std-Initial**.
- b. In the **Policy Type** field, select **Standard**.
- c. Enable the **Data Transformation** option.

Name *

DFSR-Std-Initial

Policy Type

Standard

Description

Learn Mode: ☐

Data Transformation: ☒

- d. Click **Next**.
- e. On the Security Rules page, make sure there is a security rule with the action **key_op** and the effect **permit, applykey**. If CipherTrust Manager did not add this security rule automatically, go back to the General Info page and make sure that the **Data Transformation** option is enabled.
- f. On the Security Rules page, click **Create Security Rule** and add another security rule that prevents any other process from accessing the data while it is being encrypted:
 - In the **Action** field, click **Select** and choose **all_ops**.
 - In the **Effect** field, click **Select** and choose **Deny**.

When you are done, click **Add** to save the security rule.

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit,applykey	Yes
	Local_NT_AUTH	DFSR-Processes		permit,applykey	Yes

- g. Click **Next**.
- h. On the Key Rules page, click **Create Key Rule**. In the **Current Key Name** field, click **Select** and choose **clear_key**.

Resource Set	Current Key Name	
	clear_key	...

Caution

In a DFS(R) environment, you must apply the initial encryption policy on unencrypted data **ONLY** (the current key must be set to clear_key). If your data is already encrypted, you must decrypt it and completely remove the existing GuardPoint before re-encrypting the data with a new key from scratch. For details, see [Considerations with DFS\(R\)](#).

- i. Click **Add** to save the key rule.
- j. Click **Next**.
- k. On the Data Transformation page, click **Create Data Transformation Rule**. In the **Transformation Key Name** field, click **Select** and choose the symmetric key you want to use for data transformation.
- l. Click **Add** to save the data transformation rule.

Resource Set	Transformation Key Name	
	DFS(R) Standard-Key	...

- m. Click **Next**.
 - n. Verify the policy information and click **Save** to save the initial encryption policy.
6. To create the **production policy**, click **Create Policy** and enter the following information.
- a. In the **Name** field, enter a name for the policy. This example uses **DFS(R) -Std-Policy**.
 - b. In the **Policy Type** field, select **Standard**.
 - c. Click **Next**.
 - d. On the Security Rules page, click **Create Security Rule** and add the following security rule:
 - In the **User Set** field, click **Select** and choose the user set you created that contains NT AUTHORITY. For details, see [Creating Required DFS\(R\) Policy Components](#).
 - In the **Process Set** field, click **Select** and choose the process set you created that contains the required DFS(R) processes `dfsrs.exe` and `ntoskrnl.exe`.
 - In the **Effect** field, click **Select** and choose **Permit**.

e. Click **Add**.

Resource Set	User Set	Process Set	Action	Effect	Browsing
*	Local_NT_AU...	DFS-R-Processes		permit,audit	Yes

f. Add any other security rules you need to your policy. When you have added all your security rules, click **Next**.

g. On the Key Rules page, click **Create Key Rule**. In the **Current Key Name** field, click **Select** and choose the symmetric key you used to encrypt the data in the initial data encryption policy.

Resource Set	Key Name
	DFS-R-Standard-Key

h. Verify the policy information and click **Save** to save the production policy.

7. To allow the system and users to access the metadata on files and folders under the DFS(R) path, you can include the metadata rule. Apply Key is not required because the metadata files and folders is never encrypted.

Rule	Permissions	Description
Action	f_rd_attr,f_rd_sec,d_rd,d_rd_attr,d_rd_sec	Allows all metadata read operations
Effect	Permit	Allows metadata to read files and folders.

8. When you have both policies ready, you can create the required DFS(R) GuardPoints as described in [Creating Standard GuardPoints with the DFS\(R\) Hub and Spoke Topology](#) or [Creating Standard GuardPoints with the DFS\(R\) Full Mesh Topology](#).

DFS(R) GuardPoint Considerations

Remember the following when configuring GuardPoints on protected data. Doing so ensures reliable replication of guarded data:

1. A GuardPoint may not be placed on any replicated folder on the BOOT drive. If the replication point is currently **C:**, consider moving it to another volume on the server (any non-BOOT drive) and use DFS utilities to re-populate any new namespace or target folder configurations. Then apply a GuardPoint to the replicated folder (dataxform or st_policy).
2. When a GuardPoint is not applied to an entire drive, ensure a sub-folder in the GuardPoint, named DFS(R) private, is also guarded with the same policy that is applied to the VDS GuardPoint. DFS(R) private is a hidden sub-folder immediately below the DFS(R) GuardPoint that is auto-generated when you configure a

folder as a DFS(R) GuardPoint. DFS(R) keeps intermediate configuration/state files in this sub-folder. The data in this folder constitutes an unstructured matchup of all data (and their deltas) organized in the DFS folders. Objects therein do not resemble their logical counterparts. Guarding this directory, however, is recommended, and will encrypt the data as intended.

Example

- If the DFS(R) GuardPoint, and the CTE GuardPoint are both `F:\data`, apply the same policy to `F:\data\DFS(R)` private that you applied to `F:\data`
- If the GuardPoint is `F:\data` and the DFS(R) pGuardPoint is `F:\data\data2`, apply the same policy to `F:\data\data2\DFS(R)` private that you applied to `F:\data`

Note

These rules apply only in situations in which the CTE GuardPoint and the DFS(R) GuardPoint are sub-directories. You do not need to guard the DFS(R) private sub-folder when the DFS(R) GuardPoint and the CTE GuardPoint are applied to the entire drive (e.g., both are the `F:\` drive).

3. A CTE GuardPoint must be the same as the DFS(R) GuardPoint configured on a folder, or the DFS(R) GuardPoint must be a sub-folder nested beneath the GuardPoint. Do not apply a GuardPoint on a sub-folder of the DFS(R) GuardPoint. Three consistency rules for Guardpoints on DFS folders:

DFS(R) GuardPoint	CTE GuardPoint	Works
<code>F:\</code>	<code>F:\</code>	Yes
<code>F:\data</code>	<code>F:\</code>	Yes
<code>F:\</code>	<code>F:\data</code>	No

Tip

- Administrators can accelerate replication completion by pre-populating target folders (seeding) with backup data.
- Always have a full backup of data in the hub node prior to restoring to a spoke.

Creating Standard GuardPoints with the DFS(R) Hub and Spoke Topology

Hub-and-spoke is the only topology that allows for encrypting the folders that need protection on each individual server, sequentially, starting with the Hub (think of it as the primary active node).

If you are using the hub and spoke DFS(R) topology, you should encrypt the data on the hub and then encrypt the data on the spokes. After you have encrypted the data on the hub server, you have two options for the data on the spoke servers:

- **Option 1: Delete the existing spoke server data and allow DFS(R) to replicate the encrypted hub data to all of the spoke servers.**

The advantage to this method is that you only need to encrypt the data on the hub. The disadvantage is that it will take time to replicate the data to all of the spoke servers.

- **Option 2: Encrypt each Spoke server using the same encryption process as you use on the hub server.**

The advantage to this method is that you do not need to wait for the full data replication process across the network. The disadvantage is that you must run the encryption process on all Spoke servers.

Prerequisites

- Make sure you have a valid backup of the data you plan to encrypt.
- Make sure you know what devices or directories you plan to protect.
- Make sure you understand how data transformation GuardPoints are created.
- Make sure you have an initial encryption and a production policy as described in [Creating Standard Policies for DFS\(R\)](#).

Note

The following procedures assume you are using `dataxform` to encrypt the data in place.

Procedure for Option 1: Use DFS(R) to Replicate the Encrypted Data

1. Disable user and application access to all devices and directories, on the hub server and all spoke servers, in the namespace, you intend to encrypt so that no users can add or change the data during the transformation process.

Note

You do *not* have to disable the namespace.

2. On the hub server:

- a. Stop the DFS(R) service.
- b. In your key manager, create the GuardPoints that you want to encrypt and apply the initial encryption policy to those GuardPoints.

Note

Make sure that all GuardPoints are at, or above, the level of the DFS(R) replication point. For example:

- If the replication point is `D:\`, the CTE GuardPoint must also be at `D:\`. Adding a GuardPoint on a directory in `D:\`, such as `D:\data\`, fails.
- If the replication point is `D:\data\`, you can add a GuardPoint at `D:\data\` or `D:\`, but you *cannot* add a GuardPoint on a subdirectory of `D:\data\` such as `D:\data\HR-files\`.

- Do not create GuardPoints for the `DfsrPrivate` directories yet.
- c. On the hub server, run the `dataxform` utility as described in the [CTE Data Transformation Guide](#).
 - d. After the data encryption process has completed, unguard the GuardPoints that use the initial encryption policy and guard them using the production DFS(R) policy.
 - e. If any of your GuardPoints are at the directory level, create a GuardPoint for the `<dir name>\DfsrPrivate` directory that goes with that GuardPoint. For example, If the GuardPoint is `D:\data\`, the private directory would be `D:\data\DfsrPrivate`. Make sure that you use the same production policy for the `DfsrPrivate` directory that you used for the main directory.

Warning

Do not start the DFS(R) service yet.

3. On each spoke server:
 - a. Stop the DFS(R) service on the spoke server.
 - b. Delete the data in all devices and directories that you added GuardPoints for on the hub server.
 - c. In your key manager, create the same GuardPoints on the spoke server that you created on the hub server, making sure that you apply the same standard policy to each GuardPoint on the spoke server that you applied on the hub server.

Make sure you also create the same `DfsrPrivate` GuardPoints on the spoke server that you created on

the hub server.

Note

Because the directories are empty, you do not need to use the initial encryption policy or the **dataxform** utility on the spoke servers. You can just guard the empty directory and the private directories directly using the production policy.

- a. **Start the DFS(R) service** on the spoke server.
4. Repeat the previous step for each spoke server in the configuration.
5. When every spoke server has the exact same production GuardPoints as the hub server, return to the hub server and do the following:
 - a. **Start the DFS(R) service** on the hub.
 - b. Force replication from the hub to the spokes.
6. When replication is complete for all spokes in the configuration, re-enable user and application access to the devices and directories that you encrypted.

Procedure for Option 2: Encrypt the Data on All Servers

1. Disable user and application access to all devices and directories that you intend to encrypt so that no users can add or change the data during the transformation process. This must be done on the hub server and all spoke servers in the namespace.

Note

You do not have to disable the namespace.

2. On the hub server:
 - a. Disable access to the hub server so that no one can change the data during the transformation process.
 - b. **Stop the DFS(R) service** on the hub.
 - c. In your key manager, create the GuardPoints that you want to encrypt and apply the initial encryption policy to those GuardPoints.
 - Make sure that all GuardPoints are at or above the level of the DFS(R) replication point.

-
- Do not create GuardPoints for the **DfsrPrivate** directories yet.
- d. Run the **dataxform** utility on the hub server as described in the [CTE Data Transformation Guide](#).
 - e. After the data encryption process has completed, unguard the GuardPoints that use the initial encryption policy and re-guard them using the production DFS(R) policy.
 - f. If any of your GuardPoints are at the directory level, create a GuardPoint for the **<dir name>\DfsrPrivate** directory that resides with that GuardPoint. For example, If the GuardPoint is **D:\data**, the private directory would be **D:\data\DfsrPrivate**. Make sure you use the same production policy for the **DfsrPrivate** directory that you used for the main directory.
 - g. [Restart the DFS\(R\) service](#) on the hub server.
3. On each spoke server:
 - a. Stop the DFS(R) service on the spoke server.
 - b. In your key manager, create the same GuardPoints on the spoke server that you created on the hub server. Make sure that you apply the same initial encryption policy to the GuardPoints on the spoke server that you applied on the hub server.
- Warning**

Do not create the **DfsrPrivate** GuardPoints yet.
- c. On the spoke server, run the **dataxform** utility.
 - d. After the data encryption process has completed, unguard the GuardPoints that use the initial encryption policy and re-guard them using the same production DFS(R) policy that you used for the corresponding GuardPoint on the hub server.
 - e. Create the same **DfsrPrivate** GuardPoints on the spoke server that you created on the hub server. Make sure that you use the same production policy for the **DfsrPrivate** directory that you used for the main directory.
 - f. Restart the DFS(R) service on the spoke server.
 - g. Re-enable user and application access to the spoke server.
4. Repeat the previous steps for each spoke server in the configuration.
 5. When data encryption is complete for all spokes in the configuration, re-enable user and application access to the devices and directories you encrypted.
-

Creating Standard GuardPoints with the DFS(R) Full Mesh Topology

If you are using the full mesh DFS(R) topology, you must restrict access to the data on all servers in the namespace until it has been encrypted on all servers in the namespace. That means the data will be inaccessible to users and applications until the encryption procedure has been completed on all servers.

Prerequisites

- Make sure you have a valid backup of the data you plan to encrypt.
- Make sure you know what devices or directories you plan to protect.
- Make sure you understand how data transformation GuardPoints are created.
- Make sure you have an initial encryption and a production policy as described in [Creating Standard Policies for DFS\(R\)](#).

Note

The following procedures assume you are using `dataxform` to encrypt the data in place.

Procedure

1. On **all** servers in the configuration:
 - Disable user and application access to all devices and directories you intend to encrypt so that no users can add or change the data during the transformation process.
 - [Stop the DFS\(R\) service.](#)
2. On one of the servers in the configuration:
 - a. In your key manager, create the GuardPoints that you want to encrypt and apply the initial encryption policy to those GuardPoints.

Note

Make sure that all GuardPoints are at, or above, the level of the DFS(R) replication point. For example:

- If the replication point is `D:\`, the CTE GuardPoint must also be at `D:\`. Adding a GuardPoint on a directory in `D:\`, such as `D:\data\`, fails.

- If the replication point is `D:\data\`, you can add a GuardPoint at `D:\data\` or `D:\`, but you *cannot* add a GuardPoint on a subdirectory of `D:\data\` such as `D:\data\HR-files\`.

- Do not create GuardPoints for the `DfsrPrivate` directories yet.

- Run the `dataxform` utility as described in the [CTE Data Transformation Guide](#).
 - After the data encryption process has completed, unguard the GuardPoints that use the initial encryption policy and re-guard them using the production DFS(R) policy.
 - If any of your GuardPoints are at the directory level, create a GuardPoint for the `<dir name>\DfsrPrivate` directory that goes with that GuardPoint. For example, If the GuardPoint is `D:\data\`, the private directory would be `D:\data\DfsrPrivate`. Make sure that you use the same production policy for the `DfsrPrivate` directory that you used for the main directory.
- Repeat the previous steps for each one of the servers in the configuration.
 - When you are finished, the production GuardPoints should be identical on every server in the namespace.
 - Restart the DFS(R) service on the each server in the namespace.
 - Re-enable user and application access to all devices and directories.

Using the LDT Encryption Method

If you want to encrypt your data using LDT, you need to create a Live Data Transformation policy and use that to create your GuardPoints. All encryption occurs in the background while users continue to access the data.

With LDT, the data will be automatically rekeyed periodically, based on the expiration date and the life span of the versioned key used to encrypt the data.

To use the LDT:

- Make sure you have created the required policy components for DFS(R) as described in [Creating Required DFS\(R\) Policy Components](#).
- Make sure that you have a versioned [encryption key](#).
- Create the LDT policy as described in [Creating a LDT Policy for DFS\(R\)](#).
- Create the GuardPoints you want to use as described in [Creating a LDT GuardPoint for DFS\(R\)](#).

Note

Make sure that all GuardPoints are at, or above, the level of the DFS(R) replication point. For example:

- If the replication point is **D:**, the CTE GuardPoint must also be at **D:**. Adding a GuardPoint on a directory in **D:**, such as **D:\data**, fails.
- If the replication point is **D:\data**, you can add a GuardPoint at **D:\data** or **D:**, but you *cannot* add a GuardPoint on a subdirectory of **D:\data** such as **D:\data\HR-files**.

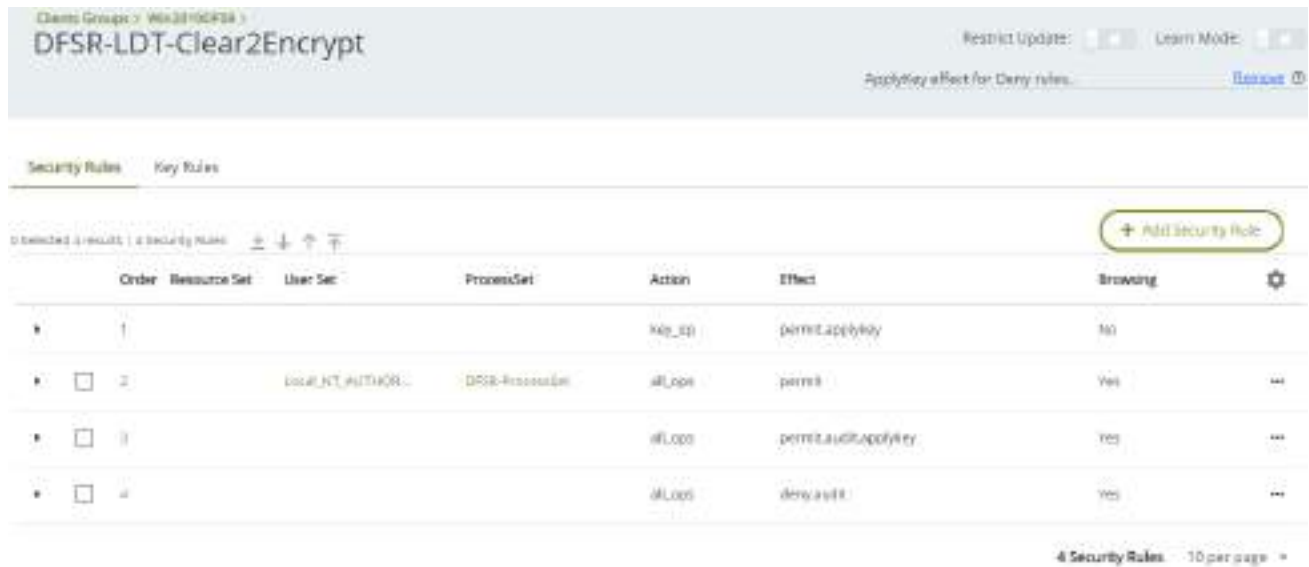
5. Consider using [QoS](#) for optimal DFS(R) performance.

Creating an LDT Policy for DFS(R)

1. Log into the CipherTrust Manager Console and switch to the correct domain if required.
2. If you do not know which versioned key you want to use to encrypt the data, or you want to create a new key to use for the DFS(R) namespace, launch the Keys & Access Management application and locate an existing versioned key, or create a new versioned key. For details on creating a versioned key for LDT, see [Creating an Encryption key](#).
3. Launch the **Transparent Encryption** application.
4. In the left-hand menu bar, click **Policies**.
5. Click **Create Policy**.
6. Enter a name for the policy in the **Name** field.
7. In the **Policy Type** field, select **Live Data Transformation**.
8. Click **Next**.
9. On the Security Rules page, make sure there is a security rule with the action **key_op** and the effect **permit,applykey**. If CipherTrust Manager does not add this security rule automatically, go back to the General Info page and make sure that the policy type is set to **Live Data Transformation**.
10. On the Security Rules page, click **Create Security Rule** and add the following security rule:
 - In the **User Set** field, select the user set you created that contains **NT AUTHORITY**. For details, see [Creating Required DFS\(R\) Policy Components](#).
 - In the **Process Set** field, select the process set you created that contains the required DFS(R) processes **dfsrs.exe** and **ntoskrnl.exe**.
 - In the **Action** field, select **all_ops**.

- In the **Effect** field, select **Permit**.

11. When you are finished, click **Add** to save the security rule.



12. Add any other security rules that you need to your policy. When you are finished, click **Next**.

13. On the Key Rules page, click **Create Key Rule** and add the following key rule:

- In the **Current Key** field, select **clear_key**.

Caution

In a DFS(R) environment, you **must** apply the LDT policy on unencrypted data **ONLY** (the current key must be set to **clear_key**). If your data is already encrypted, you must decrypt it and remove the existing GuardPoints before re-encrypting the data with a new key.

- In the **Transformation Key** field, select the LDT versioned key that you want to use to encrypt the data.

14. When you are finished, click **Add** to save the key rule.

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule
	clear_key	DFSR-LDT-Key	No

15. Click **Next**.

16. Verify the policy information and click **Save** to save the LDT policy.

Creating a LDT GuardPoint for DFS(R)

Warning

Before you can create an LDT GuardPoint, you must set LDT to ignore the DFS(R) private directory that Microsoft automatically creates when you create a DFS(R) replication point. The private directory should **not** be encrypted by LDT.

1. Log into one of the DFS(R) servers in your network as an administrator.
2. For each GuardPoint that you intend to set up on the server, exclude the matching `DfsrPrivate` directory from the LDT process using the `voradmin ldt exlist add <guard path>` command.

For example, if you are going to guard `D:\data`, `G:\HR Files`, and the entire `F:` drive, you would use the following commands:

```
voradmin ldt exlist add D:\data\DfsrPrivate
voradmin ldt exlist add G:\HR Files\DfsrPrivate
voradmin ldt exlist add F:\DfsrPrivate
```

To make sure LDT is ignoring the proper directories, use the `voradmin ldt exlist get` command:

```
voradmin ldt exlist get
```

```
Live Data Transformation exclusion list. Following ${gp}s will be excluded from the Live Data Transformation.
```

```
G:\HR Files\DfsrPrivate
D:\data\DfsrPrivate
F:\DfsrPrivate
```

3. Reboot all of the LDT agent hosts before you create any LDT GuardPoints.
4. Repeat the previous steps on each server in your configuration before you create any LDT GuardPoints.
5. After you have excluded all `DfsrPrivate` directories on all servers from LDT processing, log into your key manager and set your LDT properties. When you begin the initial encryption, Thales recommends that you throttle the LDT processing speed with a CPU cap of 20%. You can increase this cap as more of the data is encrypted and there are fewer deltas between the DFS staging area and the production area.

To set the cap, launch the **CTE** application and create a Profile with the appropriate Quality of Service configuration parameters. Then make sure that all clients in the DFS(R) configuration use that profile.

6. Create the required LDT GuardPoints using the Live Data Transformation policy you created.

Create the same set of GuardPoints, using the same Live Data Transformation policies, on each server in the configuration. For example, if you set up the following GuardPoints for the first server:

Guard Path	LDT Policy Name
D:\data	LDT-Policy-Main
D:\data\DfsrPrivate	LDT-Policy-Main
F:\	LDT-Policy-Main
F:\DfsrPrivate	LDT-Policy-Main
G:\HR Files	LDT-Policy-HR
G:\HR Files\DfsrPrivate	LDT-Policy-HR

You must then set up the same six GuardPoints, using the same two LDT policies, on each server in the configuration.

CTE QoS Throttling and Rekey Scheduling

DFS(R) servers use a local database file for organizing and replicating file deltas. They employ many consistency checks, especially while processing large volumes of file changes. Furthermore, LDT requires a lot of system resources when encrypting target data for the first time. So consider throttling the encryption process for optimal DFS(R) performance. Best practice is to start low and increase steadily as the DFS staging areas shrink (fewer deltas).

QUALITY OF SERVICE CONFIGURATION

☐ Rekey by Rate

LDT QoS Rekey Rate (MB/s)

LDT Status Check Rate (in minutes)

☒ Rekey by CPU

☐ Cap CPU Allocation

CPU Percentage

QoS Schedules

LDT QoS Schedule: ANYTIME

Create New QoS Schedule

Name	Time Range
ANYTIME	Sunday 12:00 AM - Saturday 11:59 PM

The LDT Quality of Service can be controlled by either:

- Rekey Rate in MB/S
- Percentage of CPU usage
- Time schedule

Note

Rescheduling for off-hours and increasing CPU allocation are also best practices.

Troubleshooting

Common DFS(R) Configuration Mistakes

DFS(R) uses a staging area quota when processing replication tasks. If the allocated space is too small, performance is negatively impacted. An improperly sized staging area may also cause a replication loop among downstream nodes. Due to the intensive nature of encryption processing DFS data, you should evaluate your environment readiness. For more information about proper sizing techniques, see [How to Determine the Minimum Staging Area DFSR Needs for a Replicated Folder](#).

Review the following configuration mistakes as part of site readiness preparations:

Improper or Untested Seeding

To save downtime, administrators may choose to pre-seed new member replicas with DFS data before configuring all of the members in a replication group. In this manner, the initial synch consists of mostly delta changes rather than entire object transactions. See [Replacing DFSR Member Hardware or OS \(Part 2: Pre-seeding\)](#) for information on the advantages of pre-seeding.

Common issues include:

- ACL mismatch between source and target
- Changes were made to the files after they were copied to the new member
- No UAT testing was done to verify the pre-seeding process worked as expected

High DFS(R) Backlog

Customer DFS(R) deployments should be relatively up-to-date in replicating files across multiple nodes. High backlogs, especially over an extended period of time, mean that considerable amounts of data is out-of-sync. Unwanted conflict resolution may occur during these periods. Introducing encryption in this scenario would severely degrade performance and, likely require troubleshooting.

Hub Node – Single Point of Failure

The DFS primary active node is a single-point-of-failure in a Hub-and-Spoke topology. Fortunately, if the hub server goes down, all spoke servers retain the last-known-good data. All local changes are recorded locally and will not replicate until the primary node is back online. Spoke servers retain their own copies of their deltas and do not share them with others in the topology. You can confirm this risk, and confirm that offline backups are taken nightly to ensure optimal RTO (Recovery Time Objective).

Jet Database

DFS(R) maintains one Jet database per volume. As a result, placing all of your replicated folders on the same volume puts them all in the same Jet database. If that Jet database has a problem that requires repair or recovery of the database, all of the replicated folders on that drive are affected. It is better to spread replicated folders

around, using as many drives as possible to provide maximum uptime for the data.

Windows Server patch-level

Prepare for the deployment by checking for the latest software update for their DFS(R) servers. For replication, always make sure DFS(R) and NTFS are at least at the latest version listed. Proactively patching the DFS(R) servers is advisable, even if everything is running normally, as it will prevent your servers from being affected by a known issue.

DFS(R) as Backup

DFS(R) is not a bona fide backup solution. To be fully protected, customers must backup their data offline. DFS(R) was not designed as a backup solution. One of DFS(R)'s design goals is to be part of an enterprise backup strategy in that it gets your geographically distributed data to a centralized site for backup, restoration and archiving. Multiple members do offer protection from server failure; however, this does not protect your data from accidental deletions. Encrypting customer data should never occur without a full backup.

Stopping DFS(R) Replication

Sometimes, you may need to temporarily stop replication. Changing the replication status has consequences. The proper method is to set the schedule to no replication for the Replication Group in question. The DFS(R) service must be running to be able to read updates in the journal. Additionally, do not stop the DFS(R) service for long periods of time (days, weeks). Doing so may cause a journal wrap to occur (if many files are modified, added, or deleted in the meantime). DFS(R) will recover from the journal wrap, but in large deployments, this takes a long time and replication does not occur, or happens very slowly, during the journal wrap recovery. Monitor and prepare the environment prior to encryption.

File System Policies

Do not configure file system policies on replicated folders. The file system policy reapplies NTFS permissions at every Group Policy refresh interval. This can result in sharing violations because an open file does not replicate until the file is closed.

Backup Software

Having DFS data on other servers helps protect the data against a catastrophic failure, but does nothing to protect against data corruption. If a file becomes corrupted, the corruption gets replicated to other targets. Because the data should be identical on each DFS replica, backing up only one of the replicas is usually sufficient. Thales recommends that you backup at least the primary active node or hub.

Another important consideration regarding the backup process is that it is very critical to configure the backup software to not update the archival bit. The reason for this is that file replication is triggered by file version change or a modified time stamp. Therefore, there is a chance that updating the archive bit may cause issues that trigger a replication storm.

Troubleshooting DFS(R)

Unexpected problems may arise while encrypting replicated DFS data. Following are some of the common tasks recommended when configuring CipherTrust Transparent Encryption with DFS(R).

Encrypted Files Under DFSRPrivate Folder

In situations where the LDT Exclusion Registry key was deleted, and the LDT rekeyed files are under the

DFSRPrivate folder, following are the steps to reverse this.

On all nodes:

1. Stop DFS(R) service first on both nodes.
2. Add `LDTEExclusionGPList` to `vmmgmt/Parameters` with the path to `DFSRPrivate` if not already there.
3. Unguard the `DFSRPrivate` GuardPoint.
4. Open the command line as an administrator.
5. Copy the `DFSRPrivate` directory to a temporary backup, type:

```
xcopy "E:\DFSRTTest\DFSRPrivate" c:\backupOfDFSRPrivate /E /Y /H /Q /O /K
```

6. Delete all files in the `DFSRPrivate`, type:

```
del /S /Q E:\DFSRTTest\DFSRPrivate
```

7. Guard `DFSRPrivate` again.
8. Restart the DFS(R) service
9. Test replication of new files.

Double Encryption

A common cause for data corruption is that the data may have become double-encrypted. This can happen if existing encrypted data is written into a GuardPoint because it gets encrypted a second time. You can check for this by copying the data out of the GuardPoint into a clear location with a user who has 'apply_key' rights. Next, mount a GuardPoint on top of the copied data in the clear location using the same policy as the original GuardPoint. If the data then becomes viewable inside that newly mounted GuardPoint, this means that the data was double-encrypted.

To recover the data:

1. Copy all of the double encrypted data into a clear location.
2. Unguard the original GuardPoint.
3. Copy the data back into the original location that is now unguarded.
4. Re-guard the original GuardPoint. Data should now be viewable in the original GuardPoint.

Logs

Always download and parse the domain logs before doing anything else. Note the timestamp of certain DFS(R)-related error messages and compare them against similar timestamped log entries on the DFS servers. You may also run `agenthealth` on the DFS server to gather more extensive detail of the domain information.

The **agentinfo** support collection script resides in one of the following paths on systems where CTE agent is installed, depending on version:

```
C:\program files\vormetric\DataSecurityExpert\agent\vmd\bin  
C:\program files\vormetric\DataSecurityExpert\agent\shared\bin
```

The customers DFS environment may detail a lot of issues related to encrypting data, especially in relation to replicated, malformed or open handled data.

Different Keys for Different Folders

You may require that some folders be encrypted with a different key from others, perhaps due to a required SLA. Fencing the data is an excellent method for keeping different enterprise data separate. Normally, DFS nests target folders under one namespace. To encrypt the data, you would use a single key applied to the operational policy. However, if you want to use many keys, target folders must exist under a separate namespace. Windows 2012 and subsequent versions support multiple namespaces. Plan accordingly, allocating resources where necessary and staging target folders appropriately. This is also known as root scalability.

CTE Client Groups

Another consideration is the folders that are under DFS(R) control. If the folders and volumes are identical on all nodes of the DFS topology (i.e. F:\Data) then it is considered best practice to configure all nodes within a DFS topology under a single CipherTrust Client Group. This ensures consistency when apply Guard Paths across the DFS topology.

To create a client group:

1. Open the CTE application.
2. Click **Clients > Client Groups**.
3. Click **Create Client Group**. The Create Client Group dialog box displays.
4. Enter the following:
 - Client Group name: **DFSR**
 - Password creation method: **Generate**
 - Cluster Type: **Non-Cluster**
 - Client profile: The DFSR profile you created
 - Communication Enabled: Slide to activate
5. Click **Next**.
6. On the Add Clients window, select **Client group members** and click **Next**.
7. Select **Inherit Client Group Settings** and click OK.
8. On the Add GuardPoint page, click **Create GuardPoint**.

9. Select the DFSR Policy in the Policy section. Click **Browse** to browse to the host, select the DFSR mount point and DfsrPrivate folder, then click **Create**.
10. Confirm that the GuardPoints are correct and click **Next**.
11. On the confirmation page, verify all is correct and then click **Create**.

Mixed DFS(R) Topologies with Client Groups

In those environments where the DFS(R) folders are different on the individual nodes, then the GuardPoints must be configured for each DFS(R) node. Client groups cannot be deployed as the guard paths on each node will be different. In these cases, Thales recommends stopping the DFS services on this node before guarding the path. For a full Mesh topology, all of the nodes must be transformed and guarded at the same time. The last step after guarding the data is to [Start the DFS\(R\) services](#).

Encrypt Active Directory Database with Secure Start

This section describes encrypting a Microsoft Active Directory (AD) with the Secure Start feature. It contains the following topics:

- [Secure Start Overview](#)
- [Prerequisites](#)
- [Encrypt by Moving the AD Service into a Guarded Directory](#)
- [Encrypt Data in Place with Offline Transformation](#)
- [Encrypt with an LDT Transformation Policy](#)
- [Configure the Time Out Failure](#)
- [Recover a Server After it Loses Connection to the Key Manager](#)
- [Other Use Cases](#)
- [Best Practices for Encrypting and Protecting the AD Service](#)

Secure Start Overview

Secure Start offers data protection for applications which start earlier in the boot sequence than VMD (Vormetric Daemon). For example, the Microsoft Active Directory (AD) system service starts very early in the boot sequence. To determine if another application qualifies, contact Thales technical support.

Note

- Secure Start is included with CTE. You do not have to purchase it separately.

- Secure Start is supported on Windows Server 2008 R2 and later versions.
- When Secure Start is enabled, communication with CipherTrust Manager is required for security. After the Windows boot process completes, the CTE agent attempts to communicate with CipherTrust Manager for 2 minutes. If CipherTrust Manager cannot be reached after 2 minutes, then the CTE Agent initiates a reboot of the system.
- The challenge/response or password feature is disabled with secure boot GuardPoints.
- When Secure Start is enabled, communication with CipherTrust Manager is required for security. After the Windows boot process completes, the CTE agent attempts to communicate with CipherTrust Manager for 2 minutes. If CipherTrust Manager cannot be reached after 2 minutes, then the CTE Agent initiates a reboot of the system.
- The challenge/response or password feature is disabled with secure boot GuardPoints.

There are three methods for encrypting the AD directory:

- Encrypt by Moving the AD Service into a Guarded Directory
- Encrypt Data in Place with Offline Transformation
- Encrypt with an LDT Transformation Policy

Prerequisites

Prior to using Secure Start to guard your AD database:

1. Backup your AD database:
 - a. Navigate to **Administrative Tools**.
 - b. Click **Windows Server Backup**.
 - c. Click **Action > Backup Once**.
 - d. Follow the instructions in the Backup Wizard to create a backup of the server in a local drive.

Note

When the backup operation completes, it saves the server backup in *<backup drive>:\WindowsImageBackup\<BackupComputerName>*.

2. Perform a system state backup.
3. Obtain the Microsoft DSRM (Data Services Restore Mode) password.
4. Ensure that your AD database is not in `c:\Windows\NTDS`.

Warning

Do not put your AD database in `c:\Windows` or `c:\Program files`. Secure Start cannot encrypt or decrypt any files in those folders.

Encrypt by Moving the AD Service into a Guarded Directory

You can move the AD service into a directory protected by a standard or LDT production policy. This method does not require the initial data transformation step. When you move the AD service into this directory, CTE immediately encrypts the data with either policy.

Note

This step occurs when the system is in DSRM mode, so users have no access to the AD service.

Create the AD GuardPath directory

Create the directory in which the AD service will reside.

1. Log in to the Active Directory Server in DSRM mode using the DSRM password. User ID is Administrator.
2. Create a folder to which you will move the AD database.

Apply Secure Start GuardPoints to a Directory with CipherTrust Manager

To apply Secure Start GuardPoints in **CM**:

1. In the CipherTrust Manager Applications Page, click **CTE > Clients > <clientName>**.
2. Click **Create GuardPoint**.
3. In the Policy field, select a policy.
4. Set Type to **Auto Directory**.
5. Click **Browse**, navigate to, and select, the folder that you just created for the AD database.

6. Select the option: **Secure Start**.
7. Click **Create**.
8. Click **No** to the question, "Would you like to use these GuardPoint settings on another GuardPoint with a different path?" because you are only guarding the AD database.

Verify the Secure Start GuardPoint with CLI

After the policy is pushed to the Active Directory Server, verify the GuardPoints.

To verify the GuardPoints, type:

```
voradmin ss verify <GuardPoint_path>
Successfully completed the command verify
Success from kernel -Successfully verified the secure start GP
```

Move the AD Database into the Secure Start GuardPoint

Move your AD database from the default location (c:\windows\NTDS) to this newly created protected folder. To move the AD database:

1. In DSRM mode, login using the DSRM password. User ID is Administrator.
2. Start NTDSUTIL utility, type:

```
activate instance ntds
```

- a. Type:

```
files
```

3. Type:

```
move db to \<GuardPoint>
```

4. Type:

```
move logs to \<GuardPoint>
```

5. Exit NTDSUTIL utility.
6. Reboot the system into normal mode. The Active Directory Services automatically starts after rebooting.

Note

This step occurs when the system is in DSRM mode, so users have no access to the AD service.

Encrypt Data in Place with Offline Transformation

Encrypting the AD database with a standard (production), or offline policy is very similar to encrypting other data with a standard (production), or offline policy.

The advantage to encrypting data in place is that it saves space. When you copy/move a directory into a guarded directory, you will need twice as much space to store the data because you leave a copy of the data in the original folder, as a precaution, until the original directory has been successfully moved and encrypted. Once the data is transformed, then you can delete the directory that contains the decrypted/clear data.

Using this method, you perform an Initial Data Transformation using the **dataxform** command line utility. During this transformation, access to the GuardPoint data is blocked. After initial transformation, you remove the initial policy, and then apply a production policy, so users can access the data.

Note

This step occurs when the system is in DSRM mode, so users have no access to the AD service.

If your AD service is installed in the default directory, **C:\Windows\NTDS**, you must move it to another directory before you can encrypt it. See [Encrypt by Moving the AD Service into a Guarded Directory](#) for more information.

To encrypt the data:

1. In DSRM mode, login using the DSRM password. User ID is Administrator.
2. Create and apply a **dataxform** policy to the GuardPoint directory.
3. Run the **dataxform** command.
4. Remove the **dataxform** policy on the GuardPoint and replace it with a production policy.
5. Reboot out of DSRM mode.

Encrypt with an LDT Transformation Policy

Encrypting the AD database with an LDT policy uses the same steps as encrypting with a standard production policy. The only difference is that you select an LDT policy instead of a standard one. See [Encrypt by Moving the AD Service into a Guarded Directory](#) for more information for more information.

Note

If your AD service is installed in the default directory, `C:\Windows\NTDS`, you must move it to another directory before you can encrypt it.

Configure the Time Out Failure

During the initial access to a Secure Start GuardPoint, the CTE agent sets a timer. The default duration is 30 seconds, but you can configure the duration. Minimum duration is one second, maximum duration is 300 seconds.

Data inside the GuardPoint is accessible without CipherTrust Manager connectivity until the timeout is reached. VMD service activates and makes a secure connection to the CipherTrust Manager. After the VMD makes a secure connection, the agent verifies that it is connected to correct CipherTrust Manager. If the VMD fails to connect to the CipherTrust Manager, the timeout is reached, and if AD is installed, the agent shuts down the system for data security purposes.

Note

In DSRM mode, when the timeout occurs, CTE removes the keys from memory. However, CTE does not shut down the system.

In normal mode, CTE shuts down the AD server. For any other application, or if AD is not installed, Secure Start does not shut down the server. However, the data inside the GuardPoint becomes inaccessible until CipherTrust Manager connectivity is restored, or you issue a challenge/response, or password. After the timer has expired, CTE denies any further access to the Secure Start GuardPoint.

1. To configure the timeout duration in seconds, use the `voradmin ss settimeout <timeout>` command. For example:

```
voradmin ss settimeout 220
Successfully completed the command settimeout
Successfully set the Secure Start timeout value to 220 seconds
```

2. To verify the timeout duration, type:

```
voradmin ss gettimeout
Successfully completed the command gettimeout
Secure Start timeout value is set to 220 Seconds
```

Recover a Server After it Loses Connection to the Key Manager

Prerequisites

Before rebooting your active directory servers, ensure that CipherTrust Manager connectivity is strong. If it is not strong, restore the CipherTrust Manager connectivity.

Note

When trying to fix a CipherTrust Manager connectivity issue, you can log in to DSRM mode. In DSRM mode, there is no requirement to increase the timeout, because in DSRM mode, the AD system does not shut down after timeout expires.

DSRM Mode

The first method for recovering a server relies on manual CipherTrust Manager connection troubleshooting:

1. Boot into DSRM mode.
2. Attempt to resolve why the server is not connecting to the CipherTrust Manager.
3. Fix that CipherTrust Manager connectivity issue.
4. Reboot into normal mode.

Other Use Cases

Using Secure Start GuardPoints, you can also secure an SQL Server on Microsoft Azure in certain scenarios. SQL system services in Azure also boot earlier in the boot sequence than the VMD (Vormetric Daemon) agent service.

Note

To determine if another application qualifies, contact Thales technical support.

Boot a Windows Server in Azure

To move and guard the AD database, you must boot the AD server into DSRM mode.

To boot a Windows Server 2012/2016 Domain Controller into DSRM remotely in Azure:

Note

The Windows Server 2012/2016 domain controller must be running and accessible through Windows Remote Desktop.

1. Establish a Remote Desktop session on the domain controller.
2. Open an command prompt as Administrator and type:

```
> bcdedit /set safeboot dsrepair
```

3. Reboot the domain controller. The Remote Desktop session disconnects.
4. Wait a few minutes, then establish a new Remote Desktop session. The domain controller will be running in DSRM.
5. To reboot into normal mode, open an command prompt as Administrator and type:

```
> bcdedit /deletevalue safeboot
```

6. Reboot the domain controller.

Best Practices for Encrypting and Protecting the AD Service

Thales recommends the following best practices when using Secure Start with an AD service.

Access Control with Secure Start

User can setup a restricted access control policy with encryption to prevent the unauthorized access of AD database files. The restricted policy with Secure Start:

- Prevents a rogue user from logging into the system, and moving or copying the AD database files to another directory and tampering with it.
- Denies permissions, after you setup and guard files, so that no one can move a file from the guarded directory. Plus it restricts any other unwanted/unnecessary process or users from tampering with AD files.
- Provides permission for an authorized user who needs access to AD services and files.

Creating a Minimal Policy Required for AD with Access Control

When creating a normal, strict policy for access control, you must allow access to the following processes and directories for Active Directory.

Processes

```

secfsd.exe (C:\Program
Files\Vormetric\DataSecurityExpert\agent\secfs\ sec\bin\)
lsass.exe (C:\Windows\System32\)
vds.exe (C:\Windows\System32\)
vssvc.exe (C:\Windows\System32\)
wbengine.exe (C:\Windows\System32\)
ntoskrnl.exe (C:\Windows\System32\)

```

Users

NT AUTHORITY\SYSTEM

To create a minimal policy:

1. Create a User Set named **AD_Minimum_User_Set** with the following parameters:

ID	Uname	osDomains
1	SYSTEM	NT AUTHORITY

2. Create a Process Set named: **AD_Process_Set** with the following parameters:

ID	Directory	Base Name
1	C:\Program Files\Vormetric\ DataSecurityExpert\agent\secfs\ sec\bin	secfsd.exe
3	c:\Windows\ System32\ntoskrnl.exe	
4	c:\Windows\System32\vds.exe	
5	c:\Windows\System32\vssvc.exe	
6	c:\Windows\ System32\wbengine.exe	
7	c:\Windows\System32\lsass.exe	

3. Create a Security rule set with the following parameters:

Order	User	Process	Action	Effect	Browsing
1	AD_Minimum_U ser_Set	AD_Process_S et	all_ops	Audit, Permit, Apply	key
2				Audit, Deny	Yes

Creating a Restricted Policy in DSRM Mode

Create the following policy for the initial transformation of an AD database in DSRM mode. The policy allows access to the local administrator.

In DSRM mode, you use the **NTDSUTIL** utility to perform maintenance for an Active Directory.

To create a restricted policy:

1. Create a User Set named **AD_Minimum_User_Set** with the following parameters:

ID	uname	osDomains
1	SYSTEM	NT AUTHORITY
2	Administrator	localhost

2. Create a Process Set named: **AD_Process_Set** with the following parameters:

ID	Directory	Base Name
1	C:\Program Files\Vormetric\DataSecurityExpert\agent\secfs\sec\bin	secfsd.exe
2	c:\Windows\System32\	ntdsutil.exe
3	c:\Windows\System32\	ntoskrnl.exe
4	c:\Windows\System32\	vds.exe
5	c:\Windows\System32\	vssvc.exe
6	c:\Windows\System32\	wbengine.exe
7	c:\Windows\System32\	lsass.exe

3. Create a Security rule with the following parameters:

Order	User	Process	Action	Effect	Browsing
1	AD_Minimum_User_Set	AD_Process_Set	all_ops	Audit, Permit, Apply key	Yes
2				Audit, Deny	Yes

Guard Directories

The best practice for guarding a directory with a Secure Start GuardPoint is to:

1. Create a directory.

2. Guard that directory with a standard production or LDT policy. Follow the steps in [Apply Secure Start GuardPoints to a Directory with CipherTrust Manager](#).
3. Move the AD service into that directory.

Perform Subsequent System State Backups

After you move an AD service into a guarded directory, or out of a guarded directory:

1. Perform another system state backup.
2. Save this subsequent backup to a different location.

Exchange DAG

This section describes encrypting email databases using Microsoft Exchange database availability group (DAG). It contains the following topics:

- [Exchange DAG Overview](#)
- [CTE Policies for Exchange DAG](#)
- [Encrypting with LDT in an Exchange DAG Environment](#)
- [Encrypting with a Standard CTE Policy in the Exchange DAG Environment](#)
- [Decrypting with LDT in an Exchange DAG Environment](#)

Exchange DAG Overview

A DAG is a high-availability (HA) and data-recovery feature of the Microsoft Exchange Server. A DAG, which can consist of up to 16 Exchange mailbox servers, automates recovery at the database level after a database, server or network failure. You can now use CTE for Windows to encrypt Exchange DAG mailboxes.

You can encrypt the Exchange databases with a standard (offline) policy or an CTE-Live Data Transformation (LDT) policy. In an offline policy, users cannot access the database during initial data encryption. With an LDT policy, CTE encrypts the data while users and applications are accessing the files. LDT is used for Initial data transformation as well as transparent encryption and decryption.

Note

For more information about LDT and standard data transformation, see *CTE-Live Data Transformation with CipherTrust Manager*, *CTE-Live Data Transformation with Data Security Manager*, or the *CTE Data Transformation Guide*.

Supported Use Cases for CTE in an Exchange DAG Environment

CTE has been tested by Thales in the following scenarios:

- Initial data transformation of Exchange databases using either CTE-Live Data Transformation or standard data transformation.
- Transparent encryption or decryption of the Exchange database on DAG nodes.
- Key rotation using an LDT policy.
- Adding a new node to the Exchange DAG Environment.

Thales has only tested an Exchange DAG environment with two nodes, however, Thales does **not** anticipate any issues with using more than two nodes.

Thales also tested the following Exchange DAG operations during the above scenarios:

- Failover/Failback of databases from one node to another node and making both databases active on each node.
- Adding new Databases to the existing nodes.

Unsupported Use Cases

The following scenarios are not supported:

- Using different encryption keys on Exchange DAG nodes; both nodes must use the same encryption key
- The encryption of Exchange Binaries.
- Using nodes in a different subnet, data center, or site. (Thales is not testing this scenario, but we do not believe it will cause any issues.)

CTE Policies for Exchange DAG

The CTE policies you need depend on the type of encryption you will be using.

- When you use LDT encryption, you only need to create one Live Data Transformation policy. This policy will be used for both the initial data encryption and guarding the data in production. LDT requires a versioned CBC or CBC_CS1 key in order to perform automatic key rotation.
- When you use standard encryption, you need to create two policies:
 - The **initial encryption** policy specifies the current encryption key (if any) and the encryption key you want CTE to use when it encrypts the data. This policy also denies access to any other process trying to access the GuardPoint.

You apply the initial encryption policy when you first create the GuardPoint, and you leave it in place until all

of the data has been encrypted. After that, you remove this policy from the GuardPoint.

- The **production policy** specifies the same encryption key as the initial encryption policy along with any security rules you want to use to protect your data in production. After the initial encryption has completed, you apply the production policy to the GuardPoint and allow users and applications to access the now-protected data.

Note

There are no special CTE policy requirements for Exchange DAG with either LDT or Standard encryption. Therefore, you can use the same policies in an Exchange DAG environment that you use for any other CTE-protected directory.

The only special requirement for Exchange DAG is the guard path you specify when you create the GuardPoint. You must guard the Mailbox directory only. Do not guard above or below the Mailbox directory. For details, see [Encrypting with LDT in an Exchange DAG Environment](#) or [Encrypting with a Standard CTE Policy in the Exchange DAG Environment](#).

How you create these policies depends on the key manager that you are using. For details, see one of the following:

- [Creating a Policy for LDT Encryption with CipherTrust Manager](#)
- [Creating Policies for Standard Encryption with CipherTrust Manager](#)

Creating a Policy for LDT Encryption with CipherTrust Manager

When you use LDT encryption, you only need to create one policy. This policy will be used for both the initial data encryption and guarding the data in production. LDT requires a versioned CBC or CBC_CS1 key in order to perform automatic key rotation. For details, see the *CTE-Live Data Transformation with CipherTrust Manager* guide for the version of CTE that you are using.

1. Log into CipherTrust Manager and launch the **CTE** application.
2. In the left-hand menu bar, click **Policies**.
3. Click **Create Policy**.
4. For **Name**, make sure you use a name that clearly designates this as an LDT policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
5. For **Policy Type**, select **Live Data Transformation**.
6. Click **Next** to go to the Security Rules page. CipherTrust Manager should have automatically added a security rule for **Action: key_op**, **Effect: permit, applykey**. If this security rule is not there, click **Back** and make sure you have selected **Live Data Transformation** in the **Policy Type** field.
7. Enter any other security rules you want to use based on your production environment requirements. You can add as many security rules as you need to define who should have access to the protected data.

For more information about the type of rules you may want to use, or ways to exclude some data from encryption, see the *CTE-Live Data Transformation with CipherTrust Manager* guide for the version of CTE that you are using.

8. When you are done specifying your security rules, click **Next** to go to the Key Rules page.
9. Click **Create Key Rule** and enter the following information:
 - In the **Current Key Name** field, click **Select** to specify the current encryption key used for the data. If the data is unencrypted, specify `clear_key` as the encryption key.
 - In the **Transformation Key Name** field, click **Select** to specify the versioned encryption key you want to use to encrypt the data. When you are done, click **Add**.

Tip

You can also create a new key at this point if desired. For details on creating an encryption key, see your CipherTrust Manager documentation.

For example:

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule
	<code>clear_key</code>	VersionedKey-AES256	No ***

10. Click **Next** to go to the Confirmation page.
11. Verify your selections and click **Save** to save the policy.

Creating Policies for Standard Encryption with CipherTrust Manager

When you use standard encryption, you need to create two policies:

- The *initial encryption* policy specifies the current encryption key (if any) and the encryption key you want CTE to use when it encrypts the data. This policy also denies access to any other process trying to access the GuardPoint.

You apply the initial encryption policy when you first create the GuardPoint, and you leave it in place until all of the data has been encrypted. After that, you remove this policy from the GuardPoint.

- The *production* policy specifies the same encryption key as the initial encryption policy along with any security rules you want to use to protect your data. After the initial encryption has completed, you apply the production policy to the GuardPoint and allow users and applications to access the now-protected data.

Creating the Initial Encryption Policy

1. Log into CipherTrust Manager and launch the **CTE** application.
2. In the left-hand menu bar, click **Policies**.
3. Click **Create Policy**.
4. For **Name**, make sure you use a name that clearly designates this as an initial-encryption policy and not a production policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
5. For **Policy Type**, select **Standard**.
6. Enable the **Data Transformation** check box.
7. Click **Next** to go to the Security Rules page. CipherTrust Manager should have automatically added a security rule for **Action: key_op**, **Effect: permit, applykey**. If this security rule is not there, click **Back** and make sure you have enabled the **Data Transformation** check box.
8. Click **Create Security Rule** and do the following:
 - a. In the **Action** field, select **all_ops**.
 - b. In the **Effect** field, select **deny**.
 - c. Click **Add** to return to the Security Rules page.

You should now have two security rules, as shown:

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit, applykey	Yes
			all_ops	deny	Yes

9. Click **Next** to go to the Key Rules page.
10. Click **Create Key Rule**.
11. In **Current Key Name**, click **Select** to specify the current encryption key used for the data. If the data is unencrypted, specify **clear_key** as the encryption key. When you are done, click **Add**. For example:

Resource Set	Current Key Name
	clear_key

Tip

You can also create a new key at this point if desired. For details on creating an encryption key, see your CipherTrust Manager documentation.

12. Click **Next** to go to the Data Transformation page.
13. Click **Create Data Transformation Rule**.
14. In the **Transformation Key Name** field select the encryption key you want to use to encrypt the data. This key must match the one specified in the production policy you intend to apply to the GuardPoint after the data has been encrypted. For example, if you want to encrypt the data with the key CS1_AES256, you would specify the following transformation rule:

Resource Set	Transformation Key Name
	CS1_AES256

15. Click **Next** to go to the Confirmation page.
16. Verify your selections and click **Save** to save the policy.

Creating the Production Policy

1. Launch the **CTE** application.
2. In the left-hand menu bar, click **Policies**.
3. Click **Create Policy**.
4. For **Name**, make sure you use a name that clearly designates this as a production policy and not an initial encryption policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
5. For **Policy Type**, select **Standard**.
6. Click **Next** to go to the Security Rules page. Enter the security rules you want to use based on your production environment requirements. You can add as many security rules as you need to define who should have access to the protected data.
7. When you are done, click **Next** to go to the Key Rules page.
8. Click **Create Key Rule**.
9. In **Key Name** field, click **Select** to specify the encryption key used to transform the data in the initial encryption

policy. When you are done, click **Add**. For example:

Resource Set	Key Name
	CS1-AES256

10. Click **Next** to go to the Data Transformation page.
11. Click **Create Data Transformation Rule**.
12. In the **Transformation Key Name** field select the encryption key you want to use to encrypt the data. This key must match the one specified in the production policy you intend to apply to the GuardPoint after the data has been encrypted. For example, if you want to encrypt the data with the key CS1_AES256, you would specify the following transformation rule:

Resource Set	Transformation Key Name
	CS1-AES256

13. Click **Next** to go to the Confirmation page.
14. Verify your selections and click **Save** to save the policy.

Encrypting with LDT in an Exchange DAG Environment

Prerequisites

Before you can start the LDT data encryption process, you need to:

- Create or identify the CTE policy you want to use for data encryption. LDT uses a single Live Data Transformation policy for both initial encryption and subsequent rekeys, so the policy you use should have all the access control rules you want to use for your data when it is in production. For details, see [CTE Policies for Exchange DAG](#).
- Set your Quality of Service (QoS) settings. QoS enables administrators to manage and control LDT impact to application workloads by monitoring and controlling the use of host system resources, such as memory or I/O utilization, during data transformation.

For details about using LDT, see *CTE-Live Data Transformation with Data Security Manager* or *CTE-Live Data Transformation with CipherTrust Manager* for the version of CTE that you are using.

Procedure

1. In the **Exchange Admin Center**, make Exchange node 1 the primary node.

Make node 1 the active node and move all of the databases to that node.

2. Make all of the databases active on node 1.
3. Suspend all databases on node 2. Wait for 2-3 minutes for the database to finish with replication so the database will be suspended.

Warning

Make sure that all of the Exchange services in node 2 are down and not accessing the Exchange databases. All Exchange Services must be stopped, all databases must be suspended, and all data replication between the nodes must be stopped. Any file access on the node during the encryption process could cause data corruption.

4. When you are certain that all Exchange DAG services have been suspended on node 2, create the GuardPoints you want to use on node 2 with the appropriate Live Data Transformation policy. When you create the GuardPoints:
 - Make sure you are guarding each host individually. Do not assign the GuardPoints using a Host or Client Group because you only want these GuardPoints to exist on node 2 at this point.
 - **Important:** When you specify the guard path, only guard the Mailbox Database. Do *not* guard at a higher or lower directory. For example:
 - **Correct:** C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\
 - **Incorrect:** C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\Inbox\ — This is *not* correct because it's below the mailbox database directory.
 - Make sure that **Secure Start** is on for the GuardPoints.

The following example shows two correctly-specified GuardPoints in CipherTrust Manager:

Status	Policy	Protected Path	Type	Client Group	T	Rekey Status	Enabled	T
Active	Datashield...	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 2035273564	directory_auto	-		N/A	Yes	—
Active	Datashield...	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171	directory_auto	-		N/A	Yes	—

Live data transformation on node 2 begins as soon as the GuardPoints become active on node 2.

5. Wait until LDT has finished transforming the data in all GuardPoints on node 2.
6. In the **Exchange Admin Center**, go to the Exchange Database tab and **Resume** all Passive database copy

on node 2.

7. Wait for the server to move to the healthy state. If it does not, wait for some more time for the Content Index state to change to Healthy.

Warning

It may take a few minutes for the Exchange Service to resync. Monitor the Exchange logs on the system and make sure that replication is working. Make sure that database replication finishes and databases are in a healthy state before proceeding.

8. In the **Exchange Admin Center**, move all of the databases from node 1 to node 2.

Now the databases on node 1 are mounted as passive. All databases on node 2 are mounted as active.

9. Create the same GuardPoints on node 1 that you created on node 2.

Warning

- Make sure that all GuardPoints on node 1 are identical to those on node 2.
- You must guard the same databases with the same Live Data Transformation Policy and the same encryption key on both nodes.

Encrypting with a Standard CTE Policy in the Exchange DAG Environment

Prerequisites

Before you can start the standard (offline) data encryption process, you need to:

- Decide if you will be using the copy/restore method or the *CTEdatasync* utility in order to perform the initial encryption. For details about these methods and their specific benefits and limitations, see the *CTE Data Transformation Guide* for the version of CTE that you are using.
- Create or identify the encryption key that you want to use for the initial data encryption.
- Create or identify the Standard policies that you want to use for the initial data encryption and for protecting the data in production after it has been initially encrypted. For details, see [Creating Policies for Standard Encryption with CipherTrust Manager](#).

Procedure

1. In the **Exchange Admin Center**, make Exchange node 1 the primary node.

This means that node 1 is mounted as the active node and node 2 is mounted as the passive node.

2. Make all of the databases active on Exchange node 1.
3. Go to the Exchange Database tab and suspend all database on node 2.

Make sure that all of the exchange database services in node 2 are down and not accessing the Exchange databases. This process can take several minutes.

Warning

Make sure that all of the Exchange services in node 2 are down and not accessing the Exchange databases. All Exchange Services must be stopped, all databases must be suspended, and all data replication between the nodes must be stopped. Any file access on the node during the encryption process could cause data corruption.

4. When you are certain that all Exchange DAG services have been suspended on node 2, create the GuardPoints you want to use on node 2 with the appropriate Standard data transformation policy that you want to use for the initial data encryption. When you create the GuardPoints:
 - Make sure you are guarding each host individually. Do not assign the GuardPoints using a Host or Client Group because you only want these GuardPoints to exist on node 2 at this point.
 - **Important:** When you specify the guard path, only guard the Mailbox Database. Do not guard at a higher or lower directory. For example:
 - **Correct:** C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\
 - **Incorrect:** C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\Inbox\ — This is *not* correct because it's below the mailbox database directory.
 - Make sure that **Secure Start** is on for the GuardPoints.

The following example shows two correctly-specified GuardPoints in CipherTrust Manager:

Status	Policy	Protected Path	Type	Client Group	T	Rekey Status	Enabled	T
Active	Default...	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 2035273564	directory_auto	-		N/A	Yes	—
Active	Default...	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1089388171	directory_auto	-		N/A	Yes	—

- After all GuardPoints on node 2 have been enabled, run the `dataxform` utility for each GuardPoint:

```
dataxform --rekey --print_stat --gp <directory>
```

- After the data transformation is finished, unguard each mailbox on node 2, then re-guard each mailbox on node 2 with the appropriate Production policy.

Note

Use the same Key/Policy on both nodes.

- In the **Exchange Admin Center**, go to the Exchange Database tab and resume all databases on node 2.

After a few minutes, all nodes should become Healthy.

Warning

It may take a few minutes for the Exchange Service to resync. Monitor the Exchange logs on the system and make sure that replication is working. Make sure that database replication finishes and databases are in a healthy state before proceeding.

- In the **Exchange Admin Center**, try to move a database from node 1 to node 2. If the data move is successful this means that node 2 is mounted as the active node and node 1 is mounted as the passive node.
- Create the same GuardPoints on node 1 that you created on node 2. Make sure that all GuardPoints on node 1 are identical to those on node 2.

Warning

You must guard the same databases with the same Standard Policy and the same encryption

key on both nodes.

Decrypting with LDT in an Exchange DAG Environment

Prerequisites

- Make sure that the LDT state is set to REKEYED before unguarding.
- Make sure that all of the files inside the GuardPoint are at the same version of the key.
 - Run the LDT report to find the version:

```
voradmin ldt report <GuardPoint path> [<logfile>]
```

- Run the Key map report to find the version:

```
voradmin ldt key [report|map] <key_name, version> <GuardPoint path>
```

Procedure

1. Make sure that all of the Exchange services in node 2 are down and not accessing the Exchange databases.

Note

Suspension can take 2-3 Minutes.

2. In the **Exchange Admin Center**, make Exchange node 1 the primary node.

This means that node 1 is mounted as the active node and node 2 is mounted as the passive node.

3. Make all of the databases active on Exchange node 1.
4. Go to the Exchange Database tab and suspend all databases on node 2.
5. Unguard the database folders that you previously guarded on node 2.
6. Delete all of the metadata on all of the database folders on node 2, type:

```
voradmin ldt attr delete [<file name path> | <guard path>]
```

7. Guard with an LDT policy set for Encryption to Clear on node 2.

Note

You must clone the current version of the encryption key to use as the current key in the new LDT policy and `clear_key` as the transformation key.

8. Go to the Exchange Database tab and resume all databases on node 2.

Note

After a few minutes, the databases should become healthy automatically. If not, wait for the LDT process to decrypt the data. Make sure that all of the data is transformed back to clear and that the LDT state is set to **REKEYED**.

9. Move the database from node 1 to node 2.
10. Repeat this procedure for node 1.
11. After both nodes are rekeyed and transformed from encryption to clear, unguard them:
 - a. In the **Exchange Admin Center**, make Exchange node 1 the primary node.

This means that node 1 is mounted as the active node and node 2 is mounted as the passive node. 2. Make all of the databases active on Exchange node 1.
 - b. Go to the Exchange Database tab and suspend all databases on node 2.
 - c. Unguard the database folders that you previously guarded on node 2.

Warning

Always ensure that you are unguarding a passive node.

- d. Repeat this procedure for Node 1.

Storage Spaces Direct

This chapter describes how CTE integrates with Windows Storage Spaces Direct (S2D) hyper-converged clusters. It contains the following sections:

- S2D Overview
- Deployment Options
- Supported Use Cases

S2D Overview

S2D uses industry-standard servers with local-attached drives to create high-availability (HA) software-defined storage. S2D is included in Windows Server 2019 Data center and Windows Server 2016 Data center, both of which are supported by CTE.

S2D extends the stack of usable storage devices to storage devices such as SATA and SAS HDD's, SSD's and NVMe (Non-Volatile Memory Express) disks to create shared disk volumes. S2D supports clusters of a minimum of two nodes, and a maximum of 16 nodes and 400 drives. S2D aggregates the available storage into a Storage Pool.

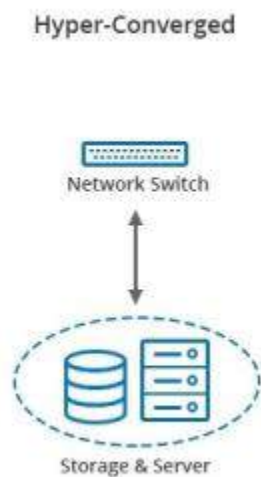
The hyper-converged deployment option runs virtual machines on the servers providing the storage.

A complete description of the S2D product, and instructions on how to set up the S2D environment is available on the Microsoft website at <https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/storage-spaces-direct-overview>

Deployment Options

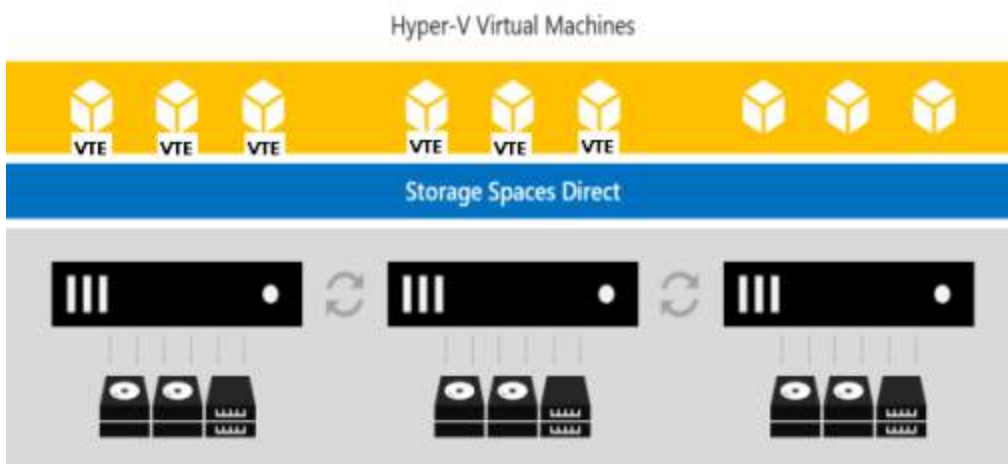
CTE supports S2D in a hyper-converged infrastructure where computing and storage components are in a single cluster as shown in the following figure.

Hyper-converged infrastructure



Hyper-converged with S2D and CTE virtual machines run on the servers providing the storage. In the following figure, CTE is installed inside 6 of the VMs to protect the data.

High-Level view of S2D



You can use all the capabilities of CTE to protect the data in the VMs in a S2D hyper-converged deployment. These capabilities are described in [Supported Use Cases](#).

Supported Use Cases

Thales tested only Hyper-converged deployments in the following scenarios.

- Initial Data Transformation of data using:
 - Live Data Transformation
 - Offline Data Transformation
- Transparent Encryption/Decryption of structure and unstructured data
- Key rotation using a Live Data Transformation policy

Using CTE with Quantum StorNext

This chapter describes how to configure CTE and Quantum StorNext devices to interoperate to allow CTE policies to apply to storage managed by Quantum StorNext.

This section contains the following topics:

- [Overview of using CTE with Quantum StorNext](#)
- [CTE and Quantum StorNext Compatibility](#)
- [Setting up CTE and Quantum StorNext Integration](#)

Overview of using CTE with Quantum StorNext

Quantum StorNext Fibre Channel-connected devices provide shared file access to third party storage for workstation clients and are optimized for simultaneous access to very large files such as video files. The Quantum StorNext file system is known as SNFS or by its older name, CVFS.

You can encrypt and control access to SNFS files with policies by installing CTE Agents on Windows clients that are configured for access to the SNFS file system. Some limitations apply to this integration, such as supported operating systems, supported SNFS features, concurrent read/write access by multiple clients, and GuardPoint settings (see the next section for more information about these limitations).

CTE and Quantum StorNext Compatibility

The following sections list the supported operating systems and CTE settings supported for use with Quantum StorNext file systems. Important unsupported configuration parameters are also listed.

Supported StorNext Server and Client Configurations

The CTE integration with SNFS file systems works only with certain SNFS versions, SNFS storage policies, and client operating systems.

Configuration parameter	Windows
StorNext (SNFS) operating system version	6.x
StorNext metadata controller (MDC) server OS type	Windows MDC supported
StorNext replication policy	Not supported
StorNext deduplication policy	Not supported
StorNext truncation	Supported
StorNext full and partial backup	Supported
StorNext expand file system	Supported
StorNext data migration	Supported
StorNext read-ahead cache	Disable for use with CTE
Client operating systems	Windows Server 2012 R2, Windows Server 2016
StorNext LAN client	DLC
StorNext mount method: locally mounted directory	Supported
StorNext mount method: CIFS	Not supported
StorNext mount method: NFS	Not supported

Supported GuardPoint and Key Settings for SNFS File Systems

When configuring CTE GuardPoints and keys for SNFS, keep in the mind the compatibility limitations listed in the following table.

Configuration element	Windows
Offline data transformation	Supported
Live Data Transformation (LDT)	Not supported
Key manager compatibility	See the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> or the <i>Compatibility Matrix for CTE</i>

Configuration element	Windows
	<i>Agent with Data Security Manager</i> for your CTE version
Guard unstructured data	Supported
Guard structured data	Not supported
GuardPoint type: Directory (including entire SNFS volume)	Supported
GuardPoint type: Raw device	Not supported
GuardPoint type: Block device	Not supported
GuardPoint mount option: manual guard	Not applicable
GuardPoint mount option: auto guard	Supported
GuardPoint mount option: automount	Not supported
AES-CBC key type	Supported
AES-CBC-CS1 key type	Not supported

Supported Concurrent Access Read/Write Scenarios

If you want to allow access by multiple clients (users) to CTE-protected SNFS files under the same GuardPoint, just read-only access is supported. StorNext file locking is not implemented in CTE, so there is currently no way to prevent concurrent conflicting writes to the same file. As a result, Thales does not support write access to the same GuardPoint from multiple clients.

To enable read access to the same GuardPoint from multiple clients, ensure that all clients are configured to use the same policy and key.

Configuration parameter	Windows
Read/write access from a single LAN client to a GuardPoint	Supported
Read/write access from two or more LAN clients to the same GuardPoint	Not supported
Read-only access from one, two, or more LAN clients to the same GuardPoint	Supported

Setting up CTE and Quantum StorNext Integration

For the most part, CTE integration with Quantum StorNext is the same as for any standard file system. The next section provides an overview of the steps involved in making CTE work with SNFS. Later sections provide more information about the steps that are new or differ significantly from a typical CTE setup.

Integration Task Overview

The table below provides an overview of the steps involved in setting up SNFS and CTE to work together. As noted in the table, some of these tasks are described in the documentation for your selected key manager. Some of these steps may need to be performed by other staff members at your organization if you have divided the

security administration duties as recommended by Thales and you don't have access to the key manager.

Task	Key configuration notes	For more information
Install and configure a Quantum StorNext MDC server for use with CTE	Disable the StorNext read-ahead cache. Only certain StorNext policies, features, and mount types are supported. See Supported StorNext Server and Client Configurations .	See Installing and Configuring a Quantum StorNext MDC Server for Use with CTE .
Install and configure Quantum StorNext clients for use with CTE	Only certain operating systems are supported. See Supported StorNext Server and Client Configurations .	See Installing and configuring Quantum StorNext DLC Clients for Use with CTE .
Create a domain for one or more SNFS hosts, or add them to an existing domain	No difference from standard CTE agent configuration.	See "Domain Management" in your key manager documentation.
Add the host to the key manager	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager documentation.
Install and register the CTE Agent on the host system	No difference in installation.	See Getting Started with CTE for Windows
Create encryption keys (optional)	AES-CBC-CS1 keys are not supported on Windows. See the note in Supported GuardPoint and Key Settings for SNFS File Systems .	See "Managing Keys" in your key manager documentation. For information about AES-CBC-CS1 keys, see Enhanced Encryption Mode .
Configure host groups containing one or more StorNext LAN clients (optional)	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager documentation.
Configure policies (including user, process, and resource sets) to control access or enable encryption	No difference from standard CTE agent configuration.	See "Configuring Policies" in your key manager documentation.
Configure one or more GuardPoints	Some GuardPoint settings are not supported. See Supported GuardPoint and Key Settings for SNFS File Systems .	See "Managing GuardPoints" in your key manager documentation

Installing and Configuring a Quantum StorNext MDC Server for Use with CTE

Install and configure a Quantum StorNext metadata controller (MDC) server using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Windows StorNext MDCs. Ensure that you configure the StorNext server to work with the settings supported by CTE as listed in [Supported StorNext Server and Client Configurations](#). For example, you must disable the StorNext read-ahead cache and only certain StorNext policies, features, and mount types are supported.

Installing and Configuring Quantum StorNext DLC Clients for Use with CTE

Install and configure Quantum StorNext DLC clients using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Windows StorNext DLCs.

Ensure that you configure DLC clients to work with the settings supported by CTE as listed in [Supported StorNext Server and Client Configurations](#). For example, only certain operating systems are supported.

Note

Just read-only access is supported if multiple StorNext LAN clients will access files in the same GuardPoint. For more information, see [Supported Concurrent Access Read/Write Scenarios](#).

Choosing a Mounting Method

There are two methods for mounting a StorNext file system on Windows in the StorNext Client Configuration application:

- Map to Drive Letter
- Map to Directory

Both methods are supported in CTE. If you mount the StorNext file system using the Map to Directory method, you must create the directory on the Windows computer before assigning that directory in the Client Configuration application. For example, the default Map to Directory folder is `C:\Mount\snfs1`. If you use that default, you must create `C:\Mount\snfs1` before mounting the StorNext file system in the Client Configuration application.

If you change mounting methods (drive letter to directory or vice versa), you may need to close and reopen Windows Explorer or reboot the computer for the change to take effect.

Installing the CTE Agent on Each StorNext LAN client

Install a CTE Agent on each computer that is set up as a StorNext LAN client and for which you want to set policies. For supported operating systems, see the table in [Supported StorNext Server and Client Configurations](#).

Use any installation method supported for your operating system. For details, see [Getting Started with CTE for Windows](#).

Setting up Microsoft DPM with CTE

Microsoft System Center Data Protection Manager (DPM) is a robust enterprise backup and recovery system that contributes to your BCDR (Business Continuity and Disaster Recovery) strategy by facilitating the backup and recovery of enterprise data. The DPM is a server-agent configuration setup. DPM agent is usually pushed over to the managed host by the DPM server. See [Data Protection Manager](#) for more information.

Prerequisite

If you are using LDT, create two new LDT policies. If you are not using LDT, create two new standard policies.

LDT No-View policy

1. In CipherTrust Manager, create a new LDT policy.
2. In that policy, create a process set called **DPM process** which contains the following directory and file:

Directory	File
C:\Program Files\Microsoft Data Protection Manager\DPM\bin	DPMRA.exe

3. Create a security rule for a noview key that contains the following criteria:

Order	Field	Value
1	Action	key_op
	Effect	permit, applykey
2	Process Set	DPM process
	Action	all_ops
	Effect	permit, audit
3	Action	all_ops
	Effect	permit, applykey, audit
4	Action	all_ops
	Effect	deny, audit

Note

Once you have the policy with the Process Set (No-View) rule applied, you can guard any directory, disk, or even a bare metal system backup and recovery, and the encrypted data is backed up.

LDT Open Policy

1. In CipherTrust Manager, create a new LDT policy.
2. Create a security rule for an open key, (where the backup job backs up decrypted data to clear format), that

contains the following criteria:

Order	Field	Value
1	Action	key_op
	Effect	permit, applykey
2	Action	all_ops
	Effect	permit, applykey, audit
3	Action	all_ops
	Effect	deny, audit

Note

If you use an open security rule, the backed up data is not encrypted. You can restore the backup job to a baseline directory. It is clear and readable.

Standard No-View Policy

1. In CipherTrust Manager, create a new standard policy.
2. In that policy, create a process set called **DPM process** which contains the following directory and file:

Directory	File
C:\Program Files\Microsoft Data Protection Manager\DPM\bin	DPMRA.exe

3. Create a security rule for a noview key, (where the backup job backs up the encrypted data), that contains the following criteria:

Order	Field	Value
1	Process Set	DPM process
	Action	all_ops
	Effect	permit, audit
2	Action	all_ops
	Effect	permit, applykey, audit
3	Action	all_ops

Order	Field	Value
	Effect	deny, audit

Note

Once you have the policy with the Process Set (No-View) rule applied, you can guard any directory, disk, or even a bare metal system backup and recovery, and the encrypted data is backed up.

Standard Open Policy

If you are not using LDT, create a standard policy:

1. In CipherTrust Manager, create a new standard policy.
2. Create a security rule for an open key, (where the backup job backs up decrypted data to clear format), that contains the following criteria:

Order	Field	Value
1	Action	all_ops
	Effect	permit, applykey, audit
1	Action	all_ops
	Effect	deny, audit

Note

If you use an open security rule, the backed up data is not encrypted. You can restore the backup job to a baseline directory. It is clear and readable.

Installing and Setting up CipherTrust Transparent Encryption

1. Copy dataset `E:\office2007_bk` folder to `E:\data` folder.
2. [Install Windows CTE agent](#) and register the host to your key manager.
3. Using the policy that you created in the Prerequisites section, guard the `to E:\data` folder

Installing and Configuring DPM

- Setup and configure [DPM v2022](#) for your Windows 2019 Server.

Setting up DPM

1. Start **System Center 2022 DPM Administrator Console**.
2. Add a DPM Storage pool volume:
 - a. Click **Management > Disk Storage > Add**.
 - b. Select an available volume (ex. F:) and click **OK**.
 - c. Click **Yes** to allow DPM to format the volume before adding it to storage pool.
3. Create a **Protection Group**.
 - a. Click **Protection > New** and click **Next**.
 - b. Select **Server** and click **Next**.
 - c. Select **All volumes > E:\data** and click **Next**.
 - d. Enter the **Protection group name** (ex. Protection Group 1) and click **Next**.
 - e. Click **Specify Short-term Goals** and click **Next**.
 - f. Choose **Replica Creation Method (Automatically or manual)** and click **Next**.
 - g. Select **Run a consistency check if a replica becomes inconsistent** or **Run a daily consistency check according to the following schedule** and click **Next**.
4. Click **Create Group**.
5. Set up **Recovery**:
 - a. Click **Recovery > Select Recover** and click **Next**.
 - b. In Review Recovery Selection, select **Recover to the original location** or **Recover to an alternate location** and then enter the alternate location in the field and click **Next**.
 - c. Select recovery type:
 - Create Copy
 - Skip
 - Overwrite

-
- d. Click **Recover** to start.

Validating Setup

1. Run **Windiff** to compare the original dataset **E:\office2007_bk** folder and recovery GuardPoint **E:\data** folder. Make sure that there is no data corruption.
2. View a text file from **E:\restore**. Make sure that you see cipher text.
3. Using the policy that you created in the Prerequisites section, guard the **E:\restore** folder.
4. View a text file from GuardPoint **E:\restore** folder and make sure that you see clear text.
5. Run **Windiff** again to compare GuardPoint **E:\data** folder and the recovery GuardPoint **E:\restore** folder. Make sure that there is no data corruption.
6. Update GuardPoint **E:\data** folder by adding, deleting or modifying a text file.
7. In **DPM**, click **Protection**, then right-click on **E:\data** and select **Create recovery point**.
8. Choose **Create a recovery point after synchronizing** and click **OK**.
9. Click **Recovery**, then right-click on **E:\data** and select **Show All Recovery Points**.
10. Select latest protection and click **Recovery > Select Recover** and click **Next**.
11. In Review Recovery Selection, select **Recover to the original location** or **Recover to an alternate location** and then enter the alternate location in the field. Click **Next**.
12. Select recovery type:
 - Create Copy
 - Skip
 - Overwrite
13. Click **Recover** to start.
14. Using the policy that you created in the Prerequisites section, guard the **E:\restore1** folder.
15. Run **Windiff** to compare the GuardPoint **E:\data** folder and recovery GuardPoint **E:\restore1\data** folder. Make sure that there is no data corruption.



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

CTE Terminology 3

CTE Terminology

The guide uses the following terminology:

Term	Description
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. Note: This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". For example, the default installation directory is <code>/opt/vormetric/DataSecurityExpert/agent/</code> for Linux and AIX, and <code>C:\Program Files\Vormetric\DataSecurityExpert\agent\</code> for Windows.
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.
key manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers CipherTrust Manager - a key manager for use with CTE.
host / client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.
GuardPoint	A device or directory to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.

After the CTE Agent has encrypted a device on a host, that device is called a GuardPoint. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.

- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you

can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Thales offers CipherTrust Manager, next generation key manager that supports most CTE for Linux and Windows features, most CTE features on Linux and Windows, and all CTE features on AIX.

CipherTrust Manager can be set up as either a security-hardened physical appliance or a virtual appliance. It provides access to the protected hosts through a browser-based, graphical user interface as well as an API and a CLI.

CipherTrust Manager versions support all CTE for Linux features *except* for the following:

- Container Security

Support for these features will be included in future releases of the CipherTrust Manager.

CipherTrust Manager versions 2.7 and higher support all CTE for Windows features *except* for the following:



CipherTrust Transparent Encryption

Version: v7.8.0 (latest)

30 January 2026

Contents

Learn Mode Tool 3

Learn Mode Tool

The Learn Mode Policy Builder (**lmpb**) is an OpenSource Python-based tool for processing the CipherTrust Transparent Encryption Learn Mode audit logs and generating security policies. Learn Mode allows access to guarded paths while logging access details. This tool helps administrators understand the gap between the current policy and the required policy and suggests corrective changes. The CipherTrust Manager and file system administrators are advised to review the changes before pushing them to CipherTrust Manager.

Note

This is an unsupported tool. Users are free submit request for enhancements and bugs, but Thales will not treat them as escalations.

Prerequisite

To collect logs that can be processed by the Learn Mode tool, enable the Learn Mode toggle on the CipherTrust Manager GUI while creating a policy.

Using the Learn Mode Tool

The Tool is available from the Thales site [CipherTrust Transparent Encryption Git repository](#).

After you have the logs for Learn Mode, proceed as follows:

1. Clone the CipherTrust Transparent Encryption Git repository.

```
git clone https://github.com/thalescpl-io/CipherTrust_Transparent_Encryption.git
```

2. Navigate to the `learn-mode-policy-builder` directory.

```
cd CipherTrust_Transparent_Encryption/tools/learn-mode-policy-builder
```

3. View the common commands.

```
./lmpb -h
```

Sample Output

```
usage: lmpb [-h] [--logdir LOGDIR] {log,policy} ...
```

```
positional arguments:
  {log,policy}
    log          cte learn mode logs
    policy       learn mode policy updates

options:
  -h, --help          show this help message and exit
  --logdir LOGDIR     log directory, defaults to /var/log/vormetric
```

Log Related Commands

```
./lmpb --logdir /home/logs/logs/ubu0/ log
```

Sample Output

```
positional arguments:
  {status,process,report}
    status          logs status
    process         process logs
    report          print log report in text format

options:
  -h, --help          show this help message and exit
```

View the log status:

```
./lmpb --logdir /home/logs/logs/ubu0/ log status
```

- If unprocessed logs are present, output displays as follows:

Sample Output

```
Found 181 log files in /home/logs/logs/ubu0/ with unprocessed entries.
Total size of unprocessed entries is 326.62 MB
```

- If all log files are already processed, output displays as follows:

Sample Output

```
No new log entries in /home/logs/logs/ubu0/ since Mon Dec 5 17:34:39 2022
```

- For processing the unprocessed log files, run the command:

```
./lmpb --logdir /home/logs/logs/ubu0/ log process
```

Sample Output

```
Successfully parsed all log files
Other log entries: 9, saved to /tmp/lmskip.340576
Log output saved as JSON at /home/logs/logs/ubu0/output.json
```

- Input the `output.json` file to Splunk to visualize the data.

```
cat /home/logs/logs/ubu0/output.json | nc 10.171.56.220 6666
```

In the example above, the SPLUNK server is configured to listen on port 6666 for `json_no_timestamp` events. The IP address `10.171.56.220` is an example.

- For viewing the log report:

```
./lmpb --logdir /home/logs/logs/ubu0/ log report
```

Sample Output

The output will show all processes, accesses performed by them, and the directories over which they have been performed.

```
Process: [ /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generi
c/build/env/linux/5.4.0-48-generic/build/scripts/genksyms/genksyms ]
Access: [ write_app read_file_sec_attr read_attr ]
Files/dirs: 20
-----
1 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/crypto/
sha2/.tmp_sha256.ver
2 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/vmcore/
cfg/.tmp_vm_cfg_upd.ver
3 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/vmcore/
cfg/.tmp_vm_cfg.ver
...
19 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/vmcor
e/common/.tmp_hexbin.ver
20 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/vmcor
e/ktctl/.tmp_vm_tc.ver
```

After the logs are processed by the Learn Mode policy builder tools, the following policy related commands can be run to list the existing policies or show updates recommended by the tool.

Policy Related Commands

```
./lmpb --logdir /home/logs/logs/ubu0/ policy
```

Sample Output

```
positional arguments:
  {list,show,upload}
  list                list policies with learn mode updates
  show                show learn mode policy updates
  upload              upload learn mode policy to CM

options:
  -h, --help          show this help message and exit
```

- List the policies with Learn Mode updates:

```
./lmpb --logdir /home/logs/logs/ubu0/ policy list
```

Sample Output

```
Policies with learn mode updates:

audit
```

- Show Learn Mode policy updates:

```
./lmpb --logdir /home/logs/logs/ubu0/ policy show
```

Sample Output

```
User sets:
  audit-uset-0
    [ audit ]
  audit-root-uset-1
    [ root ]

Process sets:
  audit-group-pset-0
    [ /sdb/anom/vtebuild/_obj_pem_64_perf_vor_ulinux_ubuntu20/mk/generate_messages_h.pl
      /usr/bin/dh_installdeb /usr/bin/dh_testroot /usr/lib/rpm/check-files /usr/lib/gcc/x86_64-linux-gnu/9/collect2 /usr/bin/ar /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/build/env/linux/5.4.0-48-generic/build/scrip
```

```

ts/mod/modpost /usr/bin/make /bin/gzip /usr/bin/fakeroot
...]

audit-group-pset-1
[ /bin/mount /bin/df /bin/chmod /usr/bin/make /bin/bash /bin/sh /usr/bin/fa
keroot /usr/bin/updatedb.mlocate /bin/ls ]

Resource sets:
audit-rset-0
[ /sdb/anom* ]

Security rules:
Rule 0
  User set      audit-root-uset-1
  Process set   audit-group-pset-1
  Resource set  audit-rset-0
  Action        d_chg_att,d_rd_att,d_rd_sec,f_rd,d_rd
  Effect        permit,applykey
Rule 1
  User set      audit-uset-0
  Process set   audit-group-pset-0
  Resource set  audit-rset-0
  Action        f_ren,d_chg_att,f_rm,d_rmdir,f_cre,d_rd_att,f_chg_sec,writ
e,f_rd_sec,d_rd_sec,f_rd_att,f_chg_att,f_wr,f_wr_app,f_rd,d_mkdir,d_rd
  Effect        permit,applykey

```

- Policies can be viewed based on users or processes. By default, it is user-based.

```
./lmpb --logdir /home/logs/logs/ubu0/ policy show --type user
```

- The output of policy show in this case will be sorted, based on user sets. This is the default setting for policy show command.

```
./lmpb --logdir /home/logs/logs/ubu0/ policy show --type process
```

- The output of policy show in this case will be sorted, based on process sets.

Sample Output

```

Learn mode updates for policy audit:

User sets:
  audit-uset-0

```

```

[ uset ]
audit-root-uset-1
[ root ]

Process sets:
...
audit-cc1-pset-10
[ /usr/lib/gcc/x86_64-linux-gnu/9/cc1 ]
audit-fixdep-pset-11
[ /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/build/ev
nv/linux/5.4.0-48-generic/build/scripts/basic/fixdep ]
...
Resource sets:
...
audit-rset-10
[ /sdb/anom/vtebuild/fspem* ]
audit-rset-11
[ /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/agent*
]
...
Security rules:
...
Rule 10
  User set      audit-uset-0
  Process set   audit-which-pset-26
  Resource set  audit-rset-2
  Action        d_rd_att
  Effect        permit,applykey
Rule 11
  User set      audit-root-uset-1
  Process set   audit-ls-pset-57
  Resource set  audit-rset-0
  Action        d_rd_att,d_rd,d_rd_sec
  Effect        permit,applykey
...

```

Uploading Policy to CipherTrust Manager

- To upload the policy to the CipherTrust Manager, run the command:

```

./lmpb --logdir /home/logs/logs/ora policy upload --policy-name LEARNMODE --typ
e user --upload-name learn-mode-policy --cmaddr IP-ADDR-OF-CM --username admin
--password PASSWORD

```

The above command will upload a policy to the CipherTrust Manager with modifications on top of the original policy suggested by the Learn Mode policy builder tool. Note that the above command will fail if the original policy is not found on the specified CipherTrust Manager.

CipherTrust Live Data Transformation

Zero-Downtime Encryption and Key Rotation

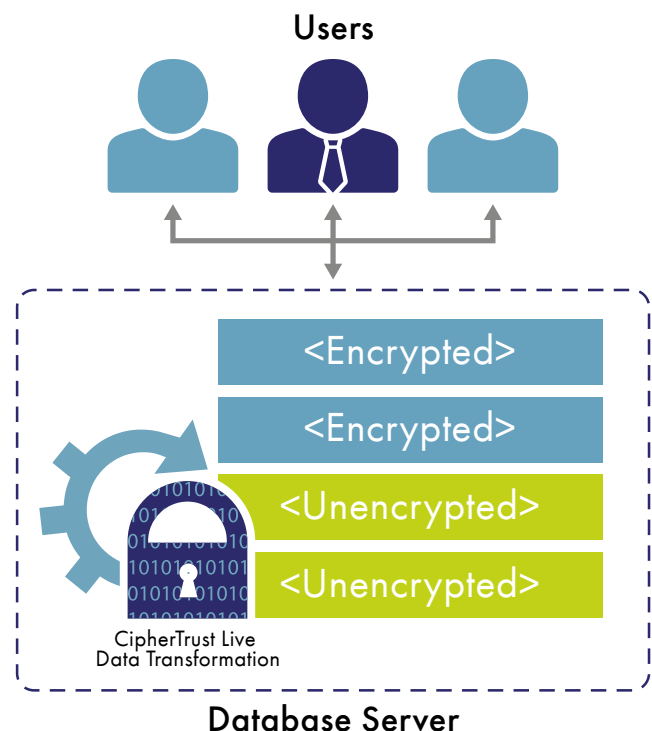


Apply encryption and access controls to files, volumes and Hadoop environments without taking applications offline

- Meet compliance requirements for encryption and access control without taking applications offline
- Expand encryption implementations with minimal impact on application operations and users
- Reduce the impact and cost of implementing encryption by eliminating encryption and rekeying downtime
- Accelerate recovery of data encrypted with older keys

The challenge: implementing and maintaining encryption with minimal application impact

In the face of escalating threats and compliance mandates, data encryption has become a best practice component integral to layered IT security strategies. For many, two critical barriers to the adoption of encryption with existing databases, files, and big data implementations have been:



A database protected with CipherTrust Transparent Encryption and Live Data Transformation enables non-disruptive initial encryption and simplified, more-compliant encryption key rotations. Users continue to work as usual while encryption is in process.

- **Initial encryption time.** With a large dataset, the process of initially converting from clear-data text to ciphertext has typically meant that applications using the data must be taken off-line during the initial conversion process. Even when state-of-the-art cloning and synchronization techniques are used, there is substantial downtime. For mission critical applications required to run with “five nines” of uptime, this can result in failure to meet SLAs, operational disruptions, and loss of revenue.
- **Downtime caused by re-keying of data sets.** Best practices and compliance regimes frequently require encrypted data be re-keyed with a new encryption key at specified intervals. This operation typically requires a large maintenance window, and results in the same disruption level as initially encrypting the data. The result is IT, compliance, and security teams face tough decisions about the balance between security, availability, uptime, and levels of compliance.

The solution: CipherTrust Live Data Transformation extension for CipherTrust Transparent Encryption

Customers have relied on CipherTrust Transparent Encryption for over a decade. It eliminates many of the challenges associated with implementing encryption in an enterprise. CipherTrust Transparent Encryption breaks down data security silos, encrypts both structured databases and unstructured files, centralizes key management across the enterprise, and provides privileged user access controls and detailed data access audit logs that integrate with major Security Information and Event Management (SIEM) systems.

CipherTrust Transparent Encryption operates with minimal disruption, effort, and cost. Its transparent architecture enables security organizations to implement encryption without changing application, networking, or storage architectures.

CipherTrust Live Data Transformation builds on these advantages, offering patented capabilities that deliver breakthroughs in availability, resilience, and efficiency.

Delivering patented capabilities for deploying and maintaining encryption without downtime

- **Zero-downtime encryption deployments.** CipherTrust Live Data Transformation enables administrators to encrypt data with minimal downtime or any disruption to users, applications, or workflows. Users need to plan minimal application downtime to configure Live Data Transformation policies, after which applications continue to work with no downtime while encryption is in progress.
- **Seamless, non-disruptive key rotation.** To address compliance requirements and best practices, Live Data Transformation enables organizations to perform key rotation without having to duplicate data or take associated applications offline.

Key features

CipherTrust Transparent Encryption agents operate on Windows and Linux servers that store or access any data that needs to be secured and controlled. CipherTrust Live Data Transformation is enabled in the CipherTrust Manager by applying a license for each agent on which it will operate. CipherTrust Live Data Transformation licenses can be enabled at any time, at which point users can secure their mission-critical data without any disruption or maintenance windows.

Live Data Transformation includes features to assure that its operation is transparent to users and applications independent of the size and scale of the deployment:

- **CPU resource management.** Encrypting large data sets can require significant CPU resources for an extended time. Live Data Transformation provides sophisticated CPU management rules to enable administrators to balance resources between encryption and other CPU operations upon which users depend. For example, a resource management rule can define that, during business hours, encryption can consume up to 10% of system CPU, reserving the balance of 90% for users. Then, the rule can define that on nights and weekends, encryption can consume 70%, when there are lower user demands on CPU resources. And encryption and re-keying processes can be manually paused and resumed as desired.
- **Versioned backups and archives.** With key versioning management, CipherTrust Live Data Transformation ensures efficient backup and archive recovery to enable more immediate access. In a data recovery operation, archived encryption keys, recovered from the CipherTrust Manager, are automatically applied to an older data set. Restored data is encrypted with the current cryptographic keys.
- **Resiliency.** By storing encryption metadata with the target files or database volumes, CipherTrust Live Data Transformation is resilient in the face of storage failures, system issues, or network downtime. Any interrupted encryption process will seamlessly recover without having to have the entire process restarted. This architecture ensures that data is never corrupted, no matter how, when, or where a failure occurs, and, scales with the size of the file system, rather than being limited by design.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

CipherTrust Live Data Transformation

Zero-Downtime Encryption and Key Rotation

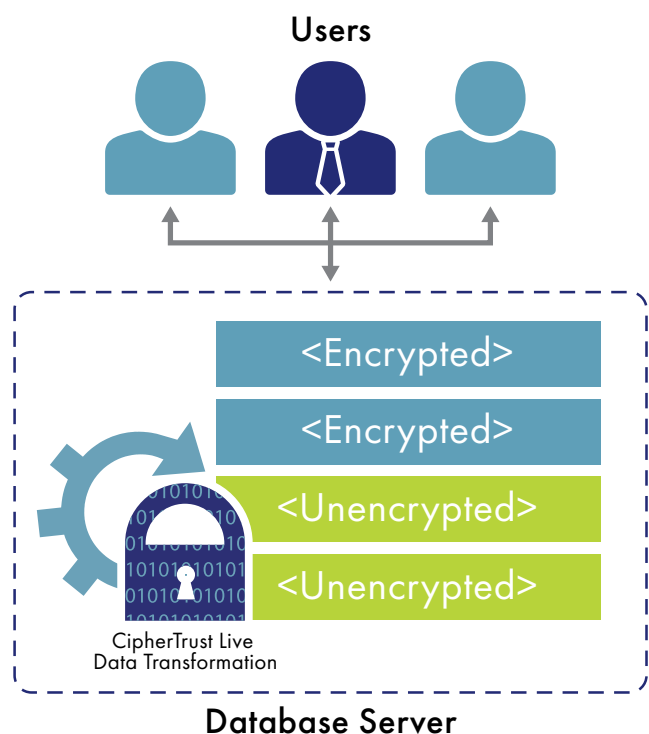
Apply encryption and access controls to files, volumes and Hadoop environments without taking applications offline

- Meet compliance requirements for encryption and access control without taking applications offline
- Expand encryption implementations with minimal impact on application operations and users
- Reduce the impact and cost of implementing encryption by eliminating encryption and rekeying downtime
- Accelerate recovery of data encrypted with older keys

The challenge: implementing and maintaining encryption with minimal application impact

In the face of escalating threats and compliance mandates, data encryption has become a best practice component integral to layered IT security strategies. For many, two critical barriers to the adoption of encryption with existing databases, files, and big data implementations have been:

- **Initial encryption time.** With a large dataset, the process of initially converting from clear-data text to ciphertext has typically meant that applications using the data must be taken off-line during the initial conversion process. Even when state-of-the-art cloning



A database protected with CipherTrust Transparent Encryption and Live Data Transformation enables non-disruptive initial encryption and simplified, more-compliant encryption key rotations. Users continue to work as usual while encryption is in process.

and synchronization techniques are used, there is substantial downtime. For mission critical applications required to run with “five nines” of uptime, this can result in failure to meet SLAs, operational disruptions, and loss of revenue.

- **Downtime caused by re-keying of data sets.** Best practices and compliance regimes frequently require encrypted data be re-keyed with a new encryption key at specified intervals. This operation typically requires a large maintenance window, and results in the same disruption level as initially encrypting the data. The result is IT, compliance, and security teams face tough decisions about the balance between security, availability, uptime, and levels of compliance.

The solution: CipherTrust Live Data Transformation extension for CipherTrust Transparent Encryption

Customers have relied on CipherTrust Transparent Encryption for over a decade. It eliminates many of the challenges associated with implementing encryption in an enterprise. CipherTrust Transparent Encryption breaks down data security silos, encrypts both structured databases and unstructured files, centralizes key management across the enterprise, and provides privileged user access controls and detailed data access audit logs that integrate with major Security Information and Event Management (SIEM) systems.

CipherTrust Transparent Encryption operates with minimal disruption, effort, and cost. Its transparent architecture enables security organizations to implement encryption without changing application, networking, or storage architectures.

CipherTrust Live Data Transformation builds on these advantages, offering patented capabilities that deliver breakthroughs in availability, resilience, and efficiency.

CipherTrust Transparent Encryption and Live Data Transformation are available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

Delivering patented capabilities for deploying and maintaining encryption without downtime

- **Zero-downtime encryption deployments.** CipherTrust Live Data Transformation enables administrators to encrypt data with minimal downtime or any disruption to users, applications, or workflows. Users need to plan minimal application downtime to configure Live Data Transformation policies, after which applications continue to work with no downtime while encryption is in progress.
- **Seamless, non-disruptive key rotation.** To address compliance requirements and best practices, Live Data Transformation enables organizations to perform key rotation without having to duplicate data or take associated applications offline.

Key features

CipherTrust Transparent Encryption agents operate on Windows and Linux servers that store or access any data that needs to be secured and controlled. CipherTrust Live Data Transformation is enabled in the CipherTrust Manager by applying a license for each agent on which it will operate. CipherTrust Live Data Transformation licenses can be enabled at any time, at which point users can secure their mission-critical data without any disruption or maintenance windows.

Live Data Transformation includes features to assure that its operation is transparent to users and applications independent of the size and scale of the deployment:

- **CPU resource management.** Encrypting large data sets can require significant CPU resources for an extended time. Live Data Transformation provides sophisticated CPU management rules to enable administrators to balance resources between encryption and other CPU operations upon which users depend. For example, a resource management rule can define that, during business hours, encryption can consume up to 10% of system CPU, reserving the balance of 90% for users. Then, the rule can define that on nights and weekends, encryption can consume 70%, when there are lower user demands on CPU resources. And encryption and re-keying processes can be manually paused and resumed as desired.
- **Versioned backups and archives.** With key versioning management, CipherTrust Live Data Transformation ensures efficient backup and archive recovery to enable more immediate access. In a data recovery operation, archived encryption keys, recovered from the CipherTrust Manager, are automatically applied to an older data set. Restored data is encrypted with the current cryptographic keys.
- **Resiliency.** By storing encryption metadata with the target files or database volumes, CipherTrust Live Data Transformation is resilient in the face of storage failures, system issues, or network downtime. Any interrupted encryption process will seamlessly recover without having to have the entire process restarted. This architecture ensures that data is never corrupted, no matter how, when, or where a failure occurs, and, scales with the size of the file system, rather than being limited by design.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

CipherTrust Transparent Encryption

Ensure the protection of sensitive data with advanced data-at-rest encryption, robust access controls, and comprehensive audit logging for data access. Achieve compliance and adhere to best practices with a reliable hardware-accelerated encryption solution that secures files, volumes, and connected cloud storage across physical, virtual, and cloud environments.

Challenge: Securing Sensitive Data Across Changing Environments and Increasing Threats

Safeguarding sensitive data requires much more than just securing a data center's on-premises databases and files. The typical enterprise today uses three or more IaaS or PaaS providers, along with fifty or more SaaS applications, big data environments, container technologies, and their own internal virtual environments and private clouds.

To further complicate the problem, cyberattacks have grown in sophistication and power. New compliance and regulatory mandates around protection of sensitive information keep on coming, and existing regulations have become more stringent. SAS PCE Enterprise IAM can seamlessly integrate with existing infrastructure and applications, minimizing disruptions and ensuring smooth operations.

Solution: CipherTrust Transparent Encryption

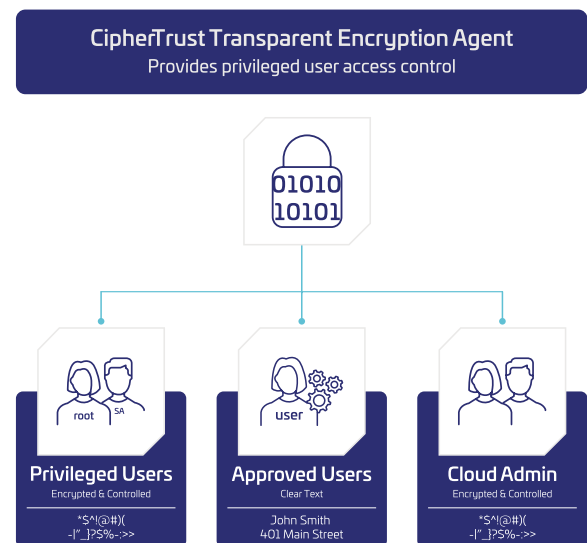
CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control, and detailed data access audit logging that helps organizations meet compliance and best practice requirements for protecting data, wherever it resides. The FIPS 140-3 L1 certified CipherTrust Transparent Encryption agent resides at the operating file-system or device layer, and encryption and decryption is transparent to all applications that run above it. CipherTrust Transparent Encryption provides rich access controls, which allow organizations to determine who can access data, when they can access it, and what type of access they have.

Key Requirements for Securing Sensitive Data-at-Rest:

- **Compliance and best practices:** Meet encryption, access control, and data access logging requirements with a proven, hardware-accelerated encryption solution. Secure files, volumes, and linked cloud storage, while enabling detailed access controls and audit logging across physical, virtual, and cloud environments.
- **Simple, scalable deployment:** Easily deploy a solution that scales across multiple clouds, on-premises, big data, and container environments. Centralized key management, encryption,

and access policies ensure streamlined operations.

- **Privileged user access control:** Protect sensitive data by enabling administrators to continue their work while preventing unauthorized access by potential threats among users and groups.



- **Actionable security insights:** Utilize detailed, actionable security event logs to gain valuable insights into file access activities and quickly detect and stop potential threats.
- **Broad platform support:** Secure both structured and unstructured data across Linux, FreeBSD, AIX, and Windows systems. Extend transparent encryption and access controls to data stored in S3 buckets.
- **No downtime for encryption and re-keying:** Use the Live Data Transformation connector to eliminate downtime during initial encryption and re-keying processes. This unique feature sets CipherTrust Transparent Encryption apart from other solutions.

Key Features

Transparent data protection: Continuously enforces file-level encryption that protects against unauthorized access by users and processes and creates detailed data access audit logs of all activities without requiring changes to applications, infrastructure, systems management tasks, or business practices.

Seamless and easy to deploy: CipherTrust Transparent Encryption agents are deployed on servers at the file system or volume-level and support both local disks as well as cloud storage environments, such as Amazon S3 and Azure Files.

Define granular access controls: Apply granular, least-privileged user access policies that protect data from external attacks and

misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop and containers. Controls also include access by process, file type, time of day, and other parameters.

High-performance hardware accelerated encryption: CipherTrust Transparent Encryption only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs.

Comprehensive security intelligence: Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance requirements, but also enable data security analytics.

In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.

Broadest system and environment support: The agent is available for a broad selection of Windows, Linux, and AIX platforms, and can be used in physical, virtual, cloud, Kubernetes and big data environments, regardless of the underlying storage technology.

Advanced Security Benefits

Integration with cloud and container environments: Protects data in dynamic cloud and container environments.

Key rotation: Automatically rotates encryption keys to enhance security.

Data destruction: Ensures sensitive data is permanently erased when no longer needed.

Zero-downtime data transformation: Live Data Transformation option eliminates the downtime required for initial encryption and scheduled rekeying operations. This patented technology allows for databases or files to be encrypted or re-keyed with a new encryption key while the data is in use without taking applications off-line.

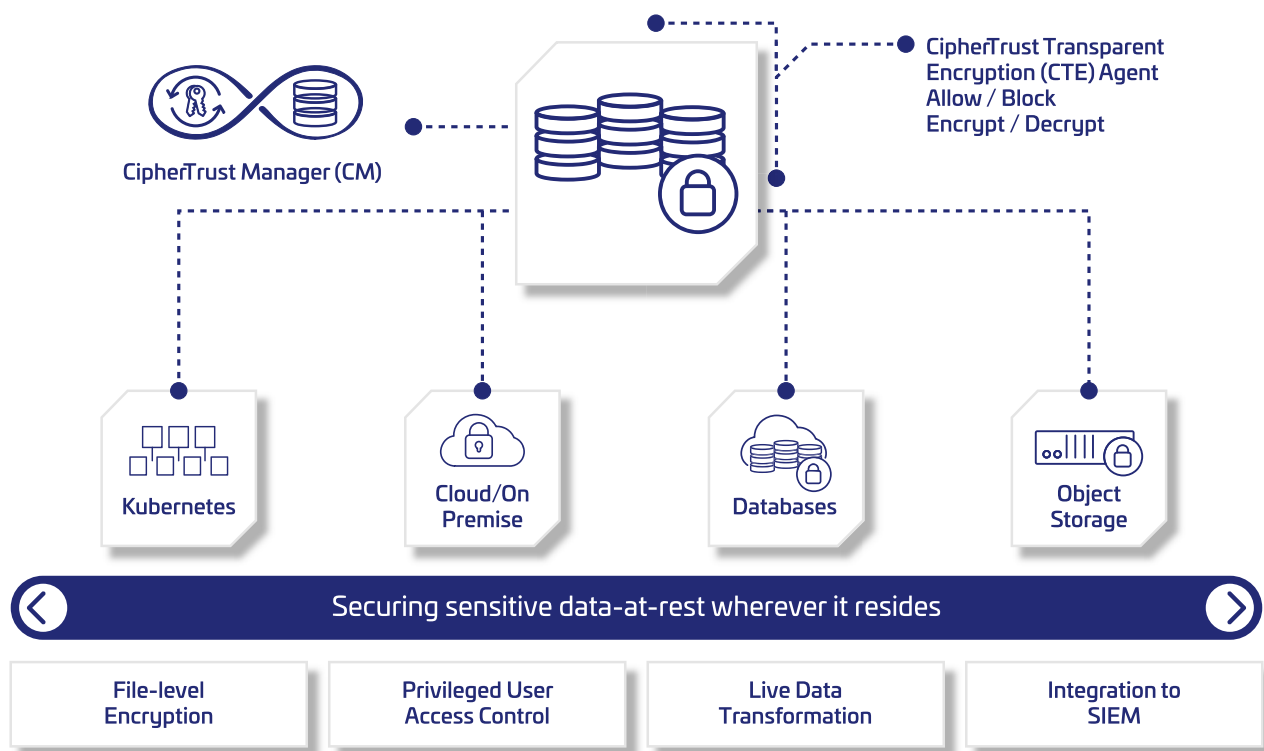
SAP HANA and teradata qualified: SAP and Teradata have qualified CipherTrust Transparent Encryption with SAP HANA and Teradata database respectively to deliver data encryption, key management, privileged user access control, and granular file access audit logs

CipherTrust transparent encryption userspace: Provides scalable and robust file encryption solution based on Linux FUSE that is not affected by kernel upgrades on Linux servers.

Solution Architecture

Deployment consists of CipherTrust Transparent Encryption connectors and CipherTrust Manager appliances. Policy and key management is centralized at the CipherTrust Manager. The CipherTrust Manager is available as a FIPS 140-2 Level 1 or FIPS 140-2 Level 3 with HSM compliant appliance.

Data-at-rest security wherever it resides



Benefits of CipherTrust Transparent Encryption:

Enhanced Data Security:

Data-at-rest encryption: Protects sensitive data from unauthorized access, even if the underlying storage is compromised.

Centralized key management: Manages encryption keys securely, reducing the risk of key exposure.

Privileged user access control: Controls access to encrypted data, even for privileged users, ensuring data confidentiality.

Improved Compliance:

Detailed data access audit logging: Provides a comprehensive audit trail, helping organizations meet compliance requirements such as PCI DSS, HIPAA/HITECH, and GDPR.

Strong data protection: Enhances overall data security posture, reducing the risk of data breaches and regulatory fines.

Operational Efficiency:

Transparent encryption: Encrypts data without requiring changes to applications or user workflows, minimizing disruption to business operations.

Scalability: Easily scales to protect large volumes of data across diverse environments, simplifying management.

Flexible deployment: Supports various deployment options to adapt to different use cases.

Additional Benefits:

Integration with cloud and container environments: Protects data in dynamic cloud and container environments.

Key rotation: Automatically rotates encryption keys to enhance security.

Data destruction: Ensures sensitive data is permanently erased when no longer needed.

By leveraging these benefits, CipherTrust Transparent Encryption empowers organizations to safeguard their sensitive data, meet compliance obligations, and maintain operational efficiency.

CipherTrust Data Security Platform

CipherTrust Transparent Encryption is part of the CipherTrust Data Security Platform. Featured in Gartner's Market Guide to Data Security Platforms, CipherTrust Data Security Platform is an integrated set of data-centric solutions that remove complexity from data security, accelerate time to compliance, and secure cloud migrations.

The CipherTrust Platform unifies data discovery, classification, data protection, and centralized management for keys and secrets into a single platform. This results in fewer resources dedicated to security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored, or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

CipherTrust Transparent Encryption



Challenge: securing sensitive data across changing environments and increasing threats

Safeguarding sensitive data requires much more than just securing a data center's on-premises databases and files. The typical enterprise today uses three or more IaaS or PaaS providers, along with fifty or more SaaS applications, big data environments, container technologies, and their own internal virtual environments and private clouds.

To further complicate the problem, cyber-attacks have grown in sophistication and power. New compliance and regulatory mandates around protection of sensitive information keep on coming, and existing regulations have become more stringent.

Solution: CipherTrust Transparent Encryption

CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control, and detailed data access audit logging that helps organizations meet compliance and best practice requirements for protecting data, wherever it resides. The FIPS 140-2 compliant CipherTrust Transparent Encryption agent resides at the operating file-system or device layer, and encryption and decryption is transparent to all applications that run above it. CipherTrust Transparent Encryption provides rich access controls, which allow organizations to determine who can access data, when they can access it, and what type of access they have.

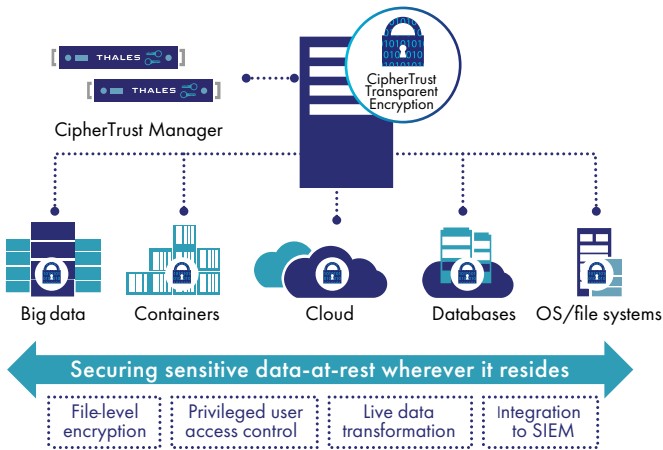
CipherTrust Transparent Encryption is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

Securing sensitive data-at-rest wherever it resides

- Meet compliance and best practice requirements for encryption, access control, and data access logging using a proven hardware accelerated encryption solution, that secures files, volumes and linked cloud storage while enabling access control and data access audit logging in physical, virtual, and cloud environments.
- Deployment is simple, scalable and fast with centralized key management, encryption, and access policies that reach across multiple clouds, on-premises, and within big data, and container environments.
- Easily implement privileged user access controls to enable administrators to work as usual but protect against users and groups that are potential threats to data.
- Leverage detailed, actionable security event logs that provide unprecedented insight into file access activities to identify and stop threats faster.
- Broadest platform support in the industry. Protects structured and unstructured data accessed by Linux, AIX and Windows systems, as well as transparent encryption and access control for data residing in S3 buckets.

- Eliminate the downtime required for initial encryption and re-keying operations by adding the Live Data Transformation option. There is no other data encryption solution that offers this unique capability.

CipherTrust Transparent Encryption



Key advantages

Transparent data protection. Continuously enforces file-level encryption that protects against unauthorized access by users and processes and creates detailed data access audit logs of all activities without requiring changes to applications, infrastructure, systems management tasks, or business practices.

Seamless and easy to deploy. CipherTrust Transparent Encryption agents are deployed on servers at the file system or volume-level and support both local disks as well as cloud storage environments, such as Amazon S3 and Azure Files.

Define granular access controls. Apply granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop and containers. Controls also include access by process, file type, time of day, and other parameters.

High-performance hardware accelerated encryption. CipherTrust Transparent Encryption only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs.

Comprehensive security intelligence. Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance requirements, but also enable data security analytics.

In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.

Broadest system and environment support. The agent is available for a broad selection of Windows, Linux, and AIX platforms, and can be used in physical, virtual, cloud, container, and big data environments, regardless of the underlying storage technology.

Advanced security

Zero-downtime data transformation. Live Data Transformation option eliminates the downtime required for initial encryption and scheduled rekeying operations. This patented technology allows for databases or files to be encrypted or re-keyed with a new encryption key while the data is in use without taking applications off-line.

Advanced access controls for big data (Hadoop). When implemented in Hadoop environments, access controls are extended to Hadoop users and groups.

SAP HANA qualified. SAP has qualified CipherTrust Transparent Encryption with HANA v2.0 to deliver data encryption, key management, privileged user access control, and granular file access audit logs.

CipherTrust Transparent Encryption UserSpace. Provides scalable and robust file encryption solution based on Linux FUSE that is not affected by kernel upgrades on Linux servers.

Solution architecture

Deployments consist of CipherTrust Transparent Encryption agents and CipherTrust Manager appliances. Policy and key management is centralized at the CipherTrust Manager. The CipherTrust Manager is available as a FIPS 140-2 level 1, 2 or 3 compliant appliance.

CipherTrust Data Security Platform

CipherTrust Transparent Encryption is part of the CipherTrust Data Security Platform. The CipherTrust platform unifies data discovery, classification, data protection, and provides unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations, and reduces risk across your business. You can rely on Thales CipherTrust Data Security Platform to help you discover, protect and control your organization's sensitive data, wherever it resides.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

CipherTrust Transparent Encryption

CTE Performance With Oracle TPCC Benchmark

Documentation Version 1

May 13, 2022



All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2009-2022 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Contents

Chapter 1: Introduction	1
Summary of Activity	1
Terminology	1
Chapter 2: Methodology	2
About TPC-C	2
Metrics	3
Chapter 3: ASM Storage	4
Only TPCC tablespace guarded	4
Conclusion	5
Appendix A: Tools Used	6
Infrastructure	6
Machine Details	6
Oracle Server Details	6
Filesystem Storage	6
ASM Storage	6
Application versions	6
Other systems	7
HammerDB client	7
Jenkins	7

Chapter 1: Introduction

This document details the CTE Linux performance using the Oracle TPCC benchmark.

Summary of Activity

This test used the industry wide OLTP benchmark standard Transaction Processing Performance Council (TPC-C) (<http://www.tpc.org/tpcc/detail5.asp>), which was executed using the HammerDB benchmark tool (<https://hammerdb.com/>). A baseline benchmark on an unguarded schema was first created and then compared against a benchmark run on the same schema protected by a CTE GuardPoint.

For establishing the baseline, several combinations of numbers of warehouses and number of virtual users was tried in order to arrive at a combination that provided optimum saturation, which was 500 warehouses driven by 125 virtual users.

The common approach was used to benchmark both SecFS as well as SecVM performance, using Oracle with filesystem and ASM storage respectively.

The test systems and the benchmarking system were hosted on a dedicated VMware ESX server which had no other machines. The benchmark tablespaces only used SSD storage. All benchmark runs were conducted for an hour after first rebooting the test machines. The details of the test systems are in the appendices.

Terminology

- **Redo logs**

A set of files used by Oracle to perform recovery in case of failures. These files store all changes made to the database as they occur. When the redo log files reach maximum capacity, they can be archived through an Oracle tunable parameter. However, this affects performance, so Thales did not archive log files while we were conducting the benchmark testing.

- **Undo logs**

These files contain information which can be used by Oracle to save the changes made during a transaction.

- **Temporary tablespace**

Used by Oracle for storing temporary data which is generated when SQL statements perform sort operations.

Chapter 2: Methodology

The HammerDB benchmark tool was used for carrying out the performance evaluation. A baseline benchmark on an unguarded schema was first created, and then compared against, a benchmark run on the same schema protected by a CTE GuardPoint.

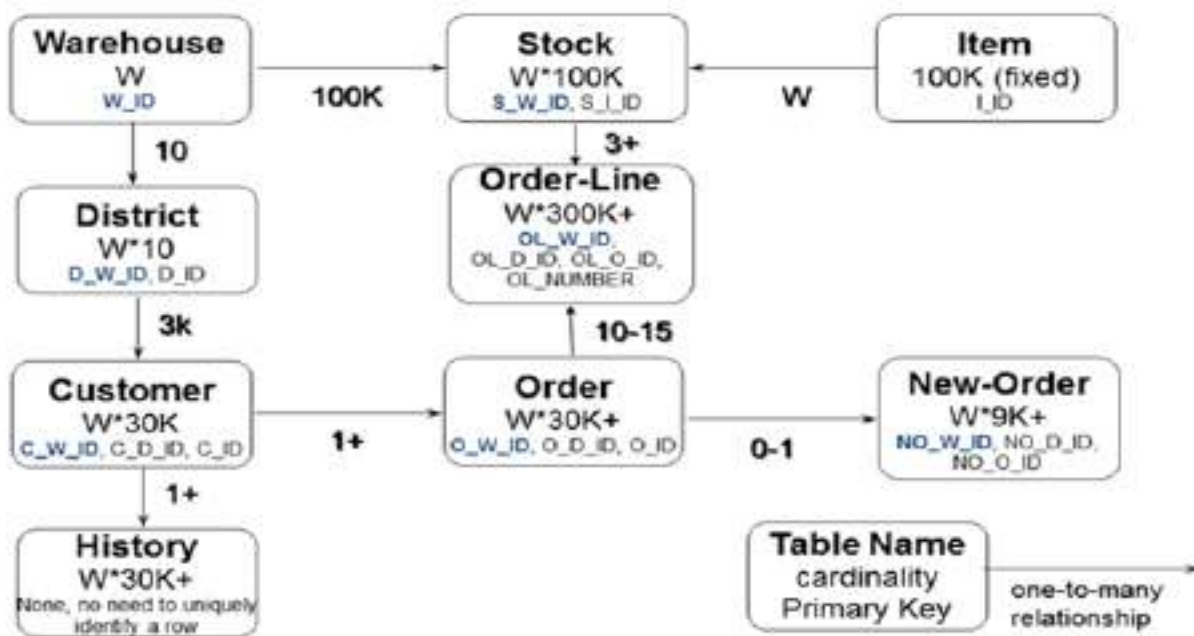
For establishing the baseline, several combinations of numbers of warehouses, and numbers of virtual users, were tried in order to arrive at a combination that provided optimum saturation.

The common approach was used to benchmark both SecFS, as well as SecVM performance, using Oracle with a file system and ASM storage, respectively.

About TPC-C

As an OLTP system benchmark, the TPC-C simulates a complete environment where a population of terminal operators executes transactions against a database. The TPC policies allow for derivations of TPC benchmark standards that comply with the TPC fair use rules. TPROC-C is the OLTP workload implemented in HammerDB derived from the TPC-C specification with modifications to make running HammerDB straightforward and cost-effective on any of the supported database environments. The rest of the content of this section has been excerpted from the HammerDB documentation available at <https://hammerdb.com/docs/ch03s05.html>.

The TPROC-C schema is shown below. Note how the number of rows in all of the tables, apart from the ITEM table which is fixed, is dependent upon the number of warehouses used to create the schema.



The workload is defined by a mix of 5 transactions selected at random according to the balance of the percentage value shown as follows:

1. **New-order:** Receive a new order from a customer: 45%
2. **Payment:** Update the customers balance to record a payment: 43%
3. **Delivery:** Deliver orders asynchronously: 4%
4. **Order-status:** Retrieve the status of customers most recent order: 4%
5. **Stock-level:** Return the status of the warehouses inventory: 4%

For the benchmark comparison, the GuardPoints were always applied to the TPCC tablespace. In one scenario, the redo logs, the temporary tablespace and the undo tablespace were in cleartext. In another scenario, the temporary and undo table space, as well as the redo logs, were guarded.

Metrics

The benchmark provides the transactions per minute (TPM) counter, which is used to compare the baseline with guarded schemas.

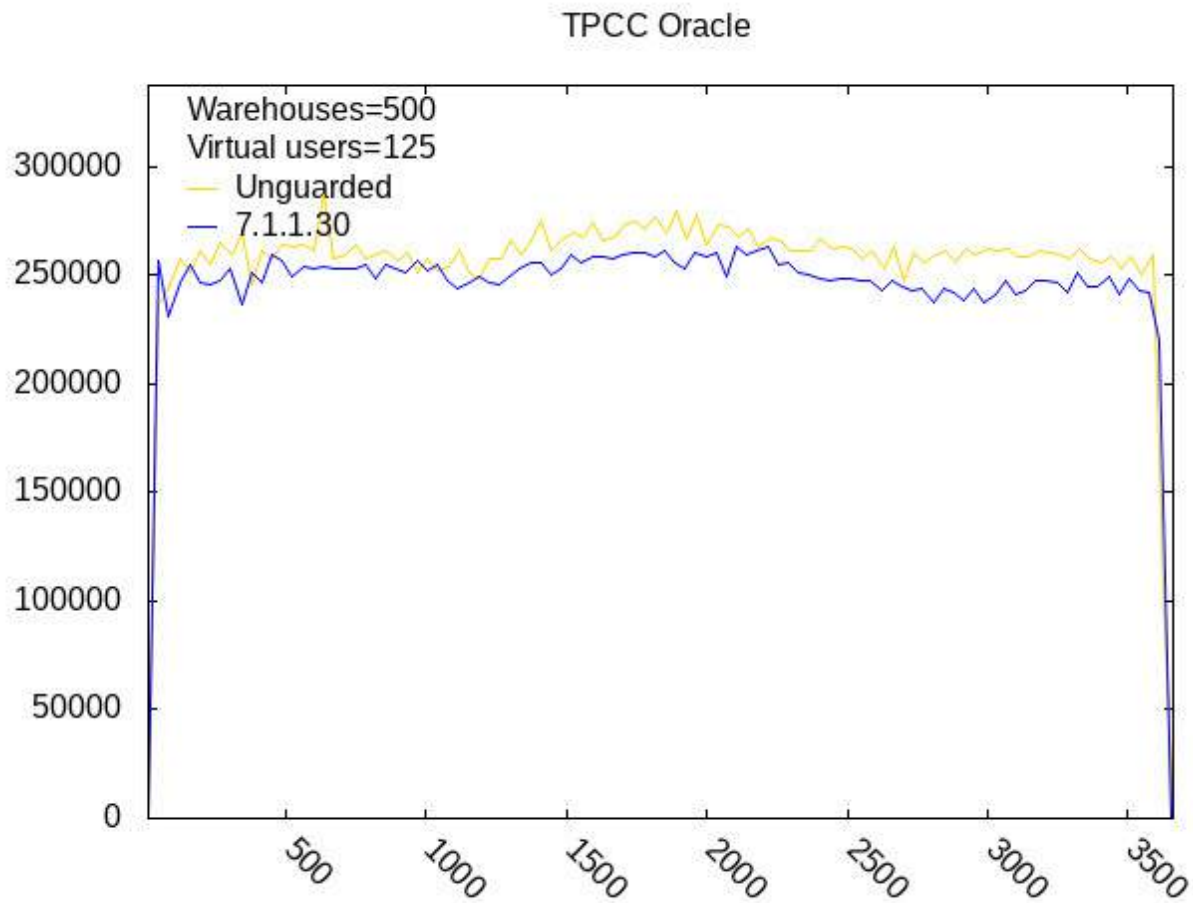
Chapter 3: ASM Storage

Only TPCC tablespace guarded

The TPM metric comparison is as follows:

	Baseline	CTE	Drop
Average TPM	258141.3	247410	4.2
Median TPM	261897	250164	4.5

This graph compares the TPM for 60 minutes.



The following table compares the IO metrics for the duration of the benchmark run. These figures only compare the IO numbers for the TPCC tablespace.

	Baseline	CTE	Drop
Read Requests/second	19,994.64	18,891.42	5.83
Read/second	156.30	147.66	5.85

	Baseline	CTE	Drop
Write Requests/second	14,449.41	12,605.30	14.62
Writes/second	185.73	171.62	8.22

Conclusion

Based on the average TPM comparison of the baseline vs the guarded benchmarks, with the redo logs, undo tablespace, temporary tablespace and TPCC tablespace guarded, the performance drop is 5.6% when the database uses ASM storage (using SecVM).

Appendix A: Tools Used

The following tools were used in this testing:

Infrastructure

The benchmark was conducted on a dedicated ESX (ProLiant DL360 Gen10) with the following hardware:

- CPU: 48 CPUs x Intel(R) Xeon(R) Gold 6252 CPU @ 2.10GHz
- Memory: 255.68 GB

The tablespace used in the benchmark, the redo logs, and the undo and temporary tablespace, were created on SSD storage. The ESX had three virtual machines, namely the Oracle server, the benchmark slave, and a Jenkins master. For the details of the resources allotted to the Oracle server, see ["Machine Details" below](#).

Machine Details

Oracle Server Details

This section lists the most significant details of the Oracle server for the filesystem as well as the ASM benchmark systems:

Filesystem Storage

- **File server:** Red Hat Enterprise Linux release 8.3
- **Kernel:** 4.18.0-240.el8.x86_64
- **CPU count:** 8
- **Memory:** 32 GB
- **Filesystem:** XFS

ASM Storage

- **File server:** Red Hat Enterprise Linux release 8.4
- **Kernel:** 4.18.0-305.17.1.el8_4.x86_64
- **CPU count:** 8
- **Memory:** 32 GB

Application versions

- **Oracle:** Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 – Production, Version 19.3.0.0.0
- **File system IO options:** setall
- **CTE:** 7.1.1.30
- **CipherTrust Manager:** 2.4.0.6018
- **Key Type:** AES 256 (CBC)

Other systems

HammerDB client

- **File server:** Ubuntu 20.04.2 LTS
- **Kernel:** 5.4.0-80-generic
- **CPU count:** 4
- **Memory:** 16 GB
- **Filesystem:** XFS
- **HammerDB:** 4.1

Jenkins

- **File server:** CentOS Linux 8 (Core)
- **Kernel:** 4.18.0-193.6.3.el8_2.x86_64
- **CPU count:** 1
- **Memory:** 4 GB
- **Filesystem:** XFS

CipherTrust Transparent Encryption

CTE Agent for Linux Advanced Configuration and Integration Guide

Release 7.0.0

Document Version 2

September 28, 2020

The bottom half of the page features a dark blue background with abstract geometric shapes. On the left, there is a large, bright blue triangle pointing upwards. Below it, a smaller, darker blue triangle points upwards. In the bottom left corner, there is a blue circle with a dotted pattern. The right side of the page has a vertical gradient from dark blue at the top to a lighter blue at the bottom, with a dotted pattern at the very bottom.

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2009-2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Contents

Preface	17
The CTE Agent Documentation Set	17
Document Conventions	17
Typographical Conventions	17
Notes, tips, cautions, and warnings	18
Sales and Support	19
 Chapter 1: Overview of CTE	 20
CTE Terminology	20
CTE Components	20
How to Protect Data with CTE	21
 Chapter 2: Getting Started with CTE for Linux	 22
Installation Workflow	22
Additional Considerations	22
Tracking and Preventing Local User Creation	22
Restricted Directories	23
Restricted Mode	23
Linux Package Installation	24
Installing the Unsigned RPM Package	25
Installing the Signed RPM Package with Yum	25
Installing the Signed RPM Package Manually	26
Installing CTE with No Key Manager Registration	27
Configuring CTE for Linux with CipherTrust Manager	28
Installation Overview	28
Installation and Registration Options	28
Installation Method Options	28
Hardware Association (Cloning Prevention) Option	28
Installation Prerequisites	28
Recommendations and Considerations	29
Network Setup Requirements	29
Port Configuration Requirements	29
Interactive Installation on Linux	29
Before You Begin	29
Silent Installation on Linux	32
Guarding a Device with CipherTrust Manager	34
Access the CipherTrust Manager Domain	34
Create an Encryption Key	34

Create a Standard Policy	36
Create a GuardPoint	38
Configuring CTE for Linux with a DSM	39
Installation Overview	39
Installation Prerequisites	39
Recommendations and Considerations	40
Network Setup Requirements	40
Host Name Resolution Requirements	40
Port Configuration Requirements	40
One-way Communication Option	41
Determining Kernel Compatibility With CTE	41
Installation and Registration Options	42
Installation Method Options	42
CTE Registration Method Options	42
Hardware Association (Cloning Prevention) Option	42
CTE Linux Installation Checklist	43
Interactive Installation on Linux	43
Installing CTE and Registering Using the Certificate Fingerprint	44
Installing CTE and Registering Using the Shared Secret Registration Method	47
Silent Installation on Linux	51
Silent Installation on Linux Using the Shared Secret Registration Method	51
Silent Installation on Linux Using the Fingerprint Registration Method	53
Registering CTE with the Shared Secret Registration Method After Installation is Complete	56
Registering CTE with the Fingerprint Registration Method After Installation is Complete	58
Guarding a Device with the DSM	61
Access the DSM Domain	62
Create an Encryption Key	62
Create a Standard Policy	62
Create a GuardPoint	63
Chapter 3: Special Cases for CTE Policies	65
More Information About Configuring CTE Policies	65
Re-Signing Executable Files on Secfs GuardPoints	65
Re-Enabling Automatic Signing for Host Settings	66
Restricting Access Overrides from Unauthorized Identities	66
Chapter 4: Concise Logging	68
Overview of Concise Logging	68
Using Concise Logging	68

Considerations	68
Configuring Concise Logging for CTE Clients or Client Groups with CipherTrust Manager	69
Configuring Global Concise Logging with the DSM	69
Configuring Concise Logging for a Registered Host with the DSM	69
Chapter 5: Enhanced Encryption Mode	70
Compatibility	70
Difference between AES-CBC and AES-CBC-CS1	71
Disk Space	71
Encryption Migration	71
File Systems Compatibility	71
File System Requirements	72
Samba Share	72
Storing Metadata	72
Missing IV file	73
HDFS	73
Backups	73
Container Compatibility	74
Using the AES-CBC-CS1 Encryption Mode in DSM	74
Using the AES-CBC-CS1 Encryption Mode in CM	74
Exceptions and Caveats	74
Best Practices for AES-CBC CS1 Keys and Host Groups	75
Chapter 6: CTE and systemd	76
Overview of CTE and systemd	76
Linux Distributions that Support CTE and systemd	76
CTE Agent Control Changes on systemd	76
CTE Configuration Changes Required on systemd	77
About systemd Dependency Changes for Unit Configuration Files	78
Location of Application Unit Configuration Files	79
Adding Dependencies to systemd Unit Configuration Files	79
Adding Applications to the secfs-fs-barrier.service File	79
Adding Dependencies to the saslauthd.service File	80
Supported Use Cases	80
Manually Stop 3rd Party Applications on a Live System	81
Chapter 7: Utilities for CTE Management	82
secfsd Utility	82
secfsd syntax	82

secfsd Examples	83
Display GuardPoint Information	83
Display GuardPoint Information in a Different Format	84
Display Host Settings	84
Display Key Status	84
Display Lock Status	84
Display CTE Log Status	85
Display Applied Policies	85
Display CTE Process Information	85
Display CTE Version Information	85
Manually Enable a GuardPoint in DSM	85
Manually Enable a GuardPoint in CipherTrust Manager	86
secfsd and Raw Devices	86
vmsec Utility	86
vmsec Syntax	87
vmsec Examples	87
Display CTE Challenge String	87
Display CTE Status	87
Entering a Password	87
Display Kernel Status	88
Display CTE Build Information	89
Display Contents of Conf files	89
Binary Resigning	89
Enable Automatic Signing for Host Settings	90
Restricting Access Overrides from Unauthorized Identities	91
Using Advanced Encryption Set New Instructions (AES-NI)	91
vmd utility	92
Syntax	92
Display the Installed Version	92
agenthealth Utility	92
The Agent health check script	92
agentinfo Utility (Java version)	93
check_host Utility	93
check_host Syntax	94
register_host Utility	94
fsfreeze and xfs_freeze	94
Restrictions	94
Platform Restrictions	94
Target Restrictions	95
File System Restrictions	95

LDT Restrictions	95
Offline Data Transformation Restrictions	95
Chapter 8: Installing CTE on Hadoop	96
Overview	96
Overview of CTE on HDFS	96
HDFS Administrator:	96
DSM Security Administrator:	97
HDFS Administrator:	97
Implementing CTE on HDFS	97
CTE on HDFS Implementation Assumptions	97
Configure the HDFS NameNodes	97
Create an Encryption Zone in HDFS Name Space for AWS EMR	98
Using the Original Information from HDFS	99
Create a HDFS Host Group and Host Group GuardPoint	99
Take a DataNode Offline and Perform Data Transformation	101
Implementing CTE on HDFS on a Single Host	102
Adding a New DataNode to a CTE-protected HDFS	103
CTE Installed on the Cluster Nodes Before Ambari Installs Hadoop	103
HDFS Upgrade with CTE	104
Upgrading one node at a time	104
Upgrade CTE with CTE-LDT in an HDFS Cluster	104
Rolling Upgrades	104
Configure the Hadoop Cluster for CTE	106
Create a Vormetric Configuration Group	106
Update the Hadoop-env Template with CTE Settings	107
Modify the HDFS IOCTL	107
Change the HDFS File Rename Check	107
User Information Push	107
Create Kerberos Principal for CTE	108
Uninstalling CTE for the Hadoop Cluster	108
CTE Installation and Configuration	108
Installing and Configuring CTE on an HDFS Node	109
Modifying host settings for HDFS hosts on the DSM	109
Simple Modification	109
Using Kerberos	110
Modifying Host Group for HDFS NameNodes HA on DSM	110
Configuring Hadoop to Use CTE	111
Verify secfsd is Running with Hadoop Environment	111
HDFS Name Cache	111

Enabling CTE on HDFS	112
Deleting Metadata in HDFS when Migrating Out of LDT	112

Chapter 9: Using CTE with Oracle 114

Oracle RAC ASM and ASMLib	114
Using CTE with an Oracle RAC ASM	114
ASMLib	114
Important ASM Commands and Concepts	114
Rebalancing Disks	114
Mapping Raw Devices	115
Checking Rebalance Status	115
Determining Best Method for Encrypting Disks	116
Online Method (No Application / Database Downtime)	116
Offline Method (Backup the DB)	116
General Prerequisites	117
Setup	117
Modify the UDEV Rules	117
Altering ASM_DISKSTRING on ASM	117
Specific Prerequisites	118
Establishing a Starting Point	118
The Importance of Device Mapping	118
Important Note about Raw Devices on UNIX	118
Oracle RAC ASMLib Multi-Disk Online Method	119
Assumptions	119
About Oracle RAC ASM Raw Devices	119
When Not Using ASMLib	119
Devices using Raw Bindings	119
Multipath I/O Devices	120
Standard Devices	120
Consistent Naming of Devices across RAC Nodes	120
Oracle RAC ASM Multi-Disk Online Method	120
Checking for Space	120
Adding a Disk to the Diskgroup	121
Troubleshooting	121
Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)	122
Troubleshooting	122
Surviving the Reboot and Failover Testing	123
Preparing for Failover Testing with ASMLib	123
CTE Load Order and Startup Scripts	123
Failover Testing	123

Issues with Device Mapper and Invalid Guard Path	123
Basic Troubleshooting Techniques	123
Verifying Database Encryption	124
Option 1	124
Option 2	125
Option 3	125
Chapter 10: Configuring Support for SAP HANA	126
Overview	126
Customizing CTE for SAP HANA in HA Mode	126
Using SAP HANA with LDT	128
Setting Memory Allocation	128
Chapter 11: Container Security	129
Installing Docker Automatically	129
Container Security Overview	129
Container Terminology	129
Docker Containers with CTE	130
CTE: Virtual Machine versus Docker	130
Using the CTE Agent	130
Docker containers in custom paths won't start after CTE agent is installed	131
Set the Docker Storage Driver	131
Change the Storage Driver	132
Administering the Docker Host	132
Creating Policies	132
Adding Security Rules	133
Create Resource Set	133
Create User Set	133
Create Process Set	134
Enable Docker through Host Settings	135
CTE Docker GuardPoints	135
Image-based GuardPoints	135
Container-based GuardPoints	136
GuardPoints for Docker Containers	136
Creating GuardPoints	136
Viewing GuardPoints	136
Data Security for Docker Images and Containers	137
Setting up an image based GuardPoint	137
Setting up a Container-Based GuardPoint	138

Setting up a GuardPoint for an Exported Docker Volume	139
Configuring Audit Logging	139
Configure Docker Log Settings	139
Searching for Docker Log Messages	140
Generating Reports	140
System Level Reports	140
Domain Level Reports	140
RedHat OpenShift Containers with CTE	141
Using the CTE Agent	141
CTE: Virtual Machine versus OCP	141
Set the OpenShift Storage Driver	141
Administering the OpenShift Host	141
Enable OpenShift through Host Settings	141
CTE OCP GuardPoints	141
Types of GuardPoints	141
Image-based GuardPoints	142
Container/POD-based GuardPoints	142
Creating GuardPoints	142
Viewing GuardPoints	142
Data Security for OpenShift Images and Containers	142
Setting up an Image-based GuardPoint	142
Setting up a POD-based GuardPoint	142
Setting up a GuardPoint for an exported OCP volume	142
Configuring Audit Logging	142
Generating Reports	142
Creating an OCP Project in CLI with API Commands	143
Creating an OCP Project with a Template	143
Deploying an OCP Project	143
Available OpenShift commands	144
Available OPC Options	144
Container secfsd Utilities	145
Chapter 12: NetApp Snapshot Directory	146
Overview	146
Accessing snapshots	146
Enabling Snapshots	146
Dataxform Considerations	146
Best Practices	147

Chapter 13: Using CTE with Quantum StorNext	148
Overview of using CTE with Quantum StorNext	148
CTE and Quantum StorNext Compatibility	148
Supported StorNext Server and Client Configurations	148
Supported GuardPoint and Key Settings for SNFS File Systems	149
Supported Concurrent Access Read/Write Scenarios	149
Setting up CTE and Quantum StorNext Integration	150
Integration Task Overview	150
Installing and Configuring a Quantum StorNext MDC Server for Use with CTE	151
Installing and configuring Quantum StorNext DLC Clients for Use with CTE	151
Ensuring that the StorNext SNFS File System Starts Before secfs	151
Installing the CTE Agent on Each StorNext LAN client	151
Stop secfs Before Upgrading StorNext LAN Clients	152
 Chapter 14: Using CTE with McAfee Endpoint Security for Linux Threat Prevention	 153
Supported McAfee Versions and Linux Operating Systems	153
Ensuring Correct McAfee Service Startup Order	153
Ensuring Correct McAfee Service Startup Order in systemd	153
Ensuring Correct McAfee Service Startup Order Manually	154
Updating McAfee	154
Virus Scanning Behavior Differences for CIFS and NFS GuardPoints	154
 Chapter 15: Using CTE with Trend Micro Deep Security Software	 155
Supported Deep Security Versions and Linux Operating Systems	155
Ensuring Correct Deep Security Service Startup Order	155
Ensuring Correct Deep Security Service Startup Order in systemd	155
Ensuring Correct Deep Security Service Startup Order Manually	156
Updating Deep Security	156
 Chapter 16: CTE COS for Amazon S3	 157
Overview	157
Supported operations	158
Limitations	158
Multi-part Upload Restrictions	159
System and Software Requirements	159
Client Software Requirements	159
CTE COS S3 Installation Overview	159
Install Required Linux Packages	160

Install CTE	160
Configure the AWS CLI to use the COS Root CA Certificate	161
Configure the AWS CLI Network Proxy	161
Configure CTE COS S3	162
Setting the Default Chunk Size	162
Optionally Configure a CTE COS S3 Role for Guarded Buckets	163
Secure an S3 Bucket with the CTE COS S3 Role	166
Disable the CTE COS S3 Role for an S3 Bucket	166
Guard an AWS Bucket	167
Create a CBC_CS1 Key in DSM	167
Create the Cloud Object Storage (COS) policy in DSM	168
Creating GuardPoints in a Host	169
Additional COS Proxy Root CA Certificate Information	170
Protecting Python Programs with CTE	172
Benefits of Using PyInstaller with CTE	172
Getting PyInstaller	172
Example Usage	172
Chapter 17: CTE-Efficient Storage for Linux	174
Introduction to CTE-Efficient Storage	174
Requirements and Considerations	174
CTE-Efficient Storage Enhanced Storage Arrays	175
Storage Arrays Compatible with CTE-Efficient Storage	175
Sharing Encryption Keys	175
Storage Array Registration	176
Efficient Storage Device Header and CTE Private Region	176
Device Size	176
DSM Domain Enabled for KMIP	177
ES GuardPoint Encryption Keys	177
Key Attributes - Example	178
KMIP Key Object	179
Policy Requirements for ES GuardPoints	179
Guarding an Efficient Storage Device on Linux	180
Requirements for Efficient Storage GuardPoints on Linux	180
Register the Host with DSM	181
Initialize Linux Efficient Storage Devices	182
Initialize a New Linux Device	182
Initialize and Resize an Existing Linux Device	183
Guard the Linux Device with an ES GuardPoint	184
Data Relocation on Existing Linux Devices	186

Data Transformation on Existing Linux Devices	186
Example of Creating an ES GuardPoint on an Existing Linux Device	187
Guarding a CTE-Efficient Storage Device with Multiple IO Paths on Linux	189
Linux System and ES GuardPoint Administration	189
voradmin ESG Commands on Linux	189
Viewing Device Status and the ES Header on Linux	189
File System Mount Points on Linux	190
Auto Mount Options for File System Devices on Linux	190
Linux System Utilities for Signing	191
Changing the Encryption Key on Linux ESG Devices	192
Creating a New DSM Policy for Key Rotation	192
Prepare an ES GuardPoint for Rekey	193
Resizing Guarded Efficient Storage Devices	194
Example: Resizing a Linux Device	195
Use Cases involving Efficient Storage GuardPoints	196
Use Case 1: Single Encryption Key	196
Use Case 2: Device-Level GuardPoints	196
Use Case 3: Directory-Level GuardPoints	197
Challenges with Root Access on Linux	199
Use Case 4: Using CTE-Efficient Storage with LVM	204
Alerts and Errors on Linux	205
Encryption key on device has not been made available	205
Specified policy disagrees with metadata set on the Guard Path	205
Device has not been configured for Efficient Storage	205
Device not resized for guarding as Efficient Storage	206
Data transformation failed	206
Data transformation in progress	206
Device <device-name> is configured to guard as Efficient Storage GuardPoint	206
Device <device-name> is configured as Efficient Storage GuardPoint	206
GuardPoint for device <device-name> still guarded on DSM	206
Failed to open device <device-name>, error Device or resource busy	207
Device <device-name> is not configured as Efficient Storage	207
Abort! Error: Could not stop secfs, secvm device(s) busy	207
Abort! Error: Could not unmount file systems	207
A dependency job for esg.mount failed. See 'journalctl -xe' for details	207
ESG-ALERT: IO error on header for [GuardPoint]	207
ESG-ALERT: Data transformation failure on [GuardPoint]	207
ESG-INFO: Data transformation complete on [GuardPoint]	208
ESG-ALERT: Failed to resize <device-name>	208
FSADM-ALERT: ESG required Signature Set for system utilities may have to be resigned	208

File System is not automatically mounted after IDT completes	208
Chapter 18: CipherTrust InPlace Data Transformation for Linux	209
Introduction to CipherTrust InPlace Data Transformation (IDT)	209
Requirements for IDT-Capable GuardPoints	209
The CTE Private Region and IDT Device Header	210
CTE Private RegionLocation	210
Device Size	211
IDT-Capable GuardPoint Encryption Keys	211
Key Attributes - Example	212
Policy Requirements for IDT-Capable GuardPoints	213
Guarding an IDT-Capable Device on Linux	214
Initializing an IDT-Capable Device	215
Initialize a New Linux Device	215
Initialize a Linux Device with Existing Data	216
Guard the Linux Device with an IDT-Capable GuardPoint	218
Data Relocation and Transformation on Existing Linux Devices	220
Example of Creating an IDT-Capable GuardPoint on an Existing Linux Device	221
Changing the Encryption Key on Linux IDT-Capable Devices	222
Guarding an IDT-Capable Device with Multiple IO Paths on Linux	225
Viewing Device Status and the IDT Device Header	225
Linux System and IDT-Capable GuardPoint Administration	226
voradmin IDT Commands on Linux	226
File System Mount Points on Linux	226
Auto Mount Options for File System Devices on Linux	226
Linux System Utilities for Signing	227
Resizing Guarded IDT Devices	228
Use Cases Involving IDT-Capable GuardPoints	228
Alerts and Errors on Linux	228
Encryption key on device has not been made available	228
Specified policy disagrees with metadata set on the Guard Path	229
Device has not been configured for IDT-Capable or Efficient Storage	229
Device not resized for guarding as IDT-Capable or Efficient Storage	229
Data transformation failed	229
Data transformation in progress	229
Device <device-name> is configured to guard as Efficient Storage GuardPoint	229
Device <device-name> is configured as Efficient Storage GuardPoint	230
Device <device-name> is configured to guard as IDT-Capable GuardPoint	230
Device <device-name> is configured as IDT-Capable GuardPoint	230
GuardPoint for device <device-name> still guarded on DSM	230

Failed to open device <device-name>, error Device or resource busy	230
Device <device-name> is not configured as IDT-Capable	230
Abort! Error: Could not stop secfs, secvm device(s) busy	231
Abort! Error: Could not unmount file systems	231
A dependency job for idt.mount failed. See 'journalctl -xe' for details	231
ESG/IDT-ALERT: IO error on header for [GuardPoint]	231
ESG/IDT-ALERT: Data transformation failure on [GuardPoint]	231
ESG/IDT-INFO: Data transformation complete on [GuardPoint]	231
ESG/IDT-ALERT: Failed to resize <device-name>	231
FSADM-ALERT: ESG/IDT required Signature Set for system utilities may have to be resigned ..	231
File System is not automatically mounted after IDT completes	232
Chapter 19: CTE with Teradata Database Appliances	233
IDT-Capable GuardPointsand Teradata Database Appliances	233
Requirements and Considerations	233
Location of the CTE Private Region	233
Metadata File Access and Teradata Clusters	234
Additional Requirements and Considerations	234
Guarding a Teradata Database Device	235
Install CTE on the Teradata Database Appliance	235
Identify the Devices to Be Guarded	236
Select the Initial Configuration Method	237
Initialize and Guard the Database Devices Using the Standard Initialization Method	237
Guard the Devices as IDT-Capable GuardPoints	238
Viewing Device and Data Transformation Status	240
Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method	240
Changing the Encryption Key on Teradata Devices	243
Access Rules to Apply on the Teradata Database Appliance	244
Replication of IDT Metadata Files Across Members of a Clique	248
Specific Issues to Consider	248
General PCL Error	248
Offline Node in Clique During Data Transformation	249
Adding a New Node to a Clique	249
Interoperability with Host Groups	249
Best Practices	250
Using a of Host Group to Guard Metadata Directories	250
Using a Host Group for Guarding Teradata Devices in a Clique	250
Best Practice for Preparation for Initial Data Transformation or Rekey	251
Uninstalling CTE from the Teradata Cluster	251
Alerts and Errors	252

General Errors	252
IDT-TD-ALERT: Node <node name> did not respond to pcl command	253
IDT-TD-ALERT: Node <node name> failed to perform voradmin task	253
IDT-TD-ALERT: Failed to find clique for disk <device>	253
IDT-TD-ALERT: Failed to move or rename IDT-Capable metadata file on remote nodes	253
IDT-TD-ALERT: Failed to get GuardPoint status on remote nodes	253
Operation Errors	253
IDT-TD-ALERT: Failed to distribute IDT-Capable metadata file to remote nodes	253
IDT-TD-WARNING: Failed to delete IDT-Capable metadata file on remote nodes	254
IDT-TD-ALERT: Failed to complete rekey on remote nodes	254
 Chapter 20: Upgrading CTE on Linux	255
Upgrading CTE	255
Scheduled Upgrade Feature	256
Warnings for CTE for Linux	256
Using the Scheduled Upgrade Feature	256
Performing a Manual Upgrade When an Upgrade is Already Scheduled	257
Voradmin Commands for the Scheduled Upgrade Feature	258
 Chapter 21: Uninstalling CTE from Linux	260

Preface

The CTE Agent for Linux Advanced Configuration and Integration Guide provides information about advanced installation, configuration, and integration options for CTE for Linux.

The CTE Agent Documentation Set

The following guides are available for CTE Agent:

- *CTE Agent for Linux Quick Start Guide*
- *CTE Agent for Linux Advanced Configuration and Integration Guide*
- *CTE Agent for Windows Quick Start Guide*
- *CTE Agent for Windows Advanced Configuration and Integration Guide*
- *CTE Agent for AIX Installation and Configuration Guide*
- *CTE-Live Data Transformation with Data Security Manager*
- *CTE-Live Data Transformation with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with Data Security Manager*
- *Compatibility Matrix for CTE Agent for AIX with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent for AIX with Data Security Manager*
- *Release Notes for CTE for Linux Version 7.0.0.47*
- *Release Notes for CTE for Windows Version 7.0.0.47*
- *Release Notes for CTE for AIX Version 7.0.0.11*

Document Conventions

The document conventions describe common typographical conventions and important notice and warning formats used in Thales technical publications.

Typographical Conventions

This section lists the common typographical conventions for Thales technical publications.

Table 3-1: Typographical Conventions

Convention	Usage	Example
bold regular font	GUI labels and options.	Click the System tab and select General Preferences.
<i>bold italic monospaced font</i>	variables or text to be replaced	https://<Token Server name>/admin/ Enter password: <Password>
<code>regular monospaced font</code>	Command and code examples XML examples	Example: session start iptarget=192.168.253.102

Table 3-1: Typographical Conventions (continued)

Convention	Usage	Example
<i>italic regular font</i>	GUI dialog box titles	The <i>General Preferences</i> window opens.
	File names, paths, and directories	<i>/usr/bin/</i>
	Emphasis	<i>Do not</i> resize the page.
	New terminology	<i>Key Management Interoperability Protocol (KMIP)</i>
	Document titles	See <i>CTE Agent for Linux Advanced Configuration and Integration Guide</i> for information about CipherTrust Transparent Encryption.
quotes	File extensions Attribute values Terms used in special senses	"js", ".ext" "true" "false", "0" "1+1" hot standby failover

Notes, tips, cautions, and warnings

Notes, tips, cautions, and warning statements may be used in this document.

A Note provides guidance or a recommendation, emphasizes important information, or provides a reference to related information. For example:

Note

It is recommended to keep tokenization keys separate from the other encryption/decryption keys.

A tip is used to highlight information that helps you complete a task more efficiently, such as a best practice or an alternate method of performing the task.

Tip

You can also use Ctrl+C to copy and Ctrl+P to paste.

Caution statements are used to alert you to important information that may help prevent unexpected results or data loss. For example:



CAUTION

Make a note of this passphrase. If you lose it, the card will be unusable.

A warning statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data. For example:



WARNING

Do not delete keys without first backing them up. All data that has been encrypted with deleted keys cannot be restored or accessed once the keys are gone.

Sales and Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

For support and troubleshooting issues:

- <https://supportportal.thalesgroup.com>
- (800) 545-6608

For Thales Sales:

- <https://cpl.thalesgroup.com/>
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

Chapter 1: Overview of CTE

CTE includes several unique utilities to help you encrypt and manage your data. It also integrates with several third-party platforms such as Oracle, Teradata Database Appliances, and Amazon S3.

This document describes the installation and advanced configuration options for CTE, as well as detailed information about how to integrate CTE with the supported third-party products.

CTE Terminology

The CTE documentation set uses the following terminology:

Term	Description
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. Note This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". For example, the default installation directory is <code>/opt/vormetric/DataSecurityExpert/agent/</code>.
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.
key manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers two key managers for use with CTE, the Vormetric Data Security Manager (DSM) and CipherTrust Manager.
host / client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed. The difference comes from the key manager you are using. The DSM refers to the machines as hosts, while the CipherTrust Manager refers to them as clients.
GuardPoint	A device or directory to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.
After the CTE Agent has encrypted a device on a host, that device is called a *GuardPoint*. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.
- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Thales offers two key managers that work with CTE:

- CipherTrust Manager, Thales's next generation key manager that supports most CTE for Linux features.
- The *Vormetric Data Security Manager* (DSM), Thales's legacy key manager that supports all CTE for Linux features.

Both key managers can be set up as either a security-hardened physical appliance or a virtual appliance. Both provide access to the protected hosts through a browser-based, graphical user interface as well as an API and a CLI. Thales recommends that you use the CipherTrust Manager unless you need a feature that is only supported by the DSM, as described below.

The CipherTrust Manager currently supports all CTE for Linux features *except* for the following:

- Container Security
- CTE-Efficient Storage
- CipherTrust InPlace Data Transformation
- CTE with Teradata Database Appliances

Support for these features will be included in future releases of the CipherTrust Manager.

For details about any of these features, see the *CTE Agent for Linux Advanced Configuration and Integration Guide*.

You must select one and only one key manager per host or host group. While you could have some hosts registered with a CipherTrust Manager and some registered with a DSM, you cannot have the same host registered to both a CipherTrust Manager and a DSM.

Note: For a list of CTE versions and supported operating systems, see the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.

How to Protect Data with CTE

CTE uses policies created in the associated key manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your protected hosts. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of GuardPoints.

Policies specify:

- Whether or not the resting files are encrypted.
- Who can access decrypted files and when.
- What level of file access auditing is applied when generating fine-grained audit trails.

A Security Administrator accesses the DSM or CipherTrust Manager through a web browser. You must have administrator privileges to create policies using either key manager. The CTE Agent then implements the policies once they are pushed to the protected host.

CTE can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

Chapter 2: Getting Started with CTE for Linux

This chapter describes how to install CTE for Linux, register it with your selected key manager, and then create a simple GuardPoint on the protected host. It contains the following sections:

Installation Workflow	22
Linux Package Installation	24
Installing CTE with No Key Manager Registration	27
Configuring CTE for Linux with CipherTrust Manager	28
Configuring CTE for Linux with a DSM	39

Installation Workflow

In order to install and configure CTE, you need to perform the following high-level tasks:

1. Select which key manager you want to use. The Vormetric Data Security Manager and the CipherTrust Manager have different requirements and support different features, so you must make this decision first. For details, see ["CTE Components" on page 20](#).
2. If you want to include the CTE Agent software with the Linux distribution files, see ["Linux Package Installation" on page 24](#).
3. If you want to install the CTE Agent without registering with a key manager, see ["Installing CTE with No Key Manager Registration" on page 27](#). However, you cannot protect any data on the host until it has been registered. Otherwise, set up your systems according to the requirements of the selected key manager. For details, see one of the following:
 - ["Configuring CTE for Linux with CipherTrust Manager" on page 28](#)
 - ["Configuring CTE for Linux with a DSM" on page 39](#)
4. Create your policies, encryption keys, and GuardPoints using the selected key manager. For an example, see one of the following:
 - ["Guarding a Device with CipherTrust Manager" on page 34](#).
 - ["Guarding a Device with the DSM" on page 61](#).

Additional Considerations

The following sections describe some of the things to keep in mind when configuring CTE.

Tracking and Preventing Local User Creation

CTE allows you to track attempts to change user authentication files using the host settings `audit` and `protect`. This includes, but is not limited to user creation, modification, and deletion, or to deny users.

- The `audit` setting is set to on by default. It audits access to the system credential files but does not prevent account creation.
- The `protect` setting both audits and prevents local user account creation. You must manually enable the `protect` setting for tracking and prevention of local user account creation.

You can tag the following files with either `audit` or `protect`. If you tag a file with both options, CTE uses the `protect` setting.

- `/etc/passwd`
- `/etc/group`
- `/etc/shadow`
- `/etc/gshadow`

Notes

- You do not have to restart CTE after applying or removing these host settings.
- To see the audit messages in the DSM, you must use DSM version 6.x or later. Audit messages are not available in DSM versions 5.x and earlier.

Restricted Directories

Linux does not allow you to guard the following directories:

- `<secfs install root>/agent/secfs/`
- `/etc`
- `/tmp`
- `/usr`
- `/usr/lib`
- `/usr/lib/pam`
- `/var/log/vormetric`

Linux does not allow you to guard the following directories and all of their subdirectories:

- `<install root>/agent/secfs/bin`
- `<secfs install root>/agent/vmd`
- `/etc/vormetric`
- `/etc/pam.d`
- `/etc/security`
- `/usr/lib/security`
- `/etc/rc*`

Restricted Mode



CAUTION

If you install or upgrade in restricted mode, you cannot revert to unrestricted mode without uninstalling CTE.

You can install CTE in restricted mode. This mode prevents any user other than `root` from accessing the following directories:

- `/var/log/vormetric`
- `/opt/vormetric/DataSecurityExpert`

Restricted Mode also prevents non-`root` users from running the following utilities:

- `agenthealth`
- `agentinfo`
- `check_host`
- `register_host`
- `secfsd`
- `vmd`
- `vmsec`
- `voradmin`

Key Agents and Restricted Mode

- On systems where CTE is installed in restricted mode, you cannot install a key agent (pkcs11) or CipherTrust TDE Key Management.
- On systems where a key agent (pkcs11) or CipherTrust TDE are already installed, you cannot install CTE in restricted mode.

Restricted Mode Installation

To install in restricted mode, use the `-r` option.

```
# ./vee-fs-<release>-<build>-<system>.bin -r
```

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -r
```

RPM Installation

If installing from an RPM directly, prior to installation, type:

```
# export VOR_RESTRICTED_INSTALL_MODE=yes
```

Upgrade in Restricted Mode

The upgrade mode is the same as the installation mode.

Linux Package Installation

This section describes how to access the Linux RPM installation package so that the CTE Agent installation integrates with the distribution software. To access the Linux RPM file, you can:

- Extract the RPM file from the CTE Agent install bin file. This is the easiest method, but the files in the package are not signed and therefore cannot be verified. For details, see ["Installing the Unsigned RPM Package" on the next page](#).
- Download the package from the Yum repository. If you use Yum, the files in the package are signed and the signatures are automatically verified when the package is installed. For details, see ["Installing the Signed RPM Package with Yum" on the next page](#).
- Manually download the RPM package outside of Yum and manually verify the package signatures. For details, see ["Installing the Signed RPM Package Manually" on page 26](#).



CAUTION

Do not use package installation for SUSE Linux. Instead, use the interactive or silent installation.

Installing the Unsigned RPM Package

The CTE installation `bin` files contain the unsigned native packages. Extract them by running the `bin` file with the `-e` flag.

1. Log on to the host system as root and copy or mount the installation file to the host system.
2. Extract the RPM file using the following command:

```
# ./vee-fs-<release>-<build>-<system>.bin -e
```

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -e
```

Contents extracted.

```
# ls *rpm
```

```
vee-fs-7.0.0-47-rh8-x86_64.rpm
```

3. To start the installation using the RPM file, use the following command:

```
# rpm -ivh vee-fs-7.0.0-47-rh8-x86_64.rpm
```

4. Follow the prompts to install and register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

- If you are going to register the system with a CipherTrust Manager, see ["Configuring CTE for Linux with CipherTrust Manager" on page 28](#).
- If you are going to register the system with a Vormetric Data Security Manager (DSM), see ["Configuring CTE for Linux with a DSM" on page 39](#).

Installing the Signed RPM Package with Yum

Note

Before you can download and install the package using the Yum repository, you must contact Thales Customer Support to get the username and password for the package repository on which the package resides.

1. Create the repository file, `/etc/yum.repos.d/Vormetric-VTE.repo`, with the following contents:

```
[vormetric-vte]
releasever=REL_VERSION
name=Vormetric VTE Packages $releasever - $basearch - Source
baseurl=https://USER:PASSWORD@packages.vormetric.com/vte/VERSION/rhel-$releasever/
gpgkey=https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
enabled=1
gpgcheck=1
repo_gpgcheck=1
sslverify=1
```

where:

- **REL_VERSION** is the the version of RHEL that you are running. This would be `rhel-6`, `rhel-7`, or `rhel-8`.
- **USER:PASSWORD** is the username and password for the CTE package repository you obtained from Thales Customer Support.
- **VERSION** is the CTE release version number. For example, `7.0.0`.

2. Clean up the Yum cache directory:

```
# yum clean all
```

3. Use Yum to install the CTE binary. For example, if the cte binary name is vee-fs-7.0.0-.x86_64, you would enter:

```
# yum install vee-fs-7.0.0-.x86_64
```

Note: The first time you install CTE through Yum, you will be asked to import the GPG key. Make sure that you download this key or the install will fail. For example:

```
vormetric-vte/7Server/signature | 198 B 00:00:00
Retrieving key from https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
Importing GPG key 0x628536B7:
  Userid      : "Vormetric (PKG-GPG-KEY) <support@vormetric.com>"
  Fingerprint: 7cb5 4f55 40d4 1b63 bf91 c896 f00a 13b0 6285 36b7
  From        : https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
Is this ok [y/N]: y
```

4. Follow the prompts to install and register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

- If you are going to register the system with a CipherTrust Manager, see ["Configuring CTE for Linux with CipherTrust Manager" on page 28](#).
- If you are going to register the system with a Vormetric Data Security Manager (DSM), see ["Configuring CTE for Linux with a DSM" on page 39](#).

Installing the Signed RPM Package Manually

If you want to manually verify the signed version of the CTE RPM package, you can download the public key from the Thales package repository and manually verify the rpm signature.

1. Import the public key from the Thales package repository:

```
# rpm --import https://packages.vormetric.com/pub/PKG-GPG-KEY-vormetric
# rpm -qa gpg-pub*
gpg-pubkey-628536b7-56f9887b : Imported CTE GPG public key.
gpg-pubkey-fd431d51-4ae0493b
```

2. Verify the signature of the package using the `rpm -Kv` command.

```
# rpm -Kv vee-fs-7.0.0-.x86_64.rpm
vee-fs-7.0.0-.x86_64.rpm:
  Header V4 DSA/SHA1 Signature, key ID 628536b7: OK
  Header SHA1 digest: OK (ed3d33dca580c66c70961cfee143e9877a09544c)
  MD5 digest: OK (95273b36ef1c205a7cea444e14bef15f)
  V4 DSA/SHA1 Signature, key ID 628536b7: OK
```

The output should show that the keys match is OK.

3. To start the installation using the RPM file, use the following command:

```
# rpm -ivh vee-fs-7.0.0-.x86_64.rpm
```

4. Follow the prompts to install and register CTE.

For details about the installation and registration process, see the appropriate installation procedure.

- If you are going to register the system with a CipherTrust Manager, see ["Configuring CTE for Linux with CipherTrust Manager" on page 28](#).
- If you are going to register the system with a Vormetric Data Security Manager (DSM), see ["Configuring CTE for Linux with a DSM" on page 39](#).

Installing CTE with No Key Manager Registration

The following procedure installs the CTE Agent on the host but does not register it with a key manager. You cannot protect any data on the host until the CTE Agent is registered with one of the supported key managers. For a comparison of the available key managers, see ["CTE Components" on page 20](#).

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note: If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type `y` and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.47
```

```
In order to register the CipherTrust Transparent Encryption File System Agent
with a Vormetric Data Security Manager
```

- 1) you must know the host name of the machine running the DSM (the host name is displayed on the Dashboard window of the Management Console), and
- 2) unless you intend to use the 'shared secret' registration method, the agent's host machine must be pre-configured on the DSM as a host with the 'Reg. Allowed' checkbox enabled for this agent type on the Hosts window of the Management Console.

```
In order to register with a CipherTrust Manager you need a valid registration
token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Type `n` and press Enter to end the installation procedure without registering the CTE Agent with either key manager.

When you are ready to register the CTE Agent with a key manager, see one of the following:

- ["Configuring CTE for Linux with CipherTrust Manager" on the facing page](#)
- ["Configuring CTE for Linux with a DSM" on page 39](#)

Configuring CTE for Linux with CipherTrust Manager

This section describes how to install and configure CTE on Linux systems that you plan to register with a CipherTrust Manager. If you want to register CTE with a Vormetric Data Security Manager (DSM), see ["Configuring CTE for Linux with a DSM" on page 39](#).

Installation Overview

The installation and configuration process when you are using CTE with a CipherTrust Manager consists of three basic steps:

1. Gather the information needed for the install and set up your network as described in ["Installation Prerequisites" below](#).
2. Install CTE on the protected host as described in ["Interactive Installation on Linux" on the next page](#) or ["Silent Installation on Linux" on page 32](#).
3. Register the protected host with CipherTrust Manager and make sure that they can communicate with each other. Registration can be done as part of the initial installation or at any point after the CTE Agent has been installed.

Installation and Registration Options

CTE provides the following installation and registration options. The options you choose determine the information you need to supply during the actual install procedure.

Installation Method Options

There are two methods for installing CTE on Linux platforms:

- **Typical:** Most common and recommended type of installation. Use this method for installing the CTE Agent on one host at a time. See ["Interactive Installation on Linux" on the next page](#).
- **Silent:** Create pre-packaged installations by providing information and answers to a set of installation questions. Use silent installations when installing on a large number of hosts. See ["Silent Installation on Linux" on page 32](#).

Hardware Association (Cloning Prevention) Option

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware clients.

You can enable hardware association during CTE registration process. You can disable hardware association by re-running the registration program.

To verify if hardware association (cloning prevention) is enabled on a Linux host, on the command line enter the following:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/access
```

If you see `usehw:true`, then hardware association is enabled. If you see `usehw:false`, it's disabled.

Installation Prerequisites

This section lists the tasks you must complete, and the information you must obtain, before installing CTE.

Recommendations and Considerations

- The host on which you want to install CTE *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE to release 7.0.0 or later will fail.
- Thales recommends that you install CTE in the default location.
- Do not install CTE on network-mounted volumes such as NFS.
- Make the Installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -d /home/hello/
```

- Ensure read/write permission is granted to other users accessing your shared resource.

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the Linux system on which you plan to install CTE to the CipherTrust Manager. After the Linux system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.
- If the system is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

If a protected client must communicate with the CipherTrust Manager through a firewall, see the CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

The default port for communication between the CipherTrust Manager and the CTE Agent is 443. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

Interactive Installation on Linux

The Linux typical install is an interactive script that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see ["Silent Installation on Linux" on page 51](#)).

After you install CTE, you are prompted to register it immediately with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

Note

Do not install CTE on network-mounted volumes like NFS.

Before You Begin

Make sure you have the following information from the CM Administrator:

- The registration token for the CipherTrust Manager with which you plan to register the CTE Agent.
- The name of the profile you intend to assign to the client if you want to use a profile other than the default client profile.
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.

3. Install the CTE Agent. A typical installation uses the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note: If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type `y` and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.47
```

```
In order to register the CipherTrust Transparent Encryption File System Agent
with a Vormetric Data Security Manager
```

- 1) you must know the host name of the machine running the DSM (the host name is displayed on the Dashboard window of the Management Console), and
- 2) unless you intend to use the 'shared secret' registration method, the agent's host machine must be pre-configured on the DSM as a host with the 'Reg. Allowed' checkbox enabled for this agent type on the Hosts window of the Management Console.

```
In order to register with a CipherTrust Manager you need a valid registration
token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Enter `y` to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE. For example:

```
Do you want to continue with agent registration? (Y/N) [Y]: y
```

```
Please enter the primary key manager host name: 10.3.200.141
```

```
You entered the host name 10.3.200.141
```

```
Is this host name correct? (Y/N) [Y]: y
```

6. Enter the client host name when prompted.

Please enter the host name of this machine, or select from the following list.

```
[1] sys31186.qa.com
[2] 10.3.31.186
```

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: **2**
You selected "10.3.31.186".

7. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

Please enter the registration token: **12345**
Please enter the profile name for this host: **My-Profile**
Please enter the host group name for this host, if any:
Please enter a description for this host: **West Coast Datacenter server 5**

```
Token           : 12345
Profile name     : My-Profile
Host Group       : (none)
Host description : West Coast Datacenter server 5
Are the above values correct? (Y/N) [Y]: Y
```

8. At the hardware association prompt, select whether you want to enable the hardware association feature (for details, see ["Hardware Association \(Cloning Prevention\) Option" on page 28](#)). The default is **y** (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]: **Y**

9. At the LDT prompt, specify whether you want this client to use CipherTrust Transparent Encryption - Live Data Transformation (CTE-LDT).

Do you want this host to have LDT support enabled on the server? (Y/N) [N]: **Y**

10. At the Cloud Object Storage (COS) prompt, specify whether you want this client to use CTE COS.

Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:

11. CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.
Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption File System Agent with the
CipherTrust Manager on 10.3.200.141.

Installation success.
```

12. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Silent Installation on Linux

This section describes how to perform a silent (unattended) installation of the CTE on a single host. The silent installation automates the installation process by storing the answers to installation and registration questions in a separate file that you create. You can also use the silent installation to install CTE on multiple hosts simultaneously.

The silent install method installs CTE on the host, and registers the host with the CipherTrust Manager you specify in the silent installation file.

Prerequisites

Make sure you have the following information from the CM Administrator:

- The registration token for the CipherTrust Manager with which you plan to register the CTE Agent.
- The name of the profile you intend to assign to the client if you want to use a profile other than the default client profile.
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on as an administrator to the host where you will install CTE.
2. Create a parameter file and store it on your system, or copy an existing file from another location. The file can contain any of the following parameters:

Parameter	Description
SERVER_HOSTNAME	Required if you want to register CTE with a CipherTrust Manager.
REG_TOKEN	The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.
HOST_PROFILE	Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.
TMPDIR	Specifies a custom temporary directory that the installer can use during the installation process. If this value is omitted, the installer uses the default temporary directory.
HOST_DOMAIN	Specifies the domain name with which this CTE Agent will be associated.
HOST_GROUP	Specifies the optional client group with which this client will be associated.
AGENT_HOST_NAME	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
PKCS11_PASSWORD	The administrative password for the CTE Agent. Required if the CTE Agent is being registered with a CipherTrust Manager. This password allows users to access encrypted data on the client if it is disconnected from the CipherTrust Manager.
AGENT_USEIP	Use the IP address of the protected host instead of host name. Used when <code>-agent</code> is not supplied.

Parameter	Description
HOST_DESC	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
AGENT_HOST_PORT	Specifies the port number this CTE Agent should use.
USEHWSIG	Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.
ENABLE_LDT	Set this value to 1 to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.

The following example contains just the required information for registration with CipherTrust Manager. In this case, the client will be registered with the CipherTrust Manager using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
PKCS11_PASSWORD=ClientAdminP@$$w0rd
```

The following example specifies the required registration information, adds a host name and description, and enables hardware association and CTE-LDT. In this case, the client will be registered with the CipherTrust Manager using its host name instead of the IP address:

```
SERVER_HOSTNAME=DSM-Server.example.com
REG_TOKEN=12345
PKCS11_PASSWORD=ClientAdminP@$$w0rd
AGENT_HOST_NAME=myagent.example.com
HOST_DESC="West Coast Server 12"
USEHWSIG=1
ENABLE_LDT=1
```

- Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.

- Run the installer using the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin [-d <custom-dir>] -s <install-file>
```

where:

- `-d <custom-dir>` is an optional parameter that specifies the installation directory for CTE. If you omit this parameter, CTE is installed in `/opt/vormetric/DataSecurityExpert/agent/`.
- `-s <install-file>` indicates that you want to install silently using the installation options file `<install-file>`

For example, if the installation options file is called `/tmp/unattended.txt`, you would enter:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -s /tmp/unattended.txt
```

- Verify the installation by checking CTE processes on the host:
 - Run `vmc -v` to check the version of CTE matches that just installed.
 - Run `vmsec status` to display CTE kernel status.
 - Look at the log files in `/var/log/vormetric`, especially `install.fs.log.<date>` and `vorvmd_root.log`.
- In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Guarding a Device with CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

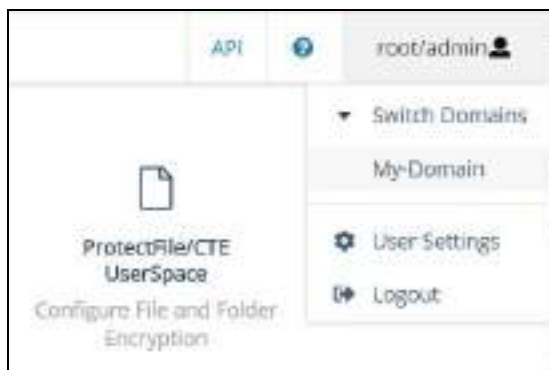
1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device or directory.
3. Identify or create a policy for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. Assign a GuardPoint to the device or directory.

The following example creates a simple policy and uses it to guard a directory on a registered client. For all of the following procedures, you must be logged into the CipherTrust Manager Console as a CipherTrust Manager Administrator, and you must be in the domain with which the client is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the CipherTrust Manager documentation.

Access the CipherTrust Manager Domain

1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to ["Create an Encryption Key" below](#). If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the user name **root/admin** on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.
 - c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

1. In the Applications page of the CipherTrust Manager Console, select **Keys & Access Management**.
2. Above the Key table, click **Create a New Key**.
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
4. In the **Key Metadata > Groups for Key sharing** section, do the following:

- a. In the **Search** box, type "cte".
- b. Add CTE Admins and CTE Clients to the key sharing groups by clicking the green **Add** button. The **Key Shared?** check box is automatically selected and the **Add** button changes to a **Remove** button.
- c. Below the Groups table, click the **CTE Key Properties** check box.

CipherTrust Manager displays the following options for CTE keys:

- **CTE Versioned:** Specify whether the key is versioned. By default, the key is set as versioned.
For a standard policy, you should clear this check box. If you do not, the key will *not* appear in the keys list when you add the key rule to the standard policy.
- **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.
When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.
When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.
- **Encryption Mode:** Encryption mode of the key. The options are:
 - CBC
 - CBC CS1
 - XTS

Encryption using the XTS and CBC CS1 keys is known as enhanced encryption. For details, see the *CTE Agent for Linux Advanced Configuration and Integration Guide*.



5. In the Key Behaviors section at the bottom of the page, clear the **Prevent this key from being exported** check box. If the key cannot be exported, the key will not appear in the keys list when you add the key rule to the policy.



6. Click **Create**. The new key appears in the Keys table.

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
2. In the sidebar on the Clients page, click **Policies**.
3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
4. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a Standard policy.
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/CTE-LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.
Data Transformation	If you select Standard as the policy type, also select the the Data Transformation option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

When you are done, click **Next**.

5. On the Security Rules page, define the security rules you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of `key_op` and the effects `Permit` and `Apply Key`. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version. This rule is required by CTE-LDT, so you cannot edit it, move it, or delete it.

To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

For this example, click **Create Security Rule** and:

- Set Action to `all_ops`.
- Set Effect to **Permit** and **Audit**.

When you are done, click **Next**.

6. On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one. If the data has not yet been encrypted, select clear_key . Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select clear_key .
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

When you are done, click **Next**.

7. On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click Select to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in "Create an Encryption Key" on page 34 .

When you are done, click **Next**.

8. Click **Next**.

- On the confirmation page, review the information for the policy and click **Save**.

Create Policy

General Info Security Rules Key Rules Data Transformation Rules Confirmation

Review the provided policy details.

General Info

Name: Create Policy
Policy Type: Standard
Description: Standard policy for new GuardPoints

Security Rules

Resource Set	User Set	Privilege Set	Action	Effect	Browsing
			key_for	perm:allow	Yes
			all_obj	perm:allow	Yes

Key Rules

Resource Set: Current Key Name: data-key

Data Transformation Rules

Resource Set: Transformation Key Name: encrypt-key

Back Save

Create a GuardPoint

- Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
 - /dir/hr/files
 - /dir/accounting/files
 - /dir/shared/hr
 - /dir/shared/accounting

Tip: If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

- In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
- In the Clients table, click on the name of the client you want to protect.
- Above the GuardPoints table, click **Create GuardPoint**.
- In the Create GuardPoint page:
 - In the **Policy** field, select the policy you created earlier.
 - In the **Type** field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
 - In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a explorer window.

If you want to enter multiple paths, put each path on its own line. For example:



- d. Click **Create**.
- e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**. For this example, click No.

The CipherTrust Manager pushes the GuardPoint configuration to the client and CTE immediately begins transforming the data in the specified folders from clear-text to cipher-text.

6. When the data transformation has finished, applications can resume accessing the now-protected data.

Configuring CTE for Linux with a DSM

This section describes how to install and configure CTE on Linux systems that you plan to register with a Vormetric Data Security Manager (DSM). This process requires actions from two roles:

- The *agent installer* or *host administrator* who uses these instructions to install and configure the CTE Agent on each Linux host whose data you want to protect.
- The DSM Administrator, who adds hosts to the DSM database using the FQDN or the IP address.

Installation Overview

The installation and configuration process for CTE with a DSM consists of three basic steps:

1. Gather the information needed for the install and set up your network as described in ["Installation Prerequisites" below](#).
2. Select the installation options you want to use as described in ["Installation and Registration Options" on page 42](#).
3. Install CTE on the protected host as described in ["Interactive Installation on Linux" on page 43](#) or ["Silent Installation on Linux" on page 51](#).
4. Register the protected host with the DSM and make sure that they can communicate with each other. This process can be done as part of the initial installation or at any point after the CTE Agent has been installed.

Installation Prerequisites

This section lists the tasks you must complete, and the information you must obtain, before installing CTE.

Recommendations and Considerations

- The host on which you want to install CTE *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE to release 7.0.0 or later will fail.
- Thales recommends that you install CTE in the default location.
- Do not install CTE on network-mounted volumes such as NFS.
- Make the Installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.
For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -d /home/hello/
```
- Ensure read/write permission is granted to other users accessing your shared resource.

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the DSM(s) to all hosts where you install CTE.
- If the host is a virtual machine, the VM must be deployed and running.

Host Name Resolution Requirements

Host name resolution is the method of mapping a host name to an IP address. During this configuration process, enter either the FQDNs, or IP addresses, of your DSM and protected hosts. If you use FQDNs, your protected hosts must be able to resolve the DSM host names, and the DSM must be able to resolve its protected hosts.

Note

The exception to this requirement is if you plan to configure one-way communication between CTE and the DSM.

A Domain Name Service (DNS) server is the preferred method of host name resolution. If you use DNS, use the FQDNs for the DSM and hosts.

If you do *not* use a DNS, you can do one of the following:

- Use the IP addresses of the DSM and protected hosts.
- Add an entry in the `/etc/hosts` file on the DSM associated with the host. The administrator must use the CipherTrust CLI, and, in an HA environment, they must add an entry to *each* DSM in the cluster because entries in the `/etc/hosts` file are not replicated across the cluster.

Port Configuration Requirements

If a protected host must communicate with the DSM through a firewall, see the *DSM Administration Guide* to determine which of the ports must be opened through the firewall.

The default port for communication between the DSM and the CTE Agent is 7024. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

One-way Communication Option

In some deployments, CTE might not be visible to the DSM through normal network communications. For example, when the host on which CTE is installed:

- is behind NAT.
- is behind a firewall.
- is not permanently connected to a communication channel to the DSM.
- is unable to resolve the host name to an IP address.

In these situations, CTE can initiate CTE-only communication to the DSM. This feature is called one-way communication and works by having CTE poll the DSM for any policy messages or changes, then downloading changes as required.

The downside of one-way communication is that the DSM cannot issue any queries to CTE. For example, the DSM Administrator cannot browse host directories or User IDs. To enable the full functionality of both CTE and the CipherTrust Manager, Thales recommends that you use two-way communication between them whenever possible.

Port Usage in One-Way Communications Mode

By default, polling from the agent host to the DSM when running in one-way communications mode uses HTTP via port 8080. If the CTE Agent is configured to use secure polling, then polling is performed using HTTPS via port 8448 (in suite B mode) or port 8445.

Determining Kernel Compatibility With CTE

As new Red Hat, SUSE, and Ubuntu Linux kernels are published, Thales regularly publishes new patch versions of CTE that are compatible with selected versions of these new kernels. Thales recommends that you check that the kernel on which you want to install CTE is verified to be compatible with CTE. CTE may appear to run correctly on an unsupported kernel. However, Thales strongly advises against running CTE on an unsupported kernel due to potential stability issues.

The table below describes several ways to verify that a kernel version is compatible with the version of CTE that you plan to install or are running. For more information, see the following sections.

Methods to check kernel compatibility with CTE

Kernel compatibility check method	How to check	Description
Compatibility Matrix for CTE Agent with Data Security Manager document	Download from Thales support site	Includes kernel compatibility and other types of compatibility such as file system, database, antivirus, and DSM version compatibility.
Automated kernel compatibility check during installation or upgrade	Kernel compatibility is checked during installation or upgrade	If an incompatible kernel is detected, a message is printed to the screen and logged to <code>syslog</code> .
Automated run-time kernel compatibility check	Kernel compatibility is checked when the CTE services start	If an incompatible kernel is detected, a message is logged to <code>syslog</code> .

Installation and Registration Options

CTE provides the following installation and registration options. The options you choose determine the information you need to supply during the actual install procedure, so you should decide what options you want to use before you start the installation.

Installation Method Options

There are two methods for installing CTE on Linux platforms:

- **Interactive:** Most common and recommended type of installation. Use this method for installing the CTE Agent on one host at a time. See ["Interactive Installation on Linux" on the next page](#).
- **Silent:** Create pre-packaged installations by providing information and answers to a set of installation questions. Use silent installations when installing on a large number of hosts. See ["Silent Installation on Linux" on page 51](#).

CTE Registration Method Options

You can register the protected hosts with a DSM using either the *Fingerprint method* or the *Shared Secret method*.

- **Fingerprint method** requires the DSM Administrator to add the FQDN, or IP address, of each protected host to the DSM before registering CTE.
During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. The security administrator must verify the fingerprint to make sure the certificate is valid.
- **Shared Secret method** requires the DSM Administrator to create a *shared secret* password—a case-sensitive string of characters—for auto-registering a domain or host group.
CTE installers use the shared secret to add and register protected hosts to the DSM for a domain or host group. The DSM Administrator can optionally add host names or IP addresses to the DSM. There is no need to verify that the protected host and DSM share valid certificates. You can add multiple protected hosts dynamically with a single shared secret password during CTE installation and registration.
After the DSM Administrator creates a shared secret for the domain or host group in which the new protected host will reside, obtain it and the validity period (one hour, day, week, or month) and register within that period.

Hardware Association (Cloning Prevention) Option

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware hosts.

You can enable hardware association during CTE registration process. You can disable hardware association by re-running the registration program.

To verify if hardware association (cloning prevention) is enabled on a Linux host, on the command line enter the following:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/access
```

If you see `usehw:true`, then hardware association is enabled. If you see `usehw:false`, it's disabled.

CTE Linux Installation Checklist

Use the following table to verify prerequisites and collect the information you need for the installation.

Checklist item	Notes
Obtain the CTE Agent installation image from Thales. The format for the installation file names is: <code>vee-fs-<release>-<build>-<system>.bin</code> For example: <code>vee-fs-7.0.0-47-rh8-x86_64.bin</code>	
Get the Fully Qualified Domain Name (FQDN) of the DSM as shown on the DSM Dashboard.	
Get the IP address or FQDN of the host. If you are using the Fingerprint registration method, this must match exactly with the name specified in the DSM.	
Make sure you have the <code>root</code> user login credentials for the host. You must install CTE as <code>root</code> .	
If using Shared Secret registration, obtain the following from the DSM Administrator: • Shared secret password • Domain • Host group, if applicable • Description of the host (Optional)	
If using the Fingerprint registration method: • Ask the DSM Administrator to add the host to the DSM and check the Registration Allowed and Communication Enabled check boxes. • Get the EC CA certificate fingerprint as shown on the DSM Dashboard.	
Make sure the host can communicate with the DSM. For details, see "Host Name Resolution Requirements" on page 40 .	
Make sure the correct ports are open. For details, see "Port Configuration Requirements" on page 40 .	
Determine if you want to use the One-way communication option. For details, see "One-way Communication Option" on page 41 .	
Determine if you want to use the Hardware Association feature. For details, see "Hardware Association (Cloning Prevention) Option" on the previous page .	
Synchronize the host clock to the DSM clock.	
Determine your preferred DNS Server (if using FQDNs).	

Interactive Installation on Linux

The Linux interactive install is a standard interactive script that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see ["Silent Installation on Linux" on page 51](#)).

After you install CTE, you are prompted to register it immediately with a DSM. CTE must be registered with a DSM before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

The procedure for installing CTE depends on the registration method you want to use. The available methods are described in ["CTE Registration Method Options" on page 42](#). After you have selected your registration method, you can use one of the following procedures:

- ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 47](#)
- ["Installing CTE and Registering Using the Certificate Fingerprint" below](#)

Note

Do not install CTE on network-mounted volumes like NFS.

Installing CTE and Registering Using the Certificate Fingerprint

The following procedure describes how to install the CTE Agent on the host and then register the CTE Agent with a DSM using the Fingerprint registration method. For more information about the available registration methods, see ["CTE Registration Method Options" on page 42](#).

For other installation options, see ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 47](#) and ["Installing CTE with No Key Manager Registration" on page 27](#).

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.

3. Install the CTE Agent. A typical installation uses the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note: If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type `y` and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.47
```

In order to register the CipherTrust Transparent Encryption File System Agent with a Vormetric Data Security Manager

- 1) you must know the host name of the machine running the DSM (the host name is displayed on the Dashboard window of the Management Console), and
- 2) unless you intend to use the 'shared secret' registration method, the agent's host machine must be pre-configured on the DSM as a host with the 'Reg. Allowed' checkbox enabled for this agent type on the Hosts window of the Management Console.

In order to register with a CipherTrust Manager you need a valid registration token from the CM.

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Enter **y** to continue with the registration process. The install script prompts you to enter the name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

```
Do you want to continue with agent registration? (Y/N) [Y]: y
```

```
Please enter the primary key manager host name: dsm630-121079.i.vormetric.com
```

```
You entered the host name dsm630-121079.i.vormetric.com
```

```
Is this host name correct? (Y/N) [Y]: y
```

6. Enter the host name when prompted. This name must match the name used on the **Add Host** page of the DSM Management Console.

Please enter the host name of this machine, or select from the following list. If using the "fingerprint" registration method, the name you provide must precisely match the name used on the "Add Host" page of the Management Console.

```
[1] host14.i.example.com  
[2] Host-RHEL-14.i.example.com  
[3] 10.3.14.90
```

```
Enter a number, or type a different host name or IP address in manually:
```

```
What is the name of this machine? [1]: 3
```

```
You selected "10.3.14.90".
```

7. When prompted for the registration method, enter **F** for fingerprint registration:

```
Would you like to register to the DSM using a  
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: F
```

8. At the hardware association prompt, select whether you want to enable the hardware association feature that prevents a clone of this machine from accessing keys in the DSM. The default is **y** (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again.

```
Do you want to enable this functionality? (Y/N) [Y]: y
```

- At this point, the install script asks you about some of the optional CTE features you may want to enable, such as CTE-Efficient Storage, CTE-LDT, and docker support.

Note: Some of these features may require a separate license in the DSM.

For example:

Do you want this host to have docker support enabled on the server? (Y/N) [N]:

Do you want this host to have Efficient Storage support enabled on the server? (Y/N) [N]:

Do you want this host to have LDT support enabled on the server? (Y/N) [N]:

Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:

- At this point, the install program generates certificate signing requests and lists the fingerprint of the EC (elliptic curve) CA (Certificate Authority) certificate. This fingerprint must match the one on the DSM Dashboard in the **Management Summary** section, **EC CA fingerprint** field.

The following is the fingerprint of the EC CA certificate.

Please verify that it matches the fingerprint shown on the Dashboard page of the Management Console. If they do not match, it can indicate an unsuccessful setup or an attack.

2F:9A:1C:DB:7E:B9:6C:63:D4:BA:D2:25:C6:7C:97:F1:E1:48:20:AE

Do the fingerprints match? (Y/N) [N]: **Y**

If the fingerprints match, enter **y**. The installer displays the fingerprint for the CTE Agent on the host and completes the installation:

The following is the fingerprint for this agent on this host.

Please verify that it matches the fingerprint shown for this host on the Edit Host window of the Management Console.

12:CF:64:A3:28:7E:2E:50:72:70:FF:8F:B2:79:5B:4F:40:1B:74:20

Successfully registered the CipherTrust Transparent Encryption File System Agent with the Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.

Installation success.

- Verify with the DSM Administrator that the CTE fingerprint matches with the fingerprint shown for this host on the **Hosts > Hostname > Edit Host** window of the DSM Management Console. CTE is installed and registered.
- Verify the installation by checking the CTE processes on the host:
 - Run `vmd -v` to check the version of CTE.
 - Run `vmsec status` to display the CTE processes.
 - Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

Installing CTE and Registering Using the Shared Secret Registration Method

The following procedure describes how to install the CTE Agent on the Linux host and then register the CTE Agent with a DSM using the Shared Secret registration method. For more information about the available registration methods, see ["CTE Registration Method Options" on page 42](#).

For other installation options, see ["Installing CTE and Registering Using the Certificate Fingerprint" on page 44](#) and ["Installing CTE with No Key Manager Registration" on page 27](#).

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note: If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type **y** and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.47
```

In order to register the CipherTrust Transparent Encryption File System Agent with a Vormetric Data Security Manager

- 1) you must know the host name of the machine running the DSM (the host name is displayed on the Dashboard window of the Management Console), and
- 2) unless you intend to use the 'shared secret' registration method, the agent's host machine must be pre-configured on the DSM as a host with the 'Reg. Allowed' checkbox enabled for this agent type on the Hosts window of the Management Console.

In order to register with a CipherTrust Manager you need a valid registration token from the CM.

Do you want to continue with agent registration? (Y/N) [Y]:

5. Enter **y** to continue with the registration process. The install script prompts you to enter the name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

Do you want to continue with agent registration? (Y/N) [Y]: **y**

Please enter the primary key manager host name: **dsm630-121079.i.vormetric.com**

You entered the host name dsm630-121079.i.vormetric.com

Is this host name correct? (Y/N) [Y]: **y**

6. Enter the host name when prompted. If the Shared Secret registration in your DSM is configured to require an existing host entry, his name must match the name used on the **Add Host** page of the DSM Management Console.

Please enter the host name of this machine, or select from the following list. If using the "fingerprint" registration method, the name you provide must precisely match the name used on the "Add Host" page of the Management Console.

```
[1] host14.i.example.com
[2] Host-RHEL-14.i.example.com
[3] 10.3.14.90
```

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: **3**
You selected "10.3.14.90".

7. When prompted for the registration method, enter **s** for shared secret registration and then enter the required information about the domain, optional host group, and optional host description. For example:

Would you like to register to the DSM using a
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: **S**

What is the registration shared secret?
Please enter the domain name for this host: **west-coast-domain**
Please enter the host group name for this host, if any:
Please enter a description for this host: **West Coast Data Center server 5**

```
Shared secret      : *****
Domain name       : west-coast-domain
Host Group        : (none)
Host description   : West Coast Data Center server 5
Are the above values correct? (Y/N) [Y]: Y
```

8. At the hardware association prompt, select whether you want to enable the hardware association feature that prevents a clone of this machine from accessing keys in the DSM. The default is **y** (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]: **Y**

9. At this point, the install script asks you about some of the optional CTE features you may want to enable, such as CTE-Efficient Storage, CTE-LDT, and docker support.

Note: Some of these features may require a separate license in the DSM.

For example:

Do you want this host to have docker support enabled on the server? (Y/N) [N]:

Do you want this host to have Efficient Storage support enabled on the server? (Y/N) [N]:

Do you want this host to have LDT support enabled on the server? (Y/N) [N]:

Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:

10. At this point the installation script completes the installation and indicates that it successfully registered the host with the DSM.

```
Generating certificate signing request for the kernel component...done.  
Signing certificate...done.  
Generating EC certificate signing request for the vmd...done.  
Signing certificate...done.  
Generating EC certificate signing request for the vmd...done.  
Signing certificate...done.  
Successfully registered the CipherTrust Transparent Encryption File System Agent with the  
Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.
```

11. Verify the installation by checking the CTE processes on the host:

- Run `vmd -v` to check the version of CTE.
- Run `vmsec status` to display the CTE processes.
- Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

Silent Installation on Linux

This section describes how to perform a silent (unattended) installation of the CTE on a single host. The silent installation automates the installation process by storing the answers to installation and registration questions in a separate file that you create. You can also use the silent installation to install CTE on multiple hosts simultaneously.

The silent install method installs CTE on the host, and registers the host with the DSM you specify in the silent installation file.

For details, see one of the following procedures:

- ["Silent Installation on Linux Using the Shared Secret Registration Method" below](#)
- ["Silent Installation on Linux Using the Fingerprint Registration Method" on page 53](#)

Silent Installation on Linux Using the Shared Secret Registration Method

This section describes how to perform a silent (unattended) installation of the CTE on a single host. The silent installation automates the installation process by storing the answers to installation and registration questions in a separate file that you create. You can also use the silent installation to install CTE on multiple hosts simultaneously.

The silent install method installs CTE on the host, and registers the host with the DSM you specify in the silent installation file using the Shared Secret registration method. To register it using the Fingerprint registration method, see ["Silent Installation on Linux Using the Fingerprint Registration Method" on page 53](#).

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on as an administrator to the host where you will install CTE.
2. Create a parameter file and store it on your system, or copy an existing file from another location. The file can contain any of the following parameters:

Parameter	Description
SERVER_HOSTNAME	Required if you want to register CTE with a DSM.
TMPDIR	Specifies a custom temporary directory that the installer can use during the installation process. If this value is omitted, the installer uses the default temporary directory.
SHARED_SECRET	Specifies the shared secret for the DSM. This value is required for shared secret registration.
AGENT_HOST_NAME	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
PKCS11_PASSWORD	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
AGENT_USEIP	Use the IP address of the protected host instead of host name. Used when <code>-agent</code> is not supplied.
HOST_DESC	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
AGENT_HOST_PORT	Specifies the port number this CTE Agent should use.
USEHWSIG	Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.
ENABLE_LDT	Set this value to 1 to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.
ENABLE_ES	Set this value to 1 to automatically enable and register CTE-Efficient Storage during silent install.
ENABLE_DOCKER	Set this value to 1 if you want to enable docker security on this host.
ONEWAY_COMMS	Set this value to 1 when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

Parameter	Description
CERT_FIELD_PARAM	If you are using CTE-Cloud Object Storage, this option specifies a custom certificate field values for the CTE COS Root CA Certificate.
SUBJECT_ALT_NAME_PARAM	If you are using CTE-Cloud Object Storage, this option specifies a custom Subject Alt Name for the CTE COS Root CA Certificate. You must also specify CERT_FIELD_PARAM to use this parameter.
STRONG_ENTROPY	Set this value to 1 to switch between /dev/random and /dev/urandom based on read speed.

The following example contains just the required information for Shared Secretregistration. In this case, the host will be registered with the DSM using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
SHARED_SECRET=Shallac112345#
HOST_DOMAIN=My-Domain
```

The following example specifies the required registration information, adds a host name and description, and enables hardware association, CTE-Efficient Storage, and CTE-LDT. In this case, the host will be registered with the DSM using its host name instead of the IP address:

```
SERVER_HOSTNAME=DSM-Server.example.com
AGENT_HOST_NAME=myagent.example.com
SHARED_SECRET=Shallac112345#
HOST_DOMAIN=My-Domain
HOST_DESC="West Coast Server 12"
USEHWSIG=1
ENABLE_ES=1
ENABLE_LDT=1
```

3. Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.

4. Run the installer using the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin [-d <custom-dir>] -s <install-file>
```

where:

- `-d <custom-dir>` is an optional parameter that specifies the installation directory for CTE. If you omit this parameter, CTE is installed in `/opt/vormetric/DataSecurityExpert/agent/`.
- `-s <install-file>` indicates that you want to install silently using the installation options file `<install-file>`

For example, if the installation options file is called `/tmp/unattended.txt`, you would enter:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -s /tmp/unattended.txt
```

5. Verify the installation by checking CTE processes on the host:
 - Run `vmd -v` to check the version of CTE matches that just installed.
 - Run `vmsec status` to display CTE kernel status.
 - Look at the log files in `/var/log/vormetric`, especially `install.fs.log.<date>` and `vorvmd_root.log`.

Silent Installation on Linux Using the Fingerprint Registration Method

This section describes how to perform a silent (unattended) installation of the CTE on a single host. The silent installation automates the installation process by storing the answers to installation and registration questions in a separate file that you create. You can also use the silent installation to install CTE on multiple hosts simultaneously.

The silent install method installs CTE on the host, and registers the host with the DSM you specify in the silent installation file using the Fingerprint registration method. To register using the Shared Secret registration method, see ["Silent Installation on Linux Using the Shared Secret Registration Method" on page 51](#).

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on as an administrator to the host where you will install CTE.
2. Create a parameter file and store it on your system, or copy an existing file from another location. The file can contain any of the following parameters:

Parameter	Description
SERVER_HOSTNAME	Required if you want to register CTE with a DSM.
TMPDIR	Specifies a custom temporary directory that the installer can use during the installation process. If this value is omitted, the installer uses the default temporary directory.
AGENT_HOST_NAME	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
PKCS11_PASSWORD	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
AGENT_USEIP	Use the IP address of the protected host instead of host name. Used when <code>-agent</code> is not supplied.
HOST_DESC	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
AGENT_HOST_PORT	Specifies the port number this CTE Agent should use.
USEHWSIG	Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.

Parameter	Description
ENABLE_LDT	Set this value to 1 to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.
ENABLE_ES	Set this value to 1 automatically enable and register CTE-Efficient Storage during silent install.
ENABLE_DOCKER	Set this value to 1 if you want to enable docker security on this host.
ONEWAY_COMMS	Set this value to 1 when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.
CERT_FIELD_PARAM	If you are using CTE-Cloud Object Storage, this option specifies a custom certificate field values for the CTE COS Root CA Certificate.
SUBJECT_ALT_NAME_PARAM	If you are using CTE-Cloud Object Storage, this option specifies a custom Subject Alt Name for the CTE COS Root CA Certificate. You must also specify <code>CERT_FIELD_PARAM</code> to use this parameter.
STRONG_ENTROPY	Set this value to 1 to switch between <code>/dev/random</code> and <code>/dev/urandom</code> based on read speed.

The following example contains just the required information for Fingerprint registration. In this case, the host will be registered with the DSM using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
```

The following example specifies the required registration information, adds a host name and description, and enables hardware association, CTE-Efficient Storage, and CTE-LDT. In this case, the host will be registered with the DSM using its host name instead of the IP address:

```
SERVER_HOSTNAME=DSM-Server.example.com
AGENT_HOST_NAME=myagent.example.com
HOST_DESC="West Coast Server 12"
USEHWSIG=1
ENABLE_ES=1
ENABLE_LDT=1
```

3. Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.

4. Run the installer using the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin [-d <custom-dir>] -s <install-file>
```

where:

- `-d <custom-dir>` is an optional parameter that specifies the installation directory for CTE. If you omit this parameter, CTE is installed in `/opt/vormetric/DataSecurityExpert/agent/`.
- `-s <install-file>` indicates that you want to install silently using the installation options file `<install-file>`

For example, if the installation options file is called `/tmp/unattended.txt`, you would enter:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -s /tmp/unattended.txt
```

5. Verify the installation by checking CTE processes on the host:
 - Run `vmd -v` to check the version of CTE matches that just installed.
 - Run `vmsec status` to display CTE kernel status.
 - Look at the log files in `/var/log/vormetric`, especially `install.fs.log.<date>` and `vorvmd_root.log`.

Registering CTE with the Shared Secret Registration Method After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 47](#) or ["Installing CTE and Registering Using the Certificate Fingerprint" on page 44](#).

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot register the CTE Agent without `root` access.
2. Launch the CTE Registration script by running the `register_host` script. The default location is `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`. For example:

```
# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.47
```

In order to register the CipherTrust Transparent Encryption File System Agent with a Vormetric Data Security Manager

- 1) you must know the host name of the machine running the DSM (the host name is displayed on the Dashboard window of the Management Console), and
- 2) unless you intend to use the 'shared secret' registration method, the agent's host machine must be pre-configured on the DSM as a host with the 'Reg. Allowed' checkbox enabled for this agent type on the Hosts window of the Management Console.

In order to register with a CipherTrust Manager you need a valid registration

token from the CM.

Do you want to continue with agent registration? (Y/N) [Y]:

3. Enter **y** to continue with the registration process. The install script prompts you to enter the name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

Do you want to continue with agent registration? (Y/N) [Y]: **y**

Please enter the primary key manager host name: **dsm630-121079.i.vormetric.com**

You entered the host name dsm630-121079.i.vormetric.com

Is this host name correct? (Y/N) [Y]: **y**

4. Enter the host name when prompted. If the Shared Secret registration in your DSM is configured to require an existing host entry, his name must match the name used on the **Add Host** page of the DSM Management Console.

Please enter the host name of this machine, or select from the following list. If using the "fingerprint" registration method, the name you provide must precisely match the name used on the "Add Host" page of the Management Console.

```
[1] host14.i.example.com
[2] Host-RHEL-14.i.example.com
[3] 10.3.14.90
```

Enter a number, or type a different host name or IP address in manually:

What is the name of this machine? [1]: **3**

You selected "10.3.14.90".

5. When prompted for the registration method, enter **s** for shared secret registration and then enter the required information about the domain, optional host group, and optional host description. For example:

Would you like to register to the DSM using a
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: **s**

What is the registration shared secret?

Please enter the domain name for this host: **west-coast-domain**

Please enter the host group name for this host, if any:

Please enter a description for this host: **West Coast Data Center server 5**

```
Shared secret      : *****
Domain name       : west-coast-domain
Host Group        : (none)
Host description   : West Coast Data Center server 5
Are the above values correct? (Y/N) [Y]: y
```

6. At the hardware association prompt, select whether you want to enable the hardware association feature that prevents a clone of this machine from accessing keys in the DSM. The default is **y** (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]: **y**

7. At this point, the install script asks you about some of the optional CTE features you may want to enable, such as CTE-Efficient Storage, CTE-LDT, and docker support.

Note: Some of these features may require a separate license in the DSM.

For example:

Do you want this host to have docker support enabled on the server? (Y/N) [N]:

Do you want this host to have Efficient Storage support enabled on the server? (Y/N) [N]:

Do you want this host to have LDT support enabled on the server? (Y/N) [N]:

Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:

8. At this point the installation script completes the installation and indicates that it successfully registered the host with the DSM.

Generating certificate signing request for the kernel component...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Successfully registered the CipherTrust Transparent Encryption File System Agent with the Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.

9. Verify the installation by checking the CTE processes on the host:
 - Run `vmd -v` to check the version of CTE.
 - Run `vmsec status` to display the CTE processes.
 - Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

Registering CTE with the Fingerprint Registration Method After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see ["Installing CTE and Registering Using the Certificate Fingerprint" on page 44](#) or ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 47](#).

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot register the CTE Agent without `root` access.
2. Launch the CTE Registration script by running the `register_host` script. The default location is `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`. For example:

```
# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.47
```

In order to register the CipherTrust Transparent Encryption File System Agent with a Vormetric Data Security Manager

- 1) you must know the host name of the machine running the DSM (the host name is displayed on the Dashboard window of the Management Console), and
- 2) unless you intend to use the 'shared secret' registration method, the agent's host machine must be pre-configured on the DSM as a host with the 'Reg. Allowed' checkbox enabled for this agent type on the Hosts window of the Management Console.

In order to register with a CipherTrust Manager you need a valid registration token from the CM.

Do you want to continue with agent registration? (Y/N) [Y]:

3. Enter `y` to continue with the registration process. The install script prompts you to enter the name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

Do you want to continue with agent registration? (Y/N) [Y]: **y**

Please enter the primary key manager host name: **dsm630-121079.i.vormetric.com**

You entered the host name dsm630-121079.i.vormetric.com

Is this host name correct? (Y/N) [Y]: **y**

4. Enter the host name when prompted. This name must match the name used on the **Add Host** page of the DSM Management Console.

Please enter the host name of this machine, or select from the following list. If using the "fingerprint" registration method, the name you provide must precisely match the name used on the "Add Host" page of the Management Console.

```
[1] host14.i.example.com
[2] Host-RHEL-14.i.example.com
[3] 10.3.14.90
```

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: **3**
You selected "10.3.14.90".

5. When prompted for the registration method, enter **F** for fingerprint registration:

Would you like to register to the DSM using a
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: **F**

6. At the hardware association prompt, select whether you want to enable the hardware association feature that prevents a clone of this machine from accessing keys in the DSM. The default is **y** (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]: **y**

7. At this point, the install script asks you about some of the optional CTE features you may want to enable, such as CTE-Efficient Storage, CTE-LDT, and docker support.

Note: Some of these features may require a separate license in the DSM.

For example:

Do you want this host to have docker support enabled on the server? (Y/N) [N]:

Do you want this host to have Efficient Storage support enabled on the server? (Y/N) [N]:

Do you want this host to have LDT support enabled on the server? (Y/N) [N]:

Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:

8. At this point, the install program generates certificate signing requests and lists the fingerprint of the EC (elliptic curve) CA (Certificate Authority) certificate. This fingerprint must match the one on the DSM Dashboard in the **Management Summary** section, **EC CA fingerprint** field.

The following is the fingerprint of the EC CA certificate.
Please verify that it matches the fingerprint shown on the Dashboard page of the Management Console. If they do not match, it can indicate an unsuccessful setup or an attack.

```
2F:9A:1C:DB:7E:B9:6C:63:D4:BA:D2:25:C6:7C:97:F1:E1:48:20:AE
```

```
Do the fingerprints match? (Y/N) [N]: Y
```

If the fingerprints match, enter **y**. The installer displays the fingerprint for the CTE Agent on the host and completes the installation:

The following is the fingerprint for this agent on this host.
Please verify that it matches the fingerprint shown for this host on the Edit Host window of the Management Console.

```
12:CF:64:A3:28:7E:2E:50:72:70:FF:8F:B2:79:5B:4F:40:1B:74:20
```

```
Successfully registered the CipherTrust Transparent Encryption File System Agent with the  
Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.
```

```
Installation success.
```

9. Verify with the DSM Administrator that the CTE fingerprint matches with the fingerprint shown for this host on the **Hosts > Hostname > Edit Host** window of the DSM Management Console. CTE is installed and registered.
10. Verify the installation by checking the CTE processes on the host:
 - Run `vmd -v` to check the version of CTE.
 - Run `vmsec status` to display the CTE processes.
 - Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

Guarding a Device with the DSM

After you register a device with a DSM, you can create as many GuardPoints on the device as you need. These GuardPoints can protect the entire device or individual directories or files.

In order to guard a device, you need to use the DSM Management Console to:

1. Access the DSM domain in which the host is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device.
3. Identify or create a policy for the device that specifies the access controls and the encryption keys to use for the device.
4. Create a GuardPoint for the device.

The following example creates a simple policy with a single key rule and no access controls and uses it to guard several directories on a registered host. For all of the following procedures, you must be logged into the DSM Management Console as a DSM Administrator, and you must be in the domain with which the host is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the *DSM Administration Guide*.

Access the DSM Domain

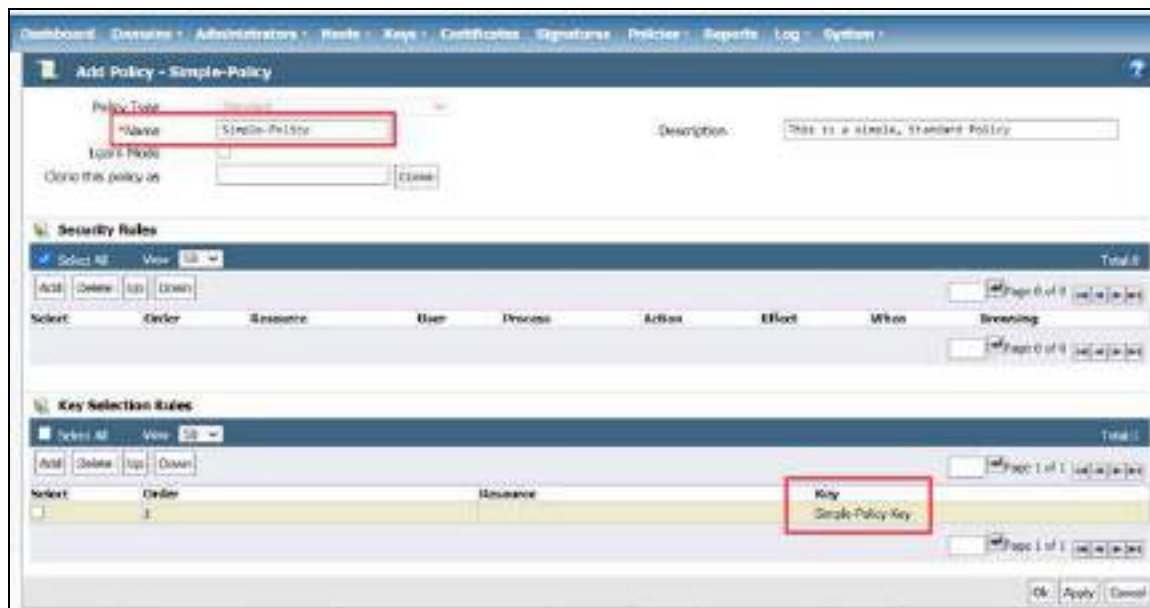
1. In a web browser, navigate to the URL of the DSM you want to use and log in with DSM Administrator credentials.
2. In the top menu bar of the DSM Management Console, select **Domains > Switch Domains**.
3. Select the domain with which the host you want to protect is registered and click **Switch to domain**.

Create an Encryption Key

1. In the top menu bar of the DSM Management Console, select **Keys**.
2. In the Key table, click **Add**
3. In the **Name** field, add a name for the key. This name must be unique. For example, Simple-Policy-Key.
4. Set any other desired options or use the defaults provided.
5. Click **Ok**.

Create a Standard Policy

1. In the top menu bar, select **Policies**.
2. In the Policy table, click **Add**.
3. In the Add Policy page:
 - a. Select a Policy Type. In this example, we will create a Standard policy.
 - b. Enter a name for the policy in the **Name** field. For example, Simple-Policy.
 - c. Enter a description for the policy in the **Description** field.
 - d. In the Key Selection Rules section, click **Add**.
 - e. In the Key field, click **Select**.
 - f. Select the key you created earlier and click **Select key**.
 - g. Click **Ok**.



4. Click **Ok** to create the policy.

Create a GuardPoint

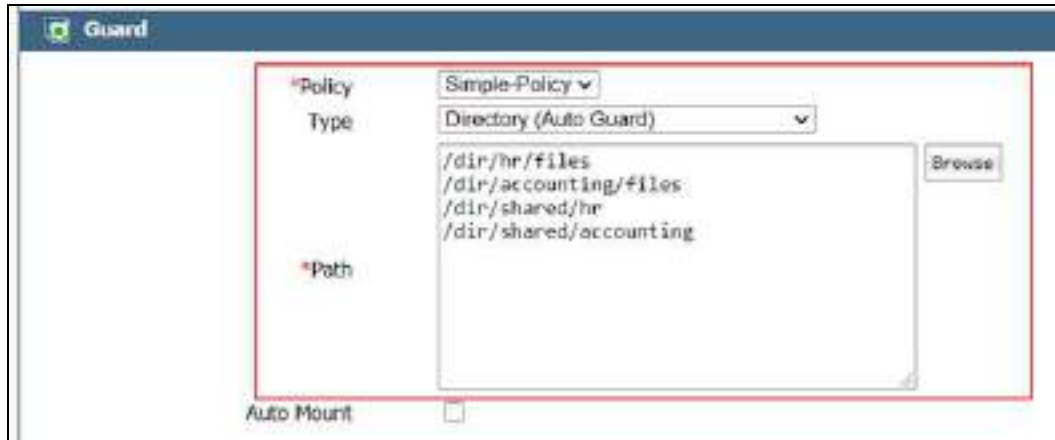
1. Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
 - /dir/hr/files
 - /dir/accounting/files
 - /dir/shared/hr
 - /dir/shared/accounting

Tip: If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

2. In the top menu bar, click **Hosts**.
3. In the Hosts table, click on the name of the host you want to protect.
4. Click the **GuardPoints** tab.
5. In the GuardPoints table, click **Guard**.

6. In the Guard page:
 - a. In the **Policy** field, select the policy you created earlier.
 - b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Directory (Auto Guard)**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a Windows-style explorer.

If you want to enter multiple paths, put each path on its own line. For example:



- d. Click **Ok**.

The DSM pushes the GuardPoint configuration to the host and CTE immediately begins transforming the data in the specified folders from clear-text to cipher-text.

7. When the data transformation has finished, applications can resume accessing the now-protected data.

Chapter 3: Special Cases for CTE Policies

This chapter describes some CTE-specific configuration tasks related to configuring policies in the DSM and contains the following sections:

More Information About Configuring CTE Policies	65
Re-Signing Executable Files on Secfs GuardPoints	65
Re-Enabling Automatic Signing for Host Settings	66
Restricting Access Overrides from Unauthorized Identities	66

More Information About Configuring CTE Policies

This chapter describes some special cases that apply only to CTE agent policy configuration. See the DSM Administration Guide for general information about configuring policies. The following chapters in the *DSM Administration Guide* pertain specifically to the information in this chapter:

- “Creating and Configuring Signature Sets”
- “Configuring Hosts and Host Groups”
- “Configuring Policies”

Re-Signing Executable Files on Secfs GuardPoints

If any of your existing VTE for Linux hosts are running VTE versions prior to version 6.1.2, an issue affects signed executables in Live Data Transformation policies. In these older VTE versions, any executable that is part of either a host setting or a Signature set, and resides in a GuardPoint that uses a Live Data Transformation policy will have a different SHA signature after every LDT key rotation. After each LDT key rotation, the host settings executables will no longer be authenticated, or the Signature Set policy rules that include those executables will no longer match them as expected. This problem occurred because VTE generated an SHA signature of the encrypted executable which changes after each key rotation. To work around these issues on these older VTE versions, the DSM Security Administrator must manually re-sign each affected executable after each key rotation. This workaround is *not* needed for any VTE for Linux release version 6.1.2 or later.

The SHA signature is created from the unencrypted executable. This new SHA signature does not change with a key rotation.

If upgrading or installing a new machine using the same signature sets that you used previously, do the following:

1. Install the current release of the CTE Agent. The previous signatures will be used until the next key rotation.
2. Before the next key rotation, the security administrator must resign the binaries.
3. Do not remove the old signatures on the DSM or CipherTrust Manager until all agents have been upgraded to the latest CTE release. Refer to the *DSM Installation and Configuration Guide* for information on how to perform a manual re-sign.
4. After all agents have been upgraded, then you can remove the old signatures.

Note

In previous releases, if the executable was in a GuardPoint protected directory, but was the same as an unguarded executable, the administrator could restrict only the guarded executable. In the current release of CTE, the unguarded executable matches the guarded executable with regards to policies.

Re-Enabling Automatic Signing for Host Settings

Starting with VTE for Linux release 6.0.2, VTE blocks automatic re-signing of the host settings. Some users may have established procedures for updating system software that are based on the assumption that restarting the `vmd` will generate new signatures when signed software is updated. This is no longer true. However, you can re-enable automatic re-signing if your environment requires it.



CAUTION

Re-enabling the automatic regeneration of signatures exposes a potential security vulnerability for CTE Agents. When enabled, host setting binaries are re-signed when CTE receives a push from the associated key manager. If an attacker were to replace a binary with a Trojan, and then force a push from the key manager by, for example, restarting the CTE Agent, CTE could generate a signature for the malicious binary and pass it.

To re-enable automatic re-signing for host settings:

1. Change to the directory where the `agent.conf` file resides. For example, type:

```
# cd /opt/vormetric/DataSecurityExpert/agent/vmd/etc/
```

2. Edit the `agent.conf` file.

3. Change or add the following line:

```
AUTO_RESIGN_HOST_SETTINGS=TRUE
```

Note: Previously this setting was known as `RE_SIGN_HOST_SETTINGS`. Starting with VTE for Linux 6.1.3, the attribute name is `AUTO_RESIGN_HOST_SETTINGS` as shown above.

4. Save your changes and exit the file.
5. Restart the `vmd` to set the changes. Type:

```
# /etc/vormetric/secfs restart
```

6. Type the following to verify that the host settings is set to true:

```
# vmsec vmdconfig
```

Restricting Access Overrides from Unauthorized Identities

In some setups, system administrators can use the host settings `> |authenticator|` feature with `su` to change identities and gain access to restricted data. Now, you can instruct CTE to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CTE can block from authenticating other processes.

Any executable path that is marked with a `|path_no_trust|` host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

CTE prevents overrides from other host settings authenticators, using the `|path_no_trust|` status. If a user runs the `su` command from a non-trusted shell, that new shell is still marked as `|path_no_trust|`, even if `|authenticator|/usr/bin/su` is specified in the host-settings. The `|path_no_trust|` feature overrides any and all authenticators under host settings.

To restrict access overrides in the DSM:

1. At the DSM Management Console, click **Hosts > Hosts**.
2. Click on an existing host name to edit the host.
3. Click **Host Settings** tab.

4. Add the following to the host settings:

```
|path_no_trust|<path of the binary>
```

For example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **OK**.

To restrict access overrides in CipherTrust Manager:

1. In the CipherTrust Manager Applications Page, click **CTE > Clients**.
2. Click on an existing client name to edit the client.
3. Click **Client Settings** tab.

4. Add the following to the client settings:

```
|path_no_trust|<path of the binary>
```

For example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **OK**.

Chapter 4: Concise Logging

This chapter contains the following sections:

Overview of Concise Logging	68
Using Concise Logging	68

Overview of Concise Logging

Thales's standard operational logging sends audit messages for each file system operation. An audit message is sent each time a file is opened, read, updated, or written. Thales's standard logging can generate high volumes of log data. Most of these messages might not be useful or required by security administrators to monitor file system activity on the system.

Concise Logging allows you to focus on relevant audit messages and important actionable messages, such as errors and warnings. It can eliminate the repetitive and less important audit messages generated by read and write activity on a file, reading and writing directory attributes, and other file system activity.

Concise Logging eliminates the following types of messages:

- Duplicate audit messages for each and every block read by the user or application. With Concise Logging, CTE only sends an audit message the *first* time a user or application performs a read/write activity. Subsequent read/write activity by that user or application is not logged.
- Audit messages that read the attributes, read the basic information of file-set attributes, and other event-based messages.
- Audit messages for directory open, read directory attributes, and directory close.

Using Concise Logging

You can enable and disable the Concise Logging option from the DSM or CipherTrust Manager for the following:

- All registered hosts in all domains; see ["Configuring Global Concise Logging with the DSM" on the next page](#).
- A host that has registered with the DSM; see ["Configuring Concise Logging for a Registered Host with the DSM" on the next page](#).

Considerations

- Concise Logging changes the set of log messages that are sent to Security Information and Event Management (SIEM) software systems. If this results in loss of data required for customer reports, then disable Concise Logging.
- Concise Logging is only supported by CTE `secfs`.
- Enable and disable Concise Logging on the host. CTE applies it to all GuardPoints and for all users on the host for which it is selected. There is no finer-grained control, such as per GuardPoint, user, or message type.
- When you enable this setting at the DSM level, it applies to all hosts in all domains, that are added to the DSM, but does not apply to any existing hosts. Hosts added after this setting is enabled inherit this setting. The default global setting is off.
- Do not use Learn mode with Concise Logging.

Configuring Concise Logging for CTE Clients or Client Groups with CipherTrust Manager

In CipherTrust Manager, when you create a Client Profile, you can select to Enable Concise Logging. Then, you can apply that Client Profile to a specific client, or to all clients in a Client Group. To enable Concise Logging, see the chapter *Managing Profiles* in the *CTE Administrator Guide*.

Configuring Global Concise Logging with the DSM

You can enable or disable Concise Logging at any time. The DSM controls the function. Any change in the Concise Logging is reflected on any newly registered hosts and their domains.

To configure global Concise Logging:

1. Log in to the DSM with System Admin privileges.
2. Click **System > Log Preferences**. Your system may contain multiple log tabs.
3. Click on a **Log** tab.
4. In the Duplicate Message Suppression Settings field, click **Enable Concise Logging**.
5. Click **Apply**.
6. Repeat steps for any other logs, as appropriate.

The host sends the following message after the administrator has enabled Concise Logging for an individual host:

```
DAO00821: Administrator "voradmin" updated Security Server configuration "Concise Logging Enabled" from "true" to "false".
```

Configuring Concise Logging for a Registered Host with the DSM

You can enable Concise Logging for a host after you have registered it with the DSM. Hosts that are added to the DSM after enabling Concise Logging inherit the global settings from the DSM. This setting can be customized at any time.

To enable Concise Logging on the DSM for a registered host:

1. Log into your host with DSM Security Administrator privileges.
2. Select the host that you would like to customize.
3. Select a **Log** tab.
4. In the Duplicate Message Suppression Settings, click **Enable Concise Logging**.
5. Click **Apply**.

After you enable or disable Concise Logging, CTE generates a log message to record that event:

```
[CGA] [INFO] [CGA3201I] [11/11/2016 10:57:18] Concise logging enable  
[CGA] [INFO] [CGA3202I] [11/11/2016 10:57:27] Concise logging disabled
```

Chapter 5: Enhanced Encryption Mode

This chapter describes the enhanced AES-CBC-CS1 encryption mode for keys. It contains the following sections:

Compatibility	70
Disk Space	71
Encryption Migration	71
File Systems Compatibility	71
Container Compatibility	74
Using the AES-CBC-CS1 Encryption Mode in DSM	74
Using the AES-CBC-CS1 Encryption Mode in CM	74
Exceptions and Caveats	74
Best Practices for AES-CBC CS1 Keys and Host Groups	75

The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

Note

AES-CBC-CS1 encryption does not require any additional license.

	AES-CBC	AES-CBC-CS1
Security Improvements		
Unique IV per-file	No	Yes
IV predictability	Yes	No
File System Support		
Local FS	EXT3/EXT4/XFS	EXT3/EXT4/XFS
Remote FS	NFS3/NFS4/CIFS	NFS3/NFS4
Block Device Support (sevm)	Fully supported	No. When a policy contains a key with CBC-CS1 encryption mode, the guarding fails on the DSM, and an error message displays.

Compatibility

- Starting with VTE for Linux version 6.1.0, CTE is backward compatible with, and fully supports, the existing AES-CBC mode for both new and existing datasets.
- Starting with VTE for Linux version 6.1.0, CTE fully supports AES-CBC-CS1 encryption for LDT and offline data transformation on CTE Linux environments.
Versions of VTE prior to version 6.1.0 are *not* backwards compatible with AES-CBC-CS1 encryption. On these earlier versions, attempting to guard a device using a policy containing an AES-CBC-CS1 key will fail.
- Protected hosts supporting AES-CBC-CS1 encryption can be added to host groups.

Difference between AES-CBC and AES-CBC-CS1

The two encryption modes are completely different from a file format standpoint.

- AES-CBC-CS1 encryption only applies to file system directories; AES-CBC encryption applies to both files and block devices.

Notes

- If you attempt to use an AES-CBC-CS1 key to guard a block device or partition, the guarding fails with an error reported on the DSM or CipherTrust Manager, similar to: Raw or Block Device (Manual and Auto Guard) GuardPoints are incompatible with Policy "policy-xxx" that contains a key that uses the CBC-CS1 encryption mode."
 - While AES-CBC-CS1 encryption is supported on both Linux and Windows environments, the file formats are incompatible. An encrypted file created with a specific AES-CBC-CS1 key on Windows cannot be read on Linux, even if that specific key were to be used and vice versa.
- AES-CBC-CS1 uses cipher-text stealing to encrypt the last partial block of a file whose size is not aligned with 16 bytes.
 - Each file encrypted with an AES-CBC-CS1 key is associated with a unique and random base IV.
 - AES-CBC-CS1 implements a secure algorithm to tweak the IV used for each segment (512 bytes) of a file.

Disk Space

Files encrypted with AES-CBC-CS1 keys consume additional disk space in contrast to files encrypted with AES-CBC keys. This is because AES-CBC-CS1 encryption requires file IVs to be created and persistently stored in contrast to AES-CBC encryption which does not consume any additional disk storage.

Therefore, administrators need to plan and provision additional disk capacity prior to deploying AES-CBC-CS1 encryption.

	AES-CBC	AES-CBC-CS1
Local Linux FS	No change to file size. No extended attribute allocation	Internal use of extended attribute per file. Extra 4KB increase in file size.
Remote Linux FS	No change to file size. No extended attribute allocation	Extra 4KB allocation in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.

Encryption Migration

You can use either LDT or offline dataxform to:

- Transform data encrypted by AES-CBC to AES-CBC-CS1 and vice versa.
- Transform AES-CBC-CS1 encrypted data to clear contents and vice versa.

File Systems Compatibility

On Linux, you can use AES-CBC-CS1 keys to guard currently supported file systems.

AES-CBC-CS1 encrypted files on Linux remote file systems like NFS and CIFS increase the file size compared to encrypted files on Linux local file systems which retain the original file size.

AES-CBC-CS1 encrypted files on Linux local file systems, in conjunction with LDT policies, can result in additional space consumption. Unlike the current AES-CBC encryption where encrypted files on all file systems, both remote or local, have the same file format, AES-CBC-CS1 encrypted file formats differ based on whether or not they were created on local or remote file systems.

AES-CBC-CS1 files on Linux remote file systems such as NFS and CIFS embed the IV in a 4K-byte header within the file. When these files are guarded, CTE masks the file header -- to applications and system utilities. The expanded file is only apparent when CTE guarding is disabled.

Note

The remote file system must have enough extra space to store the extra 4K bytes of the embedded header. You can run the following script in the GuardPoint to identify how much space to reserve before data transformation:

```
x=$(find . -type f | wc -l); y=$(echo "$x * 4 /1024" | bc); echo ${y}MB
```

File System Requirements

Unlike with AES-CBC encryption, files encrypted with AES-CBC-CS1 on remote file systems cannot be copied over to local file systems in the absence of CTE guarding. Similarly, AES-CBC-CS1 encrypted files on local file systems cannot be copied over to remote file systems in the absence of CTE guarding.

The fundamental reason for this incompatibility is the usage of extended attributes on local file systems to store the IV, in contrast to its storage as a part of the file metadata on remote file systems. This is why files cannot be transferred across these file system boundaries in the absence of CTE guarding.

	AES-CBC	AES-CBC-CS1
EXT3/EXT4 on RHEL6	None	EXT3/EXT4 must be mounted with <i>user_xattr</i> mount option
EXT3/EXT4 on other Linux distros	None	No limitation
XFS on Linux	None	No limitation
NFS v3,v4/CIFS on Linux	No limitation	No limitation

Samba Share

The remote Samba share server does not support ADS so you cannot use the CBC-CS1 key type on these GuardPoints.

Storing Metadata

AES-CBC-CS1 encrypted files on Linux store the base IV of a file in either the extended attributes or in the file metadata:

- On local FS (EXT3/EXT4/XFS), Linux saves it as an extended attribute associated with the file. The underlying file system requires that you mount it with the extended attribute mount option.
- On remote FS (NFS and CIFS), Linux saves it in the embedded header of the file.

To get the value of the base IV, type:

```
# voradmin secfs iv get <file-name>
```

Note

The base IV of a file is protected. It cannot be set/modified/removed by commands and applications. However, if a GuardPoint is unguarded, the files in the GuardPoint are no longer protected. An adversary can then corrupt the content of the files, as well as the IVs.

AES-CBC-CS1 depends on the physical file system's support for extended attributes in a manner similar to the CipherTrust Transparent Encryption - Live Data Transformation feature.

Missing IV file

If the IV for a file is missing, or CTE is unable to read the IV, then CTE denies access to the file. This access denied message may trigger an application to display an error message. This message may vary from application to application.

	AES-CBC	AES-CBC-CS1
Local Linux FS	No change	Internal extended attribute for each file
Remote Linux FS	No change	4KB embedded header for each file

HDFS

The AES-CBC-CS1 key is compatible with current Hadoop File System support.

Backups

Backups and other data protection utilities should take into account the extended attributes present in each AES-CBC-CS1 encrypted file on a Linux local file system to ensure that they are safely backed up. An AES-CBC-CS1 encrypted file whose IV is corrupted, renders the files to be corrupted and therefore unreadable. Hence all data protection software must preserve the file's extended attributes.

CTE Linux can inspect a file's IV using the following command:

```
# voradmin secfs iv get file
```

On Linux, the backup utility specified in the guarding policy should automatically backup/restore extended attributes as well. For example, you must use the options to preserve extended attributes when running `cp` or `rsync.normal`.

Due to the different file formats, the backup/restore across the local and remote file systems are not allowed. If you want to backup a GuardPoint from a local directory, you must restore it to a local directory. If a GuardPoint is backed up on a remote file system, you must restore it to a remote system.

	AES-CBC	AES-CBC-CS1
General backup utility requirement (all platforms)	Backup utility defined in guarding policy with clear view	Backup utility defined in guarding policy with clear view
Special requirement for backup/restore local fs on Linux	No	Backup utility must be run with user extended attribute enabled

	AES-CBC	AES-CBC-CS1
Special requirement for backup/restore remote fs on Linux	No	No
On Linux, backup local fs and restore to remote fs	Allowed	Not allowed, the restored files cannot be accessed with I/O error
On Linux, backup remote fs and restore to local fs	Allowed	Not allowed, the restored files cannot be accessed with I/O error

Container Compatibility

The CBC-CS1 key is compatible with current Docker and OpenShift support.

Using the AES-CBC-CS1 Encryption Mode in DSM

Deploy AES-CBC-CS1 encryption by using a symmetric agent key type created in the DSM:

1. In the DSM, click **Keys > Agent Keys > Keys**.
2. Click **Add**.
3. In the Encryption Mode dropdown, select **CBC-CS1**.
4. In the Algorithm dropdown, select **AES128** or **AES256** to create an AES-CBC-CS1 key.
5. Edit or create a policy that will use the AES-CBC-CS1 key. In this policy:
 - If you are using NFS, in the **Security Rules** section, add a security rule that specifies:
Action: `f_rd_att`
Effect: `Permit, Apply Key`
This security rule allows CTE to read the base IV value in the file's embedded header over NFS. This rule is not needed if you are not using NFS.
 - In the **Key Selection Rules** section, click **Add** and select the AES-CBC-CS1 key.
6. Click **OK** to save the policy.
7. Push the policy to the GuardPoints that you want to use this encryption key.

Using the AES-CBC-CS1 Encryption Mode in CM

When you create a key in CTE, you enable Encryption Mode by selecting CTE Key Properties. See *Creating a New Key* in the "Managing Policies" chapter in the CTE Administrator Guide.

Exceptions and Caveats

Note the following when using AES-CBC-CS1 keys.

Ensure User Extended Attributes are Enabled on RHEL 6

On RHEL6, EXT3/EXT4 are not mounted with user extended attributes enabled, by default. If a GuardPoint is on EXT3/EXT4, then remount EXT3/EXT4 with `user_xattr` as an option. Otherwise, guarding fails with the error "Extended attribute not enabled for GuardPoint."

Guarding Existing Files Without Data Transformation

You must convert an existing file with clear text through offline data transformation or LDT. If you do not transform the file, then after you guard using an AES-CBC key, the file displays garbled characters.

If you use an AES-CBC-CS1 key, access to the file is blocked with an I/O error.

Best Practices for AES-CBC CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC CS1 keys unless all hosts are running VTE for Linux version 6.1.0 or CTE version 7.0.0 or later.

Chapter 6: CTE and systemd

CipherTrust Transparent Encryption (CTE) for Linux is integrated with the `systemd` framework. To ensure that applications start after the CTE agent starts at startup, you must modify `systemd`. This is also true when the CTE agent is started and stopped manually.

This chapter contains the following sections:

Overview of CTE and systemd	76
CTE Agent Control Changes on systemd	76
CTE Configuration Changes Required on systemd	77
Supported Use Cases	80

Overview of CTE and systemd

You can use `systemd` to configure dependent applications to start up or shut down in the proper order when CTE starts up or shuts down on a live system. If applications start before CTE starts, those applications may not be guarded. This applies to cases when you manually start or stop the system, such as when you upgrade CTE.

`systemd` replaces `init` in Linux as a system and service manager. Linux inherited `init` from the UNIX System V `init`. `systemd` . The file is a collection of daemons, libraries, and utilities to provide central management and configuration for certain Linux distributions (see "[Linux Distributions that Support CTE and systemd](#)" below). In addition to providing enhanced features and performance, `systemd` is backwards compatible with System V and Linux Standard Base `init` scripts.

Linux Distributions that Support CTE and systemd

The entries in the following table are Linux distributions that are compatible with CTE. The table shows which distributions implement `systemd`, and those that do not. See the *Compatibility Matrix for CTE Agent with CipherTrust Manager* or the *Compatibility Matrix for CTE Agent with Data Security Manager* for the Linux distributions and kernels supported with your CTE version and key manager.

Distributions that support systemd	Distributions that do not support systemd
RHEL 7 RHEL 8 SLES 12 SLES 15 Ubuntu 16.04 Ubuntu 18.04	RHEL 6 SLES 11

CTE Agent Control Changes on systemd

The commands to start, stop, restart, and check CTE status on `systemd` are shown in the following table.

Command	Command syntax for distributions that support systemd
Start	<code>/etc/vormetric/secfs start</code>
Restart	<code>/etc/vormetric/secfs restart</code>

Command	Command syntax for distributions that support systemd
Stop	<code>/etc/vormetric/secfs stop</code>
Check status	<code>/etc/vormetric/secfs status</code>

The normal states of CTE services on a system with one or more active GuardPoints is shown in the following list. It is normal for `secfs-init` and `secfs-fs` to be listed as active (exited).

- `secfs-init`: active (exited) state
- `secfsd`: active (running) state
- `vmd`: active (running) state
- `secfs-fs`: active (exited) state

Example

To check the status of CTE, type:

```
# /etc/vormetric/secfs status
```

System Response

```
secfs-init service: active (exited) since Tue 2017-09-26 09:04:21 PDT; 1 day 4h ago
secfsd service : active (running) since Tue 2017-09-26 09:04:21 PDT; 1 day 4h ago
vmd service : active (running) since Tue 2017-09-26 09:04:44 PDT; 1 day 4h ago
secfs-fs service : active (exited) since Tue 2017-09-26 09:04:45 PDT; 1 day 4h ago
```

CTE Configuration Changes Required on systemd

The following table is a high-level overview of the required changes in `systemd` unit configuration files to control the applications that must be in sync with CTE during system startup and shutdown.

Typical applications that require `systemd` changes include `postgres`, `httpd`, `mongodb`, `mysqld` and `mariadb`. For example, `mongodb` requires that CTE to be running before `mongodb` starts.



CAUTION

Configuring the dependencies as recommended here mean that whenever you stop CTE or if CTE stops unexpectedly, the dependent applications will automatically stop shortly before CTE stops. Be sure you understand the implications of this behavior on your production environment.

Task	For more information
Compile a list of your applications that use GuardPoints.	See the application examples above.
Shut down the applications that use GuardPoints.	"Adding Dependencies to systemd Unit Configuration Files" on page 79
Add the following lines to the <code>[Unit]</code> section of the <code>systemd</code> unit configuration file for each application: <code>After=secfs-fs-barrier.service</code> <code>BindsTo=secfs-fs-barrier.service</code>	"Adding Dependencies to systemd Unit Configuration Files" on page 79

Task	For more information
To the <code>Before=</code> line in the <code>[Unit]</code> section of the <code>secfs-fs-barrier.service</code> file, add the following: <code>saslauthd.service</code> An entry for each application you added to the <code>systemd</code> unit configuration file.	"Adding Applications to the <code>secfs-fs-barrier.service</code> File" on the next page
Add the following lines to the <code>[Unit]</code> section of the <code>saslauthd.service</code> configuration file: <code>BindsTo=secfs-fs-barrier.service</code> <code>After=secfs-fs-barrier.service</code>	"Adding Dependencies to the <code>saslauthd.service</code> File" on page 80
Force the system to read the changed <code>systemd</code> configuration files by typing <code>systemctl daemon-reload</code> .	"Adding Dependencies to the <code>saslauthd.service</code> File" on page 80
Restart the applications that you shut down to make these changes.	"Adding Dependencies to the <code>saslauthd.service</code> File" on page 80

About systemd Dependency Changes for Unit Configuration Files

The previous table describes the effect of the required unit configuration file changes that are described in the following sections. See the [systemd documentation](#) for more information about the `After=` and `BindsTo=` unit configuration options.



CAUTION

In some cases, the unit configuration file for an application other than CTE may be overwritten when the application is upgraded. After upgrading an application, verify that changes to that application's unit configuration file are still in place. Changes to the `secfs-fs-barrier.service` file are retained after you upgrade CTE.

The `secfs-fs-barrier.service` service ensures that CTE services and dependent applications start after CTE services and stop before CTE services as needed during system startup, shutdown, and when starting and stopping services on a live system. This special service manages the dependencies between applications and the `secfs-fs`, `secfs-init`, `secfsd`, and `vmtoolsd` services that make up the CTE agent:

File and Change	Purpose
File: Application-specific unit configuration file Add this line to <code>[Unit]</code> section: <code>After=secfs-fs-barrier.service</code>	In conjunction with the <code>BindsTo=</code> option, this option ensures that the application starts after the CTE agent on system startup.
File: Application-specific unit configuration file Add this line to <code>[Unit]</code> section: <code>BindsTo=secfs-fs-barrier.service</code>	If the CTE agent shuts down, the application also shuts down.
File: <code>secfs-fs-barrier.service</code> Add each application to the existing <code>Before=</code> line in the <code>[Unit]</code> section. Add <code>saslauthd.service</code> to the existing <code>Before=</code> line in the <code>[Unit]</code> section.	Ensure that the <code>secfs-fs-barrier.service</code> starts before the application services mentioned in the <code>Before=</code> line.

Location of Application Unit Configuration Files

To configure the proper startup order of services, modify the unit configuration file for applications that require CTE to be running. You must also modify the `secfs-fs-barrier.service` file. The location of these files varies between Linux distributions as described in the following table.

Distribution	Location of systemd unit configuration files
RHEL 7 RHEL 8 SLES 12 SLES 15	<code>/usr/lib/systemd/system/<application_name>.service</code>
Ubuntu 16.04 Ubuntu 18.04	<code>/lib/systemd/system/<application_name>.service</code>

Adding Dependencies to systemd Unit Configuration Files

If your system supports `systemd` (see ["Linux Distributions that Support CTE and systemd" on page 76](#)), before you can safely reboot your protected host or use the files in the GuardPoint, you must perform the following steps to set the proper CTE dependencies for your applications.

1. Compile a list of your applications that use GuardPoints.
2. Prepare users of those applications for the interruption in service required to make these changes.
3. Shut down each of the affected applications.
4. For each application, log in as root and open the unit configuration file for that application using a text editor such as `vi`. See the table above to determine the location of the `systemd` unit file.

For example, on RHEL 7, the unit configuration file for a hypothetical `exampled` application would be located in `/usr/lib/systemd/system/exampled.service`.

5. Locate the `[Unit]` area in the file and add the following two lines at the end of the `[Unit]` section:

```
After=secfs-fs-barrier.service
BindsTo=secfs-fs-barrier.service
```

For example, on RHEL 7, the `exampled` application unit configuration file might have the following existing `[Unit]` section:

```
[Unit]
Description=Example server
After=syslog.target
After=network.target
```

In this case, you would add the two new lines after `After=network.target`.

6. Save and close the unit configuration file.
7. Repeat steps 3–6 for each application.

Continue to ["Adding Applications to the secfs-fs-barrier.service File" below](#) to make necessary changes to `secfs-fs-barrier.service`.

Adding Applications to the secfs-fs-barrier.service File

After editing the `systemd` unit configuration file for each dependent application, you must also add each application to the `secfs-fs-barrier.service` file that is installed as part of CTE. The `secfs-fs-barrier.service` file ensures that CTE starts before dependent applications during boot and CTE stops before dependent applications when the

system is shut down.

1. As a root user, open the `secfs-fs-barrier.service` file in a text editor such as `vi`.
For example, on RHEL 7, the `secfs-fs-barrier.service` file is located in `/usr/lib/systemd/system/secfs-fs-barrier.service`.
2. Add `ssld.service` along with the names of the unit configuration files that you edited in the last section to the end of the “Before=” clause.
For example on RHEL 7, the `secfs-fs-barrier.service` file might contain the following before editing:

```
Before=postgresql.service httpd.service mongodb.service mongod.service mysqld.service mariadb.service nails.service
```


To add an entry for `ssld.service` and two custom application services called `example1.service` and `example2.service`, you would edit the `Before=` line to look like this:

```
Before=postgresql.service httpd.service mongodb.service mongod.service mysqld.service mariadb.service nails.service ssld.service example1.service example2.service
```
3. Save and close the `secfs-fs-barrier.service` file.

In the future, CTE will start before each application listed in the `Before=` line and those applications will stop before CTE stops.

Continue to the next section to make the necessary changes to `ssld.service`.

Adding Dependencies to the `ssld.service` File

The `ssld.service` must start after the `secfs-fs-barrier` service.

1. As a root user, open the `ssld.service` file in a text editor such as `vi`.
For example, on RHEL 7, the `ssld.service` file is located in `/usr/lib/systemd/system/ssld.service`.
2. Locate the `[Unit]` area in the file and add the following two lines at the end of the `[Unit]` section:

```
After=secfs-fs-barrier.service  
BindsTo=secfs-fs-barrier.service
```


For example, on RHEL 7, the `ssld.service` file might have the following existing `[Unit]` section:

```
[Unit]  
After=syslog.target  
After=network.target
```


In this case, you would add the two new lines after `After=network.target`.
3. Save and close the `ssld.service` file.
4. To force the system to re-read the `systemd` configuration files that you changed in this section and the previous section, type `systemctl daemon-reload`.
5. Start each application that you shut down to make the configuration changes.

Supported Use Cases

CTE supports the following use case.

Manually Stop 3rd Party Applications on a Live System

The applications must already be configured as dependencies in the unit configuration files using the `BindsTo` clause (required). For more information, see ["Adding Dependencies to systemd Unit Configuration Files" on page 79](#).

Use the following commands to stop CTE on a live system with dependent applications running.

```
$# systemctl stop secfs-fs
$# /etc/vormetric/secfs stop

Stopping the CipherTrust Encryption Expert File System Agent.
Stopping Live Data Transform processes (if any).
WARNING: Following dependent services will be stopped in order to stop secfs services.
isecesp.service
isectpd.service
mysql.service
These services are required to start manually.
Successfully stopped the Encryption Expert File System Agent.
```



WARNINGS

- The 3rd party application services using the `BindsTo` clause that automatically stop must be restarted manually after an upgrade.
- Only guard points that are busy due to 3rd party applications are freed using the new use case. Any guard point that is busy due to other I/O operations must be stopped manually.

Chapter 7: Utilities for CTE Management

Thales provides a variety of utilities that augment the standard Linux utilities. This combination of tools helps administrators manage CTE. The following utilities are described in this chapter:

secfsd Utility	82
vmsec Utility	86
Binary Resigning	89
Restricting Access Overrides from Unauthorized Identities	91
Using Advanced Encryption Set New Instructions (AES-NI)	91
vmd utility	92
agenthealth Utility	92
agentinfo Utility (Java version)	93
check_host Utility	93
register_host Utility	94
fsfreeze and xfs_freeze	94

secfsd Utility

The `secfsd` utility displays the following attributes of CTE:

- GuardPoints defined in the *GuardPoints* tab
- Authentication parameters defined in the *Host Settings* tab
- Lock status set by enabling **FS Agent Locked** and **System Locked**
- Web destination and SSL certificate for uploading log entries
- Policies applied in the **GuardPoints** tab
- Status of required processes (`secfsd` and `vmd`)
- Version of `secfs`

The `secfsd` utility is also used to mount GuardPoints for *Directory (Manual Guard)*. Normally, CTE automatically mounts the `secfs` file system when you apply a GuardPoint to a directory. On Linux, the `secfsd` utility is located in `<install_dir>/secfs/.sec/bin` and a symbolic link to this file is placed in `/usr/bin/secfsd`.

secfsd syntax

Command	Description
<code>-help</code>	display <code>secfsd</code> options
Status Options	
<code>-status guard [-v -tree]</code>	list all GuardPoints
<code>-status keys</code>	show current encryption key state
<code>-status auth</code>	list authentication settings
<code>-status lockstat</code>	show CTE lock status

Command	Description
-status logger	list logging details
-status policy	list configured policies
-status pslist	list protected processes
-status devmap	list guarded devices
Manual GuardPoint options	
-guard path [container ID]	manually guard path
-unguard path [container ID]	manually unguard path
Version option	
-version	list version of kernel module <code>secfs2</code>

secfsd Examples

Display GuardPoint Information

To display the GuardPoint paths, applied policies, policy type, and guard status, use the `secfsd -status guard` command. For example:

```
# secfsd -status guard
GuardPoint  Policy          Type          ConfigState  Status      Reason
-----
/opt/apl/lib allow AllOps_fs  local        guarded     guarded     N/A
/dev/sdb    watchaccess_rd  rawdevice    guarded     guarded     N/A
/dev/sdc    watchaccess_rd  manualrawdevice guarded     guarded     N/A
/dev/sdd    watchaccess_rd  manualrawdevice unguarded   not guarded Inactive
/opt/apl/tmp MSSQL00123      manual       unguarded   not guarded Inactive
```

Column	Description
GuardPoint	Full path of the GuardPoint.
Policy	Name of the policy applied to the GuardPoint.
Type	Can be local, automount, manual, raw device, or manual raw device. Configured in the GuardPoints tab.
ConfigState	Guard status of the GuardPoint, as recognized by the key manager. It can be guarded or unguarded.
Status	Current guard status, as recognized by CTE. State can vary.
Reason	Additional information about the status, if any.

Notes

- Config State and Status can vary. As an example, if you apply a GuardPoint and someone is currently working in the GuardPoint, the policy cannot be applied at that time. In this case, the ConfigState is guarded and the Status is not guarded.
- When the user removes an auto-mounted GuardPoint from CipherTrust Manager or the DSM, the CTE Agent is only deleted after the configured `autofs` timeout expires. This timeout does not start until the GuardPoint is free.

The timeout can be changed in the `auto.master` file on the host.

Display GuardPoint Information in a Different Format

To display the same information in a block format, use the `secfsd -status guard -v` command. For example:

```
# secfsd -status guard -v
GuardPoint: 1
  Policy:      allowAllOps_fs
  Directory:   /opt/apps/apps1/tmp
  Type:        local
  ConfigState: guarded
  Status:      guarded
  Reason:      N/A
GuardPoint: 2
  Policy:      allowAllRootUsers_fs
  Directory:   /opt/apps/apps1/lib
  Type:        local
  ConfigState: guarded
  Status:      guarded
  Reason:      N/A
```

Display Host Settings

To display the SHA2 hash signature for each protected host setting, use the `secfsd -status auth` command. For example:

```
# secfsd -status auth
/bin/su 3E765375897E04C39AB17D4C755F50A35195535B6747DBA28DF9BD4AA672DFF9
|authenticator|/usr/sbin/sshd 98FC599D459EDEA52A60AB394B394803B5DAB96B53148DC608732DDA6777FA1A
/usr/sbin/in.rlogind 5C9A0EDD8BF54AE513F039476D21B3032507CF957AA0CB28C368EB8AB6E684FB
/bin/login 0D2EE0B995A30AE382B4B1CA5104715FC8902F457D283BDABAAD857B09259956
/usr/bin/gdm-binary 363780522E3CCF9ABF559F059E437743F9F97BBB0EE85769007A464AD696BD1
/usr/bin/kdm BAD41BBCDD2787C7A33B5144F12ACF7ABC8AAA15DA9FDC09ECF9353BFCE614B5
```

Display Key Status

To display the status of CTE keys, use the `secfsd -status keys` command. For example:

```
# secfsd -status keys
Encryption keys are available
```

Display Lock Status

To display the status of CTE locks, use the `secfsd -status lockstat` command. For example:

```
# secfsd -status lockstat
FS Agent Lock: false
System Lock: false
```


The value is **true** if the lock is applied. The value is **false** if the lock is not applied. **System Lock** corresponds to **System Locked** in the *Host* window. **FS Agent Lock** corresponds to **FS Agent Locked** in the *Host* window.

Note

Before you upgrade, remove CTE software, or change operating system files, the status of FS Agent Lock and System Lock must be false.

Display CTE Log Status

To display the status of CTE log service, use the `secfsd -status logger` command. For example:

```
# secfsd -status logger
Upload URL: https://vmSSA06:8444/upload/logupload,https://vmSSA07:8444/upload/logupload, \
https://vmSSA05:8444/upload/logupload
Logger Certificate directory: /opt/vormetric/DataSecurityExpert/agent/vmd/pem
```

This command sequence returns the URL to which the log service sends log data. It also returns the directory that contains the CTE certificate. CTE uses the certificate to authenticate CTE when it uploads the log data to the DSM.

Display Applied Policies

To display the policies that are applied to CTE, use the `secfsd -status policy` command. For example:

```
# secfsd -status policy
Policy: enc-audit
Type: ONLINE
```

Display CTE Process Information

To display CTE processes, use the `secfsd -status pslist` command. This command shows the process number associated with each CTE process. To show the details about a specific CTE process, use the `ps -fp <process #>` command, where `<process #>` is the process number from the `secfsd -status pslist` command.

For example:

```
# secfsd -status pslist
Protected pid list:      739    731
# ps -fp 739
UID      PID   PPID  C   STIME      TTY  TIME   CMD
root    739     1     0  11:04:56    -   0:00 /opt/vormetric/ \
      DataSecurityExpert/agent/vmd/bin/vmd
```

Display CTE Version Information

To display CTE version information, use the `secfsd -version` command. For example:

```
# secfsd -version
version: 7.0.0.47
```

Manually Enable a GuardPoint in DSM

To manually enable a GuardPoint on a Linux host:

1. Click **Hosts > Hosts > <hostName> GuardPoints**
2. Click **Guard**.
3. In the Policy field, select a policy.

4. Set Type to **Directory (Manual Guard)**.
5. Click **Browse** and enter the GuardPoint path.
6. Click **OK**.
7. Log onto the system hosting CTE as the root user.
8. To manually enable the GuardPoint, use the `secfsd -guard <path>` command. For example:

```
# secfsd -guard /opt/apps/etc
secfsd: Path is Guarded
```

9. To verify the change, use the `secfsd -status guard` command. For example:

```
# secfsd -status guard
GuardPoint      Policy          Type    ConfigState    Status    Reason
-----
/opt/apps/etc   allowAllOps_fs  manual  guarded        guarded   N/A
```

Manually Enable a GuardPoint in CipherTrust Manager

To manually enable a GuardPoint on a Linux host:

1. Click **CTE > Clients > <clientName> GuardPoints**
2. Click **Create GuardPoint**.
3. In the Policy field, select a policy.
4. Set Type to **Manual Directory**.
5. Click **Browse** and enter the GuardPoint path.
6. Click **Create**.
7. Log onto the system hosting CTE as the root user.
8. To manually enable the GuardPoint, use the `secfsd -guard <path>` command. For example:

```
# secfsd -guard /opt/apps/etc
secfsd: Path is Guarded
```

9. To verify the change, use the `secfsd -status guard` command. For example:

```
# secfsd -status guard
GuardPoint      Policy          Type    ConfigState    Status    Reason
-----
/opt/apps/etc   allowAllOps_fs  manual  guarded        guarded   N/A
```

secfsd and Raw Devices

CTE only creates block devices. To display them, use the `ls -l /dev/secvm/dev` command. For example:

```
# ls -l /dev/secvm/dev
brw----- 1 root    system    38, 1 Jan 29 16:37 hdisk1
brw----- 1 root    system    38, 2 Jan 29 16:37 hdisk2
crw----- 1 root    system    38, 3 Jan 29 16:37 rhdisk1
crw----- 1 root    system    38, 4 Jan 29 16:37 rhdisk2
```

vmsec Utility

The vmsec utility allows you to manage security aspects of CTE on the host. On Linux hosts, the vmsec utility is located in:

/opt/vormetric/DataSecurityExpert/agent/vmd/bin/vmsec

vmsec Syntax

checkinstall	Show vmd kernel status
challenge	Enter the dynamic host password
vmdconfig	Display the vmd configuration
check_hwenc	Display kernel configuration
hwok	Report status of hardware signature
passwd [-p <password>]	Enter the static host password
version	Display CTE version

vmsec Examples

Display CTE Challenge String

To display a CTE password challenge string and enter the response string when the DSM is not network accessible, use the `vmsec challenge` command. For example:

```
# vmsec challenge
Contact the help desk at 1-800-555-1212 for response generation.
Your host name is "Host120" Your challenge is: HPTQ-ZYLK
Response -> IHFY-W7WG-PDAO-QKKQ
```

The contact information is configured in the DSM Management Console (Domains > Manage Domains) *Add Domain* window. Contact the DSM Administrator and give them the challenge string. The DSM Administrator will give you the response string. Enter the response string in the **Response** field and press **Enter**. You have 15 minutes to enter the response string.

Display CTE Status

This utility shows you if CTE is configured and running. If it is not running, you might need to start it manually.

To display CTE status, use the `vmsec checkinstall` command. For example:

```
# vmsec checkinstall
The kernel component is installed and running.
```

Entering a Password

To enter the CTE static host password, use the `vmsec passwd` command. For example:

```
# vmsec passwd
Please enter password:
OK passwd
```

To enter CTE static host password on the command line so you can specify it in a batch script, specify the password using the `-p` option. For example:

```
# vmsec passwd -p myPass123
OK passwd
```

Display Kernel Status

To display the kernel status, use the vmsec status command. For example:

```
# vmsec status
FILE_FORMAT=2
FILE_GENERATED=08/27/2019 18:54:10
SA_QOS_STATUS=0
SA_HOST_CPU_UTIL=0
GP_1_Policy=27
GP_1_Dir=/gp
GP_1_lock=1
GP_1_type=1
GP_1_gtype=manual
GP_1_opt=gtype=2,policy=27,lock=1,type=1,dir=/gp/
GP_1_config_state=unguarded
GP_1_status=not guarded
GP_1_statuschk_tm=0-00-00 00:00:00
GP_1_config_op_retry_cnt=0
GP_1_config_op_attempt_tm=0-00-00 00:00:00
GP_1_flags=0
GP_1_reason=Inactive
GP_1_usage=free
TOTAL_GP=1
KEYS_AVAILABLE=TRUE
sdk_version=7.0.0.47
sdk_builddate=2019-08-19 15:16:46 (PDT)
coreguard_locked=false
system_locked=false
logger_upload_url=https://thl602-2114.qa.com:8447/upload/logupload,https://thl602-2116.qa.com:8447/upload/logupload
logger_cert_dir=/opt/vormetric/DataSecurityExpert/agent/vmd/pem
hostname_for_logging=vmd
QOS_PAUSED=false
vmd_STRONG_ENTROPY=false
vmd_URL=https://thl602-2114.qa.com:8446
vmd_SRV_URLS=https://thl602-2114.qa.com:8446, https://thl602-2116.qa.com:8446
vmd_PRIMARY_URL=https://thl602-2114.qa.com:8446
vmd_SUPPORTS_F8P=TRUE
vmd_SUPPORTS_CR256=TRUE
vmd_RANDHP=TRUE
learn_mode=false
concise_logging=false
vmd_listening_port=7024
vmd_initialization_time=2019-07-25 12:07:14.514
vmd_last_server_update_time=2019-07-25 12:12:04.747 policy_name_27=aes256
policy_version_27=0
policy_keyvers_27=0
policy_type_27=ONLINE
policies=27
logger_suppression_VMD=SUPPRESS
logger_intervaltime_VMD=600
logger_repeat_max_VMD=5
logger_suppression_POL=SUPPRESS
logger_intervaltime_POL=600
logger_repeat_max_POL=5
CONFIG_SA_1=27
TOTAL_CONFIG_SA=1
SA_1_NAME=27
SA_1_ALIAS=aes256
SA_1_TYPE=0
```

```
SA_1_REF=1
SA_1_HIP_REG_TIME=0
SA_1_FLAGS=1
TOTAL_SA=1
TOTAL_AUTH=0
AUTHBIN_1=|authenticator|/usr/sbin/sshd
B92A3D7EEF67B82230F7F76097D65159FCF5722A4154A249EFDC22C20F1B572C
AUTHBIN_2=|authenticator|/bin/login
4F210D1B83ACD79B006BCF7DB247ED002A45FC892C42720390BFA6AE21AEA8DC
TOTAL_AUTHBIN=2
```

Display CTE Build Information

To see the CTE build version, use the `vmsec version` command. For example:

```
# vmsec version
Version 6
7.0.0
2020-03-17 15:15:23 (PDT)
Copyright (c) 2009-2020, Thales. All rights reserved.
```

Display Contents of Conf files

To display the contents of the `agent.conf` and `.agent.conf.defaults` files, use the `vmsec vmdconfig` command. For example:

```
# vmsec vmdconfig
appender_syslogdest_Syslog_Appender_0=127.0.0.1
VMSDK_AGENT_CONFIG_FILE=/opt/vormetric/DataSecurityExpert/agent/vmd/etc/agent.conf
appender_layout_Syslog_Appender_0=Syslog_Layout
VMSDK_AGENT_VERSION=7.0.0
VMSDK_AGENT_BUILD_ID=28
PREV_URLS=https://srv.my.thales.com:8443
syslog_appender_myhost name=dev.my.thales.com
VMD_PORT=7024
...
...
appenders=Upload_Appender, File_Appender, Syslog_Appender_0
layouts=Upload_Layout, File_Layout, Syslog_Layout, Simple
CONNECT_TIMEOUT=180000
URL=https://srv.my.thales.com:8443
STRONG_ENTROPY=false
```

Binary Resigning

Note

The following issue applies to an existing VTE for Linux host registered with a DSM only. It does not apply to a CTE for Linux registered with CipherTrust Manager.

Prior to VTE for Linux version 6.1.2, any executable that is part of either a host setting or Signature Set, and that resides in a GuardPoint that uses a Live Data Transformation policy, will use a different signature for each LDT key rotation. The result is that the host settings binaries will no longer be authenticated, or the Signature Set policy rules will no longer trigger for those binaries. To prevent these issues, the security administrator must manually resign each affected binary after each key rotation.

Starting with VTE for Linux version 6.1.2, CTE includes binaries that are signed with a signature that does not change with a key rotation. The security administrator must do only one manual resigning after the first key rotation. After that, there is no longer a need to resign after each subsequent key rotation.

If you are installing a CTE Agent for the first time, there are no special steps if no signatures have been defined. The CTE Agent will sign using the new method.

If you are upgrading or installing a new machine using the same signature sets that you used previously, do the following:

1. Install the latest version of the CTE Agent. The previous signatures will be used until the next key rotation.
2. Before the next key rotation, the administrator resigns the binaries.
3. Do not remove the old signatures on the DSM until all VTE Agents have been upgraded to CTE version 7.0.0.47. For information on how to do a manual resign, see the *DSM Administration Guide*.
4. When all agents have been upgraded, remove the old signatures.

Note

In previous versions, if the binary was in a GuardPoint protected directory, but was the same as an unguarded binary, the administrator could restrict to only the guarded binary. With this change, the unguarded binary is now unrestricted. This means that if a user uses the unguarded binary and its SHA matches the guarded binary, it will now match as if it was the guarded binary.

Enable Automatic Signing for Host Settings

CTE blocks automatic re-signing of the host settings. Some users may have established procedures for updating system software based on the assumption that restarting the `vmd` will generate new signatures when signed software is updated. This process will not work with CTE unless you disable automatic signing.

To disable automatic signing:

1. Change to the directory where the `agent.conf` file resides. For example, type:

```
# cd /opt/vormetric/DataSecurityExpert/agent/vmd/etc/
```
2. Edit the `agent.conf` file.
3. Change or add the following line:

```
RE_SIGN_HOST_SETTINGS=TRUE
```
4. Save your changes and exit the file.
5. Restart the `vmd` to set the changes, type:

```
# /etc/vormetric/secfs restart
```
6. Type the following to verify that the host settings is set to true:

```
# vmsec vmdconfig
```



WARNING

Enabling the automatic regeneration of signatures exposes a potential security vulnerability for agents. When enabled, host setting binaries are resigned when it receives a push from the DSM. If an attacker were to replace a binary with a Trojan, and then force a push from the DSM by, for example, restarting the agent, CTE could generate a signature for the malicious binary and pass it to the kernel.

Restricting Access Overrides from Unauthorized Identities

In some setups, system administrators can use the host settings > `|authenticator|` feature with `su` to change identities and gain access to restricted data. You can instruct CTE to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CTE can block from authenticating other processes.

Any executable path that is marked with a `|path_no_trust|` host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

CTE prevents overrides from other host settings authenticators, using the `|path_no_trust|` status. If a user runs the `su` command from a non-trusted shell, that new shell is still marked as `|path_no_trust|`, even if `|authenticator|/usr/bin/su` is specified in the host-settings. The `|path_no_trust|` feature overrides any and all authenticators under host settings.

To restrict access overrides in **DSM**:

1. In the DSM Management Console, click **Hosts > Hosts**.
2. Click on an existing Host name to edit the host.
3. Click **Host Settings** tab.
4. Add the following to the host settings:

```
|path_no_trust|<path of the binary>
```

Example

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **OK**.

To restrict access overrides in **CM**:

1. In the CM dashboard, click **CTE > Clients**.
2. Click on an existing Client name to edit the host.
3. Click **Client Settings** tab.
4. Add the following to the settings:

```
|path_no_trust|<path of the binary>
```

Example

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **Apply**.

Using Advanced Encryption Set New Instructions (AES-NI)

To verify AES-NI hardware support, type:

```
# vmsec check_hwenc
```

Unlike the `-c algo` command above, CTE does not have to be running for this command to execute. This command displays one of the following messages to stdout:

```
"AES-NI hardware encryption is supported on this system."
```

"AES-NI hardware encryption is not supported on this system. Will default to software encryption."

vmd utility

The `vmd` utility displays CTE software version information.

The `vmd` utility is located in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin` and a symbolic link to this file is placed in `/usr/bin/vmd`.

Syntax

`vmd [OPTIONS...]`

`-h` show utility syntax

`-v` display CTE version

`-f` runs `vmd` in the foreground

Display the Installed Version

To display the installed CTE version, type:

```
# vmd -v
Version 6
7.0.0.47
2020-09-20 11:09:40 (IST)
Copyright (c) 2009-2020, Thales.. All rights reserved.
```

agenthealth Utility

The `agenthealth` utility validates:

- Super-user privilege
- CTE Agent installation
- CTE registration to DSM Server
- CTE processes/modules that are running
- Available disk resources
- Current GuardPoints
- Tests if the agent can reach the GuardPoints
- CTE log directory resource status

This directory contains pending CTE log files for upload. This utility reports the size and number of pending files for upload. These text files are logs that contain `vmd/SecFS` information. They are regenerated whenever `secfs` restarts. If the number of files is unexpectedly large, this can indicate a problem.

The Agent health check script

By default, the `Agenthealth` script is installed in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`.

To run the `Agenthealth` check script, type:


```
# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
security.manager.com is resolvable ..... OK
security.manager.com port 8446 is reachable ..... OK
security.manager.com port 8447 is reachable ..... OK
security.manager.com is resolvable ..... OK
security.manager.com port 8446 is reachable ..... OK
security.manager.com port 8447 is reachable ..... OK
Can communicate to at least one server..... OK
VMD is listening on port 7024..... OK
Time of last update from server..... 2020-082-13 20:25:37.446
Checking available disk space..... OK
Checking logging space ..... OK
    Log directory is "/var/log/vormetric"
    File system for log data is "/", 32G free (17% full)
    Log directory contains 2 of maximum 200 files (1% full)
    Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to /ofx-fs1 ..... OK
Testing access to /gpl ..... Access denied as per policy
```

agentinfo Utility (Java version)

The `agentinfo` utility collects system and CTE configuration data. The `agentinfo` utility is used to take a configuration snapshot of the system that you will send to Thales Customer Support to debug an issue, (This section describes the Java version.)

The `agentinfo` utility is a Java Script file. You can open it in a text editor to see specific functions.

The `agentinfo` utility displays status information on the screen and outputs the results to a compressed tar file. The compressed tar file name format is `ai.<os_name_ver>.qa.com.tar.gz` and it is located in the current working directory.

To create an `agentinfo` file, type:

```
# /opt/vormetric/DataSecurityExpert/agent/vmd/bin/agentinfo
```

check_host Utility

If a CTE software installation fails during the certificate generation and exchange stage, use the `check_host` utility to list the network addresses for the host. The utility checks network interfaces, `/etc/hosts`, DNS, and so on, to compare, test, and evaluate possible addresses for the host, and weights them based upon their network efficiency. FQDNs are the most preferred and stand-alone IP addresses are the least preferred. Some applications, such as silent-mode installation, use `check_host` to determine the best host address to submit to the DSM during registration.

Run the `check_host` utility on a system that is hosting CTE to display available network host names, FQDNs, and IP numbers for the host.

Type:

```
# /opt/vormetric/DataSecurityExpert/agent/vmd/bin/check_host
```

check_host Syntax

```
check_host [[-h | -i | -a ] [-s name]] |  
-l name:port[,name:port] | -r name
```

-h	Print the best host name for this machine
-i	Print the best IP address
-a	Print all the host names and IP addresses
-s	The name of the server (optional hint)
-r	The name of the server for name resolution checks
-l	The name and port of the server for listening checks

register_host Utility

Use the `register_host` utility to create certificate requests, exchange certificates between the DSM and the host, and to register CTE on the DSM. After the host is registered, you can configure CTE, apply GuardPoints, or perform database backups. Run the `register_host` utility in text mode on a terminal window.



CAUTION

The default host registration timeout is 10 minutes. If the host is unable to reach the DSM within the allotted period because of an extremely slow network connection, set the `REGISTER_HOST_TIMEOUT` environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

fsfreeze and xfs_freeze

Users can freeze, snapshot, and unfreeze a file system with an SecFS GuardPoint using `fsfreeze|xfs_freeze` for both XFS and EXT3/4.

SecFS supports freezing with `fsfreeze|xfs_freeze` or by any other program issuing the same type of requests. Freezing SecFS results in freezing the underlying file system, as well as the primary file system.

Restrictions

There are restrictions for using `fsfreeze|xfs_freeze` support with CTE.

Platform Restrictions

The following platform restrictions occur with CTE and `fsfreeze|xfs_freeze`:

- CTE supports the `fsfreeze|xfs_freeze` utility for freezing SECFS GuardPoints on all Linux distributions for kernels ≥ 3.0 for Redhat, SLES, and Ubuntu platforms on EXT3/EXT4/XFS file systems. (Earlier Kernels do not contain the proper freeze_super VFS code).

Note

The existing behavior of using `fsfreeze|xfs_freeze` in the underlying XFS file system works for XFS only. We do not support `fsfreeze|xfs_freeze` on GuardPoints located on VxFS file systems.

`fsfreeze|xfs_freeze` is supported with Redhat 6 (2.6 kernel) only with XFS file system.

Target Restrictions

The expected target of the `fsfreeze|xfs_freeze` command is the path of the GuardPoint.

For example, if `/dev/sdb` is mounted as `ext4` on `/data` and CTE contains the GuardPoint: `/data/protected`, then the target of `fsfreeze` must be `/data/protected`, not `/data`.

Valid: `# fsfreeze -f /data/protected`

Not valid: `# fsfreeze -f /data`

File System Restrictions

The following file system restrictions occur with CTE and `fsfreeze|xfs_freeze`:

- If multiple GuardPoints exist on the same file system, you only need to freeze one.

For example, if `/dev/sdb` is mounted as `ext4` on `/data` and the CTE GuardPoints are `/data/protected1` and `/data/protected2`, then issuing:

```
# fsfreeze -f /data/protected1
```

freezes `/data/protected1`, `/data/protected2` and the underlying `ext4` file system.



CAUTION

Do not unguard a GuardPoint, or restart the CTE Agent, while the file system is frozen. The only action permitted on a frozen file system is taking a snapshot or backing up.

- If you try to freeze `/data/protected2` after freezing `/data/protected1`, it returns as busy
- If you are not permitted to freeze one GuardPoint, then you cannot freeze any GuardPoints

LDT Restrictions

- You cannot freeze a file system while it is undergoing an LDT rekey operation. If it detects a rekey, the freeze returns as busy
- You cannot start an LDT rekey on a frozen file system

Offline Data Transformation Restrictions

Do **NOT** use `fsfreeze|xfs_freeze` while an offline transform policy is in effect.

Chapter 8: Installing CTE on Hadoop

This chapter describes how to protect an HDFS cluster with CTE. It contains the following sections:

Overview	96
Implementing CTE on HDFS	97
Adding a New DataNode to a CTE-protected HDFS	103
HDFS Upgrade with CTE	104
CTE Installation and Configuration	108
Deleting Metadata in HDFS when Migrating Out of LDT	112

Overview

The Hadoop Distributed File System (HDFS) is a file system that supports large files and directory structures distributed across hundreds, or even thousands, of commodity DataNode hosts in a cluster. Previously, CTE could only protect directories and files on the *local file system* rather than the actual *HDFS* files and directories. Now, CTE can protect files and directories.

A DSM Administrator can:

- Define an encryption policy for HDFS files and directories in HDFS name space
- Selectively encrypt HDFS folders with different keys providing multi-tenancy support.
- Define user-based I/O access control rules for HDFS files in HDFS name space.

At the heart of an HDFS cluster is the *NameNode* that provides the framework to support a traditional hierarchical file and directory organization. The NameNode is a master server that manages the HDFS name space and regulates access to files by clients.

HDFS files are split into one or more data blocks that are distributed across *DataNode* hosts in a cluster. The NameNode maintains the namespace tree and the mapping of data blocks to DataNodes. To deploy CTE, install CTE on all the NameNode and DataNode hosts in a cluster.

Overview of CTE on HDFS

This section lists the high-level steps for implementing CTE protection on your HDFS. The process requires that the HDFS Administrator and DSM Security Administrator to work in tandem to complete separate tasks.

You can keep the HDFS cluster alive a active if you enable HDFS data replication and activate the nodes individually. Following are the high-level steps:

HDFS Administrator:

1. Compile a list directories specified by `dfs.datanode.data.dir`. If these directories do not already exist in the NameNode local file system, create them.
2. Pass the directory list to the DSM Security Administrator.
3. Ask DSM Security Administrator to:
 - a. Add the NameNode to the HDFS Host Group.
 - b. Create a GuardPoint for the HDFS Host Group on each of these directories.

DSM Security Administrator:

1. Create an HDFS host group to contain the HDFS nodes.
2. Create a host group GuardPoint on each of the datanode directories obtained from the previous step.
3. Add the NameNode to the HDFS Host Group.

HDFS Administrator:

1. For each DataNode, take the node offline and perform a data transformation.
2. Ask the DSM Security Administrator to add the DataNode to the host group. (After the DataNode is added to the host group, it can be brought online.)
3. Repeat this process until all of the nodes have been encrypted and added to the HDFS Host Group.
4. Modify the host group policies to protect specific HDFS files and directories, as needed.

Implementing CTE on HDFS

This section describes how to implement CTE protection on your HDFS NameNode or DataNode. If you enable HDFS data replication, protecting one node at a time allows you to maintain the HDFS cluster. When all the nodes are configured, you can create GuardPoints on specific HDFS files and directories.

These instructions require that the HDFS Administrator and DSM Security Administrator work in tandem to complete separate tasks.

Note

The instructions below assume that each NameNode and DataNode exist on their own separate host. If you have a NameNode and DataNode on the same host, see ["Implementing CTE on HDFS on a Single Host" on page 102](#).

CTE on HDFS Implementation Assumptions

- You have installed, configured and registered CTE on all of the NameNodes and DataNodes in the Hadoop cluster.
- The HDFS Administrator has knowledge and experience with HDFS and Ambari.
- The DSM Administrator has knowledge and experience with CTE.
- The two can work and communicate in tandem with each other.

Configure the HDFS NameNodes

The first step to implementing CTE on HDFS is for the **HDFS Administrator** to compile a list of the DataNode HDFS local file system directories, and create them on the NameNode local file systems. After this, the DSM Security Administrator must add the NameNodes to an HDFS Host Group:

1. Compile a list of directories specified by `dfs.datanode.data.dir`. Obtain this from `hdfs-site.xml` or using Ambari go to:
HDFS > Configs > Settings > DataNode > DataNode directories



2. If these directories do not already exist in the NameNode local file system, create them on each NameNode in your Hadoop cluster
3. Pass the following information to the DSM Security Administrator:
 - The directory list and instructions to create a GuardPoint for the HDFS Host Group on each of these directories.
 - Instructions to add the NameNodes IP addresses or host names to the HDFS Host Group.

Create an Encryption Zone in HDFS Name Space for AWS EMR

HDFS requires the following manual steps if you want to have an encryption zone in the HDFS name space for AWS EMR, (Elastic MapReduce).

1. Add the following properties to `hdfs-site.xml`.

Note: The default `.sec` folder is `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec`.

```
<property>
  <name>dfs.vte.ioctl.lib</name>
  <value>vorhdfs</value>
</property>
<property>
  <name>dfs.vte.rename.check</name>
  <value>true</value>
</property>
<property>
  <name>dfs.vte.rename.check</name>
  <value>true</value>
</property>
<property>
  <name>dfs.vte.ioctl.device</name>
  <value><.sec folder name, up to the CTE installation location></value>
</property>
```

2. Save the file.
3. Restart HDFS NameNode and DataNode services.

Using the Original Information from HDFS

Update or add the following properties to `hdfs-site.xml` if you want CTE to use the original user information from HDFS.

1. Add the following properties to `hdfs-site.xml`.

```
<property>
    <name>dfs.block.access.token.enable</name>
    <value>true</value>
</property>
<property>
    <name>dfs.client.read.shortcircuit</name>
    <value>false</value>
</property>
<property>
    <name>dfs.vte.user.push</name>
    <value>true</value>
</property>
```

2. Save the file.
3. Restart HDFS NameNode and DataNode services.

Create a HDFS Host Group and Host Group GuardPoint

After configuring the NameNodes, the next steps in activating CTE on HDFS is for the DSM Security Administrator.

Create an HDFS Host Group to contain the HDFS nodes:

1. In the DSM Management Console, click **Hosts > Host Groups > Add**.
2. Enter a **Host Group Name** for the Hadoop cluster.
3. Select **HDFS Cluster** for the Cluster type.
4. (Optional) Enter a description and click **Ok**.



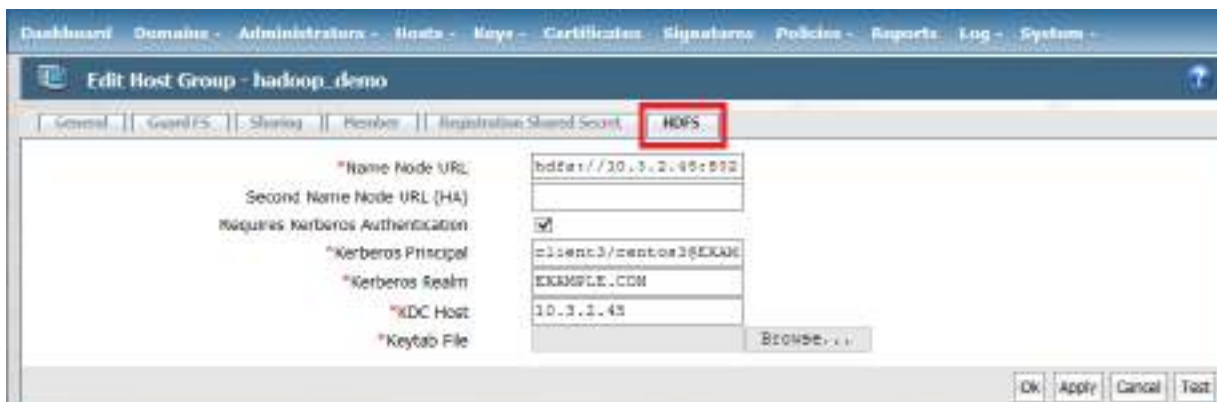
5. In the **Edit Host Group** page, click the HDFS tab.

6. For a Hadoop authentication configured as **Simple mode**, enter the NameNode URL information in the URL format: `hdfs://<host>:<port>`.

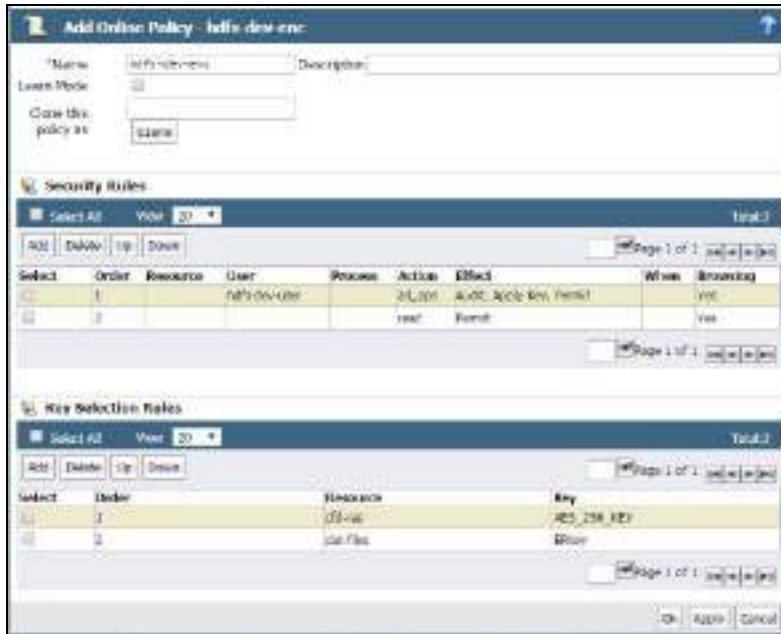
By default the port number is 8020. Check the HDFS configuration to verify this. HDFS HA cluster requires the URLs for both active and standby.



7. For Hadoop authentication configured as **Kerberos**, enter the NameNode URL information in the URL format: host name (not IP address).
8. Check the **Requires Kerberos Authentication** option and enter the following Kerberos information used for authentication:
 - **Kerberos Principal:** Unique identity to which Kerberos can assign tickets. Format is: `primary/instance@REALM`.
 - **Kerberos Realm:** Typically your domain name.
 - **KDC Host:** Hostname of your domain controller.
 - **Keytab File:** File containing pairs of Kerberos principals and encrypted keys.



9. You can create any policy you choose, but the example encryption policy, `hdfs-dev-enc`, uses the following rules:
- For the user set `hdfs-user`, the action is `all_ops`, the effect is `Audit, Apply Key, Permit`
 - For other users the action is `READ`, the effect is `Permit`.
 - For the resource set `hdfs-dev-data-1`, the key is `hdfs-dev-key-1`.
 - For the resource set `hdfs-dev-data-2`, the key is `hdfs-dev-key-2`.



10. If you haven't already done so, add the NameNode obtained from the HDFS Admin to the HDFS Host Group.

Note

Thales highly recommends Auto Guard for HDFS. You can use manual guards, but this might result in data corruption if some nodes in a running cluster are guarded, while other are not.

Take a DataNode Offline and Perform Data Transformation

The next step in activating CTE on HDFS is to switch a DataNode to offline and transform (encrypt) its sensitive data. Once the data is transformed, the HDFS Admin can add the DataNode to the HDFS Host Group. Then they can switch the DataNode back to online. Most of these procedures are completed by the **HDFS Administrator** although one is done by the **DSM Security Administrator**.

1. **HDFS Administrator:** Switch a DataNode to offline.
2. **HDFS Administrator:** Encrypt the files in the directories specified by `dfs.datanode.data.dir` (see ["Configure the HDFS NameNodes" on page 97](#)).

3. **DSM Security Administrator:** Create encryption keys and a data transformation policy to transform the data.

The following figure shows an example of a data transformation policy that transforms the Resource Set `hdfs-dev-data-1` from `clear_key` to `hdfs-dev-key-1`. It also transforms the Resource Set `hdfs-dev-data-2` from `clear_key` to `hdfs-dev-key-2`. Resource Set `hdfs-dev-data-1` consists of `/tmp/data1` and the Resource Set `hdfs-dev-data-2` consists of `/tmp/data2`.



4. **HDFS Admin:** After encrypting the data in those directories, ask the DSM Security Administrator to add the DataNode to the HDFS Host Group.
5. **DSM Security Administrator:** Add the DataNode host to the HDFS Host Group.
6. **HDFS Admin:** After the DataNode is added to the HDFS Host Group, bring the DataNode online.
7. Repeat this procedure for all the DataNodes in your HDFS cluster.

Implementing CTE on HDFS on a Single Host

It is possible, though not recommended, that an HDFS NameNode and DataNode exist as separate processes on the same host. If this is your deployment, use the following CTE deployment guidelines:

1. Configure the HDFS NameNodes (see ["Configure the HDFS NameNodes" on page 97](#)):

Note: The directories specified by `dfs.datanode.data.dir` already exist on the local file system so you do not have to create them.

2. Pass the following information to the DSM Security Administrator:
 - The `dfs.datanode.data.dir` directory list and instructions to create a GuardPoint for the HDFS Host Group on each of these directories.
 - Instructions to add the NameNodes IP addresses, or host names, to the HDFS Host Group.
3. Create an HDFS Host Group and Host Group GuardPoint (see ["Create a HDFS Host Group and Host Group GuardPoint" on page 99](#)):
 - a. DSM Security Administrator must create an HDFS Host Group to contain the HDFS nodes.
 - b. The DSM Security Administrator must create a GuardPoint for the Host Group on each of the directories specified by `dfs.datanode.data.dir`
4. Take the DataNode offline and perform a data transformation.
5. Add the NameNode/DataNode host to the Host Group.

Adding a New DataNode to a CTE-protected HDFS

Use the following procedure to add a new DataNode to a CTE-protected HDFS. If not followed, HDFS encrypted files could be exposed in cleartext.

Note

If you already have CTE installed on the cluster nodes before Ambari installs the Hadoop software, see ["CTE Installed on the Cluster Nodes Before Ambari Installs Hadoop"](#) below.

1. Install the HDFS client on the host. This option is available in Ambari when adding a new DataNode to the cluster.
2. Add the new node to DSM database and make sure that the host settings of the new node is the same as existing nodes in the cluster. See the *CTE Installation for Hadoop* chapter in the *CTE Installation and Configuration Guide*.
3. Install CTE on the new node, register to DSM, and run `config-hadoop.sh` to prepare the libraries. See the *Configuring Hadoop to use CTE* section in the *CTE Installation and Configuration Guide*.
4. Make sure that the data directories (specified in `dfs.datanode.data.dir` property) exist on the new node. They must have the same permission and ownership as the other existing nodes in the cluster. If necessary, create them.
5. Add the host to DSM HDFS Host Group that is guarding the cluster. This is important: do not rely on the DataNode to create the data directories as the data replication can occur before GuardPoints are in effect.
6. Add the DataNode service to the new node. Again this option is available through Ambari.
7. If using Kerberos, check that the keytab files are created correctly.
8. Start the DataNode service on the new node.
9. Execute some `hdfs dfs` shell commands to ensure that encryption/decryption of data works correctly.

CTE Installed on the Cluster Nodes Before Ambari Installs Hadoop

If CTE is already installed on the cluster nodes before Ambari installs the Hadoop software, Ambari can mistakenly pick up the `.sec` directory in configuration steps to store the HDFS data. Make sure the following properties do not contain the `.sec` directory:

- DataNode data directory
- NameNode data directory
- Secondary NameNode checkpoint directory
- Zookeeper directory
- `yarn.nodemanager.local-dirs`
- `yarn.nodemanager.log-dirs`
- `yarn.timeline-service.leveldb-timeline-store.path`
- `yarn.timeline-service.leveldb-state-store.path`

Note

This list is not exhaustive. Depending on the Hadoop ecosystem packages installed, there can be others.

HDFS Upgrade with CTE

To upgrade Hadoop from version 2.6.0 to version 2.7.0 and higher, configure CTE to integrate with the new HDFS instance.

Upgrading one node at a time

Once CTE is installed and configured on the node:

1. Upgrade Hadoop.
2. Make sure that HDFS services are shut down on the node.
3. Type:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/bin/config-hadoop.sh -i -y
```
4. Start HDFS services on the node.

Upgrade CTE with CTE-LDT in an HDFS Cluster

If you are using CTE-LDT with HDFS cluster, follow these steps when upgrading CTE, in order to maintain your CTE-LDT GuardPoints.

1. Suspend rekey on all data nodes.
2. Shutdown your namenodes/datanodes.
3. Upgrade CTE in the namenode first.

Note: Always upgrade namenodes before datanodes.

4. After CTE upgrade succeeds, type:

```
# config-hadoop.sh -i -y
```
5. On the Ambari admin console, start the namenode.
6. Verify that the CipherTrust java process successfully launched in the namenode. (You should not see an error message.) Type:

```
# ps -ef | grep java | grep vormetric
```
7. Check the DSM status. The DSM should show LDT rekeyed status.
8. Check the namenode status. It should display the GuardPoint status and match the state before upgrade. Type:

```
# secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
/hadoop/hdfs/data	LDT_HDFS_Sanity	local	guarded	guarded	N/A
9. Repeat the above steps for all of the datanodes in the HDFS cluster.

Rolling Upgrades

Hortonworks Data Platform has introduced rolling upgrades to automate the Hadoop upgrade process (<http://bit.ly/2pQrFo3>). The upgrade process is controlled by the Upgrade Pack (<http://bit.ly/2rkutvF>) that is predefined and certified by Hortonworks.

To integrate CTE with the upgrade, you need to temporarily change the Ambari scripts before performing the rolling upgrades and then restore the scripts after the upgrades.

1. On Ambari server machine, type:

```
# cd /var/lib/ambari-server/resources/common-services/HDFS/2.1.0.2.0/package/scripts
```

2. Copy the `utils.py` file, type:

```
# cp utils.py utils.py.org
```

3. Using a text editor, add the following commands to `utils.py`:

```
if action == "start":
    if name == "namenode" or name == "datanode":
        Execute(format("/opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/bin/c onfig-hadoop.sh
-i -h {hadoop_bin}/../ -j <java home> -p hdp -d", not_if=service_is_up, user=params.root_
user)
        # For Redhat 6.x, uncomment the following command
        # Execute(format("/etc/init.d/secfs secfsd restart"), not_if=service_is_up,
        user=params.root_user)
        # For Redhat 7.x, uncomment the following command
        # Execute(format("/etc/vormetric/secfs restart"), not_if=service_is_up, user=params.root_
        user)
        before
        Execute(daemon_cmd, not_if=service_is_up, environment=hadoop_env_exports
        The Java home of your HDFS instance should be used to replace <java home>:
        if action == "start":
            if name == "namenode" or name == "datanode":
                Execute(format("/opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/bin/config-hadoop.sh -
                i -h {hadoop_bin}/../ -j <java home> -p hdp -d", not_if=service_is_up, user=params.root_
                user)
                # For Redhat 6.x, uncomment the following command
                # Execute(format("/etc/init.d/secfs secfsd restart"), not_if=service_is_up,
                user=params.root_user)
                # For Redhat 7.x, uncomment the following command
                # Execute(format("/etc/vormetric/secfs restart"), not_if=service_is_up, user=params.root_
                user)
                Execute(daemon_cmd,
                        not_if=service_is_up,
                        environment=hadoop_env_exports)
```

4. Type:

```
# ambari-server restart
```

5. Perform rolling upgrades.

6. During the upgrade process, many of the intermediate service status checks can fail. Skip over them by clicking on **Proceed to Upgrade**.

7. Click **Finalize** to complete the upgrade. If the active NameNode fails to activate due to the incompatible HDFS layout version, manually start the NameNode with '-upgrade' option to correct the layout version file.

```
# /var/lib/ambari-server/ambari-sudo.sh su hdfs -l -s /bin/bash -c 'ulimit -c unlimited ;
/usr/hdp/current/hadoop-client/sbin/hadoop-daemon.sh --config /usr/hdp/current/hadoop-
client/conf start namenode -upgrade'
```

8. If there are excessive under-replicated blocks, run the following command to isolate them and manually start the replication:

```
# su - <$hdfs_user>
# hdfs fsck / | grep 'Under replicated' | awk -F':' '{print $1}' >> /tmp/under_replicated_
files
# for hdfsfile in `cat /tmp/under_replicated_files`; do echo "Fixing
$hdfsfile :"; hadoop fs -setrep 3 $hdfsfile; done
```

9. Restart the HDFS services. Wait for the replication to complete and the NameNodes to exit safe mode.
10. When Hbase is restarted after upgrades, it tries to rename from:
`/apps/hbase/data/.tmp/data/hbase/namespace` to: `/apps/hbase/data/data/hbase/namespace`, which may cause key conflict if the GuardPoint is set incorrectly (for example, `/apps/hbase/data/data` is guarded, but not `/apps/hbase/data/.tmp`). This results in Hbase shutting down.
Before re-starting Hbase, make sure the GuardPoint policies on the Hbase files are set correctly to cover all Hbase-related files. A broader GuardPoint (`/apps/hbase/data` instead of just `/apps/hbase/data/data` and other folders) could fix this issue.
11. Check cluster upgrade by verifying the `hadoop version`.
12. Run a few mapreduce jobs and Hbase commands to make sure that the entire Hadoop stack is working properly.
13. Rename `utils.py.org` to `utils.py`

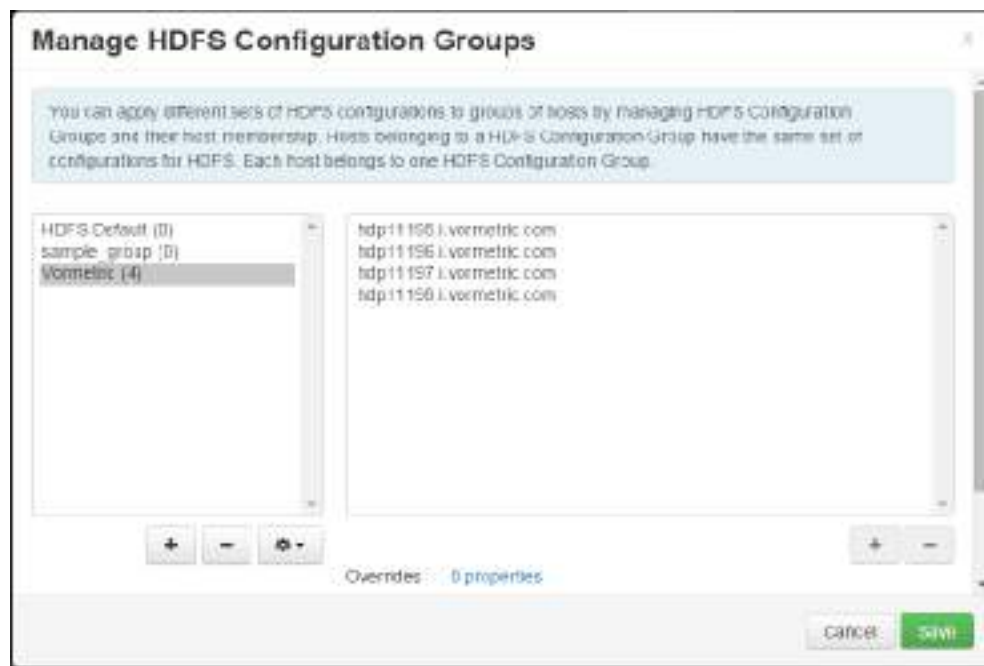
Configure the Hadoop Cluster for CTE

Configure the Hadoop cluster to use CTE before installing and configuring CTE on the nodes. Use Ambari to perform this configuration.

Create a Vormetric Configuration Group

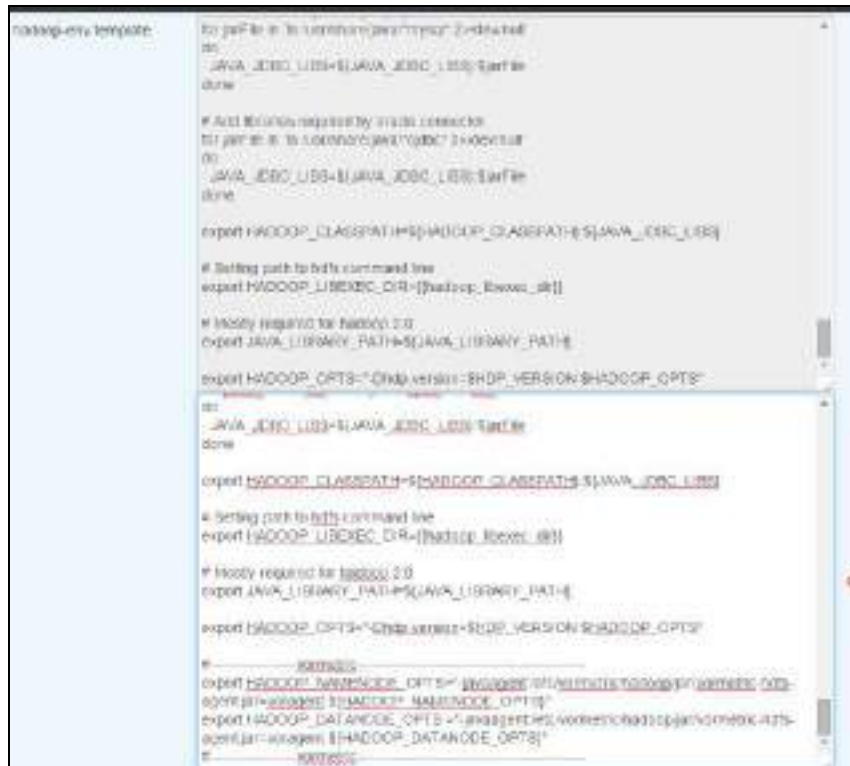
The Vormetric Configuration Group will eventually contain all the hosts in your Hadoop cluster. At first you will create an empty group and later populate it with the hosts on which you will install and configure agents.

1. On Ambari, go to **HDFS > Configs > Manage Config Groups**.
2. Add a new configuration group *Vormetric*.
3. Make group *Vormetric* the current group.



Update the Hadoop-env Template with CTE Settings

1. Go to **HDFS > Configs > Advanced > Advanced hadoop env > hadoop env template**
2. Copy and paste the original `hadoop-env` templates into the Thales template and add the following two export lines to specify that the CTE Java agent is instrumented into NameNode and DataNode.



The screenshot shows a code editor with two panes. The top pane displays the original `hadoop-env` template content, including comments about Java 8 security requirements and the setting of `HADOOP_CLASSPATH`. The bottom pane shows the updated template with additional export lines for `HADOOP_NAMENODE_OPTS` and `HADOOP_DATANODE_OPTS` added at the bottom, before the `exit` command.

```
export HADOOP_NAMENODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_NAMENODE_OPTS}"
export HADOOP_DATANODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_DATANODE_OPTS}"
```

Modify the HDFS IOCTL

1. Go to **HDFS > Configs > Advanced > Custom hdfs-site**.
2. In the `dfs.vte.ioctl.lib` field, type: `vorhdfs`
3. In the `dfs.vte.ioctl.device` field, type:

```
# /opt/vormetric/DataSecurityExpert/agent/secfs/.sec
```

Change the HDFS File Rename Check

1. Go to **HDFS > Configs > Advanced > Custom hdfs-site**.
2. Set `dfs.vte.rename.check` to `true`

User Information Push

You only need this configuration if you want to use the original user information with HDFS operation for IO access check.

Note

It has a performance cost.

1. Go to **HDFS > Configs > Advanced > Advanced hdfs-site** and uncheck **HDFS Short-circuit read**.
2. Set **dfs.block.access.token.enable** to **true**.
3. Go to **HDFS > Configs > Advanced > Custom hdfs-site** and set **dfs.vte.user.push** to **true**.

Create Kerberos Principal for CTE

If Hadoop is configured in the secure mode with Kerberos enabled (`hadoop.security.authentication=Kerberos`), you need to create the Kerberos principal for CTE. Make the principal renewable with the `maxlife` property (Maximum ticket life) larger than 1 hour and smaller than 1 day, and Maximum ticket life smaller than Maximum renewable life (which by default is 7 days).

Configure the *keytab* file and principal with HDFS using these steps:

1. Go to **HDFS->Configs->Custom hdfs-site**
2. Set **dfs.vte.keytab.file**=<CTE keytab file>.
3. Set **dfs.vte.kerberos.principal**=<CTE principal name>.

CTE calls `kinit` to initialize the Kerberos ticket and renew the ticket once per hour. You can execute the following steps from the command line to verify that the Kerberos principal was created and configured for CTE correctly:

```
kinit -r 1440m -k -t <CTE keytab file> <CTE principle>
```

```
kinit -R
```

Uninstalling CTE for the Hadoop Cluster

This section explains how to remove CTE and restore the environment back to the non-CTE cluster environment. Thales recommends uninstalling the agent from HDFS nodes one by one, starting from the DataNode. Uninstall the agent from the NameNode last.

Follow the steps below:

1. Shut down one DataNode.
2. Perform the normal agent uninstall procedure
3. Go to Ambari, remove the DataNode host from the Vormetric Configuration Group.
4. Start the DataNode.
5. Delete the Vormetric Configuration Group from Ambari when agent is uninstalled from all DataNodes.
6. Repeat these steps for each DataNode.
7. Repeat these steps for each NameNode.

CTE Installation and Configuration

After configuring the Hadoop cluster for CTE:

1. Install and register CTE on the HDFS nodes.
 - You can do this to all the nodes at once, but the HDFS is unavailable during CTE installation and configuration.
 - You can also do this one node at a time. If you install and register CTE notes one at a time, you must start from NameNode, then DataNode, and always keep NameNode service up once NameNodes are configured.
2. In either case, add the FQDN of the node to the Vormetric Configuration Group, then proceed with agent installation and configuration. See ["Installing and Configuring CTE on an HDFS Node" below](#).
 - Modify the Host Group. See ["Modifying host settings for HDFS hosts on the DSM" below](#).
 - Configure CTE by running `config-hadoop.sh` on the HDFS node. See ["Configuring Hadoop to Use CTE" on page 111](#).
 - Review the `SecFS` configuration variables that support the HDFS name cache. ["HDFS Name Cache" on page 111](#).

Installing and Configuring CTE on an HDFS Node

1. Using Ambari, add the FQDN of the node to the Vormetric Configuration Group. See ["Create a Vormetric Configuration Group" on page 106](#).
2. Install, configure, and register CTE as described in the CTE Agent for Linux Quick Start Guide.
3. Modify the host settings for each node. See ["Modifying host settings for HDFS hosts on the DSM" below](#).

Modifying host settings for HDFS hosts on the DSM

The Hadoop service can start as root and then downgrade to an unprivileged user. If the unprivileged user is not authenticated by password, CTE flags the user as fake. CTE cannot allow a user to access a resource protected by a user rule when the user is faked, even if the user matches the permit rule. Because of this, modify DSM host setting as follows:

- On Ambari, go to **HDFS > Configs > Advanced > Advanced core-site** and find out if **hadoop.security.authentication** mode is set to **simple** (no authentication) or **Kerberos**.

Simple Modification

To use **simple**, ask the DSM Administrator to add the following lines to the Host Group in the DSM Management Console:

Note

`/usr/jdk64/jdk1.8.0_40/bin/java` is the Java executable used to launch the HDFS services. Change the Java `jdk` path to reflect your end-user environment.

```
|authenticator+arg=+class=org.apache.hadoop.hdfs.server.namenode.NameNode|  
|usr/jdk64/jdk1.8.0_40/bin/java|  
|authenticator+arg=+class=org.apache.hadoop.hdfs.server.datanode.DataNode|  
|usr/jdk64/jdk1.8.0_40/bin/java|
```

The entire host settings will look like this:

```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login/
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
|authenticator|/usr/sbin/vsftpd

|authenticator+arg+=class=org.apache.hadoop.hdfs.server.namenode.NameNode|usr/jdk64/jdk1.8.0_40/bin/java
|authenticator+arg+=class=org.apache.hadoop.hdfs.server.datanode.DataNode|usr/jdk64/jdk1.8.0_40/bin/java
```

Using Kerberos

To use **Kerberos**, ask the DSM Administrator to add the following two lines to the **Host Settings** in the DSM Management Console:

Note

`/usr/jdk64/jdk1.8.0_40/bin/java` and `/usr/lib/bigtop-utils/jsvc` are the Java executables used to launch the HDFS services. Change the versions accordingly to fit your environment.

```
|authenticator+arg+class=org.apache.hadoop.hdfs.server.namenode.NameNode|usr/jdk64/jdk1.8.0_40/bin/java
|authenticator+arg+class=org.apache.hadoop.hdfs.server.datanode.DataNode|usr/lib/bigtop-utils/jsvc
```

The entire Host Group will look like this:

```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login/
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
|authenticator|/usr/sbin/vsftpd

|authenticator+arg+=class=org.apache.hadoop.hdfs.server.namenode.NameNode|usr/jdk64/jdk1.8.0_40/bin/java
|authenticator+arg+=class=org.apache.hadoop.hdfs.server.datanode.DataNode|usr/lib/bigtop-utils/jsvc
```

Modifying Host Group for HDFS NameNodes HA on DSM

To enable high availability (HA) for your HDFS NameNodes, ask the DSM Administrator to add the following lines to the Host Group in the DSM Management Console

Note

`/usr/jdk64/jdk1.8.0_40/bin/java` is the Java executable used to launch the HDFS services. Change the Java jdk path to reflect your end-user environment.

```
|authenticator+arg+class=org.apache.hadoop.hdfs.qjournal.server.JournalNode|usr/jdk64/jdk1.8.0_40/bin/java
|authenticator+arg+class=org.apache.hadoop.yarn.server.applicationhistoryservice.ApplicationHistoryServer|usr/jdk64/jdk1.8.0_40/bin/java
|trust+arg+=class=org.apache.hadoop.hdfs.tools.DFSZKFailoverController|usr/jdk64/jdk1.8.0_40/bin/java
```

The entire Host Group for HA (in this example, with Kerberos) will look like this:

```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login/
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
|authenticator|/usr/sbin/vsftpd

|authenticator+arg+class=org.apache.hadoop.hdfs.server.namenode.NameNode|usr/jdk64/jdk1.8.0_40/bin/java
|authenticator+arg+class=org.apache.hadoop.hdfs.server.datanode.DataNode|usr/lib/bigtop-utils/jsvc
|trust+arg+class=org.apache.hadoop.hdfs.qjournal.server.JournalNode|usr/jdk64/jdk1.8.0_40/bin/java
```

```
|trust+arg+=class=org.apache.hadoop.yarn.server.applicationhistoryservice.ApplicationHistoryServer| \
/usr/jdk64/jdk1.8.0_40/bin/java
|trust+arg+=class=org.apache.hadoop.hdfs.tools.DFSZKFailoverController|/usr/jdk64/jdk1.8.0_40/bin/java
```

Configuring Hadoop to Use CTE

1. On the HDFS node, type:

```
# /opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/bin/config-hadoop.sh -i.
```

HDFS prompts you for the following information:

- **Hadoop product name:** (i.e. *hdp*)
- **Hadoop product version:** (i.e. *2.6.0.2.2.0.0 2041*)
- **Path to JAVA_HOME used by Hadoop:** (i.e. */usr/jdk64/jdk1.8.0_40*)

Note: Alternatively, you can use the automated installation option:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/bin/config-hadoop.sh -i -p hdp
-v 2.6.0.2.2.0.0-2041 -j /usr/jdk64/jdk1.8.0_40 2.
```

2. Verify the configuration the using the `s` option:

```
# /opt/vormetric/DataSecurityExpert/agent/secfs/hadoop/ bin/config-hadoop.sh -s
Vormetric-Hadoop Configuration Status
PRODUCT_NAME=hdp- PRODUCT_VERSION=3.0.0.0-2557 HADOOP_HOME=/usr/hdp/current/hadoop-
client/sbin/..- HADOOP_VERSION=2.7.1 HADOOP_PRODUCT_VERSION=2.7.1.2.3.0.0-2557- HADOOP_
VERSION_MAJOR=2.7 LIBVORHDFS_
SO=/usr/hdp/current/hadoopclient/sbin/..//lib/native/libvorhdfs.so LIBHDFS_
SO=/etc/vormetric/hadoop/lib/libhdfs.so VORMETRIC_HADOOP=/etc/vormetric/hadoop-
#-----vormetric-----
export HADOOP_NAMENODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-
agent.jar=voragent ${HADOOP_NAMENODE_OPTS}"v6 . . . . 62 export HADOOP_DATANODE_OPTS="-
javaagent:/etc/vormetric/hadoop/jar/vormetric-hdfs-agent.jar=voragent ${HADOOP_DATANODE_
OPTS}"
#-----vormetric-----
/etc/vormetric/hadoop/lib/libhdfs.so ...ok
/usr/hdp/current/hadoop-client/sbin/..//lib/native/libvorhdfs.so ...ok
/etc/vormetric/hadoop/gen-vor-hadoop-env.sh ...ok
/etc/vormetric/hadoop/vor-hadoop.env ...ok
Looks ok.
Vormetric Transparent Encryption Agent 6.0.3 Installation and Configuration Guide
v6 . . . . .62 export HADOOP_DATANODE_OPTS="-javaagent:/etc/vormetric/hadoop/jar/vormetric-
hdfs-agent.jar=voragent ${HADOOP_DATANODE_OPTS}"
#-----vormetric-----
/etc/vormetric/hadoop/lib/libhdfs.so ...ok /usr/hdp/current/hadoop
client/sbin/..//lib/native/libvorhdfs.so ...ok /etc/vormetric/hadoop/gen-vor-hadoop-
env.sh ...ok /etc/vormetric/hadoop/vor-hadoop.env ...ok
Looks ok
```

Verify secfsd is Running with Hadoop Environment

Use a text editor to view the `/etc/init/secfsd.upstart.conf` file. The file should contain `env` entries, type:

```
# cat /etc/init/secfsd.upstart.conf
```

HDFS Name Cache

Obtaining the HDFS file name from the NameNode is network intensive, so the map from HDFS block file name to HDFS file name is cached in a hash table. The following `secfs` configuration variables are used to support the hash cache. They are provided in case you need to tune the memory management of the name cache for better

performance.

hdfs_cache_entry: Default is 1,024,000, which could cover up to 125TB HDFS data because the default HDFS block size is up to 128MB (128MB * 1024000 = 125TB).

hdfs_cache_bucket: Default is 10240.

hdfs_cache_timeout: Default to 30 minutes.

hdfs_cache_interval: Default wake up interval for a worker thread to update the cache entry whose timeout has expired is 10 seconds.

On Linux, you can configure each secfs configuration variable in the following file:

```
# /opt/vormetric/DataSecurityExpert/agent/secfs/.sec/ conf/<variable name>
```

For example, you can configure the variable `hdfs_cache_entry`

```
../.sec/conf/hdfs_cache_entry
```

Note

Because HDFS rename is a metadata operation inside the HDFS NameNode and does not call into the local file system, the hash cache might contain expired data. The HDFS NameNode is coded to prevent renamed data from crossing a key boundary to prevent data corruption. However, other access checks based on the HDFS file name may give incorrect information if the name is expired. Understand this risk before using this feature.

Enabling CTE on HDFS

To enable CTE on your HDFS:

1. Restart CTE agent on the node.
 - For Redhat 6.x, type:

```
# /etc/init.d/secfs restart
```
 - For Redhat 7.x, type:

```
# /etc/vormetric/secfs restart
```
2. Restart the Hadoop Services in the cluster.

You can now create GuardPoints to protect your entire HDFS.

Deleting Metadata in HDFS when Migrating Out of LDT

In an HDFS deployment, if you migrate from an LDT to a non-LDT environment, the administrator must delete the LDT `mdstore` file.

In the following example:

`/hadoop/hdfs` is the mount point

`/hadoop/hdfs/data` is the guardpoint

To manage the migration:

1. In the DSM console, click **Host > Host Groups**.
2. Click `<host group name>`. The Edit Host Group - `<host group name>` window opens.
3. Click **GuardPoints**.
4. Select the appropriate HDFS directory with an LDT GuardPoint, and click **Unguard**.

5. Using the Ambari admin console, shutdown all NameNode/DataNode one by one. Ensure that no HDFS guardpoints are busy.
6. Ensure that no guardpoints are configured on any HDFS node in the cluster, type:

```
# secfsd -status guard
```

No guardpoints configured
7. On the node running secfs, type:

```
# voradmin ldt attr delete <guard path>
```

```
# voradmin ldt attr delete /hadoop/hdfs/data
```

LDT metadata has been removed from all files in guardpoint /hadoop/hdfs/data
8. On the system, verify that the metadata store has been removed from the secfs mount points, type:

```
# voradmin ldt rmstore <mount_point>
```

```
# voradmin ldt rmstore /hadoop/hdfs
```

Enter YES if /hadoop/hdfs does not include any guardpoints associated with an LDT policy -
>YES

MDS file /hadoop/hdfs/::vorm:mds:: has been removed.
9. Verify that the metadata store has been removed from the secfs mount points, type:

```
# ls -altr <mount_point>
```

```
# ls -altr /hadoop/hdfs
```

You should not see /hadoop/hdfs/::vorm:mds:: listed.
10. Repeat the above steps for each node in the HDFS cluster.

Chapter 9: Using CTE with Oracle

This chapter describes how to install and configure CTE on Oracle RAC ASM, Linux.

It contains the following sections:

Oracle RAC ASM and ASMLib	114
Oracle RAC ASMLib Multi-Disk Online Method	119
About Oracle RAC ASM Raw Devices	119
Oracle RAC ASM Multi-Disk Online Method	120
Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)	122
Surviving the Reboot and Failover Testing	123
Basic Troubleshooting Techniques	123

Oracle RAC ASM and ASMLib

This section describes how to install and configure CTE on an Oracle RAC ASM and ASMLib.

Using CTE with an Oracle RAC ASM

You can apply CTE when the Oracle DB is active or inactive. If you choose to use it while the Oracle DB is active, it eliminates any downtime. You can apply CTE during low volume traffic time frames. If you choose to use this option, then use the **rebalance** function of ASM. This allows you to:

1. Migrate data off of a disk so that it can be dropped/removed from a **Diskgroup**.
2. Apply CTE protection.
3. Add the disk back into the diskgroup.



CAUTION

If you drop a disk from an ASM diskgroup, then add it back to the diskgroup without cleanly wiping the disk, the ASM diskname will be corrupted. To avoid this problem, clear out the disk before you add it back to diskgroup. Example: `dd if=/dev/zero of=/dev/secvm/dev/mapper/asmdg-asmlv002 bs=32k`

ASMLib

ASMLib is an optional support library for the Automatic Storage Management feature of the Oracle Database. If the customer is using ASMLib, then management is performed through an Oracle ASM command line. Using this can be simpler than the setup required for standard ASM. The commands and details of the procedure differ as well.

Important ASM Commands and Concepts

Rebalancing Disks

When you drop/remove a disk from the diskgroup, it is important to apply the proper value for the power setting for rebalance and to use the `WAIT` command.

Example ASM Command:

```
SQL> ALTER DISKGROUP <DiskGroupName> DROP DISK <diskName> REBALANCE POWER 8 WAIT;
```

- The **rebalance** command moves the data off of the disk that you are removing from the diskgroup, distributing the data across the remaining DISKS.
- The **power** setting is a number from 1 to 11. It determines how much processing power is dedicated to the rebalance, versus normal operations. Unless the encrypting occurs during heavy traffic volume, the minimum value you should use is 6. Otherwise, consult the customer's DBA for the proper setting. An appropriate value to start with is 8.

Mapping Raw Devices

You can map raw devices for this configuration using:

- **Multipath I/O**

This is typically evident when the path for the mapped devices is set to: `/dev/mapper/<device-name>`.

- **Raw devices**

Some customers use raw devices to map a name like `raw3` to a specific device name. You usually find this mapping in a file called: `/etc/sysconfig/rawdevices`.

Note

It is important to understand how the device names are used and if they are the same across all of the RAC nodes.

- **EMC PowerPath**

If using EMC PowerPath then the device names are similar to the following: `/dev/emcpowerXXXX`.

When browsing the DSM through the local host, you cannot find Power Path devices. You must manually input the paths. The guarded disk names are prepended with: `/dev/secvm`.

Checking Rebalance Status

The `wait` command is very important when ASM performs a rebalance. When you specify `wait`, the command prompt does not display until all of the data is rebalanced and migrated off of the disk. If you do not specify `wait`, the command prompt returns immediately, and you must issue the following ASM command to check the status of the rebalance:

```
SQL> select * from v$asm_operation;
```

This command returns information about the:

- State
- Current power level
- Current amount rebalanced
- Estimated work until completion
- Rate
- Estimated minutes
- Any error codes

Note

It is highly recommended that you always specify the `wait` command when performing a **Drop Disk** with Rebalance. If it is not specified, ASM may prematurely release the disk, thereby allowing CTE to place a GuardPoint on the disk before the rebalance completes. This action may corrupt the data.

Oracle cautions against this issue:



CAUTION

The **ALTER DISKGROUP...DROP DISK** statement returns before the drop and rebalance operations complete. Do not reuse, remove, or disconnect the dropped disk until the **HEADER_STATUS** column in the **V\$ASM_DISK** view for this disk changes to **FORMER**. You can query the **V\$ASM_OPERATION** view to determine the amount of time remaining for the drop/rebalance operation to complete. For more information, refer to the *Oracle Database SQL Language Reference* and the *Oracle Database Reference*.

Determining Best Method for Encrypting Disks

A diskgroup can contain one or multiple disks. You must determine if the diskgroup contains enough disks and free space for encryption. If the diskgroup contains only one disk, or multiple disks but not enough free space, then you must use the **Offline** (backup/restore) method for encryption.

If the diskgroup contains more than one, you can use the **Online** (rebalancing) method. During rebalancing, additional disks allow for migrating data from the original disk so that it can be encrypted, added back into the diskgroup, and then migrated back to the source disk. Therefore, if the customer does not want to permanently add extra disks, they can add disks temporarily, just for rebalancing.

In general, once you have completed the initial setup for the operating system with which you are working, for both ASM or ASMLib, the high-level process is the same for applying CTE protection to raw devices and using them.

Online Method (No Application / Database Downtime)

Typically, when using the online method, follow these steps:

1. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.
2. Apply CTE encryption to the disk.
3. Add each protected disk to the diskgroup.
4. Restart the nodes and the failover test.
5. Repeat the previous steps for each disk in the diskgroup.

Offline Method (Backup the DB)

Typically, when using the offline method, follow these steps:

1. Backup the database.
2. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.
3. Stop the Oracle database.
4. Delete the diskgroup.
5. Apply CTE encryption to the disk.
6. Recreate the diskgroup.
7. Add the protected disk to the diskgroup.

8. Restart the nodes and the failover test.
9. Repeat the previous steps for each disk in the diskgroup.

General Prerequisites

Setup

- Verify that you have a current backup of the database
- Install and register CTE agents on all RAC node Hosts
- Create a **Host Group** and add all RAC node hosts as members
- Create an encryption key for the Oracle RAC Database / Application
- Create an Oracle policy using the proper encryption key

Note

If the raw device mappings for the disk(s) are **not** identical across all nodes in the RAC, then you cannot use a Host Group for managing the GuardPoint within the DSM. You **must** apply the GuardPoint to each Host individually. This is typically not optimal, as a Host Group is the most effective and consistent way to manage GuardPoints for Oracle RAC environments.

Modify the UDEV Rules

Note

This applies to RHEL 5 operating systems.

Update the UDEV rules to ensure that they recognize the CTE protected raw devices:

1. Edit the file `/etc/udev/rules.d/90-dm.rules`.
2. Find and comment out the following line by adding a hash tag (`#`) to the beginning of the line.

```
# KERNEL=="dm-[0-9]*", ACTION=="add", OPTIONS+="ignore_device"
```
3. Restart the UDEV rules by executing the following command:

```
# /sbin/start_udev
```

Note

The CTE guide states that a restart is usually required once the UDEV rules have changed. However, that would defeat the purpose of an online method for conversion to CTE. Using the above `start_udev` command removes the need to restart the Host. If this command does not work, then a system restart may be required.

Altering ASM_DISKSTRING on ASM

ASM uses the `asm_diskstring` setting to identify the path where ASM will attempt to locate available disks to use. If you are using device names when adding the disk, you must modify the string to include the path to SecVM.

1. To retrieve the `ASM_DISKSTRING` setting, type:

```
SQL> SHOW PARAMETER ASM_DISKSTRING
```

2. To modify the setting, type:

```
SQL> ALTER SYSTEM SET ASM_DISKSTRING='/dev/mapper/*', '/dev/secvm/dev/mapper/*';
```

Where the path added is the path to SecVM.

ASMLib manages the binding, not ASM. ASMLib creates ASMLib devices on the SecVM devices and presents it to ASM. ASM automatically recognizes the new device. This creates the need to alter diskstrings for ASM. In addition, Oracle ASM sees a new device created using ASMLib and Raw, by default.

For example:

Using Oracle ASMLib to bind the device:

```
# oracledisk createdisk <devicename> /dev/secvm/dev/<blockdev>
```

Using the raw command to bind the device:

```
# raw /dev/raw/rawN /dev/secvm/dev/<blockdev>
```

Specific Prerequisites

Establishing a Starting Point

In many production environments, you may find that it has been a very long time since the RAC nodes have had the services restarted or have been completely rebooted. This can result in a lack of understanding of the actual state of the RAC cluster and its ability to survive a reboot on its own, prior to installing CTE.

Restarts can uncover issues in the RAC environment that are unrelated to CTE. To avoid issues after a CTE installation, Thales recommends that you restart each RAC node **AFTER** CTE is installed and **PRIOR** to establishing any GuardPoints. This may not be feasible in a single node configuration. However, by doing so, CTE is installed but inactive, and you can ensure that the platform is in a workable state prior to getting started.

The Importance of Device Mapping

It is important to use device naming and mapping in a multi-node RAC configuration. Verify the device names to ensure that the disks are mapped to the same disks on each RAC node before applying any GuardPoints. Thales recommends that RAC nodes use the same device names across all nodes. If they do not match, then problems can occur.

If the RAC nodes use the same device names, use a Host Group to create GuardPoints. If they do not match, do not use a Host Group to create GuardPoints. Set them up independently on each Host.

Important Note about Raw Devices on UNIX

In general, raw devices are created as either character or block mode devices. Any I/O performed on character devices is non-buffered, while I/O on block devices is buffered and performed in defined block sizes (that is, 4K bytes).

While the Oracle documentation for using ASM with raw devices indicates that you can use either character or block devices, **CTE REQUIRES a block device for guarding.**

Notes

- Attempting to apply a GuardPoint on a character device that *does not* have a corresponding block device may result in a GuardPoint that never encrypts data. The status of the GuardPoint never shows as guarded.
- The WebUI does not support browsing for the character devices. You would need to manually paste the name into the WebUI.

Oracle RAC ASMLib Multi-Disk Online Method

The online method describes how to remove, protect and add disks to a diskgroup.

Assumptions

Using the Online Method assumes that there is enough free space in the diskgroup so that you can drop/remove, protect and then add the disk back into the diskgroup.

Note

During the initial investigation, you may want to ensure that you have the correct raw device name for each disk that you plan on protecting. Before making any changes to the ASM configuration, obtain the definitive device names for each disk by running the following from the command prompt:

```
# oracleasm querydisk -p <diskName>
```

To add the disk to the diskgroup using the online method and make it ready for use:

1. Open a terminal session on both RAC Nodes.
2. On **RAC Node 1**, perform the following:
 - a. On the ASM, type the following to remove a disk for the diskgroup.

```
SQL> ALTER DISKGROUP <diskGroupName> DROP DISK <diskName> REBALANCE POWER 11 WAIT;
```

- b. Delete the disk from ASM, type:

```
# oracleasm deletedisk <diskName>
```

- c. Verify that the disk is deleted from the ASM and therefore, it is not listed, type:

```
# oracleasm listdisks
```

Note

If you are planning to apply a GuardPoint to a raw device that is currently in an ASM diskgroup, you must remove and delete the disk from the diskgroup before you apply the GuardPoint. ASMLib will not see the guarded disk if you skip this step. When deleting the disk, make sure that the deletion completes before continuing.

About Oracle RAC ASM Raw Devices

When Not Using ASMLib

Before starting the CTE implementation, investigate how the customer is using raw devices for their ASM configuration.

Devices using Raw Bindings

Typically, a device that uses a raw binding looks like the following to ASM:

```
/dev/raw/raw1
```

If the device is mapped this way, you must locate where the mapping is performed. Typically, you can find this in the following configuration file:

```
/etc/sysconfig/rawdevices
```

The underlying binding could be to either a **standard device** name or a **multipath** I/O device name. Either way, you must find where the bind commands are run so that you can modify them for SecVM.

Note

If raw bindings are in use, then typically no changes are needed for the `asm_diskstring`. Because the binding to the actual device is created through the `bind` command, locate where the binding occurs and change the binding to SecVM.

Multipath I/O Devices

Devices using multipath I/O are typically found with the name:

```
/dev/mapper/mpath1
```

Generally, when using multipath I/O, you create SecVM on the multipath device name.

Note

If you use multipath I/O devices in the ASM configuration to add its disk, you must modify the `asm_diskstring` parameter to include the `/dev/secvm/dev/*` path.

Standard Devices

In many cases the ASM configuration may be using plain device names, like the following:

```
/dev/sda1
```

Note

If you use standard device names in the ASM configuration to add a disk, you must modify the `ASM_DISKSTRING` parameter to include the `/dev/secvm/dev/*` path.

Consistent Naming of Devices across RAC Nodes

As previously stated, if the raw device mappings for the disk(s) are **NOT** identical across all nodes in the RAC, then you **CANNOT** use a Host Group and you **MUST** apply the GuardPoints to each Host individually. This is typically NOT optimal, as a Host Group is the most effective way to manage an Oracle RAC environment.

Oracle RAC ASM Multi-Disk Online Method

Performing encryption with the online rebalancing method requires sufficient free space to allow the drop of the largest ASM disk.

Checking for Space

In the Oracle system, use the following commands to check for available disk space:

1. Check total free space in the disk group:

```
SQL> SELECT name, free_mb, total_mb, free_mb/total_mb*100 as percentage FROM v$asm_diskgroup;
```

NAME	FREE_MB	TOTAL_MB	PERCENTAGE
DATA	7	2109	.331910858

2. Check individual ASM disk size and usage:

```
SQL> select a.name DiskGroup, b.disk_number Disk#, b.name DiskName, b.total_mb, b.free_mb, b.path, b.header_status FROM v$asm_disk b, v$asm_diskgroup a where a.group_number (+) =b.group_number order by b.group_number, b.disk_number, b.name
```

DISKGROUP	DISK#	DISKNAME	TOTAL_MB	FREE_MB	PATH	HEADER_STATUS
DATA	0	DATA_0000	1874	1273	/dev/oracleasm/disks/ATA3	MEMBER
DATA	1	DATA_0001	1992	608	/dev/oracleasm/disks/ATA4	MEMBER
DATA	3	DATA_0003	117	0	/dev/oracleasm/disks/ATA2	MEMBER
	0	DATA_ENC_0000	109	28	/dev/oracleasm/disks/ATA1_ENC	MEMBER

Adding a Disk to the Diskgroup

Using the Online Method assumes that there is enough free space in the diskgroup so that you can drop/remove a disk, protect it with CTE, and then add it back into the diskgroup.

To add the disk to the diskgroup:

1. Open a terminal session on both RAC Nodes.

2. On **RAC Node 1**, on the ASM, remove the disk from the disk group, type.

```
SQL> ALTER DISKGROUP <diskGroupName> DROP DISK <diskName> REBALANCE POWER 11 WAIT;
```

3. On the DSM, in the Host Group, apply a GuardPoint to the Raw Device: <rawDevice1Name>.

4. From **RAC Node 1**, to display the status of the guarded disks, type:

```
# secfsd -status guard
```

5. On both **RAC Node 1 and 2** type:

```
# chown oracle:oinstall /dev/secvm/<rawDevice1Name>
# chmod 660 /dev/secvm/<rawDevice1Name>
```

6. From **RAC Node**, on the **ASM**, add the protected disk to the disk group:

```
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/<rawDevice1Name> NAME <disk1Name>;
```

The disk is now added to the diskgroup and ready for use.

7. The system is now ready for a reboot and failover test. For details, see ["Surviving the Reboot and Failover Testing" on page 123](#).

Troubleshooting

Occasionally, settings do not persist when the system is rebooted. To ensure they do persist, edit the `/etc/rc.local` file and add the following lines:

```
Echo "Changing Permission for secvm devices"
chown oracle:oinstall /dev/secvm/dev/<rawDevice1Name>
chmod 660 /dev/secvm/dev/<rawDevice1Name>
```

Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)

Using the Offline Method assumes that there is not enough free space in the diskgroup.

1. Open a terminal session on both RAC Nodes.
2. On RAC Node 1, on the ASM, type the following to remove the disk group.

```
SQL> DROP DISKGROUP <diskGroupName> FORCE INCLUDING CONTENTS;
```

Note: Make sure that the disk is removed before guarding the raw devices.

3. On the DSM, in the Host Group, apply GuardPoints to the three raw devices:

```
<rawDeviceName1>  
<rawDeviceName2>  
<rawDeviceName3>
```

4. On **RAC Node 1**, to display the status of the guarded disks, type:

```
# secfsd -status guard
```

5. On both **RAC Node 1** and 2, type:

```
# chown oracle:oinstall /dev/secvm/<rawDeviceName1>  
# chmod 660 /dev/secvm/<rawDeviceName1>  
# chown oracle:oinstall /dev/secvm/<rawDeviceName2>  
# chmod 660 /dev/secvm/<rawDeviceName2>  
# chown oracle:oinstall /dev/secvm/<rawDeviceName3>  
# chmod 660 /dev/secvm/<rawDeviceName3>
```

6. From **RAC Node 1**, on the **ASM**, add the protected disk to the disk group, type:

```
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/<rawDeviceName1> NAME <diskName1>;  
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/<rawDeviceName2> NAME <diskName2>;  
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/<rawDeviceName3> NAME <diskName3>;
```

The disks are now added to the diskgroup and ready for use.

7. On **RAC Node 1**, restore the database.
8. The system is now ready for a reboot and failover test. Go to the section ["Surviving the Reboot and Failover Testing" on the next page.](#)

Troubleshooting

Occasionally, settings do not persist when the system is rebooted. To ensure they do persist, edit the `/etc/rc.local` file and add the following lines:

```
Echo "Changing Permission for secvm devices"  
# chown oracle:oinstall /dev/secvm/dev/<rawDeviceName1>  
# chmod 660 /dev/secvm/dev/<rawDeviceName1>  
# chown oracle:oinstall /dev/secvm/dev/<rawDeviceName2>  
# chmod 660 /dev/secvm/dev/<rawDeviceName2>  
# chown oracle:oinstall /dev/secvm/dev/<rawDeviceName3>  
# chmod 660 /dev/secvm/dev/<rawDeviceName3>
```

Surviving the Reboot and Failover Testing

Preparing for Failover Testing with ASMLib

When using ASMLib with the `createdisk` command, there is no requirement to make additional changes in `rc.local` or other areas for mapping device names or to use `chmod` or `chown` for SecVM. This is because it is managed for you by the `createdisk` function and you can verify this by running the following command:

```
# ls -l /dev/oracleasm/disks
```

CTE Load Order and Startup Scripts

The last change is to ensure that CTE starts before ASM starts in the startup scripts.

Failover Testing

Confirm that everything is functional:

- Ensure that the GuardPoints are all operational.
- Ensure that you receive valid results when you query the database.
- Verify that the load order ensures that CTE starts before ASM .

Once verified, you can start the failover testing for each RAC Node.

1. Reboot the RAC Node 1 and monitor the startup.
2. Once the restart is clean, reboot RAC Node 2 and monitor the startup.

Issues with Device Mapper and Invalid Guard Path

If CTE is unable to apply a GuardPoint on a raw device, the logs may generate an error similar to the following:

```
[SecFS, 0] EVENT: Failed to guard /dev/mapper/devicename (reason: Invalid Guard Path flags 0x2  
gypped 0x4 status 0x11) - Will retry later
```

If you receive this error, use the `setup` command to check the status of the disks, type:

```
# setup info <deviceName>
```

Before attempting to establish a GuardPoint, look closely at the open count value and ensure that it is 0 on all nodes.

Basic Troubleshooting Techniques

The following are some of the most common configuration issues that prevent the Oracle ASM configuration from working properly.

If you encountering errors similar to:

- ORA-15075: disk(s) are not visible cluster-wide
- ORA-15032: not all alterations performed

This could be the result of improper settings for the I/O layer, meaning that your disks are not properly configured.

Perform the following tasks to verify that the settings are correct:

1. On the DSM Management Console, in the Host Group that was created for the RAC cluster, verify that the host group for this configuration does **NOT** have the Cluster Group option set (this option is only for GPFS, which is not supported with CTE).
2. Ensure that the GuardPoints for the block devices are set at the Host Group level. This ensures that each node receives identical GuardPoints.
3. Verify that the GuardPoints are active on all nodes. When the GuardPoints are set, go to each node and verify that they are set and guarded, using the WebUI or the `secfsd -status guard` command. If they do not guard correctly:
 - Verify that the udev rules are set correctly, as described in ["Modify the UDEV Rules" on page 117](#)
 - Make sure the device names are the same across all nodes.
4. From ASM, make sure that the `asm_diskstring` parameter is modified to include the CTE devices and that the proper pathname is used, see ["Altering ASM_DISKSTRING on ASM" on page 117](#).

Verifying Database Encryption

Option 1

The best way to verify the state of the data, without impacting anything in the existing environment, is to use the Oracle `kfed` command. You can run this command against the native path of the existing GuardPoints and make sure it returns with valid header information. If it returns valid information with the GuardPoint in place, then this confirms that the data is properly encrypted. If it returns with invalid header information, then that indicates that the data is either clear, double encrypted, or not in the expected encrypted state. The syntax for running this command would look similar to the following but will vary based on your environment.

```
# /app/oracle/grid/product/11.2.0/grid/bin/kfed read /dev/rdisk/<diskName>
```

If the location is properly encrypted, following is an example of the viewable output:

```
# /app/oracle/grid/product/11.2.0/grid/bin/kfed read /dev/rdisk/<diskName>
```

System Response:

```
kfbh.endian:          1 ; 0x000: 0x01
kfbh.hard:            242 ; 0x001: 0xf2
kfbh.type:           124 ; 0x002: *** Unknown Enum ***
kfbh.datfmt:          66 ; 0x003: 0x42
kfbh.block.blk:       1088904227 ; 0x004: blk=1088904227
kfbh.block.obj:       1558192170 ; 0x008: file=8234
kfbh.check:           3321251423 ; 0x00c: 0xc5f6465f
kfbh.fcn.base:         932956641 ; 0x010: 0x379bc9e1
kfbh.fcn.wrap:        3040493590 ; 0x014: 0xb53a4016
kfbh.spare1:          3806015223 ; 0x018: 0xe2db2ef7
kfbh.spare2:          3794962182 ; 0x01c: 0xe2328706
6000000000D8000 01F27C42 40E75C23 5CE0202A C5F6465F
[.|B@.\#\..*..F_]
6000000000D8010 379BC9E1 B53A4016 E2DB2EF7 E2328706 [7.....:@.....2..]
6000000000D8020 CA2F30AD 522B4D21 99292639 004EBB34 [./0.R+M!.)&9.N.4]
6000000000D8030 A3896BE8 BD839D23 2204E19E 946C575C [...k....#"....lW\]
6000000000D8040 4CE2218F 35E1B101 AF751A70 780E6D6E [L.!5....u.px.mn]
6000000000D8050 5E7E6A38 C600ED5F 929047C4 DF372A8E [^~j8..._...G..7*.]
6000000000D8060 E103152D BA87CC03 11A7D963 9D72FCE1
[...-.....c.r..]
6000000000D8070 1EC6B48B 03EE869F 61D651F9 E7614957 [.....a.Q...aIW]
6000000000D8080 810E0353 9C461F49 69569733 501D19EF [...S.F.IiV.3P...]
6000000000D8090 B268002B 4F9457B6 BDB04AC5 D3D07446 [.h.+O.W...J...tF]
```



```
60000000000D80A0 FD9EE5E0 9B46CB66 30D10B22 F63AB77E [.....F.f0.."...~]
60000000000D80B0 6FF79075 4BBD1FAD 8F226188 7774300D [o..uK...."a.wt0.]
60000000000D80C0 A809B6FB E1F1C80B B5760E68 9747D97D [.....v.h.G.}]
KFED-00322: Invalid content encountered during block traversal: [kfbtTraverseBlock][Invalid
OSM block type][ ][124]
```

Option 2

The second option to verify the state of the data is to use the `dd` command. This requires you to specify some blocks and write it out to a file. After this completes, read the file using the `strings` command. You can do this while the device is in use. In the example below some sectors are skipped and it only dumps 10000 counts.

For example:

```
# dd if=/dev/mapper/asm_data2p1 of=/tmp/dd2.out skip=1047 count=10000
```

Option 3

The third option to verify the state of the data without impacting the existing environment is to use the `strings` command.

Note

The `strings` command cannot read a busy or large device.

You can run this command against the native path (`/dev/<deviceName>`) of the existing GuardPoints (`/dev/secvm/dev/<deviceName>`). The new path to SecVM would be similar to `/dev/secvm/dev/<deviceName>`. By executing the `strings` command against the native path `strings /dev/devicename | more`, this does not go through the SecVM device and therefore is not be decrypted. If it is encrypted the output should contain illegible text.

Chapter 10: Configuring Support for SAP HANA

This chapter describes SAP HANA, which provides automatic host-failover support. It contains the following sections:

Overview	126
Customizing CTE for SAP HANA in HA Mode	126
Using SAP HANA with LDT	128
Setting Memory Allocation	128

Overview

SAP HANA provides automatic host-failover support. CTE works with HANA fibre storage systems to enable and disable GuardPoints when a protected host starts, stops, or fails over to standby host.

CipherTrust Transparent Encryption - SAP HANA (CTE-SAP HANA) supports non-shared storage where each HANA node has its own separate storage volumes. CTE-SAP HANA provides customized scripts to support startups, shutdowns, and fail overs.

HANA attaches logical unit number (LUNs) or logical volume management (LVMs) using a Fibre Storage Connector (fcClient) providers. Thales provides hooks that are called by the HANA fcClient providers that manage guarding or unguarding of storage locations.

Note

Thales recommends using host groups to manage configuring in a clustered host environment.

Customizing CTE for SAP HANA in HA Mode



CAUTION

The following procedure only applies if multiple HANA nodes are configured in a high availability (HA) environment. If you are installing CTE on a single HANA node, do not change the default HANA or CTE settings.

1. Go to the installation directory:

```
# cd /opt/vormetric/DataSecurityExpert/agent/secfs/saphana
```
2. If required, edit the appropriate CTE `fcClient` refined script:

Script file	Use
<code>fcClientRefinedVTE.py</code>	fcClient provider for LUN
<code>fcClientLVMRefinedVTE.py</code>	fcClientLVM provider for LVMs

3. Copy the appropriate script file to a shared location that is accessible to all nodes. In a HANA cluster environment, all nodes require access to the CTE scripts.
4. Edit the storage section of the `global.ini` file to indicate the corresponding CTE `fcClient` as the High Availability (HA) provider and to point to the location of the CTE script.

LUN Example

```
[storage]
  ha_provider = fcClientRefinedVTE
  ha_provider_path = /hana/shared/myFcClient
```

If necessary, enable debug tracing:

```
[trace]
  ha_provider = debug
  ha_fcclient = debug
  ha_fcclientrefinedvte = debug
```

LVM Example

```
[storage]
  ha_provider = fcClientLVMRefinedVTE
  ha_provider_path = /hana/shared/myFcClient
```

If necessary, enable debug tracing:

```
[trace]
  ha_provider = debug
  ha_fcclientlvm = debug
  ha_fcclientlvmrefinedvte = debug
```

5. Use the same CTE agent with all hosts, including standby hosts.

6. Ensure that `/etc/sudoers` includes the following:

```
<sid>adm ALL=NOPASSWD: /usr/bin/secfsd
```

7. Enable the guard paths at the mount-point level.

For example, individual guards were placed on `/hana/data/HAN/mnt00001`, `/hana/data/HAN/mnt00002`, and so forth.

- Use a similar naming practice for log partitions, such as `/hana/log/HAN/mnt00001`, and so forth.
- Place the guard at the mount-point level. The guarded paths must match the corresponding data and log mount paths.

8. From the DSM, configure GuardPoints as type `manual`. You must enable and disable the guardpoints immediately after the device is attached, or just prior to detachment.

The reason for manual GuardPoints is that it invokes guarding and unguarding from within the HANA during the startup, shutdown, or failover process. The process resembles that of mounting and unmounting guarded auto-mount points.

9. Configure all GuardPoints so that they are available in the standby host, so that any data and log partitions that fail over from any host can be guarded on the standby.

Thales recommends that you configure all GuardPoints on all hosts, because a failed-over active host can then become the new standby, and will require all available GuardPoints.

Example

The following is an example of the data and log volumes for the host that are mounted.

<code>/dev/mapper/VG_HAN_DATA_1-LV_HAN_DATA_1</code>	793971096	3059712	750579916	1%
<code>/hana/data/HAN/mnt00001</code>				
<code>/hana/data/HAN/mnt00001</code>	793971096	3059712	750579916	1%
<code>/hana/data/HAN/mnt00001</code>				
<code>/dev/mapper/VG_HAN_LOG_1-LV_HAN_LOG_1</code>	496233160	2461764	468564152	1%
<code>/hana/log/HAN/mnt00001</code>				
<code>/hana/log/HAN/mnt00001</code>	496233160	2461764	468564152	1%
<code>/hana/log/HAN/mnt00001</code>				

Note that partition `mnt00002` is also configured, although not currently mounted by HANA. The `secfsd` status output should show the GuardPoint configuration as follows:

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/hana/data/HAN/mnt00001	my-pol	manual	guarded	guarded	N/A
/hana/log/HAN/mnt00001	my-pol	manual	guarded	guarded	N/A
/hana/data/HAN/mnt00002	my-pol	manual	unguarded	not guarded	Inactive
/hana/log/HAN/mnt00002	my-pol	manual	unguarded	not guarded	Inactive

For more information, see the *SAP HANA Fiber Channel Storage Connector Admin Guide* at <http://www.sap.com/documents/2016/06/84ea994f-767c-0010-82c7-eda71af511fa.html>

Using SAP HANA with LDT

SAP HANA is compatible with LDT. You must add additional CTE commands to the HANA administrator entry.

- Using a text editor, edit `/etc/sudoers` and add entries for `/usr/bin/voradmin` and `/usr/bin/vmsec`:

```
# hanadm ALL=NOPASSWD:  
/usr/bin/secfsd, /usr/bin/voradmin, /usr/bin/vmsec, /sbin/multipath, /sbin/multipathd, /etc/init  
.d/multipathd, /usr/bin/sq_  
persist, /bin/mount, /bin/umount, /bin/kill, /usr/bin/lsof, /sbin/vgchange, /sbin/vgscan
```

If you are using an ext3 file system, you must mount it with extended attributes.

- Using a text editor, edit the storage section of the `global.ini` file, type:

```
partition_*_data__mountOptions = -o user_xattr  
partition_*_log__mountOptions = -o user_xattr
```

Setting Memory Allocation

There is a limitation in memory allocations for SAP HANA with asynchronous direct I/O. When you use CTE in conjunction with applications like SAP HANA that can process large numbers of direct I/O writes through the Linux AIO interface, CTE can allocate more memory than is desirable.

To limit the amount of memory that CTE consumes for AIO buffers, use the following configuration to limit the amount of memory CTE consumed for AIO buffers:

```
# max_aio_memory_limit <MB>
```

The MB value specifies how much memory to allocate to temporary DIO buffers.

Note

If you do not specify a value, the default is 0, which has no memory bounding effect.

Set the option by echoing a value into the `/opt/vormetric/DataSecurityExpert/agent//secfs/.sec/conf/` configuration file. For example:

```
echo 1024 > /opt/vormetric/DataSecurityExpert/agent/ secfs/.sec/conf/max_aio_memory_limit
```

This limits the memory consumed by AIO buffers to 1GB.

Note

You **must restart** CTE after changing any values in the configuration directory to make the changes effective.

Chapter 11: Container Security

This chapter describes securing data in container environments, Docker or RedHat OpenShift, using CTE. It contains the following sections:

Installing Docker Automatically	129
Container Security Overview	129
RedHat OpenShift Containers with CTE	141
Creating an OCP Project in CLI with API Commands	143

Note

Currently, this feature is only supported on the DSM. Support for this feature will be added to CipherTrust Manager in a future release.

Installing Docker Automatically

A new option allows for automatically registering the host for Docker during registration. This allows for easily enabling Docker for a large number of hosts.

During the installation phase, the agent indicates to the DSM that it wants DOCKER. Only registration is performed at this time. After registration, the DSM will validate the Docker host to ensure that the agent and the DSM use compatible versions, and that LDT is not enabled for the host.

Note

LDT and Docker are not compatible.

During the installation phase, the agent indicates to the DSM that it wants DOCKER. Only registration is performed at this time.

Container Security Overview

CTE provides data security for container environments. You can set up data protection policies for container images. In addition to data encryption, CTE also provides container-level access control and audit logging. DSM Administrators can create GuardPoints in container images through the DSM Management Console. Users can use either of the following container options:

- **Docker Container:** CLI tool for creating containers.
- **Red Hat OpenShift with Customized Docker Container:** GUI tool for creating containers and persistent storage that mounts like NFS.

Container Terminology

• Containers

The basic unit of OpenShift/Docker Application are called containers. A container runs one or more processes inside of a portable Linux environment. Containers are started from an Image and are usually isolated from other containers on the same machine.

• Image

A layered Linux file system that contains application code, dependencies, and any supporting operating system libraries. An image is identified by a name that can be local to the current cluster or point to a remote Docker registry.

- **Pods (OpenShift only)**

A POD is a set of one or more containers that reside on a host/node and share a unique IP address and volume, (persistent storage). OpenShift leverages the Kubernetes concept of a pod.

- **Project and Users (OpenShift only)**

A namespace that provides a mechanism to scope resources in a cluster. Users interact with OpenShift. It grants permission to access applications.

Docker Containers with CTE

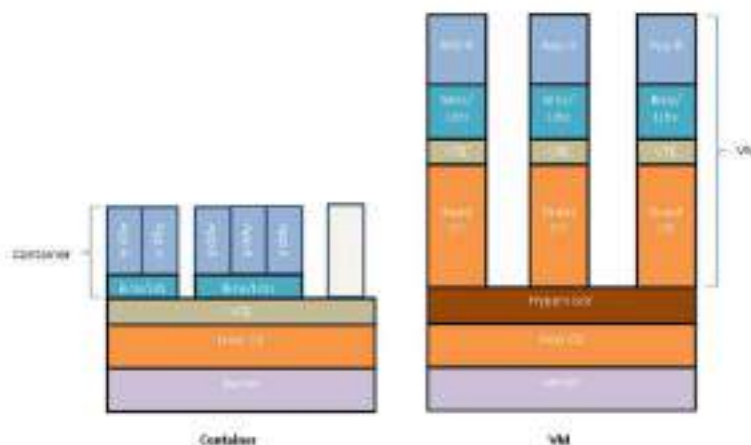
Docker allows for containerizing an environment for application deployment. Docker is an infrastructure built on top of Linux containers and various namespace components. Typically, an application deployment is bundled with all of the dependent packages in a single image called a Docker image. Docker images are ready to run applications in containers. A user can instantiate any number of Docker containers using from one or more Docker images. This makes it easy for users to move applications around on their servers. The containerization removes the pain of setting up an environment for applications and provides isolation for applications.

A Docker container can run any application, for example, a Postgres database server. Docker containers are used widely to run micro-services, which are stateless in nature. But a micro-service, when it is running, might generate a log trail inside the Docker container. This log trail might contain sensitive information. This warrants encrypting directories inside a Docker container. If a Docker container runs a database-server type of service, it will need data protection including encryption of data, granular access control and the ability to audit the log that accesses the data.

CTE: Virtual Machine versus Docker

CTE installs on the Docker container host and orchestrates security from the Docker host. It does not leave a footprint inside the Docker image or containers. You setup the GuardPoints inside individual containers at runtime. The diagram below depicts the difference between CTE deployment on a virtual machine and a Docker container host.

Figure 11-1: CTE in Docker container environment versus virtual machine environment



Using the CTE Agent

In order to use the CTE Agent to protect Docker images and containers, you must obtain a CTE Agent license for Docker. Contact Thales Support for information on obtaining a license.

There is no change to the CTE installation, however CTE agent must be installed on the Docker host system.

Docker containers in custom paths won't start after CTE agent is installed

This problem occurs if you have installed one or more Docker containers on a host in a directory path other than the Docker default of `/var/lib/docker`. After installing the CTE agent on such a host, any Docker containers installed on that host will no longer start if the CTE `secfs` service is running. This problem occurs even to docker containers not configured to work with the CTE agent.

The following error message appears when you attempt to start a Docker container:

```
exec user process caused "permission denied"
```

To work around this issue, create a symbolic link from the current installation path of the docker container to the default Docker path of `/var/lib/docker`:

```
ln -s /custom/path /var/lib/docker
```

After creating this symbolic link, affected Docker containers will start up normally even if `secfs` is running.

Set the Docker Storage Driver

On RHEL 7.x operating systems, the Docker engine default storage driver has changed from `devicemapper` to `overlayfs` for v1.13.1 and later. Currently, CTE only supports `devicemapper`. If your Docker engine uses `overlayfs` or any other storage driver, then you must change it to `devicemapper` before using CTE to protect your data.

Before you change your storage driver, verify your Docker version:

1. Login to your Docker agent CLI.
2. Check your Docker version, type:

```
# docker version
```

System Response:

Client:

```
Version:      17.04.0-ce
API version:  1.28
Go version:   go1.7.5
Git commit:   4845c56
Built:        Mon Apr  3 18:01:50 2017
OS/Arch:      linux/amd64
```

Server:

```
Version:      17.04.0-ce
API version:  1.28 (minimum version 1.12)
Go version:   go1.7.5
Git commit:   4845c56
Built:        Mon Apr  3 18:01:50 2017
OS/Arch:      linux/amd64
Experimental: false
```

3. Check to what option the storage driver is set, type:

```
# docker Info
```

System Response:

```
Containers: 2
  Running: 1
  Paused: 0
  Stopped: 1
Images: 2
Server Version: 17.04.0-ce
Storage Driver: overlay
```

Change the Storage Driver

To change the storage driver:

1. Login to your Docker agent CLI.
2. Stop the Docker daemon, type:

```
# systemctl stop docker.service
```
3. Open another CLI session of agent so you can monitor Docker.
4. In `/etc/docker/` directory, create a file called `daemon.json` if the file does not yet exist.
5. Add a storage driver to the file, type:

```
{  
  "storage-driver": "devicemapper"  
}
```
6. Save the file.
7. Restart the Docker daemon, type:

```
# systemctl start docker.service
```
8. Verify that the storage driver is set to device mapper, type:

```
# docker Info  
Containers: 2  
Running: 1  
Paused: 0  
Stopped: 1  
Images: 2  
Server Version: 17.04.0-ce  
Storage Driver: devicemapper
```
9. Verify that the docker containers are active, type:

```
# docker ps  
CONTAINER ID | IMAGE | COMMAND | CREATED | STATUS | PORTS | NAMES  
bb953565e866 | abc/rh:v1 | "bash" | 4 weeks ago | Up 4 weeks | | jdoe
```

Administering the Docker Host

To protect data inside Docker images or containers, you need to create GuardPoints in the DSM, inside a Docker image or container, to which a CTE Agent policy is applied.

This section describes the administrative tasks related to Docker hosts; creating policies, creating GuardPoints, configuring audit logs, and generating reports.

Creating Policies

Policy creation for Docker hosts is largely the same as CTE's existing policy creation procedure with a few differences described below.

The basic procedure to create a policy is as follows:

1. Log on to your DSM as an administrator of type Security, Domain and Security, or All.
2. Navigate to **Policies > Manage Policies**.
3. Click **Add** to open the *Add Online Policy* page
4. From the **Policy Type** drop down list, select **Standard**.

5. Type in a name for the policy in the **Name** field.
6. Add a description for the policy (optional).

Refer to “Configuring Policies” in the *DSM Administrators Guide* for details about creating a policy. Once you have created a policy, you must add rules to the policy to encrypt data and control access to files and directories.

Adding Security Rules

This section describes how to create security rules in the context of Docker images and containers.

Create Resource Set

A *Resource Set* specifies the hosts, files, and directories to which a user or process will be permitted or denied access.

1. After creating the policy in the previous section, click **Add** in the **Security Rules** panel to open the *Add Security Rule* page.
2. Click **Select** next to the **Resource** field to open the *Select Resource Set* page. The page displays resource sets if any currently exist.
3. Select an existing resource set that meets your requirements, otherwise click **Add** to open the *Add Resource Set* page.
4. Enter a name for the resource you want to create.
5. Click **Add** again to open the *Add Resource* page to add a resource to the resource set you want to create.
6. Click **Select** next to the **Host** field to select a Docker host from which to choose resources. Select the radio button next to the host and click **Select**.
7. Since this is a Docker host, another field displays: **Docker Image**. Click **Browse** to open the **Remote Docker Browser** to select a Docker image or container, from which to select a resource.
8. Click **Browse** next to the **Directory** field to open the **Remote File Browser**.
9. Browse the directories and files on the image or resource that you want to add to the resource set. (Select **Directory Only** or **Directory and File** to browse only directories or files and directories.)
10. Select the resources to add and click **Ok**.
11. Click **Ok** to add the resource set. The *Select Resource Set* page opens.
12. Select the resource you just created and click **Select Resource Set**.
13. Check the **Exclude** box, to the right of the **Resource** field.

This excludes the resources in the resource set and includes all other host resources. Uncheck the box to include just the resources in the resource set.

Create User Set

A *User Set* specifies users that are permitted or denied access to files and directories in a GuardPoint.

1. After creating the policy in the previous section, click **Add** in the **Security Rules** panel to open the *Add Security Rule* page.
2. Click **Select** next to the **User** field to open the *Select User Set* page. The page displays user sets if any currently exist.
3. Select an existing user set if it meets your requirements, otherwise click **Add** to open the *Add User Set* page.

4. Enter a name for the user set and click **Add** to open the *Add User* page.
5. Enter information for the **uname**, **uid**, **gname**, **gid**, and **osDomains** fields. Refer to the online help for more details.
6. If you click **Browse Users**, the *Add Users* page opens, you can select users from an LDAP server if configured, or from a selected Host.
7. To select users from docker images or containers, use the default **Agents** selection and select the host name (FQDN) of the Docker host from the list.
Since this a Docker host, another field displays: **Docker Image/Container**.
8. Click **Browse** to open the **Remote Docker Browser** to select a Docker image or container from which to select users.
9. From the **Remote Docker Browser**, expand the file icon to view the Docker image and containers from which to select users to add to the User Set.
10. Once you've made your selections, click **Ok**, a tabulated list of available users is displayed.
11. Select the appropriate users. Click **Ok** to return to the *Add User Set* page.
12. Select users. Click **Ok** to return to the *Select User Set* page.
13. Select the newly created user set and click **Ok**.

Create Process Set

A *Process Set* specifies the executables that are permitted or denied access to GuardPoint data.

1. After creating a policy in the previous section, click **Add** in the **Security Rules** panel to open the *Add Security Rule* page.
2. Click **Select** next to the **Process** field to open the *Select Process Set* page. The page displays process sets if any currently exist.
3. Select an existing process set if it meets your requirements, otherwise click **Add** to open the *Add Process Set* page.
4. Enter a name for the process set you are about to create and click **Add** to open the *Add Process* page.
5. Click **Select** next to the **Signature Set** field, a list of existing signature sets is displayed.
6. Select an existing signature set if it meets your requirements, otherwise click **Add** to open the *Add Signature Set* page.
7. If you selected **Add** then you need to provide a **Name** for the signature set.
8. Enter the name and click **Ok**, the *Signature Reference* page opens.
9. Click the name of your signature set to edit the signature set, the *Edit Signature Set* page opens.
10. Click the **Source** tab, click **Select** next to the Host field, the **Select a host to continue** page opens, select the Docker host and click **Select** to go back to the **Source** tab.
11. Click **Browse** next to the **Docker Image/Container** field, select a Docker image or container from the **Remote Docker Browser**.
12. Select a binary from the Docker image and sign it similar to a binary on a protected host.
13. Click **Back**, the *Signature Reference* page opens.
14. Select the signature set you just created and click **Select Signature Reference**, the *Add Process* page opens.

15. Select a host. Once you select a Docker host, the **Docker Image/Container** field displays.
16. Select a Docker image or container.
17. Click **Browse** and select a directory from the **Remote File Browser**, fill in the file name field as required. Click **Ok** to return to the *Add Process Set* page.
18. Choose the appropriate (newly created) process set and click **Ok**. This returns you to *Select Process Set* page.
19. Select the process set and click **Select Process Set**. This returns you to the *Add Security Rule* page.
20. Click **Ok** to add the process set to the security rule.

Enable Docker through Host Settings

You must enable Docker in the Agent.

1. At the DSM Management Console, click **Hosts > Hosts**.
2. Click **Add Host**, or click on an existing Host name to edit the host.
3. In the General tab, select **Docker Enabled**.
4. Click **Apply**.
5. Click **Host Settings** tab.
6. Add the Docker Daemon to the host settings:
For Docker v1.12 and above, type:
`|authenticator|/usr/bin/dockerd`
For Docker v1.12 and below, type:
`|authenticator|/usr/bin/docker`
7. Click **Apply**.

CTE Docker GuardPoints

Docker typically provides two types of containers:

- **Transient:** Run micro services which are stateless applications.
- **Long running:** Host stateful applications similar to a database application.

The CTE Docker security feature protects data in both type of containers. You can use CTE to protect either type of containers. You select the container type while configuring the GuardPoint.

CTE provides two types of GuardPoints:

- Image-based
- Container-based

Image-based GuardPoints

You can set up a data protection policy on a Docker image. After an image-based GuardPoint is created, all of the instances running from the protected Docker image inherit the policy and its settings. Any change to the policy is reflected across Docker containers that are started from protected Docker images. You can also refer to Image-based protection as templated protection. The GuardPoints set up on a Docker image serves as a template for protection of all the Docker containers created as CTE protected Docker images.

Users can browse a Docker image to select the path for protection and configure security rules using information from a Docker image. This process is described in the *DSM Administration Guide*.

Container-based GuardPoints

You can set up a GuardPoint for a specific Docker container. You can browse a Docker image to select the path for protection, and to configure security rules using information from a Docker image.

GuardPoints for Docker Containers

Before creating GuardPoints on Docker images and containers, the following must be taken into consideration:

- You must add the Docker engine process to the Host Settings.
- When applying GuardPoint policies to Docker containers, users must ensure that the root user has at least 'permit' effect on the GuardPoint. Otherwise, the GuardPoint is inaccessible to all users, even for users with 'apply_key', and 'permit' effects.

Creating GuardPoints

1. Log on to your DSM as an administrator of type Security, Domain and Security, or All.
2. Navigate to **Hosts**.
3. On the *Hosts* page, click the name of the host in the **Host Name** column, the *Edit Host* page opens.
4. Click the **Guard Docker** tab.
5. Click **Guard** to open the *Guard File System* page.
6. Select a policy to apply to the GuardPoint you are about to create.
7. Click **Browse** next to the **Docker Image/Container** field to browse the Docker host for an image or container to which to apply the policy.
8. Select the type of directory to guard.
9. Click **Browse** next to the **Path** text box to browse the image or container for a file path to add the GuardPoint.
10. Click **Ok**, the *Edit Host* page opens with the newly created GuardPoint listed in the table.

Note: Automount is not supported in a Docker environment.

Viewing GuardPoints

You can view GuardPoints from the Management Console GUI and from the Docker host using the CTE Agent `secfsd` utility. To view GuardPoints using the `secfsd` utility:

1. Log on to your Docker Host as root.
2. At the prompt, type:

```
# secfsd -status guard -tree
```

The output is displayed in a tabular format. The table displays the following information:

- GuardPoint location on the image or container
- Name of the policy applied to the GuardPoint
- Type of directory being guarded

- Container ID
- GuardPoint configuration status; whether or not the GuardPoint has been enabled
- GuardPoint status; whether or not the GuardPoint is currently guarded or not
- Reason for the GuardPoint not being guarded

To view information for each GuardPoint;

1. Log on to your Docker Host as root.
2. At the prompt, type the following;

```
# secfsd -status guard -v
```

The output is displayed for each GuardPoint configured on the host. The following information is displayed for each GuardPoint:

- Name of the policy applied to the GuardPoint
- Directory to which the GuardPoint is applied
- Type of directory being guarded
- GuardPoint configuration status; whether or not the GuardPoint has been enabled
- GuardPoint status; whether or not the GuardPoint is currently guarded or not
- Reason for the GuardPoint not being guarded
- Space usage on the GuardPoint location
- Container ID

Data Security for Docker Images and Containers

The CTE Agent supports data security for directories within Docker images and containers. If a new GuardPoint is added to a directory within an image or container, and that GuardPoint contains data, that data must be transformed before CTE can apply an encryption policy. Therefore, before creating a GuardPoint, determine which of the following conditions is applicable to your situation.

Setting up an image based GuardPoint

If you are setting up an image based GuardPoint:

1. Create a container from that image using the `docker run` command. For example;

```
# docker run Ubuntu
```

CTE creates a container `<container_name>`.
1. Export the container to a TAR file in a directory using the `docker export` command. The following example creates a directory and exports the TAR file:

```
# mkdir -p /tmp/export/GP1  
# docker export <container_name> > /tmp/export/GP1/<container_name>.tar
```
2. Extract TAR file using the command `tar -xvf`. The following example creates a directory and extracts the TAR file to that directory;

```
# mkdir -p /tmp/extract/GP1  
# tar -xvf /tmp/export/GP1/<container_name>.tar -C /tmp/extract/GP1/
```

3. Guard extracted folder with a data transform policy, for example guard a folder with sensitive data under `/tmp/extract`.
4. Transform files using CTE.
5. Unguard the transformed folder.
6. Create a TAR file from the extracted files using the command `tar -czf`. The following example creates a directory, a TAR file and places it in that directory;

```
# mkdir -p /tmp/import/GP1
# cd /tmp/extract/GP1
# tar -czf /tmp/import/GP1/<container_name>.tar *
```

7. Import the TAR file back to the image using the Docker command `docker import`. For example,

```
# cat /tmp/import/GP1/<container_name>.tar | docker import - <image>
sha256:d303c8b357084291f02f5e033660f469705f8e2c1744bf14516783b58b0f3bd7
```

The image `<imageName>` is created in this example, and its ID is;

```
sha256:d303c8b357084291f02f5e033660f469705f8e2c1744bf14516783b58b0f3bd7
```

8. You can now guard directories within this image or container with a production policy.

Notes

- This procedure only works with an image's local file system and cannot transform a Docker data volume or NFS mount.
- Data transformation only occurs on the directory that is guarded, and not the entire Docker image.

Setting up a Container-Based GuardPoint

If you are setting up a container based GuardPoint, stop the Docker container before setting up GuardPoints:

1. Export the container to a TAR file in a directory using the `docker export` command. The following example creates a directory and exports the TAR file;
2. Extract TAR file using the command `tar -xvf`. The following example creates a directory and extracts the TAR file to that directory;

```
# mkdir -p /tmp/export/GP1
# docker export <container_name> > /tmp/export/GP1/<container_name>.tar
```

3. Guard extracted folder with a security policy.
4. Transform files using the CTE.
5. Unguard the transformed folder.
6. Create a TAR file from the extracted files using the command `tar -czf`. The following example creates a directory and creates a TAR file and places it in that directory:

```
# mkdir -p /tmp/import/GP1
# cd /tmp/extract/GP1
# tar -czf /tmp/import/GP1/<container_name>.tar *
```

7. Import the TAR file back to the image using the Docker command `docker import`. For example,

```
# cat /tmp/import/GP1/<container_name>.tar | docker import - <image>
```


sha256:d303c8b357084291f02f5e033660f469705f8e2c1744bf14516783b58b0f3bd7
The image, *<image>* is created in this example, and its ID is;
sha256:d303c8b357084291f02f5e033660f469705f8e2c1744bf14516783b58b0f3bd7
8. You can now guard this image or container with a production policy.

Notes

- This procedure only works with an image's local file system and cannot transform a Docker data volume or NFS mount.
- Data transformation only occurs on the directory that is guarded, and not the entire Docker image.

Setting up a GuardPoint for an Exported Docker Volume

If you are setting up a GuardPoint for a Docker volume exported from a Docker host:

1. Guard a folder on a host with a data transform policy.
2. Transform files using the Thales executable `dataxform`.
3. Unguard the folder on the host.
4. You can now guard this image or container with a production policy.

This approach works with Docker data volume and NFS mount, and can not transform the image/container local file system.

Configuring Audit Logging

Configure Log settings for the CTE Agent (FS Agent Log) at the System level on the DSM. These settings are inherited by all the domains on the DSM. However, you can fine tune log settings for a specific host, and those settings will override the system settings. With the introduction of Docker support, you can now configure log settings for Docker images and containers. Docker logs evaluate GuardPoint policies.

Configure Docker Log Settings

1. Log on to your DSM and switch to a domain. Alternately, log on to a DSM as a local domain administrator of type Security with a Host role.
2. Navigate to the **Hosts** page.
3. Click the name of your Docker host in the **Host Name** column, the *Edit Host* page opens.
4. Click **Docker Log**.
5. Enter the following information in the **Configure Docker Log Setting** panel:
 - a. **Docker Image/Container:** Click **Browse** to select an image or container from the Docker host. If you select an image, the **Docker Image ID** field displays the image ID. If you select a container, the **Docker Image ID** field displays the image from which the container was created, and the **Docker Container ID** displays the container ID. You can use these IDs to search for Docker specific logs on the *Logs* page later.
 - b. **Policy Evaluation Level:** Select a log message level. For more information about log levels, refer to the *DSM Administrators Guide*.
 - c. **Policy Evaluation Duplicated:** Select to suppress or allow duplicate messages. The default is

SUPPRESS.

6. Click **Ok**. CTE saves the Policy Evaluation settings in a tabular format under the **Configure Docker Log Setting** panel.

Searching for Docker Log Messages

Docker log messages display on the Logs page. To search for Docker specific log messages:

1. Click **Logs > Logs**.
2. Enter the following information in the **Search** panel:
 - **Log Type**: Select whether you want to display logs from both the DSM and the agents, only the DSM, or only the agents. The default is All, which means from both DSM and agents.
 - **Source**: Enter the hostname of the DSM server, or agent, for which you want to return log files.
 - **Last Refreshed**: Displays the date and time of when the displayed log files were last refreshed. Format is YYYY-MM-DD HH:MM:SS
 - **Message Contains**: Type in the text string that you want to search for in the log messages.
 - **Docker Host**: Click **Browse** to select the Docker Host for which you want to return log files.
 - **Docker Image/Container**: Click **Browse** to select an image or container for which you want to display logs.
 - **Docker Image ID**: Displays the ID for the selected Docker image.
 - **Docker Container ID**: Displays the ID of the selected Docker container.
3. Click **Go**. The relevant logs display in the table under the **Search** panel.

Generating Reports

The following DSM reports have been updated to include Docker information:

System Level Reports

To view system level reports, log on to a DSM as an administrator of type System or All. The system level reports that contain Docker information are:

- **System License Usage Summary**: Includes information about the total number of Docker licenses in use for the entire DSM.
- **License Usage by Domain**: Includes information about the total number of hosts with the Docker license enabled.

Domain Level Reports

To view domain level reports, log on to a DSM as an administrator of type Domain, Domain and Security, or All. Administrators of type Domain and Security and type Security must have AUDIT role privileges to access the reports. The domain level reports that contain Docker information are:

- **License Usage by Domain Summary**: Includes information about the total number of hosts with the Docker licenses enabled.
- **Host with GuardPoint Status**: Includes identification information about Docker Images and Docker containers that have GuardPoints. The columns are **Docker Image ID** and **Docker Container ID**.

You can download and save all reports locally in CSV format by clicking **Download**.

RedHat OpenShift Containers with CTE

Red Hat OpenShift Container Platform (OCP) provides an immutable, container-based platform to deploy and run applications and micro services. It is Red Hat's on-premise private PaaS product. It is built around a core of application containers powered by Docker Container Packages and Kubernetes Container Cluster Management, on a foundation of Red Hat Enterprise Linux.

Using the CTE Agent

In order to use the CTE Agent to protect OCP images and containers, you must obtain a CTE Agent license for Docker. The Docker license covers both Docker and OCP. Contact Thales Support for information on obtaining a license.

There is no change to the CTE installation, however, CTE agent must be installed on the OCP host system.

CTE: Virtual Machine versus OCP

Similarly to Docker, CTE installs on the OCP container host and orchestrates security from the OCP host. It does not leave a footprint inside the OCP image or containers. You setup the GuardPoints inside the individual containers at runtime.

Set the OpenShift Storage Driver

Although needed for Docker, this is not needed for OCP.

Administering the OpenShift Host

To protect data inside OCP containers, you need to create GuardPoints in the DSM, inside an OCP image or container, to which a CTE Agent policy is applied.

The administrative tasks related to OCP hosts are the same as for Docker hosts. See “Administering the Docker Host” for more information.

Enable OpenShift through Host Settings

If you have obtained a Docker license and enabled it through the DSM Host Settings, then OCP is also enabled.

CTE OCP GuardPoints

OCP typically provides two types of containers:

- **Transient:** Run micro services which are stateless applications
- **Long running:** Host stateful applications similar to a database application.

The CTE OCP security feature protects data in both type of containers. You can use CTE to protect either type of containers. You select the container type while configuring the GuardPoint.

Types of GuardPoints

CTE provides two types of GuardPoints:

- Image-based
- Container (POD)-based

Image-based GuardPoints

You can set up a data protection policy on an OCP image. After an image-based GuardPoint is created, all of the instances, running from the protected OCP image, inherit the policy and its settings. Any change to the policy is reflected across OCP containers that are started from protected OCP images. You can also refer to Image-based protection as templated protection. The GuardPoints set up on an OCP image serves as a template for protection of all of the OCP containers created as CTE protected OCP images.

Users can browse an OCP image to select the path for protection and configure security rules using information from an OCP image. This process is described in the *DSM Administration Guide*. It is the same procedure as for a Docker image.

Container/POD-based GuardPoints

You can set up a GuardPoint for a specific OCP container in the same manner that you do for a Docker container. You can browse an OCP image to select the path for protection, and to configure security rules using information from an OCP image.

Creating GuardPoints

Create GuardPoints in the same manner as for Docker.

Viewing GuardPoints

View GuardPoints in the same manner as for Docker.

Data Security for OpenShift Images and Containers

The CTE Agent supports data security for directories within OCP images and PODS/containers. If a new GuardPoint is added to a directory within an image or container, and that GuardPoint contains data, that data must be transformed before CTE can apply an encryption policy. Therefore, before creating a GuardPoint, determine which of the following conditions is applicable to your situation.

Setting up an Image-based GuardPoint

Set up a GuardPoint in the same manner as for Docker.

Setting up a POD-based GuardPoint

Set up a POD GuardPoint in the same manner as for Docker GuardPoints. Select the POD as you would a container.

Setting up a GuardPoint for an exported OCP volume

Set up a GuardPoint in the same manner as for exported Docker volume.

Configuring Audit Logging

Configure Audit logging in the same manner as for Docker.

Generating Reports

Generate Reports in the same manner as for Docker.

Creating an OCP Project in CLI with API Commands

Creating an OCP Project with a Template

You can create an OCP project in the CLI as well as in the GUI.

Note

RedHat OpenShift is OpenSource technology. Therefore, commands, references and documentation are subject to change. Thales is providing CLI commands that are current at this time. Thales cannot guarantee the integrity of these commands. If commands no longer work, consult the OpenShift developer documentation located at:

https://docs.openshift.com/enterprise/3.2/cli_reference/basic_cli_operations.html#cli-reference-basic-cli-operations

1. Login to the OCP server with a user name and password, type:

```
# oc login <ocp-server> -u <username> -p <password>
```

2. Create a new project, type:

```
# oc new-project <project-name>
```

3. Add an instant application template to your project and deploy it, type:

```
# oc process openshift <instant-app-template-path> | oc create -f -
```

For example:

```
# oc process openshift//django-psql-example | oc create -f -
```

Deploying an OCP Project

Run the following commands after deployment completes.

1. Get pod details, type:

```
# oc get -o name pods
```

2. Parse JSON output and get container details, type:

```
# oc get -o json <pod-name>
```

3. Create directory to be guarded in containers

```
# oc exec <pod-name> -c <container-name> -- <command>
```

```
# oc exec postgresql-1-bag25 -c postgresql -- mkdir /var/tmp/gp
```

4. Guard path inside all containers and inside all pods, type:

- Container-based guarding

```
# vmssc host addgp -d <guard-path> -p <policy> -c <container-id> -i <image-id> <hostname>
```

- Image-based guarding

```
# vmssc host addgp -d <guard-path> -p <policy> -i <image-id> <hostname>
```

Note: You can also guard paths in the DSM Management Console.

5. Unguard all guarded paths, type:

- Container-based guarding

```
# vmssc host delgp -d <guard-path> -p <policy> -c <container-id> -i <image-id> <hostname>
```

- Image-based guarding

```
# vmssc host delgp -d <guard-path> -p <policy> -i <image-id> <hostname>
```

Note: You can also unguard paths in the DSM Management Console.

6. Delete project, type:

```
# oc delete project <project-name>
```

Available OpenShift commands

Commands	Function
clusterresourcequota	Create cluster resource quota resource.
configmap	Create a configmap from a local file, directory or literal value
deployment	Create a deployment with the specified name.
deploymentconfig	Create deployment config with default options that uses a given image.
identity	Manually create an identity (only needed if automatic creation is disabled).
imagestream	Create a new empty image stream.
namespace	Create a namespace with the specified name
policybinding	Create a policy binding that references the policy in the targetted namespace.
quota	Create a quota with the specified name.
route	Expose containers externally via secured routes
secret	Create a secret using specified subcommand
service	Create a service using specified subcommand.
serviceaccount	Create a service account with the specified name
user	Manually create a user (only needed if automatic creation is disabled).
useridentitymapping	Manually map an identity to a user.

Available OPC Options

Options	Parameter	Function
-f	--filename	Filename or URL to file to read a template.
-l	-labels	Label that you can set in all resources for this template.
-o	-o, --output='json'	Output format. It is either: describe json yaml name template templatefile.

Options	Parameter	Function
-o	--output-version	Output the formatted object with the given version (default api-version).
-o	--parameters=false	Do not process but only print available parameters.
-o	--raw=false	If true, output the processed template instead of the template's objects. Implied by -o describe.
-t	--template	Template string or path to template file to use when -o=template or -o=templatefile. The template format is go lang templates. [http://golang.org/pkg/text/template/#pkg-overview]
-v	-v, --value=[]	Specify a key-value pair (ex: -v FOO=BAR) to set/override a parameter value in the template.

Container secfsd Utilities

Move to the Container-appropriate name space for the instance.

Use the following commands for more information.

```
# secfsd -[command] [option]
```

Commands	Function
-status guard [-v/-tree]	list all GuardPoints
-status keys	show current encryption key state
-status auth	list authentication settings
-status lockstat	show status of system and agent lock
-status logger	list logging details
-status policy	list configured policies
-status pslist	list protected process
-status devmap	list guarded devices
-guard path [containerID]	manually guard path
-unguard path [containerID]	manually unguard path
-version	show version of kernel module secfs2
cmd -c debug.<level>.[on off]>	set debug logging on/off
-debug <on off>	enable verbose logging
-help	Displays this help message

Chapter 12: NetApp Snapshot Directory

This chapter describes SecFS support for NetApp .snapshot directory over NFS. It contains the following sections:

Overview	146
Accessing snapshots	146
Enabling Snapshots	146
Dataxform Considerations	146

Overview

The NetApp snapshot directory contains ONTAP snapshot data entries for a specific live volume. Each snapshot is a read-only volume that is automatically mounted over NFS.

A snapshot copy is a read-only image of a traditional, or FlexVol volume, or an aggregate, that captures the state of the file system at a specific point in time.

Data ONTAP maintains a configurable snapshot copy schedule that creates and deletes snapshot copies automatically for each volume.

Accessing snapshots

By default, every volume contains a directory named .snapshot through which users can access previous versions of files. Users can gain access to snapshot copies depending on the file-sharing protocol used, NFS or CIFS. You can also prevent access to snapshot copies.

Snapshot files carry the same read permissions as the original file. A user who has permission to read a file in the volume, can also read that file in a snapshot copy. A user without read permission to the volume cannot read that file in a snapshot copy.

Note

Snapshot copies do not have write permissions.

Snapshot directories only display at the mount point, although they actually exists in every directory in the tree. This means that the .snapshot directory is accessible by name in each directory, but is only seen in the output of the `ls` command at the mount point. The snapshots are stamped with the date and time.

Enabling Snapshots

The NetApp storage administrator, or the OnTap device, must configure this feature. No configuration is required through CTE. CTE guards the client directory mounting the OnTap data volume over NFS.

Note

The NetApp documentation is located here: <https://nt-ap.com/2vEnEeJ>

Dataxform Considerations

You cannot transform snapshot directory entries with Dataxform with a new key, because the snapshots are read only. You must keep previous keys and alter the running security policy accordingly to maintain access to the older snapshot entries alongside any new snapshots taken with the new key.

Also, any snapshots that get created during the data transform process (this may take a long time) have to be discarded/deleted as it may contain a mix of data blocks encrypted with both old and new keys.

Best Practices

Maintaining keys for access to older snapshots can be tedious and cumbersome. Therefore, the simplest and safest practice is to delete all old snapshots once the data is transformed with a new key.

This allows for all new snapshots to be readable with the new key while old keys can be discarded, unless used in other security policies.

Chapter 13: Using CTE with Quantum StorNext

This chapter describes how to configure CTE and Quantum StorNext devices to interoperate to allow CTE policies to apply to storage managed by Quantum StorNext. This chapter contains the following sections:

Overview of using CTE with Quantum StorNext	148
CTE and Quantum StorNext Compatibility	148
Setting up CTE and Quantum StorNext Integration	150
Stop secfs Before Upgrading StorNext LAN Clients	152

Overview of using CTE with Quantum StorNext

Quantum StorNext Fibre Channel-connected devices provide shared file access to third party storage for workstation clients and are optimized for simultaneous access to very large files such as video files. The Quantum StorNext file system is known as SNFS or by its older name, CVFS.

You can encrypt and control access to SNFS files with DSM policies by installing CTE Agents on Linux clients that are configured for access to the SNFS file system. Some limitations apply to this integration, such as supported operating systems, supported SNFS features, concurrent read/write access by multiple clients, and GuardPoint settings (see the next section for more information about these limitations).

CTE and Quantum StorNext Compatibility

The following sections list the supported operating systems and CTE settings supported for use with Quantum StorNext file systems. Important unsupported configuration parameters are also listed.

Supported StorNext Server and Client Configurations

The CTE integration with SNFS file systems works only with certain SNFS versions, SNFS storage policies, and client operating systems.

Configuration parameter	Linux
StorNext (SNFS) operating system version	6.x
StorNext metadata controller (MDC) server OS type	Linux MDC supported
StorNext replication policy	Not supported
StorNext deduplication policy	Not supported
StorNext truncation	Supported
StorNext full and partial backup	Supported
StorNext expand filesystem	Supported
StorNext data migration	Supported
StorNext read-ahead cache	Disable for use with CTE
Client operating systems	Red Hat Enterprise Linux (RHEL) 7.x
StorNext LAN client	DLC

Configuration parameter	Linux
StorNext mount method: locally mounted directory	Supported
StorNext mount method: CIFS	Not supported
StorNext mount method: NFS	Not supported

Supported GuardPoint and Key Settings for SNFS File Systems

When configuring CTE GuardPoints and keys for SNFS, keep in the mind the compatibility limitations listed in the following table.

Note

Because AES-CBC-CS1 keys are not supported on Windows, do not create a policy on Linux that uses AES-CBC-CS1 keys if access to the same SNFS GuardPoint is required by both Windows and Linux LAN clients.

Configuration element	Linux
Offline data transformation	Supported
Live Data Transformation (LDT)	Not supported
Key manager compatibility	See the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> or the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> for your CTE version
Guard unstructured data	Supported
Guard structured data	Not supported
GuardPoint type: Directory (including entire SNFS volume)	Supported
GuardPoint type: Raw device	Not supported
GuardPoint type: Block device	Not supported
GuardPoint mount option: manual guard	Supported
GuardPoint mount option: auto guard	Supported
GuardPoint mount option: automount	Not supported
AES-CBC key type	Supported
AES-CBC-CS1 key type	Supported

Supported Concurrent Access Read/Write Scenarios

If you want to allow access by multiple clients (users) to CTE-protected SNFS files under the same GuardPoint, just read-only access is supported. StorNext file locking is not implemented in CTE, so there is currently no way to prevent concurrent conflicting writes to the same file. As a result, Thales does not support write access to the same GuardPoint from multiple clients.

To enable read access to the same GuardPoint from multiple clients, ensure that all clients are configured to use the same policy and key.

Configuration parameter	Linux
Read/write access from a single LAN client to a GuardPoint	Supported
Read/write access from two or more LAN clients to the same GuardPoint	Not supported
Read-only access from one, two, or more LAN clients to the same GuardPoint	Supported

Setting up CTE and Quantum StorNext Integration

For the most part, CTE integration with Quantum StorNext is the same as for any standard file system. The next section provides an overview of the steps involved in making CTE work with SNFS. Later sections provide more information about the steps that are new or differ significantly from a typical CTE setup.

Integration Task Overview

The table below provides an overview of the steps involved in setting up SNFS and CTE to work together. As noted in the table, some of these tasks are described in the documentation for your selected key manager. Some of these steps may need to be performed by other staff members at your organization if you have divided the security administration duties as recommended by Thales and you don't have access to the key manager.

Task	Key configuration notes	For more information
Install and configure a Quantum StorNext MDC server for use with CTE	Disable the StorNext read-ahead cache. Only certain StorNext policies, features, and mount types are supported. See "Supported StorNext Server and Client Configurations" on page 148.	See "Installing and Configuring a Quantum StorNext MDC Server for Use with CTE" on the next page.
Install and configure Quantum StorNext clients for use with CTE	Ensure that SNFS starts before <code>secfs</code> . See "Ensuring that the StorNext SNFS File System Starts Before secfs" on the next page. Only certain operating systems are supported. See "Supported StorNext Server and Client Configurations" on page 148.	See "Installing and configuring Quantum StorNext DLC Clients for Use with CTE" on the next page.
Create a domain for one or more SNFS hosts, or add them to an existing domain	No difference from standard CTE agent configuration.	See "Domain Management" in your key manager documentation.
Add the host to the key manager	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager documentation.
Install and register the CTE Agent on the host system	No difference in installation.	See Chapter 2: "Getting Started with CTE for Linux" on page 22
Create encryption keys (optional)	No difference from standard CTE agent configuration.	See "Managing Keys" in your key manager documentation. For information about AES-CBC-CS1 keys, see Chapter 5: "Enhanced Encryption Mode" on page 70.

Task	Key configuration notes	For more information
Configure host groups containing one or more StorNext LAN clients (optional)	No difference from standard CTE agent configuration.	See “Configuring Hosts and Host Groups” in your key manager documentation.
Configure policies (including user, process, and resource sets) to control access or enable encryption	No difference from standard CTE agent configuration.	See “Configuring Policies” in your key manager documentation.
Configure one or more GuardPoints	Some GuardPoint settings are not supported. See "Supported GuardPoint and Key Settings for SNFS File Systems" on page 149 .	See “Managing GuardPoints” in your key manager documentation

Installing and Configuring a Quantum StorNext MDC Server for Use with CTE

Install and configure a Quantum StorNext metadata controller (MDC) server using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Linux StorNext MDCs. Ensure that you configure the StorNext server to work with the settings supported by CTE as listed in ["Supported StorNext Server and Client Configurations" on page 148](#). For example, you must disable the StorNext read-ahead cache and only certain StorNext policies, features, and mount types are supported.

Installing and configuring Quantum StorNext DLC Clients for Use with CTE

Install and configure Quantum StorNext DLC clients using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Linux StorNext DLCs.

Ensure that you configure DLC clients to work with the settings supported by CTE as listed in ["Supported StorNext Server and Client Configurations" on page 148](#). For example, only certain operating systems are supported.

Note

Just read-only access is supported if multiple StorNext LAN clients will access files in the same GuardPoint. For more information, see ["Supported Concurrent Access Read/Write Scenarios" on page 149](#).

Ensuring that the StorNext SNFS File System Starts Before secfs

For CTE to function properly for Linux SNFS clients, the SNFS service must start before the CTE `secfs` service. Add an entry for the SNFS file system to `/etc/fstab` on each Linux client that has a CTE agent installed on it. Use the following format:

```
/snfs_share /stornext/snfs1 cvfs defaults,diskproxy=client 0 0
```

In this example, `/snfs_share` should be a share that has been exported from the StorNext Server. It should not be a local disk. You may have completed this configuration step as part of the StorNext LAN client installation. See the [Quantum StorNext documentation](#) for more details.

Installing the CTE Agent on Each StorNext LAN client

Install a CTE Agent on each computer that is set up as a StorNext LAN client and for which you want to set policies. For supported operating systems, see the table in ["Supported StorNext Server and Client Configurations" on page 148](#).

Use any installation method supported for your operating system. For details, see [Chapter 2: "Getting Started with CTE for Linux" on page 22](#).

Stop secfs Before Upgrading StorNext LAN Clients

Before you upgrade StorNext Linux LAN clients, disable or stop the CTE `secfs` service. To stop the `secfs` service, follow these steps:

1. Log in as root on the computer that contains the LAN client that you want to upgrade.
2. Type the following command: `/etc/vormetric/secfs stop`

After you upgrade the StorNext client, start `secfs` again by logging in as root and running the `/etc/vormetric/secfs start` command.

Chapter 14: Using CTE with McAfee Endpoint Security for Linux Threat Prevention

McAfee Endpoint Security for Linux Threat Prevention detects malware such as viruses and handles the malware according to policies that you configure in McAfee ePO. This chapter describes how to configure McAfee and CTE to work together.

This chapter contains the following sections:

Supported McAfee Versions and Linux Operating Systems	153
Ensuring Correct McAfee Service Startup Order	153
Updating McAfee	154
Virus Scanning Behavior Differences for CIFS and NFS GuardPoints	154

Supported McAfee Versions and Linux Operating Systems

In general, Thales has verified that CTE is compatible with McAfee version 10.6.5 and later on Red Hat Enterprise Linux (RHEL) 7 and RHEL 8. See the most recent *Compatibility Matrix for CTE Agent with CipherTrust Manager* or *Compatibility Matrix for CTE Agent with Data Security Manager* for details about the versions of McAfee Endpoint Security for Linux Threat Prevention that have been verified to work with CTE. You can find that document on the Thales Support website: <https://supportportal.thalesgroup.com> (login account required).

Ensuring Correct McAfee Service Startup Order

CTE services and McAfee services must be started and stopped in the correct order to prevent problems with your data that is guarded by CTE. This order is important any time these services need to be started or stopped, such as:

- During normal startup and shutdown of your Linux host.
- Before enabling a scheduled upgrade of CTE.
- Before performing a manual upgrade of CTE.
- As needed for maintenance or troubleshooting.

Ensuring Correct McAfee Service Startup Order in systemd

Configuring the proper startup and shutdown order of CTE and McAfee services in `systemd` ensures that the services start in the right order during system startup and shutdown. This is also important if you configure a scheduled upgrade of CTE.

The following McAfee services must be configured to start after CTE services:

- `isecesp.service`
- `isectpd.service`

To configure this behavior, add these services to the `Before=` line in the `secfs-fs-barrier.service` file on your system. The order of these services on the `Before=` line in the `secfs-fs-barrier.service` file does not matter. See "[Location of Application Unit Configuration Files](#)" on page 79 for the location of the `secfs-fs-barrier.service` file on your system. See "[Adding Applications to the secfs-fs-barrier.service File](#)" on page 79 for information about how to add services to the `secfs-fs-barrier.service` file.

Ensuring Correct McAfee Service Startup Order Manually

Perform the following commands in this order if you need to stop McAfee and CTE services manually:

1. Stop McAfee services:

```
# systemctl stop isecesp.service isectpd.service
```

2. Stop CTE:

Linux distributions that support systemd	/etc/vormetric/secfs stop
Linux distributions that do not support systemd	service secfs stop

Perform the following commands in this order if you need to start McAfee and CTE services manually:

1. Start CTE:

Linux distributions that support systemd	/etc/vormetric/secfs start
Linux distributions that do not support systemd	service secfs start

2. Start McAfee services:

```
# systemctl start isecesp.service isectpd.service
```

Updating McAfee

It is not necessary to shut down CTE services when you update McAfee Endpoint Security to a new version. Follow the update procedure described by McAfee. Before updating, ensure that the new version of McAfee is compatible with CTE as described in ["Supported McAfee Versions and Linux Operating Systems" on the previous page](#).

Virus Scanning Behavior Differences for CIFS and NFS GuardPoints

By default on McAfee Endpoint Security, on-access virus scanning for remotely mounted file systems such as CIFS and NFS is disabled. However, for GuardPoints configured on CIFS and NFS volumes, this default is ignored. So on-access virus scanning is always on for GuardPoints configured on CIFS and NFS volumes. This means that if a process attempts to save an infected file to a GuardPoint configured on a CIFS or NFS volume, the infected file will be discovered immediately if it matches the McAfee malware detection algorithm and handled according to the appropriate malware policy in McAfee ePO.

Chapter 15: Using CTE with Trend Micro Deep Security Software

Trend Micro's Deep Security software provides comprehensive security in a single solution that is purpose-built for virtual, cloud, and container environments. Thales has verified certain versions of this Trend Deep product for compatibility with CTE on Red Hat Enterprise Linux (RHEL) 7 and RHEL 8.

This chapter contains the following sections:

Supported Deep Security Versions and Linux Operating Systems	155
Ensuring Correct Deep Security Service Startup Order	155
Updating Deep Security	156

Supported Deep Security Versions and Linux Operating Systems

CTE and Deep Security can be used with RHEL 7 and RHEL 8. See the most recent *Compatibility Matrix for CTE Agent with CipherTrust Manager* or *Compatibility Matrix for CTE Agent with Data Security Manager* for the current versions of Trend Micro Deep Security that have been verified to work with CTE. You can find that document on the Thales support website <https://supportportal.thalesgroup.com> (login account required).

Ensuring Correct Deep Security Service Startup Order

CTE services and Deep Security services must be started and stopped in the correct order to prevent problems with your data that is guarded by CTE. This order is important any time these services need to be started or stopped, such as:

- During normal startup and shutdown of your Linux host.
- Before enabling a scheduled upgrade of CTE.
- Before performing a manual upgrade of CTE.
- As needed for maintenance or troubleshooting.

Ensuring Correct Deep Security Service Startup Order in systemd

Configuring the proper startup and shutdown order of CTE and Trend Micro's Deep Security services in `systemd` ensures that the services start in the right order during system startup and shutdown. This is also important if you configure a scheduled upgrade of CTE.

The following Deep Security service must be configured to start after CTE services:

```
ds_agent.service
```

To configure this behavior, add this service to the `Before=` line in the `secfs-fs-barrier.service` file on your system. The order of these services on the `Before=` line in the `secfs-fs-barrier.service` file does not matter. See "[Location of Application Unit Configuration Files](#)" on page 79 for the location of the `secfs-fs-barrier.service` file on your system. See "[Adding Applications to the secfs-fs-barrier.service File](#)" on page 79 for information about how to add services to the `secfs-fs-barrier.service` file.

Ensuring Correct Deep Security Service Startup Order Manually

Perform the following commands in this order if you need to stop Deep Security and CTE services manually:

1. Stop Deep Security services:

```
# systemctl stop ds_agent.service
```

2. Stop CTE:

Linux distributions that support systemd	/etc/vormetric/secfs stop
Linux distributions that do not support systemd	service secfs stop

Perform the following commands in this order if you need to start Deep Security and CTE services manually:

1. Start CTE:

Linux distributions that support systemd	/etc/vormetric/secfs start
Linux distributions that do not support systemd	service secfs start

2. Start Deep Security services:

```
# systemctl start ds_agent.service
```

Updating Deep Security

It is not necessary to shut down CTE services when you update Trend Micro Deep Security to a new version. Follow the update procedure described by Trend Micro. Before updating, ensure that the new version of Deep Security is compatible with CTE as described in ["Supported Deep Security Versions and Linux Operating Systems" on the previous page](#).

Chapter 16: CTE COS for Amazon S3

This chapter discusses how to configure CTE COS for Amazon S3 buckets. It contains the following sections:

Overview	157
System and Software Requirements	159
Client Software Requirements	159
CTE COS S3 Installation Overview	159
Install Required Linux Packages	160
Install CTE	160
Configure the AWS CLI to use the COS Root CA Certificate	161
Configure the AWS CLI Network Proxy	161
Configure CTE COS S3	162
Optionally Configure a CTE COS S3 Role for Guarded Buckets	163
Guard an AWS Bucket	167
Additional COS Proxy Root CA Certificate Information	170
Protecting Python Programs with CTE	172

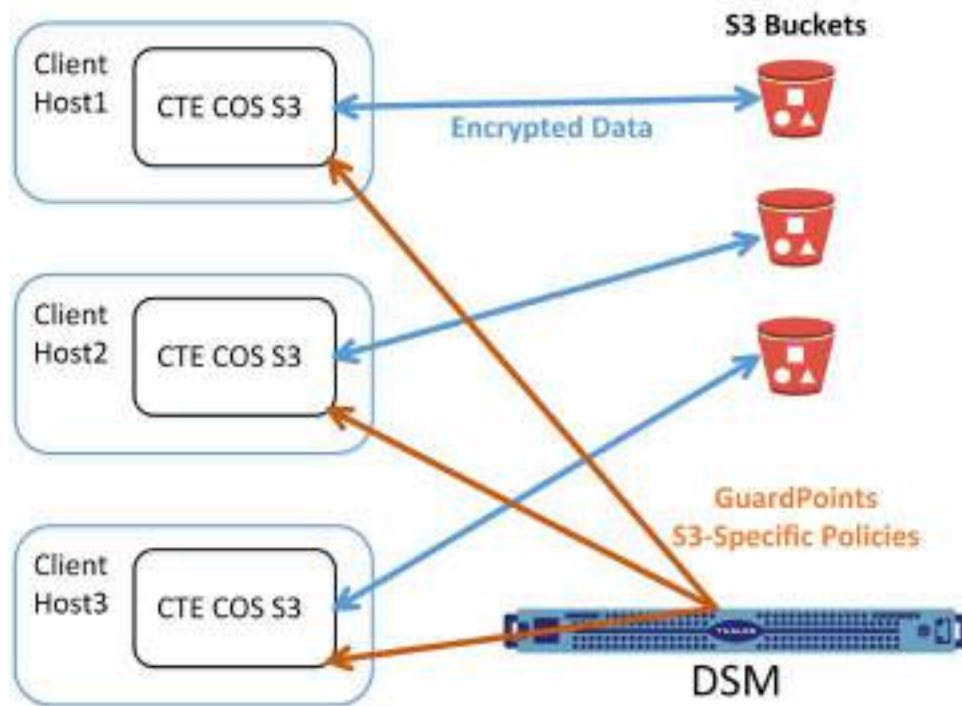
Overview

CipherTrust Transparent Encryption for Cloud Object Storage (CTE COS) is an object storage service that you can use to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. CTE COS provides management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements.

CTE COS for Amazon Simple Storage Service (CTE COS S3) is an extension to CTE for inline encryption and local host access controls involving applications performing REST-API-based operations to S3 object stores.

CTE COS S3 is not a replacement for AWS IAM access controls which are enforced independently at the AWS server end.

The following diagram shows the high-level CTE COS S3 architecture:



Supported operations

- CTE COS S3 will process only AWS S3 REST https calls issued by applications. The interception is done by a bundled TLS proxy with additional CTE services.
- CTE's traditional access controls and inline encryption are transparently applied during the following operations:
 - Create a bucket
 - Write an object
 - Read an object
 - Delete an object
 - List objects

Limitations

- CTE COS S3 is supported only on RHEL 7.
- Only REST API based S3 protocol-aware applications are supported.
- Only locally generated self-signed COS Proxy CA Certificates are supported.
- AWS S3 URL path validations are not currently implemented. CTE COS S3 requires that the user must specify the correct URLs for bucket paths.
- CTE COS S3 permits only AES CBC-CS1 encryption. Encrypted files in protected buckets therefore will prepend the 4K embedded header used in CTE's AES CBC-CS1 encryption. The DSM will enforce usage of AES CBC-CS1 keys within S3 bucket policies.

Multi-part Upload Restrictions

- All upload operations for a multi-part upload must be conducted from the same host.
- Maximum file size upload is 5TB.
- Part sizes during uploads must be identical. The part numbering must be in sequence starting with 1, e.g. 1,2,3,4,... Not 10, 20, 30, etc.
- The part size specified in CTE S3's AWS credential file must match the part size specified within the application.
- Thales recommends that the Content-MD5 header be included in the request message.

System and Software Requirements

- The RHEL 7 Linux host must meet the standard CTE requirements.
- You must have an AWS account
- We recommend that you guard the bucket by restricting it with a CTE COS S3 Role to prevent accidental data corruption from connections outside the control of CTE COS S3. For details, see ["Optionally Configure a CTE COS S3 Role for Guarded Buckets" on page 163](#).
- You must download and install the pre-requisite rpm packages before you install CTE COS S3. For details, see ["Install Required Linux Packages" on the next page](#).
- The CTE Agent must be installed in the default directory on the host. You cannot change the default path if you also enable CTE COS S3.

Client Software Requirements

- Clients must exist on the same host as CTE COS S3. External Client connections will be rejected by the COS Proxy.
- Clients must be AWS S3 protocol aware, and can directly connect to a S3 bucket without the use of an intermediary service, such as the AWS S3 Management Console website.
- Clients must be configured to divert outgoing network connection to a COS proxy (default is localhost:3128 or 127.0.0.1:3128). For more information, see ["Configure the AWS CLI Network Proxy" on page 161](#).
- Clients must use the TLS 1.2 / TLS 1.3 network encryption protocol over TCP/IP to establish connections to the COS proxy.
- Clients must be configured to use the COS CA Root Certificate of the COS proxy to verify and authenticate TLS connections. For more information, see ["Configure the AWS CLI to use the COS Root CA Certificate" on page 161](#).

CTE COS S3 Installation Overview

In order to configure CTE COS S3, you must complete the following tasks.

Note

The AWS CLI is used as a sample application to explain the detailed installation procedure.

1. Install the required packages for CTE COS S3. For details, see ["Install Required Linux Packages" on the next page](#).
2. Install CTE and generate the local COS Proxy CA Certificate. For details, see ["Install CTE" on the next page](#).

3. Configure the client to use the COS Proxy CA Certificate. For details, see ["Configure the AWS CLI to use the COS Root CA Certificate" on the facing page](#).
4. Configure the client to use the COS proxy port. For details, see ["Configure the AWS CLI Network Proxy" on the facing page](#).
5. Configure CTE COS S3 with AWS Credentials. For details, see ["Configure CTE COS S3" on page 162](#).
6. Optionally configure Role & IAM policies for CTE COS S3 for guarded buckets. For details, see ["Optionally Configure a CTE COS S3 Role for Guarded Buckets" on page 163](#).
7. Configure the guarded buckets. For details, see ["Guard an AWS Bucket" on page 167](#).

Install Required Linux Packages

CTE COS S3 requires the following pre-requisite packages:

- `boost-regex`.
- `boost-system`.
- `boost-thread`.
- `lib-curl`.
- `libtool-ltdl`.
- `libxml2`.
- `epel-release`.
- `cryptopp`. This package must be installed *after* `epel-release`.
- `log4cpp`. This package must be installed *after* `epel-release`.

For example:

```
$ sudo yum install boost-regex boost-system boost-thread libcurl libtool-ltdl libxml2 epel-release
$ sudo yum install cryptopp log4cpp
```

CTE COS S3 supports both Python2 and Python3. If both versions of Python are available, CTE COS S3 will use Python3. For either Python package, you also need to install the Python modules `"boto3"` and `"future"` after you install the main python package.

- Example for Python2:

```
$ sudo yum install python-pip
$ sudo pip install boto3 future
```

- Example for Python3:

```
$ sudo yum install python3 python3-pip
$ sudo pip3 install boto3 future
```

Install CTE

When you install CTE COS S3 for use with S3, use the instructions in the *CTE Agent for Linux Quick Start Guide*. In addition to those instructions, answer the following prompts as described in this section.

1. If you are using Fingerprint registration, make sure you know the fingerprint for this agent on the host. This Fingerprint can be seen in the Host Information shown in the DSM Management Console.
2. When the installer asks about Cloud Object Storage, type **Y** and follow the prompts as shown.

Do not change the default CTE installation directory. CTE must be installed in the default location if you enable Cloud Object Storage.

Do you want this host to have Cloud support enabled on the server? (Y/N) [N]: **Y**

CTE COS CA Cert is located in /opt/vormetric/DataSecurityExpert/agent/squid/etc/cosCA.crt
Clients must be updated to use the new CA Certificate

Generating certificate signing request for the kernel component...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done. Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.

The following is the fingerprint of the EC CA certificate. Please verify that it matches the fingerprint shown on the Dashboard page of the Management Console.
If they do not match, it can indicate an unsuccessful setup or an attack.
B0:93:C7:67:07:C9:CB:09:E2:21:F1:5C:8A:C8:79:8F:03:86:21:F2
Do the fingerprints match? (Y/N) [N]: **Y**

Successfully registered the CipherTrust Encryption Expert File System Agent with the primary CipherTrust Data Security Server on security.manager.example.com.
Starting CTE Cloud Service
Installation success.

Configure the AWS CLI to use the COS Root CA Certificate

You must configure the AWS CLI to use the COS root CA certificate. To do so, edit `~/.aws/config` and add the following line to the AWS cli configuration file:

```
ca_bundle = /opt/vormetric/DataSecurityExpert/agent/squid/etc/cosCA.crt
```

For example:

```
$ cat ~/.aws/config
[default]
output = json
Region = us-west-1
ca_bundle = /opt/vormetric/DataSecurityExpert/agent/squid/etc/cosCA.crt
```

Configure the AWS CLI Network Proxy

All communications between client applications and the AWS server must be done through the COS proxy and the environment variable `HTTPS_PROXY` or `https_proxy` should be set. If both variables are defined, then the AWS CLI will use `https_proxy`.

For example:

```
Export HTTPS_PROXY=localhost:3128
```

Configure CTE COS S3

In order for CTE COS S3 to do transparent encryption and decryption, all requests sent to the AWS S3 server must be generated and signed using valid AWS credentials. In order to retrieve these credentials for CTE COS S3, you can use any of the following methods:

- **The User Supplies the Credentials for the User's AWS Account**

The application can send the long-term credentials from the user's AWS account to CTE COS S3. These credentials do not expire.

For the AWS CLI, the credentials are in the credential file `~/.aws/credential`. The user credentials consists of an Access Key ID and a Secret Access Key. For details about accessing the user's credentials, see your AWS documentation.

To add the AWS credentials to CTE COS S3, use the `voradmin cos s3 cred add` command:

```
voradmin cos s3 cred add [<aws_key_id> <aws_secret_key>] where:
```

- `<aws_key_id>` is the AWS secret key ID from the `.aws/credentials` file.
- `<aws_secret_key>` is the AWS secret key from the same file.

For example:

```
voradmin cos s3 cred add AKIA****P KQSm****D
```

- **The User Supplies Temporary Security Credentials**

You can use temporary security credentials, which expire after a short period of time. Usually temporary security credential are obtained through IAM roles and other features of the AWS Security Token Service.

Use the `voradmin cos s3 cred add` command, described above, to add the temporary credential to CTE COS S3.

- **CTE COS S3 Captures Temporary Credentials**

CTE COS S3 can capture a temporary, newly generated, security credential and automatically add it to CTE COS S3 if the application generates the temporary security credential using the AWS Security Token Service with one of the following 3 actions *and* `HTTPS_PROXY` is set to `localhost:3128`.

- `AssumeRole`
- `AssumeRoleWithSAML`
- `AssumeRoleWithWebIdentity`

No other action is required from the application or user.

- **CTE COS S3 Retrieves Credentials from EC2 Instance Metadata Service**

When CTE COS S3 is installed on AWS EC2 instance with an attached role, CTE COS S3 automatically retrieves the credential from Instance Metadata Service and uses it. However, if CTE COS S3 already has a valid credential given by the user or admin using the `voradmin` command, then that credential will be used instead. For information about setting up an IAM Role, see your AWS EC2 documentation.

No action is required from application or user.

Setting the Default Chunk Size

Note

If a chunk size is configured in the AWS CLI configuration, you must configure the same chunk size for CTE COS S3.

The default chunk size for multi-part uploads is 8 MB. To change the chunk size, use the following command:

```
voradmin cos s3 chunk [<aws_key_id> <aws_secret_key>] [<chunk_size>] where:
```

- <aws_key_id> is the AWS secret key ID from the `.aws/credentials` file.
- <aws_secret_key> is the AWS secret key from the same file.
- <chunk_size> is the number of MB per chunk that you want to use for multi-part uploads. Enter an integer between 5 and 5120.

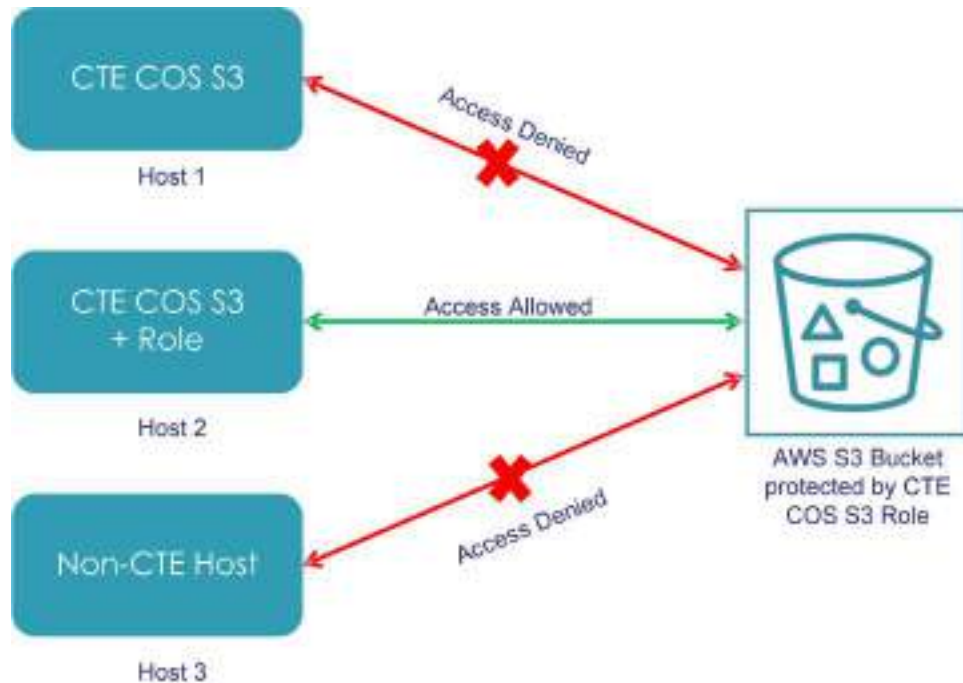
The `voradmin` command prompts for any of the optional parameters that you do not specify on the command.

For example, to set a chunk size of 250MB, you would enter:

```
voradmin cos s3 chunk AKIA****P KQSm****D 250
```

Optionally Configure a CTE COS S3 Role for Guarded Buckets

AWS provides the IAM Role feature that contains certain specific permissions. A user can assume the IAM Role and therefore take on those permissions. CTE COS S3 provides a special feature using this IAM Role to prevent access to one or more buckets outside the CTE COS S3 protection as shown in the following diagram:



Only hosts that are configured with the CTE COS S3 Role can access the protected buckets. All other access attempts from any hosts where the CTE COS S3 Role is not configured, including attempts made through the AWS S3 Console, are blocked for the protected buckets.

This is a one-time configuration process. After the CTE COS S3 Role is configured on a host by the system or security administrator, all authorized users in the host can access the protected buckets.

Prerequisites

To set up a CTE COS S3 Role, you need a delegated IAM user, role, and policy. The delegated IAM user should be created by the AWS Administrator without any specific privileges. The role and policy must be created by a user who has at least the following privileges:

- `iam:ListPolicies`
- `iam:CreatePolicy`
- `iam:GetPolicyVersion`
- `iam:ListRoles`
- `iam:ListRolePolicies`
- `iam:ListAttachedRolePolicies`
- `iam:AttachRolePolicy`
- `iam:UpdateAssumeRolePolicy`
- `iam:CreateRole`
- `iam:GetRole`

Procedure

1. In the IAM Management Console, create a policy that allows access to specific S3 resources. You can leave the policy open to include all S3 resources in the account or include only those buckets that require CTE protection. Make sure you name the policy something that you will remember.

Tip: You can also create the policy as an inline policy after you create the CTE COS S3 Role later in this procedure.

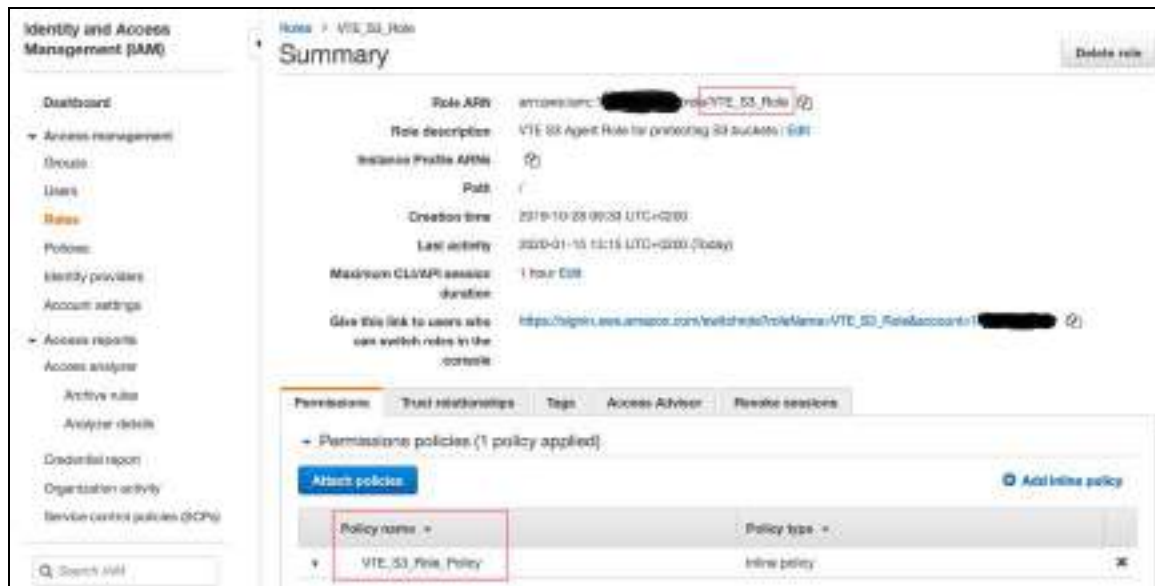
For example, you can create a policy called `VTE_S3_Role_Policy` that allows access to the single S3 bucket `vte-cos-s3-rtb`. To verify that the policy restricts access to that bucket, you can look at the Resource allocation in the Policy summary.

The full JSON for the `VTE_S3_Role_Policy` is:

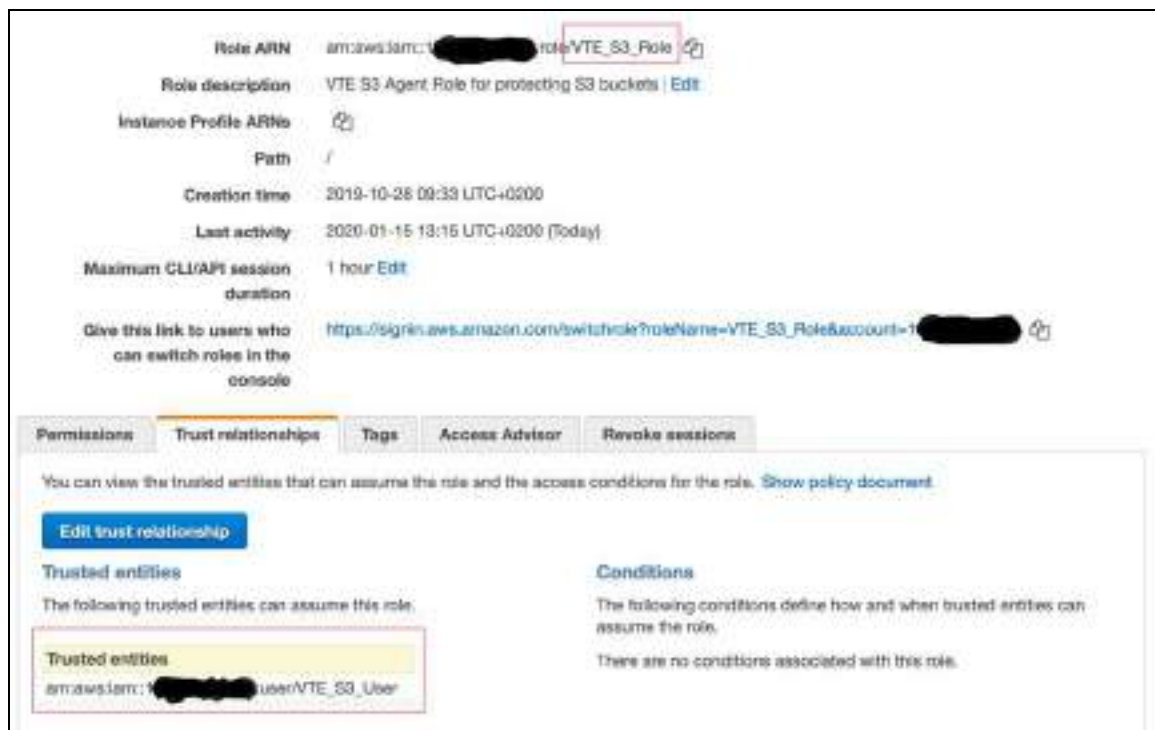
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3::vte-cos-s3-rtb",
        "arn:aws:s3::vte-cos-s3-rtb/*"
      ]
    }
  ]
}
```

2. Create a new role that you can use for the CTE COS S3 Role. For example, you could call the role `VTE_S3_Role`.

3. Assign the CTE COS S3 policy you created to the role, or click **Add inline policy** to create a new policy. For example:



4. Create a delegated IAM user for the CTE COS S3 Role. The user does not require any privileges because its only job is to assume the CTE COS S3 Role. The delegated IAM user can either be in the same account as the role or it can be in a different trusted account. For example, you could create a user called VTE_S3_User with no privileges.
5. Set "Trusted Entities" to the delegated IAM user on the **Trust relationships** tab. For example:



6. Configure the CTE COS S3 Role with the credentials of the delegated IAM user you created earlier by entering the following command in the command line on the host system:

```
voradmin cos s3 role config [<aws_key_id> <aws_secret_key> <user_arn> <role_arn>] where:
```

- <aws_key_id> is the AWS secret key ID for the delegated IAM user that you created.
- <aws_secret_key> is the AWS secret key or the delegated IAM user that you created.
- <user_arn> is the Amazon Resource Name for the delegated IAM user that you created.
- <role_arn> is the Amazon Resource Name for the delegated IAM Role that you created.

If you omit any of the optional parameters, the `voradmin` command prompts you for that information.

For example, if the AWS account number for the delegated IAM user is 1XXXXXXXXXXXX, the user name is VTE_S3_User, and the CTE COS S3 Role is VTE_S3_Role, you would enter:

```
voradmin cos s3 role config AKIA****P KQSm****D arn:aws:iam::1XXXXXXXXXXXX:user/VTE_S3_User  
arn:aws:iam::1XXXXXXXXXXXX:role/VTE_S3_Role
```

After you configure the user and assign the CTE COS S3 Role, CTE will access the S3 bucket through the delegated IAM user account using temporary credentials that CTE regenerates periodically. These credentials are maintained entirely by CTE and are never exposed to end users.

Secure an S3 Bucket with the CTE COS S3 Role

When you enable the CTE COS S3 Role for a bucket, the associated bucket policy prevents unauthorized users from accessing the contents of the bucket. To enable the CTE COS S3 Role for a bucket, use the following command:

```
voradmin cos s3 role secure-bucket <key_id> <secret key> <bucket_name> where:
```

- <aws_key_id> is the AWS secret key ID for the delegated IAM user that you created.
- <aws_secret_key> is the AWS secret key for the delegated IAM user that you created.
- <bucket_name> is the name of the S3 bucket on which you want to enable the CTE COS S3 Role.

For example, if the bucket name is `vte-cos-s3-rtb`, you would enter:

```
voradmin cos s3 role secure-bucket AKIA****P KQSm****D vte-cos-s3-rtb
```

Disable the CTE COS S3 Role for an S3 Bucket

To remove the CTE COS S3 Role restrictions associated with a bucket, use the following command:

```
voradmin cos s3 role release-bucket <key_id> <secret key> <bucket_name> where:
```

- <aws_key_id> is the AWS secret key ID for the delegated IAM user that you created.
- <aws_secret_key> is the AWS secret key for the delegated IAM user that you created.
- <bucket_name> is the name of the S3 bucket on which you want to disable the CTE COS S3 Role.

For example, if the bucket name is `vte-cos-s3-rtb`, you would enter:

```
voradmin cos s3 role release-bucket AKIA****P KQSm****D vte-cos-s3-rtb
```

Guard an AWS Bucket

To Guard an AWS bucket, you must:

1. Create a CBC_CS1 key.
 - For DSM, see ["Create a CBC_CS1 Key in DSM" below](#)
 - For CM, see "Creating a New Key" in the CTE Administrator Guide
2. Create a Cloud Object Storage (COS) policy.
 - For DSM, see ["Create the Cloud Object Storage \(COS\) policy in DSM" on the next page](#)
 - For CM, see "Creating Policies" in the CTE Administrator Guide
3. Apply the policy to the host.
 - For DSM, see ["Creating GuardPoints in a Host" on page 169](#)
 - For CM, see "Managing GuardPoints" in the CTE Administrator Guide

Create a CBC_CS1 Key in DSM

1. Log on to the Management Console as an administrator of type: All or Security Administrator with Key role permissions.
2. In the menu bar select **Keys > Agent Keys > Keys**.
The Agent Keys page displays.
3. Click **Add**. The Add Agent Key window opens.
4. Select the Symmetric tab.

5. Complete the fields in this window by using the following information.

Name: Provide a name for the key.

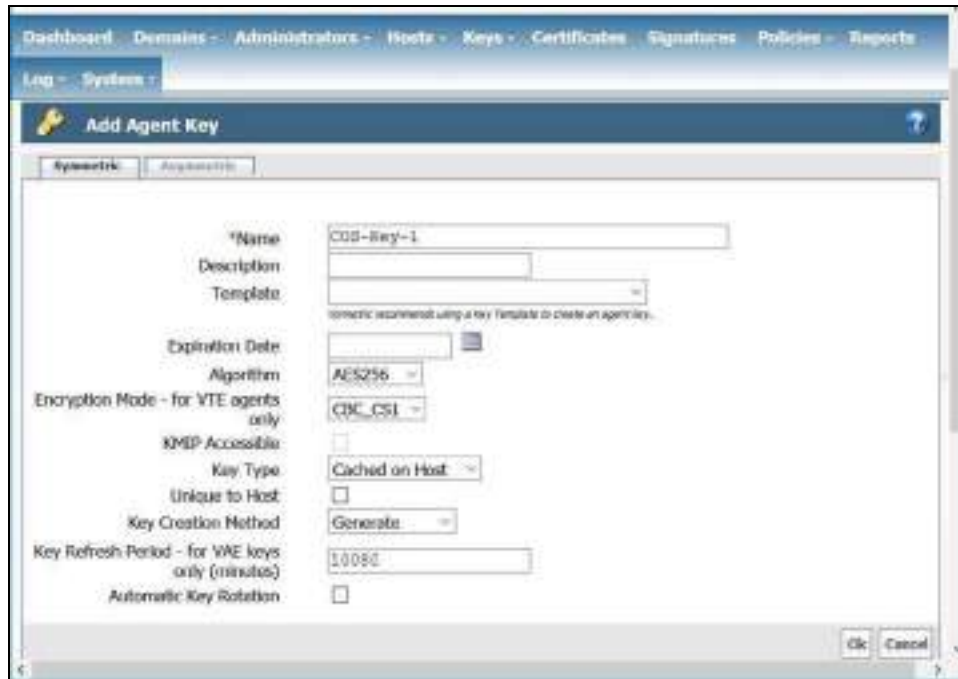
Algorithm: Select **AES256**.

Encryption Mode for CTE agents only: DSM allows only CBC-CS1 encryption mode for COS policy type.

Key Type: Cached on Host

Key Creation Method: Generate

For example:



6. Click OK.

Create the Cloud Object Storage (COS) policy in DSM

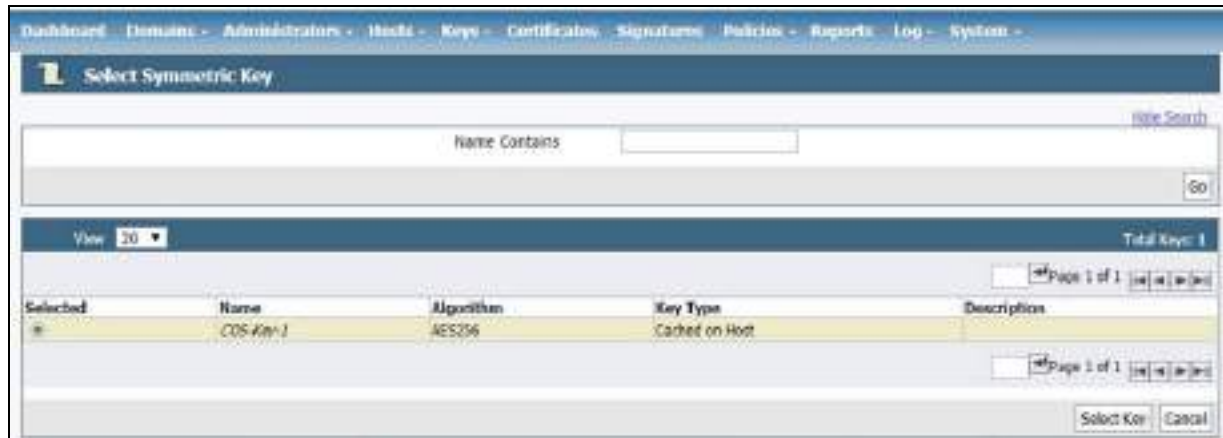
Creating a COS policy differs from creating standard policies. Some notes about COS policies:

- Allow Browsing is not supported for Cloud Object Storage policies.
- Policies for Cloud Object Storage do not contain a resource set. The resource set is automatically the cloud object storage.
- Policies for Cloud Object Storage do not contain a When/Time set.
- Key Rules for Cloud Object Storage policies only contain one Key.
- Policies for Cloud Object Storage do not support Exclusion rules.

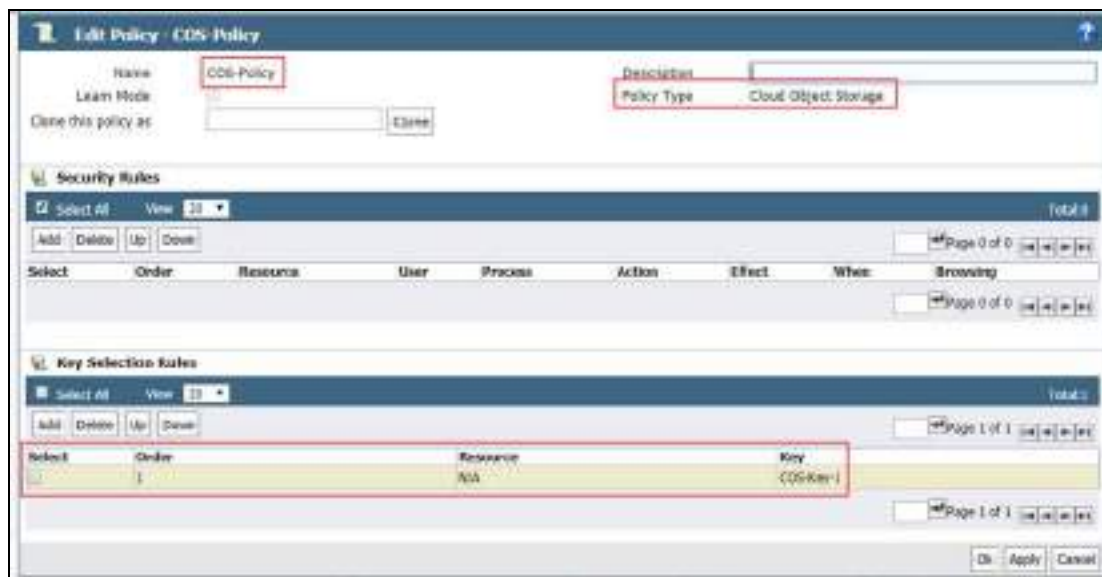
To create the policy:

1. Click **Policies > Manage Policies** to list the policies available to this domain.
2. Click **Add**. The **Add Policy** page appears.
3. For **Policy Type**, select **Cloud Object Storage**.
4. In the **Name** field, enter a name for the policy. For example
5. In the **Key Selection Rules** section, click **Add**. The Add Key Rule page appears.

- Click **Select** and choose the CBC_CS1 key you created in ["Create a CBC_CS1 Key in DSM"](#) on page 167.



- Click **Select Key**, then click **OK** to confirm that you want to use the CBC_CS1 key.
- Click **OK** to save the Policy with the CBC_CS1 key rule.



Creating GuardPoints in a Host

Security/All administrators can create new GuardPoints or edit existing host GuardPoints.

Note

DSM allows **exactly one** COS GuardPoint per S3 bucket.

The following features are NOT supported in COS GuardPoints:

- Existing data transformation, either offline or with Live Data Transformation (LDT). If you want to encrypt existing data, you must move it out of the S3 bucket, guard the bucket, then move the existing data back into the guarded bucket. When the data is moved back into the S3 bucket, it will be encrypted by CTE before it becomes accessible to users.
- Secure Start
- Host to Browse

- Auto Mount
- Efficient Storage
- Buckets inside a container or Docker
- Browsing to a bucket to be guarded

Note

In the Edit Host window, you will see that the **GuardPoints** tab has been renamed to **GuardPoints**.

To create a COS GuardPoint:

1. In the Hosts window, click on the host for which you want to set GuardPoints.
2. In the Edit Host window, click **GuardPoints**.
3. In the GuardPoints tab, click **Guard**.
4. In the Policy dropdown menu, select an appropriate policy.
5. For type, click Cloud Object Storage (Auto Guard or Manual Guard).
6. In the Path field, enter the path for the GuardPoint.
7. Click **OK**. COS GuardPoints display on the GuardPoints tab of the Host Detail page.

Additional COS Proxy Root CA Certificate Information

The CTE COS CA Certificate, not to be confused with the Kernel and VMD Kernel Certificates, is used with the COS internal Proxy Certificate Authority and must be used by Clients to validate Certificates received during their TLS connection handshake. The default COS CA Self-Signed root CA is automatically created using a locally generated Public/Private Key with the following parameters:

- `CERT_FIELD_PARAM="/C=OZ/ST=Munchkin-land/L=Emerald City/O=ACME Inc/OU=ACME Deliveries/CN=localhost"`
- `SUBJECT_ALT_NAME_PARAM="DNS.1:localhost,IP.1:127.0.0.1"`

To view the currently installed Certificate for the COS Proxy CA, use the `voradmin cos ca_cert display` command.

In the context of the internal COS Proxy CA, the FQDN of 'localhost' would be the correct value, as well as the loop-back IP address of 127.0.0.1 This results in the following locally generated Root CA Certificate.

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
2a:28:2c:c5:d6:3b:05:11:fe:6e:32:1d:aa:35:29:44:e5:0d:ce:bf
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=OZ, ST=Munchkin-land, L=Emerald City, O=ACME Inc, OU=ACME Deliveries, CN=localhost
Validity
Not Before: Feb 11 18:19:33 2020 GMT
Not After : Feb 10 18:19:33 2021 GMT
Subject: C=OZ, ST=Munchkin-land, L=Emerald City, O=ACME Inc, OU=ACME Deliveries, CN=localhost
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:b9:e6:60:c9:00:f8:00:83:b7:1b:ff:b2:31:eb:
66:5a:eb:21:87:1c:aa:3d:71:b8:08:42:4d:82:6c:
9a:5c:c7:d0:ad:ec:11:9b:be:80:15:55:ab:bc:38:
11:9c:80:c4:1e:63:31:ae:b7:33:8f:88:0b:c2:ca:
e9:e8:0d:78:5a:19:e3:d9:45:fd:4c:b4:81:24:ea:
d3:d4:b9:d2:14:07:e0:33:df:b9:75:36:57:16:4d:
6e:ee:bf:5f:1d:13:14:10:d1:ba:29:0e:1e:11:38:
84:78:8a:e8:ed:1a:24:f7:6a:ac:87:66:9b:21:23:
7b:2c:44:b3:33:6c:04:b7:aa:8c:d3:64:d2:5e:b6:
56:b5:46:54:a9:37:06:c8:e5:30:5f:2a:ba:78:00:
4a:2f:f1:66:a0:1f:fd:26:05:8d:e0:da:23:1e:1b:
1e:a8:ee:77:73:76:32:3c:5e:01:aa:0f:d5:8b:ac:
a9:08:7e:50:63:5e:88:95:e5:5f:dc:1d:7b:b0:59:
50:c1:56:ba:e6:11:da:c6:c5:79:3e:a6:46:f2:39:
db:6a:9d:aa:da:ff:68:d0:39:9c:fd:5a:d5:0e:3e:
41:07:62:32:c0:be:4f:92:56:34:92:c8:1d:bd:87:
ec:e5:3b:44:a0:8f:8c:09:f9:37:40:df:b3:24:bb:
8d:67
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Key Usage:
Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
C5:19:E5:41:B7:69:E7:10:27:2D:F6:49:0D:46:0A:4B:FE:8C:7E:CB
X509v3 Authority Key Identifier:
keyid:C5:19:E5:41:B7:69:E7:10:27:2D:F6:49:0D:46:0A:4B:FE:8C:7E:CB
X509v3 Subject Alternative Name:
DNS:localhost, IP Address:127.0.0.1
X509v3 Issuer Alternative Name:
DNS:localhost, IP Address:127.0.0.1
Signature Algorithm: sha256WithRSAEncryption
2d:3c:2b:93:c0:61:1d:35:d7:f2:5f:5c:e8:0d:61:57:f2:a8:
e0:ec:98:74:02:b5:c4:78:a4:2f:b5:2b:b4:96:56:17:93:89:
eb:45:ac:df:1e:1b:e0:d5:38:da:55:62:61:97:5b:d9:9e:31:
9b:71:f1:17:37:31:5d:12:0f:5e:c1:ea:29:ee:b2:97:6e:7c:
c0:97:a9:8d:a9:2c:c0:68:e4:fa:b1:21:f8:50:b8:c0:2e:51:
fd:f2:5b:4d:41:72:0c:48:a2:db:47:14:66:20:c7:62:bd:33:
e8:a4:f4:22:c9:07:0f:0d:58:a0:9e:a1:f9:96:9c:97:c1:28:
6a:18:6f:ea:b9:28:42:48:5a:5c:da:98:22:9f:05:59:27:82:
3f:3d:4e:0b:9d:37:04:76:0e:ec:d9:f1:25:c8:78:78:fc:31:
```

```
d0:cb:24:db:47:96:7c:fa:dc:0d:14:6c:13:44:8d:87:5b:82:
d2:0f:a9:8c:48:bd:a6:b1:b9:0c:bb:50:14:70:d0:8b:7b:8c:
a5:e5:52:83:47:25:15:d6:d0:17:e0:9f:f7:99:d0:2e:17:93:
c5:38:e0:b8:c8:d4:f2:ed:39:99:ec:19:cf:5e:39:78:7b:5f:
07:48:4b:df:ec:d9:94:c5:aa:df:4d:a9:a5:a9:e3:88:74:0e:
d7:74:83:87
```

If you want to change the defaults, you can use the silent install option with the `CERT_FIELD_PARAM` and `SUBJECT_ALT_NAME_PARAM` set to the desired values, or you can replace the default Certificate using the `voradmin cos ca_cert` command. For more details, see the `voradmin` manpage.

Protecting Python Programs with CTE

CTE uses SHA-256 to generate binary signatures that can be used to allow certain trust levels for a customer application. Capturing the signature of a binary allows CTE to determine if the application's binary has changed in any way, because those changes might mean the security of the binary has been compromised.

While this mechanism works well for executable binaries to verify an application's validity at run time, this mechanism does *not* work for applications implemented with interpreter languages because CTE can only access the interpreter's signature to validate the file. The program itself is something that is executed by the interpreter and thus CTE cannot hook into this process. Scripting languages like Python are particularly difficult because many Python programs include other Python files, which means there is no single program signature that defines the execution path.

While CTE cannot use signature sets to protect traditional Python programs, tools like PyInstaller allow for the creation of a self-contained Python executable that CTE can sign and protect.

Benefits of Using PyInstaller with CTE

Using PyInstaller allows the creation of self-contained Python binary packages. These packages contain the Python interpreter, the Python program, and all required modules and libraries. Because each package includes all of the files it needs, it is immune to changes to the Python modules or libraries on the system. This not only allows CTE to sign the binary but it also adds extra protection against an attacker trying to gain access through modifications of the underlying libraries.

Another benefit is that it provides security administrators with a stable process that reasonably immune to system updates done by a system administrator. Once the application binary has been created and signed, the behavior of the program will not change because of updates made through the OS packaging system or Python's PIP package manager.

Getting PyInstaller

PyInstaller is an OpenSource project. The instruction for installing PyInstaller as well as the documentation are available through the project page at:

<https://PyInstaller.readthedocs.io>

Example Usage

The exact usage of PyInstaller arguments varies based on the details of the Python program being packaged into an executable. This example show what is needed to generate a self-contained AWS CLI binary with PyInstaller. It uses the `--onefile` flag to generate a single, self-contained binary. It assumes that the `pip3` Python package manager is already installed on the system.

Installing PyInstaller

The following command installs PyInstaller in `${HOME}/.local/bin/PyInstaller`:

```
# pip3 install --user PyInstaller
```

Installing the Amazon AWS Command Line Utility

The following command installs the AWS utility in `${HOME}/.local/bin/aws`:

```
# pip3 install --user awscli
```

Creating a Runtime Hook

The following command creates a runtime hook that changes the Python `botocore` root directory within the packaged binary. This is necessary to make sure that we use the `botocore` packaged by PyInstaller. The hook is save to a file named `change-botocore-root.py`. For more information on runtime hooks, see the PyInstaller documentation.

```
# cat <<EOF > ${HOME}/change-botocore-root.py
import sys
import botocore

if getattr(sys, 'frozen', False):
    botocore.BOTOCORE_ROOT = sys._MEIPASS
EOF
```

In order to get the AWS CLI utility working with PyInstaller, we need to specify some hidden imports as well as add some folders from the `awscli` and `botocore` packages into the executable. For more information about hidden imports and adding files to the executable, see the PyInstaller documentation.

```
# ${HOME}/.local/bin/PyInstaller --onefile \
  --hiddenimport=awscli.handlers \
  --hiddenimport=pipes \
  --add-data=${HOME}/.local/lib/python3.6/site-packages/awscli/data:data \
  --add-data=${HOME}/.local/lib/python3.6/site-packages/botocore/data:data \
  --runtime-hook=${HOME}/change-botocore-root.py \
  ${HOME}/.local/bin/aws
```

The resulting binary will be saved in the current working directory as `dist/aws`.

Chapter 17: CTE-Efficient Storage for Linux

Storage arrays offer features such as compression and deduplication for storage efficiency. They also provide simplistic encryption that fails to deliver the requisite levels of security. CipherTrust Transparent Encryption (CTE) offers a much higher level of security. However, in deployments where storage arrays receive encrypted data streams from hosts protected by a CTE instance (protected hosts), the encrypted data streams make the efficiency of storage array systems ineffective. This is because every block written by CTE is different resulting in zero deduplication and compression on these blocks.

CTE offers CTE-Efficient Storage as the solution to the storage efficiency challenge in storage arrays on Linux.

Note

Currently, this feature is only supported on the DSM. Support for this feature will be added to CipherTrust Manager in a future release.

This chapter contains the following sections:

Introduction to CTE-Efficient Storage	174
Guarding an Efficient Storage Device on Linux	180
Guarding a CTE-Efficient Storage Device with Multiple IO Paths on Linux	189
Linux System and ES GuardPoint Administration	189
Changing the Encryption Key on Linux ESG Devices	192
Resizing Guarded Efficient Storage Devices	194
Use Cases involving Efficient Storage GuardPoints	196
Alerts and Errors on Linux	205

Introduction to CTE-Efficient Storage

CTE-Efficient Storage for Linux is a licensed feature available with CTE 7.0.0 or later. In addition, all CTE Agents must be registered with a Vormetric Data Security Manager (DSM) version 6.3 or later.

Note

All references to 'storage array' in this document assume storage array systems capable of supporting CTE-Efficient Storage functionality.

With CTE-Efficient Storage, CTE offers the same degree of security for the data stored on the arrays while offering a new type of encryption key and GuardPoint. The new type of key enables storage array systems to achieve storage efficiencies with encrypted data streams. The coordination between the storage array and CTE is essential for achieving storage efficiency with encrypted data.

In the context of this solution, a LUN exported from a storage array system to a CTE-managed host, is referred to as an *ES GuardPoint*. An ES GuardPoint is a guarded device configured with the CTE-Efficient Storage capability.

Requirements and Considerations

- CTE-Efficient Storage requires XTS-AES mode of the AES algorithm for encryption.
- CTE only supports CTE-Efficient Storage on servers with microprocessors integrated with Advanced Encryption Standard instruction set (AES-NI).

- CTE-Efficient Storage requires that the encryption keys be stored in the KMIP server on the DSM. Therefore, all hosts on which you want to create ES GuardPoints must be registered with a KMIP-enabled domain in the DSM.

Note: Starting with CTE version 6.3 and DSM version 6.4.2, you can also use CipherTrust InPlace Data Transformation to protect storage arrays without needing to store the encryption keys in the KMIP server. For details, see [Chapter 18: "CipherTrust InPlace Data Transformation for Linux" on page 209](#).

CTE-Efficient Storage Enhanced Storage Arrays

CTE shares the encryption key associated with the LUN with a storage system that exports the LUN to a protected host. In this solution, the LUN is a device configured for CTE-Efficient Storage that can be guarded as an ES GuardPoint. When the device is guarded, the storage system and protected hosts coordinate operations for sharing the encryption key applied to the ES GuardPoint.

By sharing the key, the storage system decrypts the encrypted data streams that the protected host writes to the LUN, and then performs the data reduction process on the clear data before encrypting and storing the final encrypted data in the storage array system. The storage system does the reverse operations when the protected host reads data from Efficient Storage devices.

Storage Arrays Compatible with CTE-Efficient Storage

Currently, FlashArray from Pure Storage is the only storage system compatible with CTE-Efficient Storage ES GuardPoints.

FlashArray from Pure Storage is enhanced with CTE-Efficient Storage capabilities and inter-operates with CTE to provide CTE-Efficient Storage on Linux. The Pure Storage system is a client of the Vormetric Data Security Manager (DSM) and shares the encryption keys protecting the LUNs exported from the storage system to the protected hosts registered with the same DSM.

Note

See the EncryptReduce Installation Guide from Pure Storage for information on setting up interoperability with CTE.

Sharing Encryption Keys

CTE shares the encryption key for a LUN with the storage system using the KMIP protocol. In this solution, the DSM is the KMIP server, and the storage system is a KMIP client registered with the DSM. Any host accessing and protecting the LUNs from the storage system is a CTE managed host registered with the same DSM. The protected hosts register with the DSM using the `register_host` script executed on the protected hosts.

With the host and the storage system registered with the same DSM, the protected host continues enforcing policy and security rules on device and directory GuardPoints. The protected host stores an Efficient Storage Device Header, (ES Header) on each LUN configured as ES GuardPoint. The ES Header includes the UUID of the encryption key applied to the LUN and identifies the LUN as an ES GuardPoint to the storage array exporting the LUN. The storage array recognizes the ES Header on the LUN when the protected host writes the header, and then uses the UUID of the key from the header to retrieve the key attributes and material from the DSM (KMIP Server). This process enables the storage array and the protected host to share and apply the same key for encryption and decryption of data streams exchanged between them.

Note

The hosts accessing a shared LUN must be protected hosts registered with the same DSM as the storage array.

When the LUN is permanently de-configured as an ES GuardPoint, the ES Header must be removed. The storage array also detects the removal of the ES Header from the LUN and de-configures the LUN as an CTE-Efficient Storage device. Both the protected host and the storage array stop encryption and decryption of data streams exchanged between hosts and the storage array.

Storage Array Registration

The storage array administrator creates a certificate for the storage array and communicates the certificate to the DSM Administrator. The DSM Administrator produces a corresponding certificate specific to the array which is given to the storage array administrator. The DSM and the storage array system register both certificates and uses them each time they establish a secured session.

Note

See the EncryptReduce Installation Guide from Pure Storage for detailed instructions on registering the FlashArray as KMIP client with the with the DSM's KMIP server.

Efficient Storage Device Header and CTE Private Region

The key sharing aspect of an ES GuardPoint requires a small amount of disk space in the storage device reserved for CTE private use. The reserved space is where CTE shares information with the storage array that is exporting the device to the protected host. The reserved space starts the beginning of the device.

The protected host writes the ES Header to the device when the device is guarded for the first time. The storage array recognizes the header written to the LUN and begins the key sharing process and encrypting/decrypting data streams transferred between the protected host and the storage array on the LUN.

CTE allocates a small amount of storage space on each device configured as CTE-Efficient Storage. This region is reserved for exclusive use by CTE and is referred to as the CTE Private Region. The CTE Private Region is 63 megabytes.

CTE stores the ES Header and other metadata information to allow CTE and the storage array to exchange information. The ES Header occupies the first sector on the device. The method that CTE uses to claim the CTE Private Region on a device depends on whether the device is new (holds no data) or has existing data that you want to preserve. CTE writes the ES Header when guarding the device for the first time. The storage array recognizes the header written to the device and begins the key sharing process for exchange of encrypted data streams between the protected host and the storage array on the device.

Device Size

After you create the ES GuardPoint on the device, the device size reported to applications is the size of the device minus the space reserved for the CTE Private Region. This can lead to a discrepancy between the disk size reported by some applications versus the size reported by system utilities such as `fdisk`.



WARNING

Do not shrink ES GuardPoints. Due to relocation of user data from CTE Private Region, if you shrink the device, you may corrupt data on the device.

The ES Header contains both the available device size and the size of the CTE Private Region. To view the ES Header, use the `voradmin esg status <device-name>` command. The **Exported Disk Size** field shows the disk size available for use by other applications. The **Private Region Size** field shows the disk size reserved for CTE. For example:

```
# voradmin esg status /dev/sdh
ESG Header on /dev/secvm/dev/sdh
    Version: 1
    Change: 0
    Notifications: None
    Storage Status: None
    Private Region Size: 129024 sectors
    Exported Device Size: 20842496 sectors
    Key UUID: 2c3ee4af-010c-3593-898e-f2f62d29222d
    Mount Path: None
```

The `voradmin esg status` command also reports the UUID of the XTS-AES 256 key applied to the device. The reported UUID matches the UUID of the key as shown on the DSM key property and KMIP key object.

DSM Domain Enabled for KMIP

The KMIP protocol is the interface between the DSM and the storage arrays registered with the DSM. The Domain in the DSM for serving security requirements of storage arrays and protected hosts must be KMIP enabled. For deployment of CTE-Efficient Storage, you must create a new domain with the **Enable KMIP** option checked or modify an existing domain so that the **Enable KMIP** box is checked. This allows the DSM to make the keys for guarding CTE-Efficient Storage devices within the domain available to KMIP clients (storage arrays). Existing keys in a domain before checking **KMIP Enable** checkbox will not be accessible through KMIP.

A DSM domain can serve any number of FlashArrays as a KMIP client, but a FlashArray registered with a DSM domain *cannot* register with other domains in the DSM or with another DSM. This restriction forces the FlashArrays registered with a DSM domain to serve LUNs *only* to the CTE hosts registered with that specific DSM domain in that specific DSM.

Note

See the EncryptReduce Installation Guide from Pure Storage for detailed instructions on registering the FlashArray as KMIP client with the DSM's KMIP server.

ES GuardPoint Encryption Keys

ES GuardPoints must be encrypted using XTS-AES 256 keys. An XTS-AES 256 type key is a 512-bit key composed of two components:

- The first 256 bits of the key is the AES 256 encryption key component
- The second 256 bits is the tweak component

You create XTS keys on the DSM using the “Add Key” function, similar to non-XTS keys.

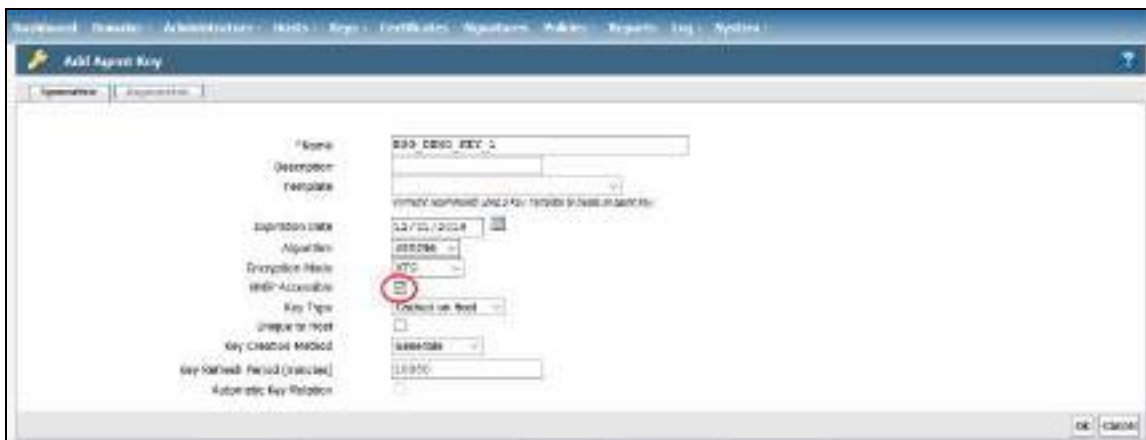
Note

You *must* check the **KMIP Accessible** check box on the “Add Agent Key” page to make the key available to KMIP clients through KMIP. If you do not check the **KMIP Accessible** option, storage arrays cannot get keys for CTE-Efficient Storage devices from the DSM (KMIP server) for sharing those keys with protected hosts.

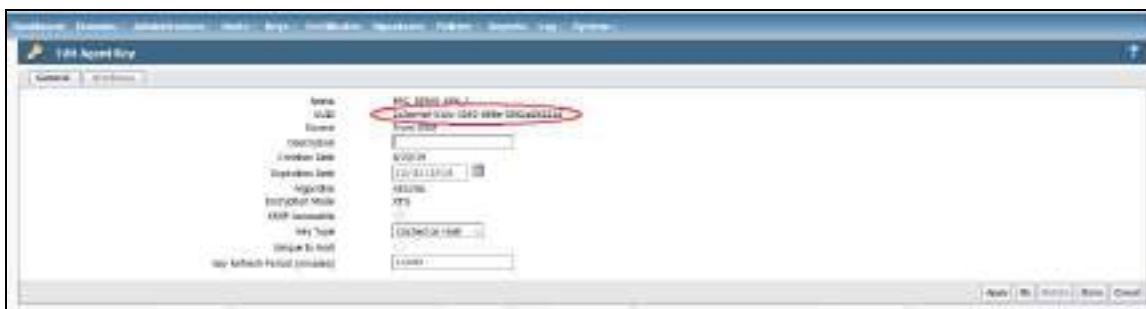
The DSM also generates a UUID for a newly added key. The DSM provides the key and its attributes to the protected hosts for guarding the CTE-Efficient Storage device. The protected host for the device writes the ES Header to the device, including the UUID of the key, before the initial attempt to enable an ES GuardPoint. The storage array recognizes the ES Header written to the device, retrieves the UUID from the ES Header, and retrieves information and attributes of the AES 256 component of the XTS-AES 256 key from the DSM using KMIP.

Key Attributes - Example

The following figure illustrates the parameters you should specify to add a new XTS-AES 256 key named ESG_DEMO_KEY_1. Note the key algorithm and encryption mode specified for the key and the checked “KMIP Accessible” option.



The following figure illustrates the general properties of ESG_DEMO_KEY_1 after adding the key. Note the UUID of the key.



The following figure illustrates the attributes of ESG_DEMO_KEY_1 after adding the key. Note that this tab displays both the UUID of the key and the UUID of the tweak component.



The attribute “x-deactivation-date” represents the date on which ESG_DEMO_KEY_1 expires. When the expiration date is reached, the key is no longer valid. It is important to choose an expiration date that exceeds any data retention period imposed on the data stored in the protected LUNs where the key is used. Note that any snapshot of a protected LUN inherits the same key protecting the primary LUN, therefore, if the key expires before reaching the end of retention period, the LUN and its snapshots will not be accessible. More importantly, do not delete the key before the data retention period expires on the LUN. The data on the LUN and its snapshots cannot be decrypted if the key is deleted prior to the data retention period.

KMIP Key Object

The following figure shows the attribute of the KMIP object for the specified UUID. The UUID specified in the example is the UUID of ESG_DEMO_KEY_1.



The following figure shows the KMIP attributes of the KMIP objects associated with ESG_DEMO_KEY_1.



The following figure shows the KMIP attributes of the KMIP object associated with the tweak component of ESG_DEMO_KEY_1.



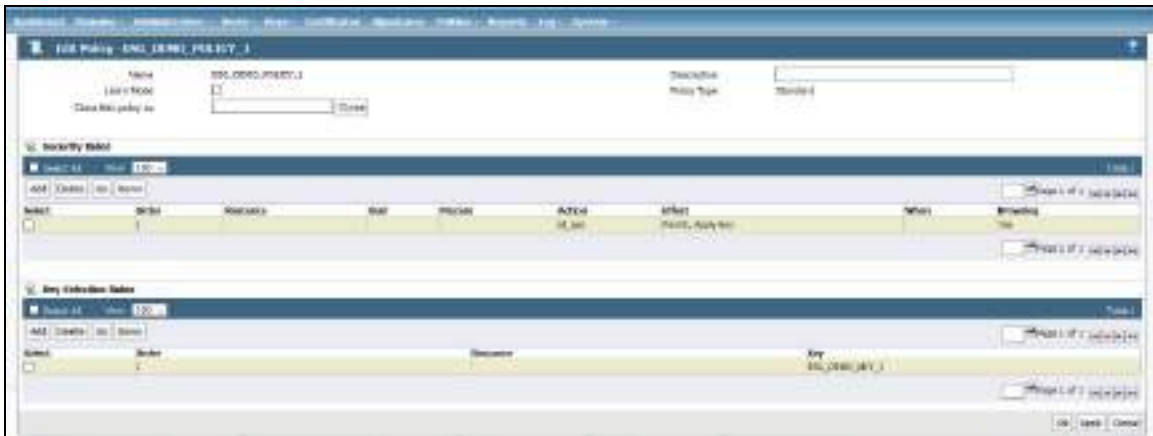
Policy Requirements for ES GuardPoints

Initializing an ES GuardPoint requires a Standard or In-place Data Transformation - Device policy with a KMIP-accessible XTS-AES 256 key as described in ["Initialize Linux Efficient Storage Devices" on page 182](#).

Rekeying an ES GuardPoint requires an In-place Data Transformation - Device policy with a KMIP-accessible XTS-AES 256 key as described in ["Changing the Encryption Key on Linux ESG Devices" on page 192](#).

You may add security rules to restrict certain user/process access to protected devices. For suggestions about what security rules you may want to use, see ["Use Cases Involving Efficient Storage GuardPoints" on page 196](#).

The following figure shows an example of a simple Standard policy that uses ESG_DEMO_KEY_1 key to guard devices.



Guarding an Efficient Storage Device on Linux

The following sections discuss how to guard an efficient storage device on Linux. If you want to guard an efficient storage Windows device, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.

In order to guard a Linux efficient storage device, you need to:

1. Make sure the devices you intend to guard meet the requirements for ES GuardPoints. For details, see ["Requirements for Efficient Storage GuardPoints on Linux" below](#).
2. Register the protected host with the DSM with CTE-Efficient Storage enabled. For details, see ["Register the Host with DSM" on the next page](#).
3. Initialize the storage device to create a CTE Private Region for the Efficient Storage Device Header. For details, see ["Initialize Linux Efficient Storage Devices" on page 182](#).
4. Log on to the DSM to apply the ES GuardPoint to the storage device. For details, see ["Guard the Linux Device with an ES GuardPoint" on page 184](#).

Requirements for Efficient Storage GuardPoints on Linux

A LUN must meet the following requirements before it can be protected as an ES GuardPoint:

- The LUN is exported from a storage array must be enhanced with the CTE-Efficient Storage capability.
- The storage array exporting the LUN to the protected host must be a KMIP client registered with the same DSM as the protected host.
- The protected host must have direct physical access to the LUN through Fiber Channel Protocol (FCP) or iSCSI.
- The entire LUN must be protected as one and only one ES GuardPoint.
- In an ESXi environment:
 - The LUN added to a virtual machine must be configured for Raw Device Mapping in physical mode or the LUN must be part of a VVol datastore.
 - The LUN *cannot* be a VMDK or a disk in a datastore.
- Devices protected by an ES GuardPoint cannot currently be initialized/added as physical volumes for use by LVM. When LVM support is added, it will be announced in the CTE Release Notes.

- Existing devices divided into one or more logical partitions cannot be guarded as ES GuardPoints. Logical partitions in such devices cannot be accessed or separately guarded after guarding the device.

For example, the logical partition `/dev/sda1` or `/dev/sda2` inside `/dev/sda` cannot be accessed after guarding `/dev/sda` as an ES GuardPoint. Using `/dev/secvm/dev/sda1` is invalid as `/dev/secvm/dev/sda1` is not a GuardPoint and cannot be guarded, and, as such, would not provide access to clear-text data on `/dev/sda1`.

Note: If you want to use VVol datastores with CTE-Efficient Storage devices, see the available documentation from the Storage Array system vendor.

Register the Host with DSM

If the host is already registered with a DSM, you can initialize the devices you want to protect as ES GuardPoints as described in ["Initialize Linux Efficient Storage Devices" on the facing page](#) as long as:

- The host is part of a domain that has KMIP enabled.
- A license for the Efficient Storage feature has been uploaded to the DSM.

To verify this, have the DSM Administrator check the host settings in the DSM.

If the host is not already registered with a DSM, you need to register it before you can protect the devices on that host. When you register the host with the DSM, you must have AES-NI available on the host, a current license for registering host, and a current license for CTE-Efficient Storage.

- If you are planning to use the fingerprint registration method, make sure the DSM Security Administrator has added the host to the appropriate KMIP-enabled domain.
- If necessary, install CTE on the host. Follow the installation prompts as until you get to the registration portion of the installation. If CTE is already installed, you can start the registration process by running `/opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host`.
- Follow the prompts to register the host with the DSM. During the registration process, make sure that you enable Efficient Storage support when prompted.

```
Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]:
You selected "vmfsodtl.i.vormetric.com".
```

```
Would you like to register to the Security Server using
a registration shared secret (S) or using fingerprints (F)? (S/F) [S]: F
```

```
It is possible to associate this installation with the hardware of this
machine. If selected, the agent will not contact the DSM or use any
cryptographic keys if any of this machine's hardware is changed. This
can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]: n
```

```
Do you want this host to have docker support enabled on the server? (Y/N) [N]:
```

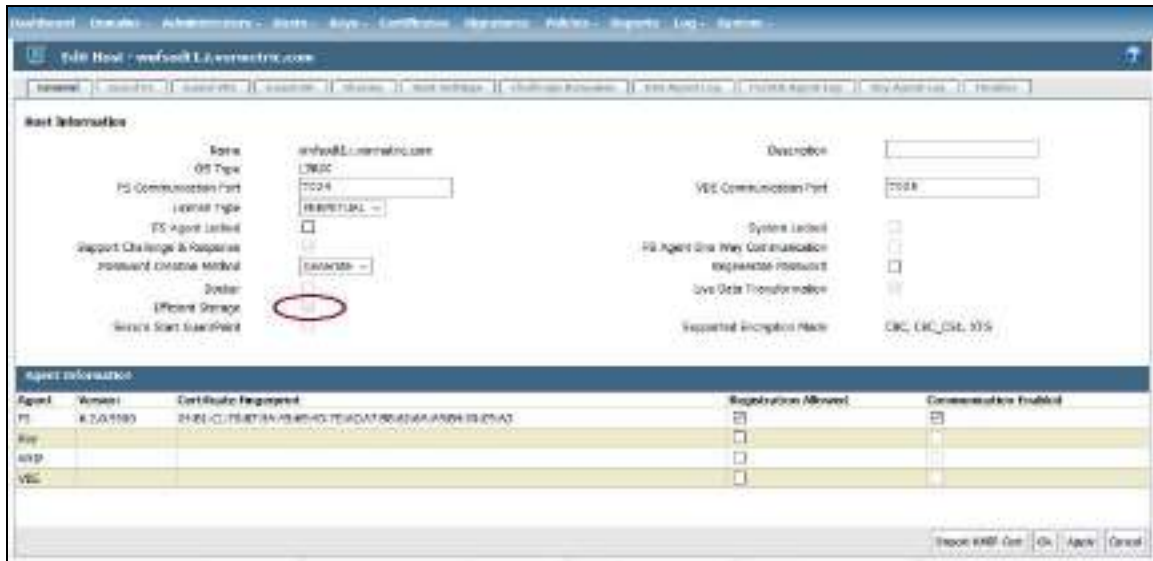
```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]: y
```

```
Do you want this host to have Efficient Storage support enabled on the server? (Y/N) [N]: y
```

```
Generating certificate signing request for the kernel component...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
```

- Complete the registration process as normal.

5. To verify that the host is properly registered with the CTE-Efficient Storage option enabled, have the DSM Administrator verify that **Efficient Storage** is checked for the host as shown below.



6. After the host is registered with the DSM, initialize each device that you want to guard as described in the next section.

Initialize Linux Efficient Storage Devices

When you initialize a Linux efficient storage device, the process creates a private region on the device for CTE to write the Efficient Storage header along with metadata that identifies the ES device as a guarded device. The CTE private region also contains the metadata for the initial transformation of clear-text data on device to cipher-text, and for the subsequent transformation of cipher-text on the device to another encryption key as needed.

How you initialize the device depends on whether it is a new device or an existing device that already has data that needs to be transformed into cipher-text. For details, see:

- ["Initialize a New Linux Device" below](#)
- ["Initialize and Resize an Existing Linux Device" on the next page](#)

Initialize a New Linux Device

Run the `voradmin esg config new` command to initialize a new device. The `new` option specifies that the device does not hold user data, and that CTE can reserve the first 63MB of storage on the device for the CTE private region. The remaining storage space is available for new user data. The device size reported to applications is the actual device size minus CTE private region size.

For a shared device that is accessed from multiple protected hosts, you must initialize the device only once and on only one protected host.

Note

To configure devices with multiple IO paths for Linux, see ["Guarding a CTE-Efficient Storage Device with Multiple IO Paths on Linux" on page 189](#).

1. Log into the device as root.
2. Run the `voradmin esg config new [-c <n>] <device-name>` command, where:
 - `new` (required) indicates that the device contains no data (it is a new disk). CTE will create the CTE private region at the beginning of the disk and the rest of the disk will be available for user data.
 - `-c <n>` (optional). If you use this option on Linux, CTE sets the number of data transformation jobs to run in parallel to the number specified in `<n>`. `<n>` can be an integer between 1 and 60 (default: 8).

Each data transformation job transforms 1MB worth of data and requires CPU resources in addition to three I/O operations as part of data transformation. Each job reads 1MB of data from the device, preserves the data in the CTE private region, rekeys the data to cipher-text, and writes the transformed data to the device. If you increase the number of parallel jobs, the data transformation process will complete faster but there will be an increased performance impact on the system. Only increase the `-c` option if you are certain that the system resources are available to handle the additional load.

The value for the `-c` option you specify here remains in effect for all subsequent data transformations (such as any data rekeys) until you specify a new value.
 - `<device-name>` (required). Specifies the device name. For example, `/dev/sdh`.

For example, if you want to initialize a new Linux disk named `/dev/sdh` using 10 parallel data transformation jobs, you would specify:

```
# voradmin esg config new -c 10 /dev/sdh
```

 3. To verify that the disk has been initialized, run the `voradmin esg status` command.

```
# voradmin esg status /dev/sdh
```

Device /dev/sdh is configured to guard as an Efficient Storage GuardPoint.
 4. At this point the DSM Administrator can protect the device as an ES GuardPoint through the DSM Management Console. For details, see ["Guard the Linux Device with an ES GuardPoint" on the facing page](#).

Note

The initialization process prepares the device to be guarded but does not actually guard it. You need to assign an ES GuardPoint to the device in the DSM before the device is actually protected. In addition, the initialization process is only kept in memory until the device is guarded or rebooted. If the device is rebooted before you guard it, you will need to perform the initialization procedure again.

Initialize and Resize an Existing Linux Device

If the device has existing data, you need to use the `voradmin esg config xform` command to initialize the disk for CTE-Efficient Storage. This command examines the current disk size and computes the size required to hold the existing data plus the CTE Private Region at the beginning of the device. After the CTE initialization is complete, you then need to resize the device before you can guard it with an ES GuardPoint.

The following procedure describes how to initialize the device for CTE. Note that the existing data is not altered in any way until after you perform this procedure and you guard the data with an ES GuardPoint. CTE does *not* begin transforming the data from clear-text to cipher-text until the ES GuardPoint has been applied and the encryption key has been pushed to the device through the GuardPoint Policy.

1. Log into the device as root.
2. Run the `voradmin esg config xform [-c <n>] <device-name>` command, where:
 - `xform` (required) indicates that the device contains existing data. CTE will transform all existing data on the device from clear-text to cipher-text as soon as you guard the device. The device will be inaccessible until the transformation is complete, and the device must remain offline during the entire transformation process. No user access will be permitted until all data has been transformed.

- `-c <n>` (optional). If you use this option on Linux, CTE sets the number of data transformation jobs to run in parallel to the number specified in `<n>`. `<n>` can be an integer between 1 and 60 (default: 8).

Each data transformation job transforms 1MB worth of data and requires CPU resources in addition to three I/O operations as part of data transformation. Each job reads 1MB of data from the device, preserves the data in the CTE private region, rekeys the data to cipher-text, and writes the transformed data to the device. If you increase the number of parallel jobs, the data transformation process will complete faster but there will be an increased performance impact on the system. Only increase the `-c` option if you are certain that the system resources are available to handle the additional load.

The value for the `-c` option you specify here remains in effect for all subsequent data transformations (such as any data rekeys) until you specify a new value.

- `<device-name>` (required). Specifies the device name. For example, `/dev/sdh`.

For example, if you want to initialize an existing Linux disk named `/dev/sdh` using 10 parallel data transformation jobs, you would specify:

```
# voradmin esg config xform -c 10 /dev/sdh
```

Device `/dev/sdh` must be resized to at least 21100544 sectors (20606 MBs) before guarding as Efficient Storage GuardPoint.

In this case you must manually resize the Linux disk by at least 20606 MBs before you can guard it. After you guard the disk, you can expand it again later but you cannot shrink it unless you remove the GuardPoint.

3. To verify that the disk has been initialized, run the `voradmin esg status` command.

```
# voradmin esg status /dev/sdh
```

Device `/dev/sdh` is configured to guard as an Efficient Storage GuardPoint.

4. At this point, you need to resize the device using your standard disk management tools before you can guard it. Make sure you increase the device size by at least the amount shown in the `voradmin esg config xform` message.

You cannot assign an ES GuardPoint to the device until it has been resized. If you do not resize the device, the GuardPoint assignment will fail.

5. After the device has been resized, the DSM Administrator can protect the device as an ES GuardPoint through the DSM Management Console as described in ["Guard the Linux Device with an ES GuardPoint" below](#).

Note

The initialization process prepares the device to be guarded but does not actually guard it. You need to assign an ES GuardPoint to the device in the DSM before the device is actually protected. In addition, the initialization process is only kept in memory until the device is guarded or rebooted. If the device is rebooted before you guard it, you will need to perform the initialization procedure again.

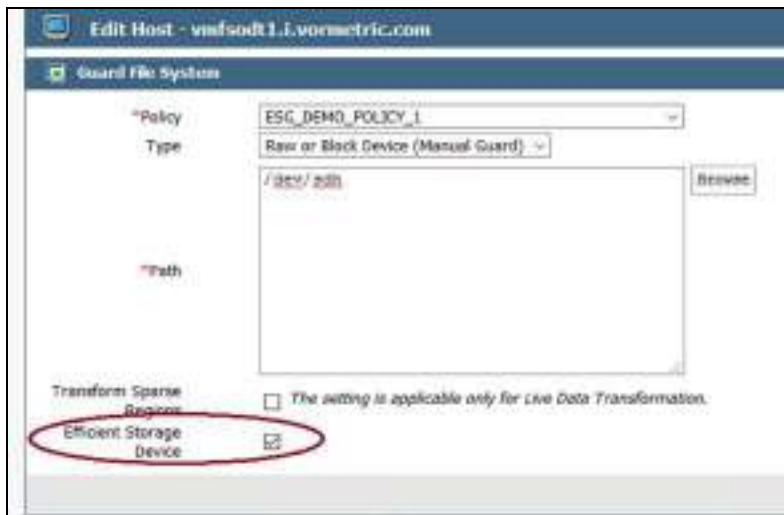
Guard the Linux Device with an ES GuardPoint

Note

For details about how to create a GuardPoint, see the chapter, "Managing GuardPoints", in the *DSM Administration Guide*.

After the device has been initialized, you can guard the device as an ES GuardPoint from the DSM Management Console. For existing devices, as soon as the GuardPoint configuration has been pushed to the host and the status changes to guarded, CTE begins transforming the data on the disk using the encryption key associated with the GuardPoint Policy.

1. Log on to the DSM Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.
2. Make sure that you know what Policy you want to associate with the ES GuardPoint or create a new standard policy if needed. The policy you use for CTE-Efficient Storage must use an XTS-AES 256 key as the key rule. For details, see ["ES GuardPoint Encryption Keys" on page 177](#).
3. Select **Hosts > Hosts** on the menu bar. The *Hosts* window opens.
4. Click the target host in the **Host Name** column. The Edit Host window opens to the General tab for the selected host.
5. Click the **GuardPoints** tab and then click **Guard**. The Guard window opens.
6. In the **Policy** field, select the Policy you identified or created earlier in this procedure. CTE will use the XTS-AES 256 key associated with this policy to encrypt the data on the device.
7. In the **Type** field, select either **Raw or Block Device (Auto Guard)** or **Raw or Block Device (Manual Guard)**.
If you select **Auto Guard**, CTE starts the guard process as soon as the policy is pushed to the host. You enable, disable, guard, and unguard the GuardPoint in the DSM. If you want to have the device automatically guarded and mounted at system start up, add the device to `/etc/fstab`. For details, see ["Auto Mount Options for File System Devices on Linux" on page 190](#).
If you select **Manual Guard**, You guard the GuardPoint on the protected host with the `secfsd -guard <path>` and `secfsd -unguard <path>` commands. At system startup, you must guard the device and then mount it. This gives you more control over when data transformations occur because CTE will not start encrypting or rekeying the device until you manually start the process.
8. In the **Path** field, add the path for the device you want to guard. For example, `/dev/sdh`.
If you specify multiple paths in this field, all specified devices will be guarded and all will be encrypted with the encryption key specified in the associated policy.
9. Make sure the **Efficient Storage** check box is checked. If this option is not selected, the host will *not* enable the device as an ES GuardPoint.



10. Click **OK**.

The DSM pushes the policy and the GuardPoint configuration to the host and the CTE agent on the host writes the ES Header into the CTE private region for the specified devices. If this is a new device, the status changes to guarded and the disk is available for user access immediately.

If there is existing data on the device, CTE begins transforming the data from clear-text to cipher-text as soon as the GuardPoint configuration is available and the device status changes to guarded. The device will remain inaccessible until this data transformation completes. The length of time required to transform the data depends on the amount of existing data and the number of parallel data transformation jobs specified on the `voradmin config` command. For details, see ["Data Relocation on Existing Linux Devices" below](#) and ["Data Transformation on Existing Linux Devices" below](#).

To see the data transformation progress, use the `voradmin esg xform status <device-name>` command, as described in ["Viewing Device Status and the ES Header on Linux" on page 189](#).

After the device is initialized and guarded, the protected device must be accessed through the CTE device pathname. This pathname corresponds to the `secvm` device. For example, the Linux device pathname `/dev/sdh` becomes `/dev/secvm/dev/sdh` as soon as the process is complete.

Notes

- Be sure to use the `secvm` device name when using file system management tools such as `mkfs` and `fsck`.
- Do not use the device mapper names corresponding to ES GuardPoints for GuardPoint administration on protected hosts.

Data Relocation on Existing Linux Devices

When you add an ES GuardPoint to a device that has been initialized with the `xform` option, CTE first relocates existing data in the region of the device designated as CTE Private Region. The data is relocated to the end of the LUN, into the new space allocated. The relocation occurs once when the device is guarded for the first time.

Relocation of data is transparent to applications accessing data through the ES GuardPoint. CTE will map application I/O requests over the CTE Private Region to the relocated region. After guarding the device, you can grow the device size further if necessary. However, you cannot shrink the device size.

Data Transformation on Existing Linux Devices

As the ES Header is written before data transformation begins, the data transformed to cipher-text and written back to the device during data transformation process is subject to data reduction process through the storage array.

Existing devices populated with data are transformed from clear-text to cipher-text using the encryption key applied to each device. Data transformation is also called CipherTrust InPlace Data Transformation (CTE-IDT).

CTE-IDT is not the same as the legacy offline data transformation. CTE-IDT is a block level data transformation with built-in resiliency to recover from system crashes during the data transformation process. CTE-IDT uses the CTE Private Region on the device to manage the entire transformation process. CTE-IDT partitions the data on a device in segments of 1MB in size and transforms one or multiple segments, up to 60 segments, in parallel. The CTE-IDT process preserves existing data in a segment during transformation in the private region of the device, and then transforms the data in-place. CTE-IDT also maintains the segments undergoing transformation in the private region. In the event of system crash, CTE-IDT will recover the segments undergoing transformation at the time of crash and then resume the transformation process.

You can specify the number of segments to transform concurrently using `-c` option of the `voradmin` command when initializing the device. Choose a concurrency level that does not affect performance of your production workload. By default, CTE-IDT transforms 8 segments concurrently, if the concurrency level has not been specified through the `voradmin` command.

Note

When choosing the concurrency level for your system you must consider the number of CPU cores, the total IOPS of your storage system and production workload, the size of the device to transform, and the duration for the data transformation.

Another advantage of CTE-IDT over legacy offline data transformation is that CTE-IDT does not require a separate policy for data transformation. With the same production policy applied to the device, CTE-IDT determines whether the device is in need of data transformation, per specification of `xform` option when device was initialized, and starts the CTE-IDT process when transformation is required. During the CTE-IDT process, access to the device is blocked until the CTE-IDT process completes.

```
# voradmin esg status xform /dev/sdb
Status: In-Progress
Relocation time 2155544 (relocated = 1)
SegSp: 27, Xformation Range: 3217 ... 4799, SegID: 4795 4796 4781 4782 4787 4795 4799
KeyID: 988905 Key Name: ESG DEMO_KEY_1
Old KeyID: 0 Old Key Name: clear_key
# dd if=/dev/securem/dev/sdb of=/dev/null bs=512 count=1
dd: failed to open '/dev/securem/dev/sdb': Resource temporarily unavailable
# voradmin esg status xform /dev/sdb
Status: Complete
Relocation time 2245544 (relocated = 1)
SegSp: 27, Xformation Range: 3217 ... 20189, SegID: none
KeyID: 988905 Key Name: ESG DEMO_KEY_1
Old KeyID: 0 Old Key Name: clear_key
# dd if=/dev/securem/dev/sdb of=/dev/null bs=512 count=1
140 records in
140 records out
512 bytes (512 B) copied: 0.000988039 s, 518 kB/s
```

Thin-Provisioned Devices

CTE-IDT skips transforming thin-provisioned regions of a device. Data returned to CTE-IDT as sequence of clear-text zeros, in sector size granularity, is indication of possible sparse or un-allocated regions of the device that do not have to be transformed.

CTE-IDT Recovery From Crash

CTE-IDT is fault tolerant in the event of system crashes. CTE-IDT keeps track of the transformation process over the entire device. In the event of a crash, CTE-IDT will automatically resume transformation from the point of failure as soon the GuardPoint is enabled after system startup.

If you find the transformation status set to **In-Progress** when the GuardPoint is not enabled, the **In-Progress** state reflects an earlier system crash after which the GuardPoint has not been enabled to recover from the interruption in the CTE-IDT process.

Example of Creating an ES GuardPoint on an Existing Linux Device

The following figure shows an example of initializing an existing Linux device using `voradmin esg config xform` and guarding it as an ES GuardPoint from the viewpoint of the Linux root user.


```
# voradmin esg status /dev/sdh
Native device /dev/sdh is not labeled as ESG

# fdisk -l /dev/sdh

Disk /dev/sdh: 21.2 GB, 21169700864 bytes, 41347072 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes

# mkfs.xfs /dev/sdh
meta-data=/dev/sdh          isize=512    agcount=4, agsize=1288064 blks
                         =   sectsz=512   atime=1, noctime=1
                         =   dir=1        info=0*0, sparse=0
data      =   bsize=4096   blocks=6132256, leap=0-33
                         =   sunit=0      swidth=0 blks
naming     =version 2      bsize=4096   ascii-ci=0 ftype=1
log        =internal log   bsize=4096   blocks=1360, version=2
                         =   sectsz=511   sunit=0 blks, lazy-count=1
realtime   =none          extsz=4096   blocks=0, rtextents=0

# mount -t xfs /dev/sdh /xfs
# cd /bin/* /xfs
# umount /xfs
# voradmin esg config xfs /dev/sdh
Device /dev/sdh must be resized to at least 41347072 sectors (40376 MBs) before guarding as Efficient Storage GuardPoint
```

Now you must resize the device on the storage array to the specified size or larger, and then guard the device on the DSM as ES GuardPoint using Manual Guard. For details about guarding the device on the DSM, see ["Guard the Linux Device with an ES GuardPoint" on page 184](#).

After resizing the device and configuring the GuardPoint in the DSM:

```
# fdisk -l /dev/sdh

Disk /dev/sdh: 21.2 GB, 21169700864 bytes, 41347072 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes

# secfsd -guard /dev/sdh
secfsd: Path is guarded
```

At this point CTE begins data relocation and transformation. Data transformation will require some amount of time to complete. You can monitor the transformation process with the `voradmin esg status xform <device-name>` command.

```
# voradmin esg status xform /dev/sdh
Status: In-Progress
Relocation done 11111111 (Relocated = 1)
SegSpr 27, Xformation Range: 128 ... 139, SegID: 139
KeyID: 988905 Key Name: ESG DEMO KEY_1
Old KeyID: 0 Old Key Name: clear_key

Wait for data transformation to complete:

# voradmin esg status xform /dev/sdh
Status: Complete
Relocation done 11111111 (Relocated = 1)
SegSpr 27, Xformation Range: 1281 ... 13189, SegID: none
KeyID: 988905 Key Name: ESG DEMO KEY_1
Old KeyID: 0 Old Key Name: clear_key

# voradmin esg status /dev/sdh
ESG Header on /dev/secure/dev/sdh
Version: 1
Change: 0
Notification: None
Storage Status: None
Private Region Size: 128016 sectors
Exported Device Size: 41315048 sectors
Key UUID: 2c3e6af-010c-3595-359e-e2661d19121d
Mount Path: None

# mount -t xfs /dev/secure/dev/sdh /xfs
# for file in $(ls /xfs); do cmp /bin/$file /xfs/$file done
# umount /xfs
```


Guarding a CTE-Efficient Storage Device with Multiple IO Paths on Linux

Each individual IO path from a server node to a storage controller is treated as a separate device on the host. DM-Multipath on a Linux host provides a management framework to group the individual IO paths to the same LUN into a single multipath device. If you use DM-Multipath to manage devices on the protected host, the individual devices that correspond to each IO path to the LUN cannot be configured for guarding as ES GuardPoints, as those devices are under control of DM-Multipath. To guard such devices, you must guard the device mapper generated by DM-Multipath (multipathd) under the `/dev/mapper` directory.

Note

CTE-Efficient Storage is the only feature of CTE that exclusively supports guarding of device mapper generated devices under DM-Multipath framework.

The following example illustrates the procedure for guarding a device mapper generated device with the alias name `/dev/mapper/mpathA`.

1. Create a standard policy using an XTS key as the key rule.
2. On the host, prepare the device to be configured as ESG using the `voradmin` command with `new` or `xform` option. For example:

```
# voradmin esg config new /dev/mapper/mpathA
```
3. On the DSM, guard `/dev/mapper/mpathA` as Device GuardPoint using the policy created above. Be sure to check the **Efficient Storage** check box.
4. For Manual-Guard configuration, enable the GuardPoint using the `secfsd` command as follows:

```
# secfsd -guard /dev/mapper/mpathA
```
5. For Auto-Guard, wait for the `/dev/mapper/mpathA` device to be guarded on the protected host.
6. Once the device is guarded, provide the pathname of the `secvm` device to applications and/or file system operations. For example, `/dev/secvm/dev/mapper/mpathA`.

Linux System and ES GuardPoint Administration

voradmin ESG Commands on Linux

The `voradmin` command is a command line utility for management of CTE specific configuration and status reporting. The `voradmin` command also supports configuration management related to ES GuardPoints (ESG).

For details about the Linux `voradmin esg` command options, see the man page for the `voradmin` command.

Viewing Device Status and the ES Header on Linux

After you guard a device, you can view the status of that device using the `voradmin esg [xform] status <device-name>` command, where:

- `xform` (optional). If you specify this option, CTE shows the status of any data transformation processes happening on the device. If you do not specify this option, CTE displays the ES Header for the device.
- `<device-name>` (required). The standard Linux name of the device whose status you want to view. (For example, `/dev/sdh`.)

For example, if you want to view the ES Header for the Linux device `/dev/sdh`, you would enter:

```
# voradmin esg status /dev/sdh
ESG Header on /dev/secvm/dev/sdh
  Version:          1
  Change:           0
  Notifications:    None
  Storage Status:   None
  Private Region Size: 129024 sectors
  Exported Device Size: 20842496 sectors
  Key UUID:         2c3ee4af-010c-3593-898e-f2f62d29222d
  Mount Path:       None
```

If you want to view the data transformation status on `/dev/sdh`, you would enter:

```
# voradmin esg xform status /dev/sdh
  Status:           In-Progress
  Relocation Zone 22939646 (relocated = 1)
  SegSpc 27, Xformation Range: 3217 ... 4799, SegIDs: 4795 4796 4791 4792...
  KeyID:            988905 Key Name: ESG_DEMO_KEY_1
  Old KeyID:        0      Key Name: clear_key
```

The **Status** field displays **In-Progress** if a data transformation process is running, and **Completed** if the process has finished.

File System Mount Points on Linux

You can create and mount a file system on an ES GuardPoint. CTE imposes one restriction on the mount point pathname selected for a device. Once you mount the device on a pathname, you cannot change the mount point to a different pathname. This restriction is enforced to allow the file system mount point to be guarded using a separate policy to enforce access control rules on the mounted file system namespace. For a use case involving a directory GuardPoint guarded over a mounted ES GuardPoint, see ["Use Case 3: Directory-Level GuardPoints" on page 197](#).

The following example shows the mount point of the ES GuardPoint as the `/xfs` directory. The example also shows a failed attempt to mount the file system on a different directory pathname.

```
# voradmin esg status /dev/sdh
ESG Header on /dev/secvm/dev/sdh
  Version:          1
  Change:           0
  Notifications:    None
  Storage Status:   None
  Private Region Size: 129024 sectors
  Exported Device Size: 41218048 sectors
  Key UUID:         b1c045bd-d81e-3e22-b822-5033dd22dd00
  Mount Path:       /xfs
# mount /xfs
# mount /other-xfs
# mount -t xfs /dev/secvm/dev/sdh /other-xfs
mount: permission denied
# mount -t xfs /dev/secvm/dev/sdh /xfs
```

Auto Mount Options for File System Devices on Linux

ES GuardPoints containing file systems can also be added to the `/etc/fstab` configuration file for auto mount at startup or unmount at shutdown. An entry can be for an ES GuardPoint configured for Auto Guard or Manual Guard. For more information about Auto and Manual Guard options, see ["Guard the Linux Device with an ES GuardPoint" on page 184](#).

Use the device path corresponding to an ES GuardPoint device when specifying `fstab` entries, such as `/dev/secvm/dev/sdh`. Do not use the native device pathnames, such as `/dev/sdh`, or device mapper device names. You must also include several settings in the `fstab` entry for each ES GuardPoint, as shown in the following table:

Option	Description
<code>x-systemd.requires=secvm-barrier.service</code>	Ensure that the ES GuardPoint is enabled before the device is mounted at startup and disabled after the device is unmounted at shutdown. The <code>secvm-barrier.service</code> service is a proxy for all the services that make up CTE.
<code>nofail</code>	The system boot will proceed without waiting for the ES GuardPoint device if it can't be mounted successfully.
<code>x-systemd.wanted-by=<es device>.device</code>	Required for Linux distributions running <code>systemd</code> 242 or later. Instructs <code>systemd</code> to add a <code>Wants=</code> dependency on the ES device to ensure that, when the device becomes available, this mount operation is executed. <code><es device>.device</code> is the name of the device specified in <code>fstab</code> with the <code>'/'</code> replaced with <code>'.'</code> . For example, <code>/dev/secvm/dev/sdb</code> becomes <code>dev-secvm-dev-sdb.device</code> .

This is an example of an entry in `/etc/fstab` for an ES GuardPoint with an `xfs` file system that is mounted on `/xfs`:

```
/dev/secvm/dev/sdh /xfs xfs x-systemd.requires=secvm-barrier.service, \
x-systemd.wanted-by=dev-secvm-dev-sdh.device,nofail 0 0
```

For information about configuring `systemd` for CTE, see [Chapter 6: "CTE and systemd" on page 76](#).

Linux System Utilities for Signing

The following table includes recommendations on the system and file system specific utilities for inclusion in the signature set to allow or deny root execution.

EXT Utilities	Deny/Allow	XFS	Deny/Allow	Generic Utilities	Deny/Allow
<code>badblock</code>	Allow	<code>fsck.xfs</code>	Allow	<code>mount</code>	Allow
<code>debugfs</code>	Deny	<code>mkfs.xfs</code>	Allow	<code>umount</code>	Allow
<code>e2freefrag</code>	Allow	<code>xfs_repair</code>	Allow	<code>dmsetup</code>	Allow
<code>e2fsck</code>	Allow	<code>xfs_admin</code>	Allow		
<code>e2image</code>	Allow	<code>xfs_bmap</code>	Allow		
<code>e2label</code>	Allow	<code>xfs_check</code>	Allow		
<code>e2undo</code>	Allow	<code>xfs_copy</code>	Deny		
<code>filefrag</code>	Allow	<code>xfs_db</code>	Deny		
<code>fsck.ext2</code>	Allow	<code>xfs_estimate</code>	Allow		
<code>fsck.ext3</code>	Allow	<code>xfs_freeze</code>	Allow		
<code>fsck.ext4</code>	Allow	<code>xfs_fsr</code>	Allow		
<code>logsave</code>	Allow	<code>xfs_growfs</code>	Allow		
<code>mke2fs</code>	Allow	<code>xfs_info</code>	Allow		
<code>mkfs.ext2</code>	Allow	<code>xfs_logprint</code>	Allow		
<code>mkfs.ext3</code>	Allow	<code>xfs_mdrestore</code>	Allow		
<code>mkfs.ext4</code>	Allow	<code>xfs_metadump</code>	Allow		

EXT Utilities	Deny/Allow	XFS	Deny/Allow	Generic Utilities	Deny/Allow
resize2fs	Allow	xfs_mkfile	Deny		
tune2fs	Allow	xfs_ncheck	Allow		

Changing the Encryption Key on Linux ESG Devices

To meet various compliance requirements, you may want to change the key that CTE has used to encrypt ES GuardPoints. Thales refers to this changing of encryption keys as “Key rotation” or “Rekey”. Unlike the CipherTrust Transparent Encryption - Live Data Transformation product offered by Thales for file systems on traditional storage devices, to change the encryption key on an ES GuardPoint, the device must be taken offline. The data on the device will be inaccessible during the key rotation process.

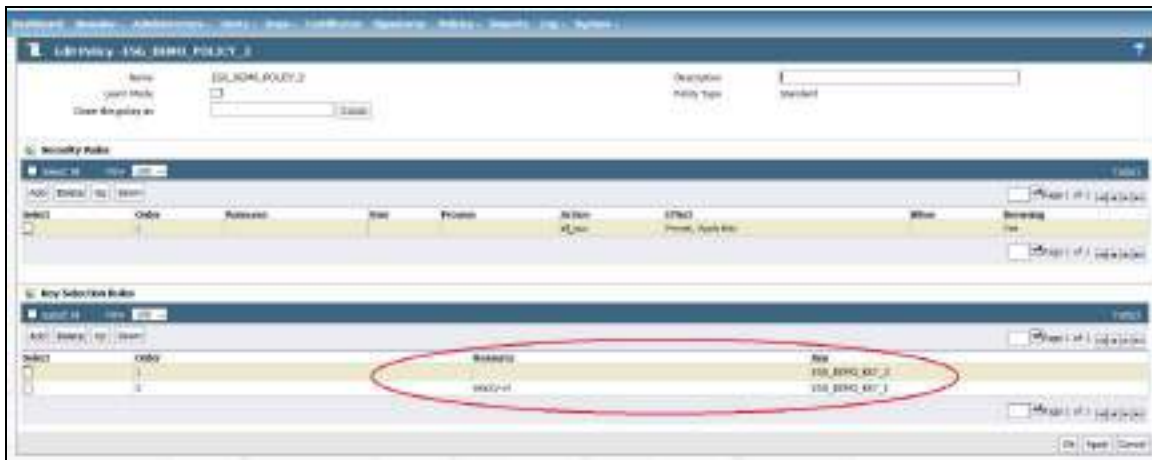
The key rotation process involves the following:

- Creating a new policy for key rotation
- Preparing the CTE-Efficient Storage device for key rotation
- Applying the new policy to the CTE-Efficient Storage device on the DSM

See the following sections for details of key rotation. If your organization has separated security duties, some of the steps below may need to be completed by different people.

Creating a New DSM Policy for Key Rotation

As part of rekeying the data on a CTE-Efficient Storage device, you must create a new policy with a key rule specifying the new key and include a second key rule that specifies the current key. The screenshot below depicts a policy named ESG_DEMO_POLICY_2 for rekey:



Similar to the policy ESG_DEMO_POLICY_1, the above production policy applies the key specified in the first key rule, ESG_DEMO_KEY_2, on the device guarded with the policy. The second key rule is actually ineffective, because the first key rule is always selected for IO operations to devices guarded with ESG_DEMO_POLICY_2, hence never selecting the second key rule for key operations.

The reason for inclusion of the second key rule is the availability of the key specified in the second key rule (ESG_DEMO_KEY_1) to the protected host. Note that the name and the ID of the key applied to the data on ES GuardPoints are persistently recorded in the CTE private region on the device. However, the recording of the key name and ID in the private region may not be sufficient for availability of ESG_DEMO_KEY_1 to the protected host without the second key rule listed in ESG_DEMO_POLICY_2 policy. If another GuardPoint on the protected host guarded with a

policy that specifies ESG_DEMO_KEY_1 as a key rule, the key ESG_DEMO_KEY_1 is available to the protected host, and the policy ESG_DEMO_POLICY_2 does not have to include the second key rule listing ESG_DEMO_KEY_1. Absence of any GuardPoint not guarded with a policy specifying ESG_DEMO_KEY_1 causes the DSM not to push the key ESG_DEMO_KEY_1 to the protected host.

Notice the resource set empty-Ø listed as the resource set in the second key rule. This is an empty resource set that does not associate any object in a guarded GuardPoint with the key specified in the key rule. An empty resource set is specified in the second key rule because a resource set is required for adding the second or additional key rules to the policy.

Prepare an ES GuardPoint for Rekey

Before you apply the new policy, you must shutdown any applications accessing the ES GuardPoint. This also includes unmounting file system if the ES GuardPoint is a device mounted as a file system. The next step is to unguard the guarded device on the protected host and then on the DSM. Unguarding the device on the DSM deletes the ES GuardPoint on the host.

The following screenshot enumerates the administrative steps for rekeying ES GuardPoints. The following figure shows the transformation from ESG_DEMO_POLICY_1 using ESG_DEMO_KEY_1 to the new policy ESG_DEMO_POLICY_2 using ESG_DEMO_KEY_2.

```
# secfed -status guard | grep adh
/dev/adh          ESG_DEMO_POLICY_1      manualrekeydevice guarded   guarded   N/A
# secfed -unguard /dev/adh
secfed: Path is not guarded
# voradmin esg status xform /dev/adh
Status:          Complete
Relocation Zone  22939040 (relocated = 1)
SegSpd 17, Xformation Range: 0000 --- 0000, SegIter none
KeyID:           000000 Key Name:      ESG_DEMO_KEY_1
Old KeyID:       0      Old Key Name: clear_key
```

Notice the key name and the old key name associated with the device as recorded in the device private region.

Next, unguard the device on the DSM and then run the `voradmin` command to prepare the device for rekey. Be sure the device is unguarded on the DSM before running the `voradmin` command, otherwise the `voradmin` command refuses to prepare the device for rekey. Notice that the ES Header is temporarily deleted from the device in preparation for rekey.

```
# secfed -status guard | grep adh
# voradmin esg rekey /dev/adh
Enter Y/N to prepare device /dev/adh for rekey -> YES
# voradmin esg status /dev/adh
Native device /dev/adh is not labeled as ESG
```

Next, guard the device on the DSM as an Efficient Storage device using the policy ESG_DEMO_POLICY_2. After the DSM pushes the configuration on the ES GuardPoint, proceed with guarding the device on the protected host. The guard operation detects the policy/key change on the device and begins the CTE-IDT process to transform data from ESG_DEMO_KEY_1 to ESG_DEMO_KEY_2. During the CTE-IDT process, user access to the ES GuardPoint is blocked until IDT completes the transformation process.

```
# secfed -status guard | grep adh
/dev/adh          ESG_DEMO_POLICY_2      manualrekeydevice unguarded  not guarded Inactive
# secfed -guard /dev/adh
secfed: Path is guarded
# voradmin esg status xform /dev/adh
Status:          In Progress
Relocation Zone  22939040 (relocated = 1)
SegSpd 17, Xformation Range: 0000 --- 0000, SegIter 3317 3318 3319 3320 3321 3322 3323 3324 3325 3326 3327 3328 3329 3330 3331
KeyID:           000000 Key Name:      ESG_DEMO_KEY_2
Old KeyID:       000000 Old Key Name: ESG_DEMO_KEY_1
```

After CTE-IDT completion you can restart application workloads on the guarded device.

```
# voradbin esg status xform /dev/ada
Status:      Complete
Relocation Done 22939408 (relocated = 1)
SeqNo 27, Information Range: 20159 .. 20159, SeqIDat none
VerID1:      988888 Key Name:   ES0_DSMO_KEY_1
Old KeyID:    688601 Old Key Name: ES0_DSMO_KEY_1
# mount -t xfs /dev/secure/dev/ada /xfs
```

Resizing Guarded Efficient Storage Devices

Devices configured for Efficient Storage can be resized using the system-provided resizing utilities. If you are using a file system on the GuardPoint, you can mount the file system after resizing the device and then grow the file system to the new size using the appropriate utility such as `xfs_growfs` or `resize2fs`.



WARNING

Do not shrink ES GuardPoints. Due to relocation of user data from CTE private region, if you shrink the device, you may corrupt data on the device.

1. Stop applications from accessing the GuardPoint.
 - Unmount the file system if the device is mounted.
 - Disable GuardPoints: auto-guard if is enabled on the DSM, or manual-guard if is enabled on the protected host.
2. Use the native disk management tools to resize the device.
3. After resizing the device, check the size of the device. For Linux, you can use the `fdisk -l` command.
4. If the reported size does not match what you expect, you may need to rescan your storage devices using the command appropriate for the device's connection type.
5. Once the expected size is achieved, enable the GuardPoint and restart your applications.

Example: Resizing a Linux Device

The following example show the administrative steps to grow an XFS file system mounted on an ES GuardPoint. The example shows a device of size 41,347,072 sectors resized to 43,395,072 sectors .

```
# fdisk -l /dev/ada

Disk /dev/ada: 31.3 GB, 3316876800 bytes, 41347072 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes

# xfs_info /dev/secvm/dev/ada
meta-data=/dev/secvm/dev/ada      isize=512    bcount=4, agsize=1288064 blks
                                   secbs=512     bsize=4096, firstblock=0, inoctx=25
                                   crc=1          finit=0, rmapnodes=0
                                   bsize=4096     blocks=41347072, maxpct=25
                                   sunit=0        swidth=0 blks
                                   bsize=4096     ascll-ci=0 ftype=1
                                   bsize=4096     blocks=2560, version=2
                                   sector=512     conit=0 blks, lazy-count=1
                                   extsize=4096    blocks=0, rtextents=0

# voradmin esp status /dev/ada
ESG Header on /dev/secvm/dev/ada
  Version: 1
  Change: 0
  Notifications: None
  Storage Status: None
  Private Region Size: 128024 sectors
  Reported Device Size: 41347040 sectors
  Key UUID: 61644444-6164-6164-6164-616461646164
  Mount Path: N/A (GuardPoint not enabled)

# umount /xfs
# secfd -unguard /dev/ada
secfd: Path is not guarded
```

In this example we resize the device on the storage array to 43395072 sectors. Notice that the `voradmin` command reports the old device size until the device is guarded.

```
# fdisk -l /dev/ada

Disk /dev/ada: 31.3 GB, 3316876800 bytes, 43395072 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes

# voradmin esp status /dev/ada
ESG Header on /dev/secvm/dev/ada
  Version: 1
  Change: 0
  Notifications: None
  Storage Status: None
  Private Region Size: 128024 sectors
  Reported Device Size: 41347040 sectors
  Key UUID: 61644444-6164-6164-6164-616461646164
  Mount Path: N/A (GuardPoint not enabled)

# secfd -guard /dev/ada
secfd: Path is guarded

# voradmin esp status /dev/ada
ESG Header on /dev/secvm/dev/ada
  Version: 1
  Change: 0
  Notifications: None
  Storage Status: None
  Private Region Size: 128024 sectors
  Reported Device Size: 43395040 sectors
  Key UUID: 61644444-6164-6164-6164-616461646164
  Mount Path: /xfs
```


The final step shown in below is to mount and resize the XFS file system to include the extended space into the file system.

```
# mount -t xfs /dev/sector/0x500 /xfs
# xfs_info /xfs
meta-data=/dev/sector/0x500  isize=512    agcount=4, agsize=131072 bke
=          =          sectsz=512    attr=0, projid32bit=1
=          =          crc=1        finobt=0, inoobt=0
data      =          =          bsize=4096  blocks=512256, logsect=25
=          =          sunit=0      bsize=4096  ascll-ci=0, ftype=1
naming    =version 2   bsize=4096  blocks=2560, version=1
log       =internal    sectsz=512   sunit=0 bke, lazy-count=1
realtime  =none        sectsz=4096  blocks=0, rtextents=0
data blocks changed from 512256 to 540256
# xfs_info /dev/sector/0x500
meta-data=/dev/sector/0x500  isize=512    agcount=5, agsize=131072 bke
=          =          sectsz=512    attr=0, projid32bit=1
=          =          crc=1        finobt=0, inoobt=0
data      =          =          bsize=4096  blocks=540256, logsect=25
=          =          sunit=0      bsize=4096  ascll-ci=0, ftype=1
naming    =version 2   bsize=4096  blocks=2560, version=2
log       =internal    sectsz=512   sunit=0 bke, lazy-count=1
realtime  =none        sectsz=4096  blocks=0, rtextents=0
```

Use Cases involving Efficient Storage GuardPoints

ES GuardPoints support three use cases for managing customer's data in GuardPoints. This section describes those potential use cases.

Use Case 1: Single Encryption Key

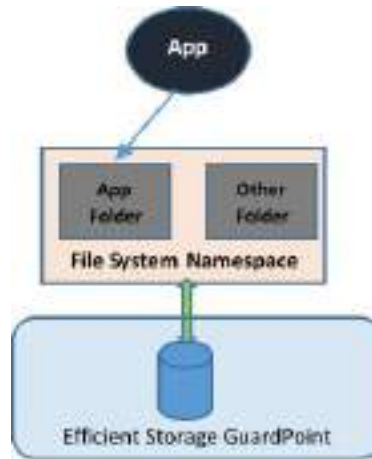
Applications, such as an Oracle Database, store structured data in one or multiple LUNs guarded as an ES GuardPoint. In this use case, a LUN may be an independent datastore or a member of a disk group managed by an application, for example an Oracle ASM disk group. In this use case, the policy applied to the GuardPoints specifies one key rule for encryption, and, potentially, a second key rule with an empty resource set for rekey. The policy may include access rules for user or process level access control.



Use Case 2: Device-Level GuardPoints

Protect structured or unstructured data stored in data files. The data files are organized inside one or more directories or folders within a file system namespace, such as ext4 or XFS, without any protection on the folders or the file system namespace. In this use case, the file system resides in the device guarded as Efficient Storage using a policy with a key rule and *no user specified access rule*. Access rules are not applicable in this use case and should not be used. Similar to use case 1, Linux policies supporting this use case can also specify the second key rule with an empty resource set for rekey.

Figure 17-1: File system resides in device guarded as ES GuardPoint



Example

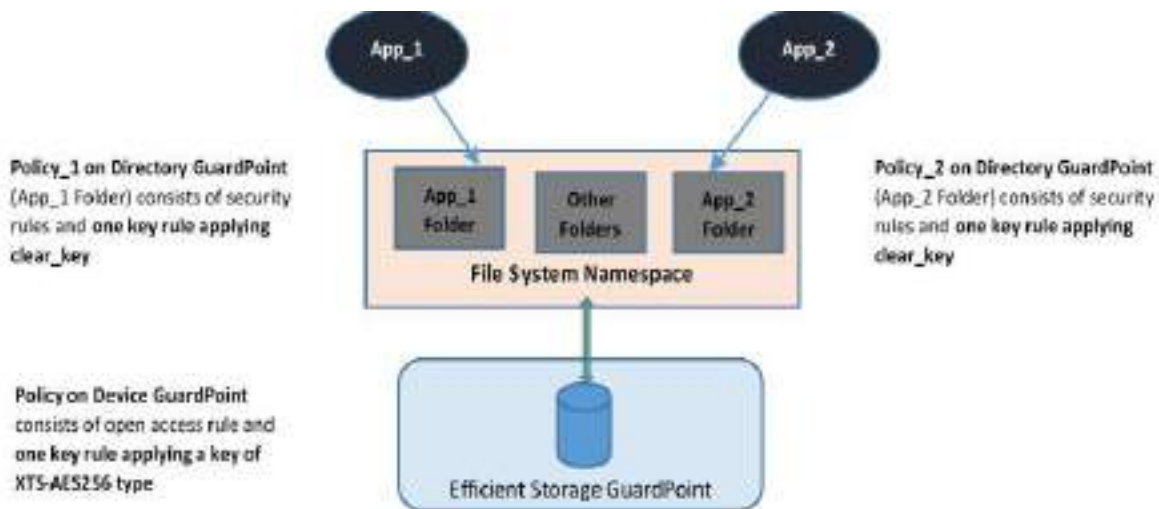
Below is an example of this use case where a Linux file system is created in an ES GuardPoint and then mounted. The policy used for the GuardPoint does not specify user or process-level access rules because I/O operations to the GuardPoint are from the file system module accessing the device on behalf of application I/O operations to the files inside the mounted file system.

```
# secctl -status guard | grep adh
/dev/adh          ESG_POLICY_1          manualrawdevice  unguarded      not guarded  inactive
# voreadmin esg config new /dev/adh
# secctl -guard /dev/adh
secctl: Path is guarded
# voreadmin esg status /dev/adh
ESG Header on /dev/secvm/dev/adh
  Version:          1
  Change:           0
  Notifications:    None
  Storage Status:   None
  Private Region Size: 128024 sectors
  Expected Device Size: 43166040 sectors
  Key UUID:         b16448d4-2d1a-3a8f-b42a-5693d31f9c00
  Mount Path:       None
# mke2fs -t xfs /dev/secvm/dev/adh
mke2fs-data=/dev/secure/adv      inode=612      agcount=4, agsize=1362961 blks
      =          sector=512      attr=2, projid32bit=1
      =          nro=1          finobt=0, sparse=0
data      =          bsize=4096   blocks=540256, imaxpct=21
      =          sunit=0        swidth=0 blks
logging   =version 2          bsize=4096   aextl=0 ftype=1
log       =internal log      bsize=4096   blocks=240, version=2
      =          sectsz=512     sunit=0 blks, lazy-count=1
realtime  =none              bsize=4096   blocks=0, stextents=0
# mount -t xfs /dev/secvm/dev/adh /xfs
# mount | grep xfs
/dev/secvm/dev/adh on /xfs type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
```

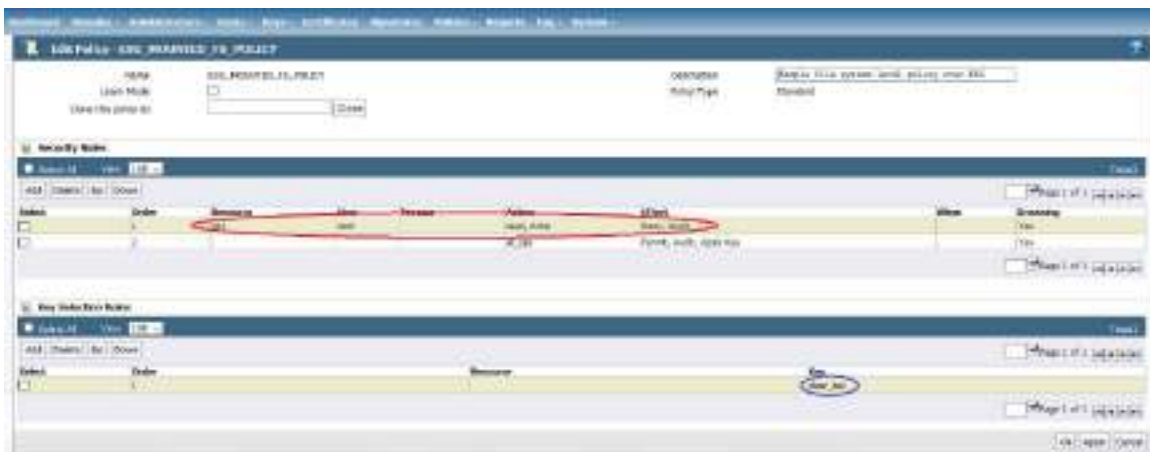
Use Case 3: Directory-Level GuardPoints

Protect structured or unstructured data stored in data files. The data files are organized inside one or multiple directories or folders within a file system namespace, such as ext4 or XFS, where the entire file system namespace is guarded with one policy as a Directory GuardPoint. In this use case, the file system resides in a device guarded as ES GuardPoint. Similar to use case 1, Linux policies supporting this use case can also specify the second key rule with an empty resource set for rekey.

Figure 17-2: All Data in file system Device Encrypted through an ES GuardPoint



In this use case, two policies are enforced to protect the data in the device. As stated, one policy protects the entire file system namespace guarded under the Directory GuardPoint, and the guarded directory is the mount point pathname of the mounted file system. The policy on the mount point directory must specify *clear_key* in the key rule. Specifying a key other than *clear_key* must be avoided because all the data in the file system device is encrypted through the ES GuardPoint corresponding to the file system device. The screen shot below represents a sample Linux policy over the file system mount point where the policy blocks root access to read/write files under the subdirectory *dir1* in the mounted file system.



The second policy protecting the device is the same policy as use case 2.

Example

Below is an example of this use case where a file system created in a guarded device and mounted on */xfs* is protected under a policy that denies root access to the files under */xfs/dir1*:

```
# mount | grep xfs
/dev/secure/dev/ssh on /xfs type xfs (rw,relatime,seclabel,attr1,inode64,noquota)
# find /xfs -xsync
/xfs
/xfs/non-secret
/xfs/dir1
/xfs/dir1/secret
cat /xfs/dir1/secret
this file holds highly sensitive data.
cat /xfs/non-secret
this file does not hold sensitive information.
# secfsd -guard /xfs
secfsd: Path is guarded
# secfsd -status guard | grep ssh
/dev/ssh          ESG_DEMO_POLICY_2      manual:secretview guarded   guarded   N/A

# ls /xfs
dir1 non-secret
cat /xfs/dir1/secret
cat: /xfs/dir1/secret: Permission denied
cat /xfs/non-secret
this file does not hold sensitive information.
```

As depicted above, the root user is denied access to read/write the files associated with the resource set representing files under /xfs/dir1 subdirectory.

Challenges with Root Access on Linux

As demonstrated in the example in use case 3, data is protected at two levels using two separate policies and GuardPoints. The data is encrypted at the device level through the policy on the device guarded as Efficient Storage, and user access controls are enforced at the file system level through the policy on the mount point directory. Splitting the full protection through separate GuardPoints poses new challenges with respect to root privilege on Linux.

With the GuardPoint on the file system mount point enabled, the access rule(s) denying root access is enforced. However, when the GuardPoint on the file system mount point is disabled, root gains full access to the files in the file system. As shown below, the file holding secret information and protected against root is exposed as soon as the GuardPoint on file system mount point is disabled.

```
# secfsd -status guard | grep ESG
/dev/ssh          ESG_DEMO_POLICY_2      manual:secretview guarded   guarded   N/A
/xfs              ESG_MOUNTED_FS_POLICY manual          guarded   guarded   N/A
# cat /xfs/dir1/secret
cat: /xfs/dir1/secret: Permission denied
# secfsd -unguard /xfs
secfsd: Path is not guarded
# cat /xfs/dir1/secret
this file holds highly sensitive data.
```

The next two sections describe the challenges with root access and solutions to overcome these challenges.

Challenge 1 - Deny root access to the files in mounted Linux file system

As the above example shows, the policy ESG_MOUNTED_FS_POLICY denies the root user access to the files associated with the resource set dir1. Enforcement of the rule become ineffective as soon as the GuardPoint on the file system mount point is disabled. Since data is in clear-text at the file system level, root would gain access to clear-text in the files associated with the resource set, which includes files with sensitive information.

The solution to this problem is to force the file system to unmount when the GuardPoint on the file system mount point is disabled. Basically, the file system is guarded/enabled immediately when the file system mounts, and the file system is unmounted as soon as the GuardPoint is disabled. To enforce this, the GuardPoint on the file system mount point directory must be guarded with **Auto Mount** option checked on the DSM. With this option, CTE immediately guards the mount point directory as soon as the file system mounts, and similarly, CTE disables the GuardPoint before unmounting the file system. As shown below, the file system mount point is guarded with **Auto Mount** option checked.



This solution imposes one policy protecting the entire file system namespace. Enforcement of a single policy over entire file system namespace may seem restrictive if you wish to impose different sets of access rules to different directories within the file system name. Basically, your option of enforcing one policy with a set of specific access rules for guarding a specific directory within the mounted file system namespace is not possible with this solution. Instead, you have to create a resource set for each directory, which you would have guarded, and specify the desired access rules specific to the directory through association of the rule with the resource set. Let's see the effect of auto-mount on root user attempts to view files that root users are not allowed to read. As shown below, the GuardPoint `/xfs` is automatically mounted as soon as the file system mounts, and the file system unmounts as soon as the GuardPoint is disabled, hence there is no opportunity for root, or any other privileged user, to read the protected files.

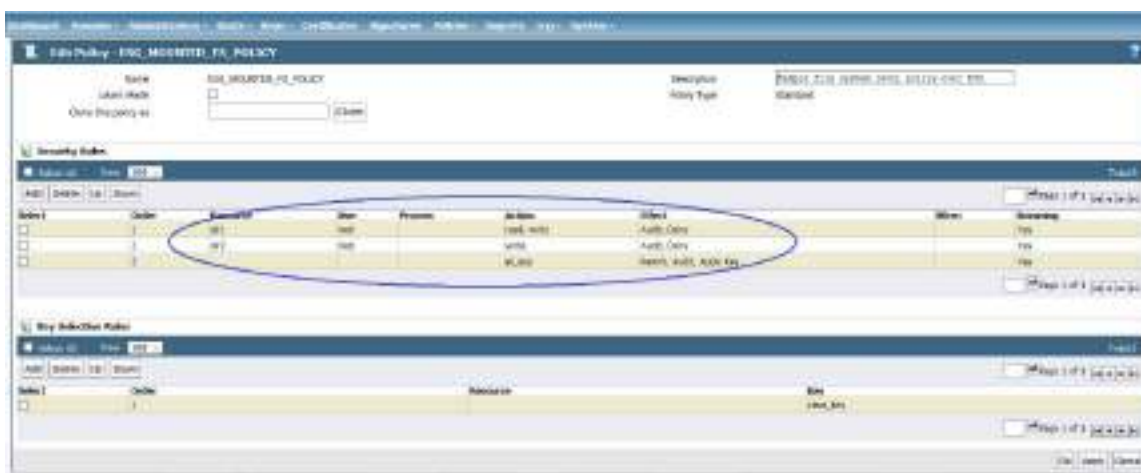
```
# mount -t xfs /dev/sectest/dev/ssh /xfs
# secadm -status guard | grep SSG
/dev/ssh          ESB_DEMO_POLICY_1      mandatorydevice  guarded        guarded        N/A
/xfs              ESB_MOUNTED_FS_POLICY  automount        guarded        guarded        N/A

# cat /xfs/dixl/secret
cat: /xfs/dixl/secret: Permission denied

# umount /xfs
# secadm -status guard | grep SSG
/dev/ssh          ESB_DEMO_POLICY_1      mandatorydevice  guarded        guarded        N/A
/xfs              ESB_MOUNTED_FS_POLICY  automount        guarded        not guarded    inactive

# cat /xfs/dixl/secret
cat: /xfs/dixl/secret: No such file or directory
```

As depicted above, the policy `ESG_MOUNTED_FS_POLICY` enforces a single rule to block root access to the files under the `dir1` subdirectory under the mounted file system GuardPoint. We need to add another security rule to the policy to grant root user access to read the files under `dir2` subdirectory under the guarded file system mount point. Note that `dir1` and `dir2` may have been guarded separately under different policies.



Challenge 2 - Deny root access to view sensitive data in protected Linux files

Another challenge with root user privilege is that root can still view sensitive information stored in the ES GuardPoint device. As explained, the policy `ESG_MOUNTED_FS_POLICY` denies root access to the read/writes files under `/xfs/dir1`. Although this policy enforces the rule on the Directory GuardPoint `/xfs`, the rule is not enforced if the root user dumps the content of the ES GuardPoint. As the example below shows, the root user can view sensitive information in the protected files under `/xfs/dir1`.

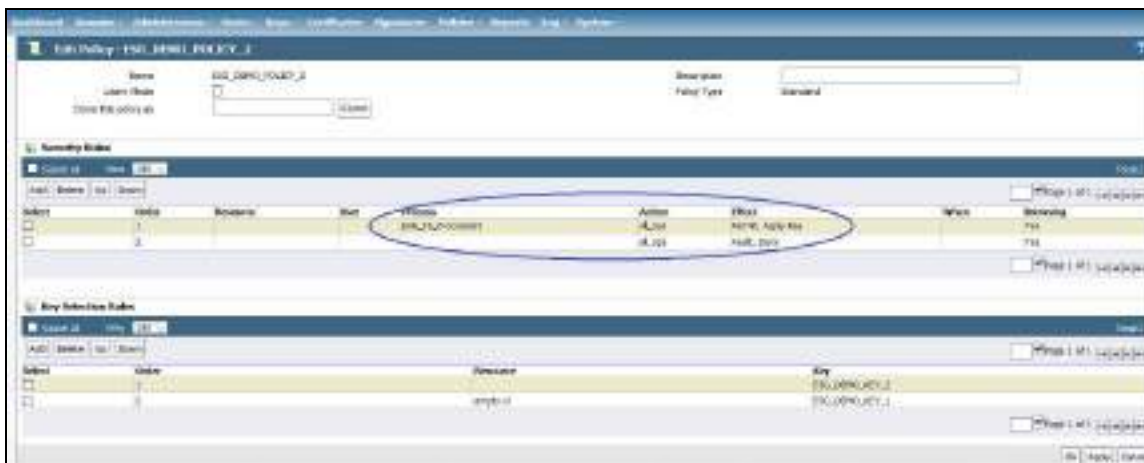
[illegible]

To block the root user from dumping context of the device, the policy on the ES GuardPoint must enforce a security rule that denies root access to the GuardPoint device. However, denying root access to GuardPoint devices is not feasible because file system utilities require root access for file system administration. Rather than enforcing complete denial of root access, you can impose a restriction that allows only a limited set of system utilities to access ES GuardPoints, such as `mount`, `fsck`, `mkfs`, `dmsetup`, etc., and deny access to other utilities, such as `dd`.

The solution is to restrict root to execute a limited set of utilities, which do not expose content of the file system devices, on Efficient Storage Devices. If the root user attempts to execute other utilities on the device, the root user will be denied access. You can impose this restriction by selecting the administrative utilities that root must execute on ES GuardPoints. See ["Linux System Utilities for Signing" on page 191](#) for the list of utilities that root must be able to execute.

To implement this solution, you can create a signature set on your DSM and add the system utilities that root is permitted to execute on ES GuardPoints. Those utilities can be added to the signature set for signing. After signing the binary files of those system utilities, you can add a security rule to the policy on the ES GuardPoint that grants root the right to execute the system utilities in the signature set to access the ES GuardPoint. In the above example, since `dd` is not in the signature set, the `dd` command is denied access to read the file system device guarded as an ES GuardPoint.

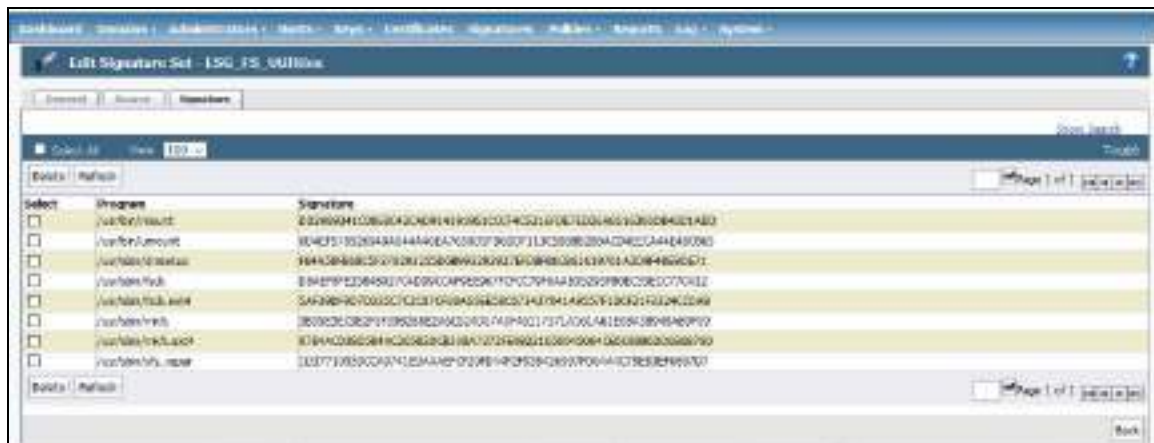
The following screenshot depicts the policy that restricts root access to the ES GuardPoint limited to the system utilities listed in ESG FS ResourceSet.



The resource set `ESG_FS_ResourceSet` consists of the binary files listed in the next screenshot. Let's walk through the steps to add the security rule to limit root access:

1. Select the system utilities that must be granted access to Efficient Storage devices.
2. On the DSM, click on **Signature** in the top menu bar to get to the **Signature Sets** page, and then click **Add** to add a signature set.
3. On the **Add Signature Sets** page, enter the name of the signature set to create and then click on OK. This creates an empty signature set with the name you have selected for the signature set. The name appears on the **Signature Sets** page.
4. On the **Signature Sets** page, click on the name of the signature set to get to the **Edit Signature Set** page to edit your signature set.
5. On the **Edit Signature Set** page, click on the **Source** tab to select the protected host where the file system utilities are located. Click **Select** to select the protected host.
6. Click **Add** to add each system utility from the selected host to the signature set. After adding the system utilities to the set, then click **Sign** to sign the binary files on the selected protected host.

In the example below, the signature set named `ESG_FS_Uutilities` includes sample of file system utilities whose binary files have been signed on the protected host. You may add other system utilities to the set as necessary.



At this point, you have created a signature set consisting of the system utilities that root is allowed to execute on Efficient Storage devices. Next, create a process set from the signature set. The process set will be included in a security rule in the policy protecting the ES GuardPoint. The security rule will allow root or other privileged users to access the device only through the system utilities in the signature set. Continue with the following steps:

1. For Policies in the top menu bar, then click on **Manage Policies**, and then click on **Process Sets** to get to **Process Sets** page.
2. Click **Add** to get to **Add Process Set** page to add a process set.
3. Enter the name of the process set in the **Name** entry and then click **Add** to get to **Add Process** page.
4. Click **Select** next to the **Signature Set** entry to select a signature set. Select the signature set that you just created.

After clicking **Select**, you will be on the **Select Signature Reference** page, and you will see the signature set you just created, for example, the ESG_FS_Utilities signature set. Click on the **Select** button to the left of the signature set and then click on **Select Signature Reference**. You will go back to **Add Process** page with the selected signature set name entered in **Signature Set** box.

- Click **Select** next to the **Host** entry to select the protected host the process set. On the Select a Host to Continue page, select the protected host and then click on **Select**.
- On the **Add Process Set** page, click OK to create the process set associated with the selected signature set and the protected host.
- You have selected the signature set and the protected host. Skip **Directory** and **File** entries, and then click OK to go back to **Add Process Set**.

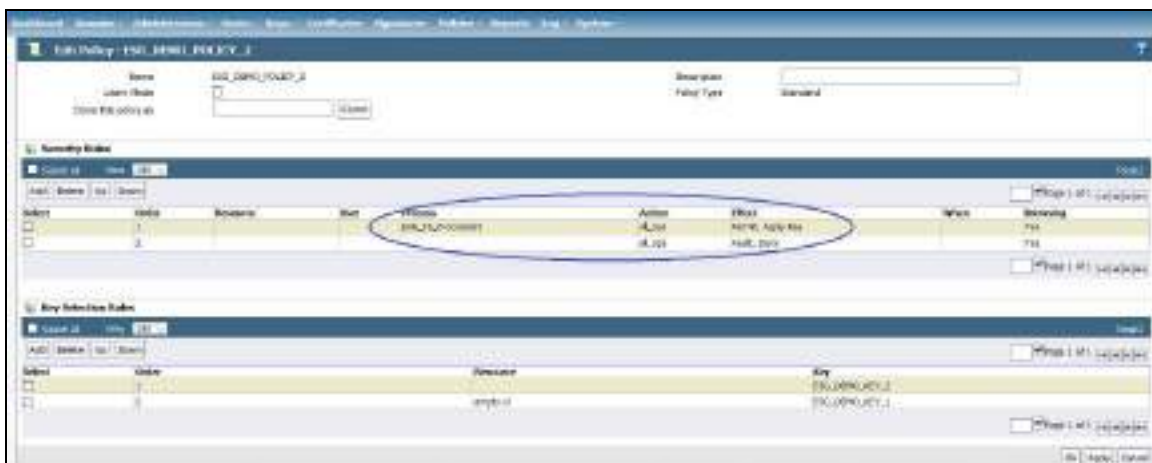
In the following figure, the process set named ESG_FS_ProcessSet has been created using the ESG_FS_Uutilities signature set which includes system utilities whose binary files have been signed on the protected host.



- Edit the policy protecting ES GuardPoints to add a security rule. In the following figure, the process set that you just created is included in the security rule. The rule allows only the processes listed in the process set to access the ES GuardPoints. This rule prevents any privileged user from reading or dumping the content of an ES GuardPoint.



After adding the security rule, the policy protecting ES GuardPoints will be the same policy as ESG_DEMO_POLICY_2.



After applying the revised policy over the ES GuardPoint, root can no longer dump the contents of the device.

```
# cat /etc/passwd | grep ESTP
/dev/sdb      ESTP DEMO POLICY 2      manualraidwrite    unguarded          not guarded       Inactive
/dev/sdc      ESTP MOUNTED_FS_POLICY   automount          guarded            not guarded       Inactive
# cat /etc/guard /dev/sdb:
cat: /etc/guard /dev/sdb: Not a directory
# cat /etc/guard /dev/sdc:
cat: /etc/guard /dev/sdc: Not a directory
# mount -t xfs /dev/sdc00m /dev/sdb /xfs
mount: /dev/sdb: permission denied
cat: /etc/guard /dev/sdb: Not a directory
cat: /etc/guard /dev/sdc: Not a directory
# dd if=/dev/urandom /dev/sdb bs=1048576 && grep --binary-files=text "file holds highly sensitive data"
dd failed to open '/dev/urandom/dev/sdb': Permission denied
```

Use Case 4: Using CTE-Efficient Storage with LVM

Security rules for access control enforcement on I/O operations are based on the context of real users and/or processes requesting the I/O operations. For ESG devices, security rules are checked and enforced at the CTE `secvm` layer. If the context of the real user or process that requested the I/O operation is not available at the `secvm` layer, then the enforcement of access rules is invalid and may have unpredictable results and potentially cause system failures.

The previous use cases have described environments where CTE can get the context of the real users or processes requesting I/O operations at the `secvm` layer and can properly enforce the access rules in those environments. For example, as described in ["Use Case 3: Directory-Level GuardPoints" on page 197](#), CTE can detect when an ESG device is mounted with a file system and it can apply the access rules in the policy on the ESG device without enforcing the rules on I/O operations from the file system layer.

However, there are other environments where CTE cannot determine how the ESG device is actually used and whether a real user or process context is available at the `secvm` layer. In these environments, CTE cannot properly enforce the access control rules on the ESG device. An example of such an environment is Linux LVM (Logical Volume Manager). A physical device under LVM control is a shared storage resource that can be fully or partially allocated to a logical volume. Adding an ESG device as a physical device to LVM is fully supported for data encryption but not for access control enforcement. In this case, access rules cannot be enforced because when the logical volume with file system is mounted, the mount operation is on the logical volume, not the ESG device. Consequently, CTE cannot determine that the ESG device is part of mounted file system, and therefore, it cannot get the real user or process context for applying access rules.

In order to use CTE in an environment like LVM, the CTE system administrator needs to explicitly tell CTE whether or not it should enforce the access rules for I/O operations on the device when they initialize the device using the `voradmin esg config` command. As described in ["Initialize a New Linux Device" on page 182](#), this initialization must be done *before* the device is guarded as an ES GuardPoint for the first time.

In addition, for LVM specifically, the device must be a new device with no existing data. Existing LVM disks cannot be used with CTE unless CTE can get the proper context at the `secvm` layer.

When you initialize the new device, use the `voradmin esg config -noacc new [-c <n>] <device-name>` command where:

- `-noacc` (required) tells CTE to disable access control rules on this device at the `sevm` layer level.
- `new` (required) indicates that the device contains no data (it is a new disk).
- `<device-name>` (required). Specifies the device name. For example, `/dev/sdh`.

For example, if you want to initialize a new LVM Linux disk named `/dev/sdh`, you would specify:

```
# voradmin esg config -noacc new /dev/sdh
```




CAUTION

When you use `-noacc`, CTE will not perform *any* access checks on read/write operations to the specified device, even if the policy for guarding the device includes security rules enforcing read and/or write access checks. Before you use this option, make sure that your environment requires it. You should always use the options described in the first three use cases if at all possible, so that CTE can apply access controls to all I/O operations and therefore perform all required read/write access checks.

The following example shows the steps for initializing and guarding the device `/dev/sdb`, then adding or using the guarded device under LVM to create a file system.

1. Initialize the device using the `-noacc` option:

```
# voradmin esg config -noacc new /dev/sdb
```

2. Guard the device as described in ["Guard the Linux Device with an ES GuardPoint" on page 184](#).

3. Create and mount the file system.

```
# pvcreate /dev/secvm/dev/sdb
# vgcreate secvm_sdb_vg /dev/secvm/dev/sdb
# lvcreate -y -l 100%FREE -n my_volume
# mkfs.xfs /dev/mapper/my_volume
# mount /dev/mapper/my_volume /mnt
```

Alerts and Errors on Linux

This section lists the alerts and errors that may be encountered during system operations.

Encryption key on device has not been made available

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the encryption key specified in the policy for the GuardPoint has not been made available to the protected host.

Solution: Check the host's connectivity with the DSM.

Specified policy disagrees with metadata set on the Guard Path

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the key specified in the policy for the GuardPoint does not match with the key stored in the ES Header.

Solution: Un-guard the device and check the name and UUID of the key in the ES Header using `voradmin esg status <device-name>` and `voradmin esg status xform <device-name>` and, compare the name and UUID with the key name specified in the policy. Correct the discrepancy and re-guard the device.

Device has not been configured for Efficient Storage

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the device has been properly guarded as ES GuardPoint on the DSM but the device has not been initialized for guarding as Efficient Storage.

Solution: The most probable cause of this error is that you did not initialize the device for guarding as Efficient Storage on protected host. It's also possible that the guarded device has already configured for guarding as ES GuardPoint. If the device needs to be initialized for guarding as Efficient Storage, follow the steps to initialize a device for guarding as Efficient Storage.

Device not resized for guarding as Efficient Storage

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the newly guarded ES GuardPoint, which has been initialized with `xform` option of `voradmin`, has not been resized to accommodate storage space for CTE private region.

Solution: Unguard the GuardPoint from the DSM, resize the LUN and verify that the host sees the expanded size, and then guard the GuardPoint from the DSM.

Data transformation failed

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the protected host encountered an error while transforming the data on the device during IDT.

Solution: Consult with the system and/or storage admin to check on the health of the LUN in the storage array. You may contact Thales Support for troubleshooting and recovery if there has not been a report of any error on the LUN.

Data transformation in progress

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the protected host is transforming the data on the device.

Solution: You must wait for data transformation to complete. Check the status of transformation by running `voradmin esg status xform <device name>`. Access to the device is blocked until transformation completes.

Device <device-name> is configured to guard as Efficient Storage GuardPoint

This error message is reported by the `voradmin` command when initializing a device that has already been initialized for guarding as Efficient Storage.

Solution: The device has already been initialized for guarding as Efficient Storage and is probably waiting to be guarded as an ES GuardPoint. Alternatively, if the device was incorrectly initialized for guarding as Efficient Storage, you can remove the configuration by running `voradmin esg delete <device-name>`.

Device <device-name> is configured as Efficient Storage GuardPoint

This error message is reported by the `voradmin` command when initializing a device that is already being guarded as an Efficient Storage GuardPoint.

Solution: None. The device is already an Efficient Storage device.

GuardPoint for device <device-name> still guarded on DSM

This error message is reported by the `voradmin` command when attempting to initialize a device for rekey or removing the device as Efficient Storage.

Solution: Unguard the GuardPoint from the DSM, wait for the protected host to process the update, and then rerun the `voradmin` command.

Failed to open device <device-name>, error Device or resource busy

This message occurs when `voradmin` detects that the target device is busy.

Solution: The device may already be in use by other application. Rerun the `voradmin` command when the device is no longer in use.

Device <device-name> is not configured as Efficient Storage

This error message is reported by the `voradmin` command when attempting to delete a device as ES GuardPoint.

Solution: This message indicates that the target device has been not initialized for guarding as Efficient Storage. The message may also be reported if the specified device has been initialized for guarding as Efficient Storage but it has not been guarded yet. In this case, it removes the preparation made by `voradmin`. You can remove the Efficient Storage configuration status on the device by running `voradmin esg delete <device-name>`. You may see the same error message again, and if you do, you can ignore it.

Abort! Error: Could not stop secfs, secvm device(s) busy

This error occurs during CTE shutdown when there is a busy CTE protected device.

Solution: Verify that all applications directly accessing `secvm` protected GuardPoints have been shut down. Ensure that all file systems on top of a `secvm` protected devices are under the control of `systemd` and have been unmounted before attempting to shut down the agent.

Abort! Error: Could not unmount file systems

This error occurs during CTE shutdown when a file system under the control of `systemd` fails to unmount.

Solution: Verify that file systems on top of an ES GuardPoint devices are not busy and then rerun the agent shut down command.

A dependency job for `esg.mount` failed. See '`journalctl -xe`' for details

This error occurs during CTE startup when system fails to mount a file system. This error message is typically accompanied by a long timeout during the CTE startup process.

Solution: Check that the underlying device is available and that the ES GuardPoint was successfully applied on the device. Once the device is available, the file system will automatically finish mounting.

ESG-ALERT: IO error on header for [GuardPoint]

This is an alert message to the DSM. It occurs when CTE encounters a general error when attempting to access the private region on an Efficient Storage device.

Solution: An I/O error attempting to read or write to the device may have been caused by errors on the host or storage array. Consult with the system and/or storage admin to check on the health of the LUN in the storage array. You may contact Thales Support for troubleshooting and recovery if there has been no report of errors on the LUN.

ESG-ALERT: Data transformation failure on [GuardPoint]

This is an alert message to the DSM. It occurs when protected host encounters an error transforming the data on device during IDT process.

Solution: Please contact Thales Support for troubleshooting and recovery.

ESG-INFO: Data transformation complete on [GuardPoint]

This message is a notification to the DSM admin that the protected host has completed the data transformation of the specified ES GuardPoint.

ESG-ALERT: Failed to resize <device-name>

This alert is a notification to the DSM admin that the protected host has failed to update the change to the device size in the ES Header on the device.

Solution: Please contact Thales Support for troubleshooting and recovery.

FSADM-ALERT: ESG required Signature Set for system utilities may have to be resigned

This alert is a notification to the DSM admin that the recent system upgrade to the protected host may have updated the binary files listed in the signature set for restricting root access.

Solution: Upon this notification you must immediately re-sign the affected or all the binary files to prevent them from accessing protected data. Refer to "[Linux System Utilities for Signing](#)" on page 191.

File System is not automatically mounted after IDT completes

An Efficient Storage device with a file system that has been configured to automatically mount may fail to automatically mount while the device undergoes data transformation through IDT. Following is a sample log message in the kernel ring buffer that reports a failed attempt to access a device during IDT. You can ignore this message.

```
Vormetric SecVM: secvm_map during IDT ((dc 00000000c3537611)
```

When access to a device is to mount the file system, the kernel ring buffer may also report a second error message indicating that a file system failed to mount due to data corruption. You can ignore this message. This occurs because the mount command is issued after the device has been guarded but before data transformation through IDT is complete. While IDT is in progress, the device cannot be used, so any attempt to mount the file system will fail.

Solution: Manually mount the file system after IDT is complete.

Chapter 18: CipherTrust InPlace Data Transformation for Linux

This chapter contains the following sections:

Introduction to CipherTrust InPlace Data Transformation (IDT)	209
Requirements for IDT-Capable GuardPoints	209
The CTE Private Region and IDT Device Header	210
IDT-Capable GuardPoint Encryption Keys	211
Guarding an IDT-Capable Device on Linux	214
Changing the Encryption Key on Linux IDT-Capable Devices	222
Guarding an IDT-Capable Device with Multiple IO Paths on Linux	225
Linux System and IDT-Capable GuardPoint Administration	226
Resizing Guarded IDT Devices	228
Use Cases Involving IDT-Capable GuardPoints	228
Alerts and Errors on Linux	228

Note

Currently, this feature is only supported on the DSM. Support for this feature will be added to CipherTrust Manager in a future release.

Introduction to CipherTrust InPlace Data Transformation (IDT)

CTE offers CipherTrust InPlace Data Transformation (IDT) Capable Device GuardPoints on Linux. IDT-Capable GuardPoints allow you to guard devices by transforming the plain-text data to cipher-text on the host device. The data transformation process is called CipherTrust InPlace Data Transformation (IDT). The term “IDT-Capable” refers to the data transformation capability available on IDT-Capable GuardPoints.

IDT is not the same as the legacy offline data transformation. IDT is a block level data transformation with built-in resiliency to recover from system crashes during the data transformation process. IDT uses the CTE Private Region to manage the entire transformation process (For details, see ["The CTE Private Region and IDT Device Header" on the next page](#)).

IDT partitions the data on a device in segments of 1MB in size and transforms one or multiple segments, up to 60 segments, in parallel. The IDT process preserves existing data in a segment during transformation in the CTE Private Region, and then transforms the data in-place. IDT also maintains the segments undergoing transformation in the CTE Private Region. In the event of system crash, IDT will recover the segments undergoing transformation at the time of crash and then resume the transformation process.

Another advantage of IDT over legacy offline data transformation is that IDT does not require a separate policy for data transformation. Instead, IDT allows you to initialize each device as either a “new device” with no existing data or as an “existing device” with existing data that needs to be transformed. You can then apply any IDT policy to any combination of new and existing devices and IDT will immediately guard the new devices while starting the IDT transformation process on the existing devices. New devices are immediately available for use while existing devices are inaccessible until the IDT process completes and all data has been converted from plain-text to cipher-text.

Requirements for IDT-Capable GuardPoints

- IDT-Capable GuardPoints are available for Linux with CTE 6.3.1 or later. They also require DSM version 6.4.2 or later.

- The host server must use the Advanced Encryption Standard instruction set (AES-NI).
- The DSM policy assigned to the IDT-Capable GuardPoint must be of type “In-place Data Transformation - Device” and use an XTS-AES 256 encryption key.
- In order to create an IDT-Capable GuardPoint on a raw device, the device must be either:
 - Exported from an external storage system to the host device.
 - On a locally-attached disk.
- Devices protected by an IDT-Capable GuardPoint cannot currently be initialized/added as physical volumes for use by LVM. When LVM support is added, it will be announced in the CTE Release Notes.
- Existing devices divided into one or more logical partitions *cannot* be guarded as IDT-Capable Device GuardPoints. Logical partitions in such devices cannot be accessed or separately guarded after guarding the device.

For example, the logical partition `/dev/sda1` or `/dev/sda2` inside `/dev/sda` cannot be accessed after guarding `/dev/sda` as IDT-Capable GuardPoint. Using `/dev/securem/dev/sda1` is invalid as `/dev/securem/dev/sda1` is not a GuardPoint and cannot be guarded, and, as such, would not provide access to clear-text data on `/dev/sda1`. However, you can guard individual partitions, such as `/dev/sda1` or `/dev/sda2`, as IDT-Capable GuardPoints without guarding the entire `/dev/sda` device.

The CTE Private Region and IDT Device Header

IDT-Capable GuardPoints require a small amount of disk space in the standard CTE Private Region. The reserved space is where CTE stores metadata information to identify IDT-Capable GuardPoints and to perform all data transformation and rekey operations in a resilient manner to avoid data loss or integrity issues due to system failures. The IDT-specific reserved space within the CTE Private Region is known as the IDT Device Header. By default, when you initialize a device as an IDT-Capable GuardPoint, CTE reserves 63 MB of space starting at the first sector on the device for the CTE Private Region.

CTE writes the IDT Device Header into the CTE Private Region when the device is guarded for the first time. If there is existing data on the device, the data at the start of the device is relocated to the available free space on the device and CTE creates the CTE Private Region starting at the first sector. For details, see ["Initialize a Linux Device with Existing Data" on page 216](#).

CTE Private Region Location

Normally, CTE requires that the CTE Private Region be embedded at the beginning of the device. IDT, however, allows you to specify that the CTE Private Region for an IDT-Capable GuardPoint should be located in a central CTE metadata directory on the host called `/vte/vte-metadata-dir` (default: `/opt/vte/vte-metadata-dir`). If you use this option, CTE stores the CTE Private Region and IDT Device Header for the device in this directory. The location of the CTE Private Region for a device is determined when you first initialize the device as an IDT-Capable GuardPoint. For details, see ["Initializing an IDT-Capable Device" on page 215](#).



WARNING

Access to the CTE metadata directory is local to the CTE protected host. Devices whose access is shared across multiple CTE protected hosts in a cluster *must* be configured with the CTE Private Region embedded in those devices. Using a centralized metadata directory for shared devices will lead data corruption.

The location of the CTE Private Region does not affect CTE's functionality, but there are some considerations if you choose to use the centralized metadata directory `/vte/vte-metadata-dir`:

- Thales recommends that you keep the metadata for the device on the device if at all possible. You should only use the centralized metadata directory if the device cannot be expanded to accommodate the CTE Private Region.
- The centralized CTE metadata directory must be guarded by the DSM Administrator to prevent accidental modification or deletion of the CTE metadata. If the CTE metadata directory is not guarded, any attempt to configure or enable an IDT-Capable GuardPoint using the centralized metadata directory will be rejected. The policy associated with the metadata directory must:
 - Deny all users (including the root user) the ability to modify or remove any files in the metadata directory.
 - Use the key rule `clear_key` so that the metadata is stored in clear text.
- You must back up this directory whenever you back up a device that uses the directory. You will not be able to restore a protected device without access to its corresponding metadata in `/vte/vte-metadata-dir`.
- Devices with existing data do not need to be resized to accommodate the CTE Private Region, so there are no disk size discrepancies between system utilities such as `fdisk` and any other applications. However, Thales still recommends that you do not shrink an IDT-Capable GuardPoint even if the CTE Private Region is not embedded on the device.

Device Size

If you embed the CTE Private Region on the device itself, after configuring and guarding the IDT-Capable GuardPoint on the device, the device size reported to applications is the size of the device minus the space reserved for the CTE Private Region. This can lead to a discrepancy between the disk size reported by some applications versus the size reported by system utilities such as `fdisk`.



WARNING

Do not shrink IDT-Capable GuardPoints. Due to the relocation of user data from the CTE Private Region, if you shrink the device, you may corrupt data on the device.

The IDT Device Header contains both the available device size and the size of the CTE Private Region. To view the IDT Device Header, use the `voradmin idt status <device-name>` command. The **Exported Disk Size** field shows the disk size available for use by other applications. The **Private Region Size** field shows the disk size reserved for CTE. For example:

```
# voradmin idt status /dev/sdc2
IDT Header on /dev/secvm/dev/sdc2
    Version: 1
    Change: 0
    Private Region Size: 129024 sectors
    Exported Device Size: 9627648 sectors
    Key UUID: 9cc3c8e4-7ea7-310f-85c7-6f911de1ab52
    Mount Path: None
```

The `voradmin idt status` command also reports the UUID of the XTS-AES 256 key applied to the device.

IDT-Capable GuardPoint Encryption Keys

IDT-Capable GuardPoints must be encrypted using XTS-AES 256 keys. An XTS-AES 256 type key is a 512-bit key composed of two components:

- The first 256 bits of the key is the AES 256 encryption key component.
- The second 256 bits is the tweak component.

You create XTS keys on the DSM using the "Add Agent Key" function.

Note

When you create agent keys for IDT-Capable GuardPoints, you do not need to check the "KMIP Accessible" box on the "Add Agent Key" page. If you do check the KMIP Accessible option, the IDT-Capable GuardPoint ignores this setting.

The DSM generates a UUID, along with other relevant attributes, for each newly-added key. The DSM then provides the key and its attributes to the CTE protected host when the policy containing the key is pushed to the host device. CTE stores the key and its attributes, including the key's UUID, in the IDT Device Header. The first time a device is guarded as IDT-Capable GuardPoint, CTE writes the IDT Header on the device before data transformation takes place, if data transformation is required.

Key Attributes - Example

The following figure illustrates the parameters you should specify to add a new XTS-AES 256 key named IDT_DEMO_KEY_1. Note the algorithm and encryption mode specified for the key.

The screenshot shows the 'Add Agent Key' dialog box with the 'Symmetric' tab selected. The configuration is as follows:

Field	Value
Name	IDT_DEMO_KEY_1
Description	Initial key for IDT
Template	[Dropdown menu]
Expiration Date	12/31/2020
Algorithm	AES256
Encryption Mode - for VTE agents only	XTS
KMIP Accessible	☐
Key Type	Cached on Host
Unique to Host	☐
Key Creation Method	Generate
Key Refresh Period - for VAE keys only (minutes)	18000
Automatic Key Rotation	☐

Buttons: OK, Cancel

The following figure illustrates the general properties of IDT_DEMO_KEY_1 after adding the key. Note the UUID of the key. This UUID is stored in the IDT Device Header on all devices encrypted with this key, allowing you to verify which key is being used on each device.

Edit Agent Key	
General	
Name	IDT_DEMO_KEY_1
UUID	9cc3c8e4-7ea7-31f1-85c7-8f911de1ab52
Source	From DSM
Description	Initial Key for IDT
Creation Date	5/14/20
Expiration Date	12/31/2020
Algorithm	AES256
Encryption Mode - for VTE agents only	XTS
KMIP Accessible	☐
Key Type	Cached on Host
Unique to Host	☐
Key Refresh Period - for VMS keys only (minutes)	10080

Policy Requirements for IDT-Capable GuardPoints

IDT-Capable GuardPoints require a policy of type **In-place Data Transformation - Device** with a single key rule specifying the key names for **Current Key** and **New Key**. The **Current Key** name is `clear_key` or an XTS-AES 256 key name, depending on whether the data on the device has already been encrypted.

- If there is no existing data on the device or if the existing data on the device has not yet been encrypted, specify `clear_key` for **Current Key**. In the **New Key** field, specify the name of the XTS-AES 256 key that you want to use to encrypt the data on the device.
- If the existing data on the device has already been encrypted, specify the name of the key used to encrypt the data in the **Current Key** field and the name of the new XTS-AES 256 key you want to use to rekey the data in the **New Key** field. When the policy is pushed to the host, CTE will rekey the data on the device using the key specified in **New Key**. In other words, the **New Key** field specifies the XTS-AES 256 production key name to apply to device.

In all cases, the **New Key** field specifies the XTS-AES 256 production key name that you want to use to encrypt the data on the device. After you guard an existing device with an In-place Data Transformation - Device policy, CTE transforms the existing data using the New Key. When the process is finished, the New Key becomes the Current Key for that device, and all data will be encrypted or decrypted with that key. The IDT Device Header contains the UUID of the key currently being used to encrypt/decrypt data on the device. To view the current key UUID, use the `voradmin idt status <device-name>` command.

You may add security rules to restrict certain user/process access to protected devices. For suggestions, see ["Use Cases Involving IDT-Capable GuardPoints" on page 228](#).

The following figure shows an example of a simple policy named `IDT_DEMO_POLICY_1` with policy type "In-place Data Transformation - Device", a simple security rule that permits access to all users and programs, and that uses `clear_key` as the current key and `IDT_DEMO_KEY_1` as the key to encrypt the data on any device associated with this policy.

Add Policy - IDT_DEMO_POLICY_1

Policy Type: **In-place Data Transformation - Device**

Name: IDT_DEMO_POLICY_1

Description: Initial Policy for IDT-Capable GuardPoints

Learn Mode: ☐

Clone this policy as: **Clone**

Security Rules

Select All View: 20 Total: 1

Add Delete Up Down

Select	Order	Resource	User	Process	Action	Effect	When	Browsing
☐	1				all_ops	Apply Key, Audit, Permit		Yes

Page 1 of 1

Key Selection Rules

Select All View: 20 Total: 1

Add Delete

Select	Order	Current Key	New Key
☐	1	clear_key	IDT_DEMO_KEY_1

Page 1 of 1

Ok Apply Cancel

Guarding an IDT-Capable Device on Linux

In order to guard an IDT-Capable device, you need to:

1. Make sure the devices you intend to guard meet the requirements for IDT-Capable GuardPoints. For details, see ["Requirements for IDT-Capable GuardPoints" on page 209](#).
2. Install the CTE Agent and register the host with the DSM if it is not already registered. IDT does not require any special registration options or licenses. For details, see the *CTE Agent for Linux Quick Start Guide*.
3. Initialize the device using the `voradmin idt config [new|xform]` command to specify whether there is any existing data on this device that needs to be encrypted and to configure the location of the CTE Private Region. For details, see ["Initializing an IDT-Capable Device" on the facing page](#).
4. Log on to the DSM to apply an IDT-Capable GuardPoint to the device. For details, see ["Guard the Linux Device with an IDT-Capable GuardPoint" on page 218](#).



WARNING

For devices with shared access across multiple CTE Protected hosts in a cluster, you must designate one and only one of the nodes in the cluster as the node on which you plan to initialize and guard the device for the first time. The designated node must be the only one that accesses the device until the entire initial data transformation process has completed. This requires guarding each shared device at the designated host level rather than at the host group level if you are using a host group to manage the CTE Protected nodes in your cluster. DO NOT initialize or guard any device on multiple nodes in the cluster simultaneously, because multiple nodes attempting to transform the same data can corrupt the data on the entire device.

Initializing an IDT-Capable Device

When you initialize an IDT-Capable storage device, the process specifies:

- Whether there is existing data on the device that needs to be encrypted.
- Where you want to store the CTE Private Region, which contains the IDT Device Header along with metadata that identifies the IDT-Capable device as a guarded device. You can embed the CTE Private Region on the device itself or in the central CTE metadata directory on the host. (For details, see ["The CTE Private Region and IDT Device Header" on page 210.](#))

How you initialize the device depends on whether it is a new device or an existing device that already has data that needs to be transformed into cipher-text. For details, see:

- ["Initialize a New Linux Device" below](#)
- ["Initialize a Linux Device with Existing Data" on the next page](#)

Initialize a New Linux Device

Run the `voradmin idt config new` command to initialize a new device. The `new` option specifies that the device does not hold user data so no initial data transformation is required. For a shared device that is accessed from multiple protected hosts, you must initialize the device only once and on only one protected host.

Note

To configure devices with multiple IO paths for Linux, see ["Changing the Encryption Key on Linux IDT-Capable Devices" on page 222.](#)

1. Log into the device as `root`.
2. Run the `voradmin idt config [-external] new [-c <n>] <device-name>` command, where:
 - `-external` is an optional parameter that tells CTE you want to use the centralized CTE metadata directory instead of embedding the CTE Private Region on the device itself. If you use this option, you must have configured and guarded the centralized CTE metadata directory as described in ["CTE Private RegionLocation" on page 210](#).
 - `new` (required) indicates that the device contains no data (it is a new disk). As soon as you push the IDT policy from the DSM, the device will be available as a guarded IDT-Capable GuardPoint.
 - `-c <n>` (optional). If you use this option, CTE sets the number of data transformation jobs to run in parallel to the number specified in `<n>`. `<n>` can be an integer between 1 and 60 (default: 8).

Each data transformation job transforms 1MB worth of data and requires CPU resources in addition to three I/O operations as part of data transformation. Each job reads 1MB of data from the device, preserves the data in the CTE Private Region, rekeys the data to cipher-text, and writes the transformed data to the device. If you increase the number of parallel jobs, the data transformation process will complete faster but there will be an increased performance impact on the system. Only increase the `-c` option if you are certain that the system resources are available to handle the additional load.

The value for the `-c` option you specify here remains in effect for all subsequent data transformations (such as any data rekeys) until you specify a new value.
 - `<device-name>` (required). Specifies the device name. For example, `/dev/sdc2`.

For example, if you want to initialize a new Linux disk named `/dev/sdc2` using 10 parallel data transformation jobs with the CTE Private Region embedded on the device, you would specify:

```
# voradmin idt config new -c 10 /dev/sdc2
```

If you want to initialize a new Linux disk named `/dev/sdc2` using the default number of parallel data transformations but with the CTE Private Region in the centralized CTE metadata directory, you would specify:

```
# voradmin idt config -external new /dev/sdc2
```

3. To verify that the disk has been initialized, run the `voradmin idt status` command.

```
# voradmin idt status /dev/sdc2
```

Device `/dev/sdc2` is configured to guard as IDT-Capable GuardPoint
4. At this point the DSM Administrator can protect the device as an IDT-Capable GuardPoint through the DSM Management Console. For details, see ["Guard the Linux Device with an IDT-Capable GuardPoint" on page 218](#).

Note

The initialization process prepares the device to be guarded but does not actually guard it. You need to assign an IDT-Capable GuardPoint to the device in the DSM before the device is actually protected.

Initialize a Linux Device with Existing Data

If the device has existing data, you need to use the `voradmin idt config xform` command to initialize the disk for CTE. Unless you are using the centralized CTE metadata directory, this command examines the current disk size and computes the size required to hold the existing data plus the CTE Private Region at the beginning of the device. After the CTE initialization is complete, you then need to resize the device before you can guard it with an IDT-Capable GuardPoint.



WARNING

If access to the device is shared access across multiple CTE Protected hosts in a cluster, be sure to initialize the device on one and only one of the CTE hosts.

The following procedure describes how to initialize the device for CTE. Note that the existing data is not altered in any way until after you perform this procedure and you guard the data with an IDT-Capable GuardPoint. CTE does *not* begin transforming the data from clear-text to cipher-text until the IDT-Capable GuardPoint has been applied and the encryption key has been pushed to the device through the GuardPoint Policy.

1. Log into the device as `root`.
2. Run the `voradmin idt config [-external] xform [-c <n>] <device-name>` command, where:
 - `-external` is an optional parameter that tells CTE you want to use the centralized CTE metadata directory instead of embedding the CTE Private Region on the device itself. If you use this option, you will not have to resize the device but you must have configured and guarded the centralized CTE metadata directory as described in "[CTE Private RegionLocation](#)" on page 210.
 - `xform` (required) indicates that the device contains existing data. CTE will transform all existing data on the device from clear-text to cipher-text as soon as you guard the device. The device will be inaccessible until the transformation is complete, and the device must remain offline during the entire transformation process. No user access will be permitted until all data has been transformed.
 - `-c <n>` (optional). If you use this option on Linux, CTE sets the number of data transformation jobs to run in parallel to the number specified in `<n>`. `<n>` can be an integer between 1 and 60 (default: 8).

Each data transformation job transforms 1MB worth of data and requires CPU resources in addition to three I/O operations as part of data transformation. Each job reads 1MB of data from the device, preserves the data in the CTE Private Region, rekeys the data to cipher-text, and writes the transformed data to the device. If you increase the number of parallel jobs, the data transformation process will complete faster but there will be an increased performance impact on the system. Only increase the `-c` option if you are certain that the system resources are available to handle the additional load.

The value for the `-c` option you specify here remains in effect for all subsequent data transformations (such as any data rekeys) until you specify a new value.

- `<device-name>` (required). Specifies the device name. For example, `/dev/sdc3`.

For example, if you want to initialize an existing Linux disk named `/dev/sdc3` using 10 parallel data transformation jobs with the CTE Private Region embedded on the device, you would specify:

```
# voradmin idt config xform -c 10 /dev/sdc3
```

Device `/dev/sdc3` must be resized to at least 9893888 sectors (4831 MBs) before guarding as IDT-Capable GuardPoint

In this case you must manually resize the Linux disk by at least 9893888 sectors before you can guard it. After you guard the disk, you can expand it again later but you cannot shrink it unless you remove the GuardPoint.

If you want to initialize the same device using the centralized CTE metadata directory, you would specify:

```
# voradmin idt config xform -external -c 10 /dev/sdc3
```

Note that you do not get a message about resizing the device because the CTE Private Region will not be embedded on the device.

3. To verify that the disk has been initialized, run the `voradmin idt status` command.

```
# voradmin idt status /dev/sdc3
```

Device `/dev/sdh` is configured to guard as an IDT-Capable GuardPoint

4. If you are embedding the CTE Private Region on the device, at this point, you need to resize the device using your standard disk management tools before you can guard it. Make sure you increase the device size by at least the amount shown in the `voradmin idt config xform message`.

You cannot assign an IDT-Capable GuardPoint to the device until it has been resized. If you do not resize the device, the GuardPoint assignment will fail.

5. After the device has been resized or the centralized CTE metadata directory has been configured and guarded, the DSM Administrator can protect the device as an IDT-Capable GuardPoint through the DSM Management Console as described in ["Guard the Linux Device with an IDT-Capable GuardPoint" below](#).

Note

The initialization process prepares the device to be guarded but does not actually guard it. You need to assign an IDT-Capable GuardPoint to the device in the DSM before the device is actually protected. In addition, the initialization process is only kept in memory until the device is guarded or rebooted. If the device is rebooted before you guard it, you will need to perform the initialization procedure again.

Guard the Linux Device with an IDT-Capable GuardPoint

Note

For details about how to create a GuardPoint, see the chapter, "Managing GuardPoints", in the *DSM Administration Guide*.

After the device has been initialized, you can guard the device as an IDT-Capable GuardPoint from the DSM Management Console. For existing devices, as soon as the GuardPoint configuration has been pushed to the host and the status changes to guarded, CTE begins transforming the data on the disk using the encryption key associated with the GuardPoint Policy.



WARNING

If access to the device is shared access across multiple CTE Protected hosts in a cluster, be sure to guard the device on one and only one of the CTE hosts.

1. Log on to the DSM Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.
2. Make sure that you know what Policy you want to associate with the GuardPoint or create a new **In-place Data Transformation - Device** policy if needed. The policy you use for IDT must use an XTS-AES 256 key as the key rule. For details, see ["IDT-Capable GuardPoint Encryption Keys" on page 211](#).
3. Select **Hosts > Hosts** on the menu bar. The *Hosts* window opens.
4. Click the target host in the **Host Name** column. The Edit Host window opens to the General tab for the selected host.
5. Click the **GuardPoints** tab and then click **Guard**. The Guard window opens.
6. In the **Policy** field, select the In-place Data Transformation - Device policy you identified or created earlier in this procedure. CTE will use the XTS-AES 256 key associated with this policy to encrypt the data on the device.

7. In the **Type** field, select either **Raw or Block Device (Auto Guard)** or **Raw or Block Device (Manual Guard)**.

If you select **Auto Guard**, CTE starts the guard process as soon as the policy is pushed to the host. You enable, disable, guard, and unguard the GuardPoint in the DSM. If you want to have the device automatically guarded and mounted at system start up, add the device to `/etc/fstab`. For details, see ["Auto Mount Options for File System Devices on Linux" on page 226](#).

If you select **Manual Guard**, You guard the GuardPoint on the protected host with the `secfsd -guard <path>` command and unguard it with the `secfsd -unguard <path>` command. At system startup, you must guard the device and then mount it. This gives you more control over when data transformations occur because CTE will not start encrypting or rekeying the device until you manually start the process.

8. In the **Path** field, add the path for the device you want to guard. For example, `/dev/sdc2` and `/dev/sdc3`.

If you specify multiple paths in this field, all specified devices will be guarded and all will be encrypted with the encryption key specified in the associated policy.

The devices you specify here must already have been initialized as described in ["Initializing an IDT-Capable Device" on page 215](#). They can be new devices, devices with existing data, or a mix of both.

9. Make sure the **In-place Data Transformation - Device** check box is checked. If this option is not selected, the host will *not* enable the device as an IDT-Capable GuardPoint.



10. Click **OK**.

The DSM pushes the policy and the IDT-Capable GuardPoint configuration to the host and the CTE Agent on the host writes the IDT Device Header into the CTE Private Region for the specified devices. If this is a new device, the status changes to guarded and the disk is available for user access immediately.

If there is existing data on the device, CTE begins transforming the data from clear-text to cipher-text as soon as the IDT-Capable GuardPoint configuration is available and the device status changes to guarded. The device will remain inaccessible until this data transformation completes. The length of time required to transform the data depends on the amount of existing data and the number of parallel data transformation jobs specified on the `voradmin config` command. For details, see ["Data Relocation and Transformation on Existing Linux Devices" on the next page](#).

To see the data transformation progress, use the `voradmin idt xform status <device-name>` command, as described in ["Viewing Device Status and the IDT Device Header" on page 225](#).

After the device is initialized and guarded, the protected device must be accessed through the CTE device pathname. This pathname corresponds to the `secvm` device. For example, the Linux device pathname `/dev/sdc2` becomes `/dev/secvm/dev/sdc2` as soon as the process is complete.

Notes

- Be sure to use the secvm device name when using file system management tools such as `mkfs` and `fsck`.
- Do not use the device mapper names corresponding to IDT-Capable GuardPoints for GuardPoint administration on protected hosts.

Data Relocation and Transformation on Existing Linux Devices

When you add an IDT-Capable GuardPoint to a device that has been initialized with the `voradmin idt xform` command and you opted to embedded the CTE Private Region on the device, CTE first relocates existing data in the region of the device designated as CTE Private Region. The data is relocated to the end of the device, into the new space allocated when you resized the device. The relocation occurs once when the device is guarded for the first time. No relocation is necessary for subsequent rekeys on the device.

Relocation of data is transparent to applications accessing data through the IDT-Capable GuardPoint. CTE will map application I/O requests over the private region to the relocated region. After guarding the device, you can grow the device size further if necessary. However, you cannot shrink the device size.

IDT does not require a separate policy for data transformation. If you initialized the device with the `xform` option, CTE starts the IDT process when transformation is required. During the IDT process, access to the device is blocked until the IDT process completes and all the data on the device has been encrypted.

```
# voradmin idt status xform /dev/sdc3
Status:          In-Process
                Relocation Zone 9764864 (relocated = 1)
                SegSpc 27, Xformation Range: 3217 ... 4799, SegIDs: 4795 4796 4791 4792 4797 4798
4799
                KeyID:          2793      Key Name:      IDT_DEMO_KEY_1
                Old KeyID:       0         Old Key Name: clear_key

# dd if=/dev/secvm/dev/sdc3 of=/dev/null bs=512 count=1
dd: failed to open 'dev/secvm/dev/sdc3': Resource temporarily unavailable

# voradmin idt status xform /dev/sdc3
Status:          Complete
                Relocation Zone 9764864 (relocated = 1)
                SegSpc 27, Xformation Range: 3217 ... 20189, SegIDs: none
                KeyID:          2793      Key Name:      IDT_DEMO_KEY_1
                Old KeyID:       0         Old Key Name: clear_key

# dd if=/dev/secvm/dev/sdc3 of=/dev/null bs=512 count=1
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.000989039 s, 518 kB/s
```

Thin-Provisioned Devices

IDT skips transforming thin-provisioned regions of a device. Data returned to IDT as sequence of clear-text zeros, in sector size granularity, is indication of possible sparse or un-allocated regions of the device that do not have to be transformed.

IDT Recovery From Crash

IDT is fault tolerant in the event of system crashes. IDT keeps track of the transformation process over the entire device. In the event of a crash, IDT will automatically resume transformation from the point of failure as soon the GuardPoint is enabled after system startup.

If you find the transformation status set to **In-Progress** when the GuardPoint is not enabled, the **In-Progress** state reflects an earlier system crash after which the GuardPoint has not been enabled to recover from the interruption in the IDT process.

Example of Creating an IDT-Capable GuardPoint on an Existing Linux Device

The following example shows the process of initializing an existing Linux device using `voradmin idt config xform` and guarding it as an IDT-Capable GuardPoint from the viewpoint of the Linux root user. In this example, all files in `/bin/*` are copied to a temporary location outside the device, then compared with the corresponding files on the device after the device has been resized and encrypted. The comparison proves that the file system is unchanged after the encryption process has completed.

First, we verify that the device is not protected, then we check the current size of the disk and create the copy of the files in `/bin/*`. After that, we run the `voradmin idt config xform` command to initialize the device.

```
# voradmin idt status /dev/sdc1
Device /dev/sdc1 is not configured as IDT-Capable
# fdisk -l /dev/sdc1
Disk /dev/sdc1: 21.1 GiB, 21103640576 bytes, 41218048 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes
# mkfs.xfs /dev/sdc1
meta-data=/dev/sdc1             isize=256    agcount=4, agsize=1288064 blks
      =                       sectsz=512    attr=2, projid32bit=1
      =                       crc=0        finobt=0, sparse=0
data      =                       bsize=4096   blocks=5152256, imaxpct=25
      =                       sunit=0      swidth=0 blks
naming    =version 2           bsize=4096   ascii-ci=0 ftype=1
log       =internal log       bsize=4096   blocks=2560, version=2
      =                       sectsz=512    sunit=0 blks, lazy-count=1
realtime  =none               extsz=4096   blocks=0, rtextents=0
# mount -t xfs /dev/sdc1 /xfs
# cp /bin/* xfs
# voradmin idt config xform /dev/sdc1
Device /dev/sdc1 must be resized to at least 41347072 sectors (40378 MBs) before guarding
as IDT-Capable GuardPoint
```

At this point, you need to resize the device using your device management tools. You must increase the size by at least 41347072 sectors (40378 MBs). After the device has been resized, you can verify the new size:

```
# fdisk -l /dev/sdc1
Disk /dev/sdc1: 21.2 GiB, 21169700864 bytes, 41347072 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes
```

After the device has been resized, the DSM Administrator can guard the device with the desired In-place Data Transformation - Device policy. If the DSM Administrator chooses Auto Guard, data transformation begins as soon as the policy is pushed to the host. If the DSM Administrator chooses Manual Guard, data transformation does not begin until the Linux root user initiates it with the `secfsd -guard` command. Once data transformation begins, the Linux root user can check the progress using the `voradmin idt status xform` command.

```
# secfsd -guard /dev/sdc1
secfsd: Path is guarded
# voradmin idt status xform /dev/sdc1
Status:          In-Process
Relocation Zone 9764864 (relocated = 1)
SegSpc 27, Xformation Range: 3217 ... 4799, SegIDs: 4795 4796 4791 4792 4797 4798
```

4799

```
KeyID:          2793      Key Name:      IDT_DEMO_KEY_1
Old KeyID:      0         Old Key Name:  clear_key
```

After the status has changed to completed, you can compare the current version of the files in `/bin/*` with the ones you copied earlier.

```
# voradmin idt status xform /dev/sdc1
Status:          Complete
Relocation Zone  9764864 (relocated = 1)
SegSpc 27, Xformation Range: 3217 ... 20189, SegIDs: none
KeyID:          2793      Key Name:      IDT_DEMO_KEY_1
Old KeyID:      0         Old Key Name:  clear_key

# voradmin idt status /dev/sdc1
IDT Header on /dev/secvm/dev/sdc1
Version:          1
Change:          0
Private Region Size: 129024 sectors
Exported Device Size: 41218048 sectors
Key UUID:        9cc3c8e4-7ea7-310f-85c7-6f911de1ab52
Mount Path:      None

# mount -t xfs /dev/secvm/dev/sdc1 /xfs
# for file in '/bin/ls /sfx'; do cmp /bin/$file /xfs/$file; done
# umount /xfs
```

Changing the Encryption Key on Linux IDT-Capable Devices

To meet various compliance requirements, you may want to change the key that CTE has used to encrypt IDT-Capable GuardPoints. Thales refers to this changing of encryption keys as “Key rotation” or “Rekey”. Unlike the Live Data Transformation product offered by Thales for file systems on traditional storage devices, to change the encryption key on an IDT-Capable GuardPoint, the device must be taken offline. The data on the device will be inaccessible during the key rotation process.



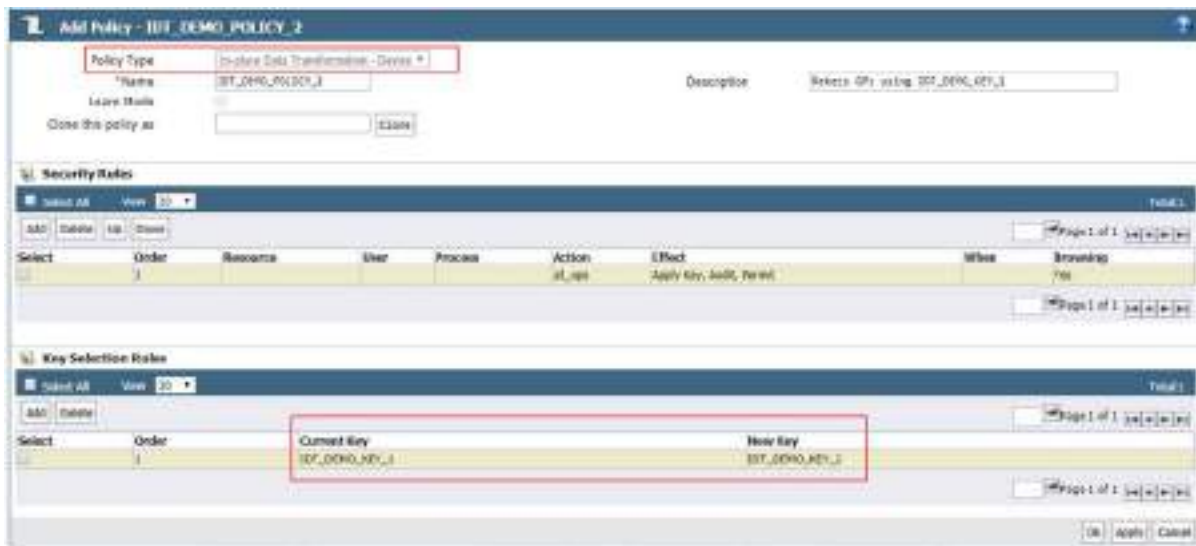
WARNING

For devices with shared access across multiple CTE Protected hosts in a cluster, you must designate one and only one of the nodes in the cluster as the node on which you plan to initialize and guard the device for rekey. The designated node must be the only one that accesses the device until the entire rekey process has completed. This requires guarding each shared device at the designated host level rather than at the host group level if you are using a host group to manage the CTE Protected nodes in your cluster. DO NOT initialize or guard any device on multiple nodes in the cluster simultaneously, because multiple nodes attempting to transform the same data can corrupt the data on the entire device.

1. Log on to the DSM Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.
2. Make sure that you know what Policy you want to associate with the GuardPoint or create a new **In-place Data Transformation - Device** policy if needed. The key rule must specify the current XTS-AES 256 key that the GuardPoint is currently using as well as the new XTS-AES 256 key that you want to use to transform the protected data.

You can either create a new In-place Data Transformation - Device policy or you can change the keys assigned to an existing In-place Data Transformation - Device policy. If you use an existing policy however, the new key you specify cannot have been previously used to encrypt the IDT-Capable GuardPoint. If you want to rekey the GuardPoint using a previously-used key, you must create a new policy in order to do so.

The following screenshot shows a policy named IDT_DEMO_POLICY_2 for rekey that uses IDT_DEMO_KEY_1 as the current key and IDT_DEMO_KEY_2 as the new key:



Including both the current key and the new key in the policy ensures that both keys will be available during the rekey process, even if something happens and the key information in stored in the CTE Private Region becomes unavailable.

Do not push this policy to the host yet.

3. Shut down any applications accessing the GuardPoint you are planning to rekey. If the GuardPoint is mounted as a file system, you must also unmount the file system.
4. Once the data can no longer being accessed, you can unguard the GuardPoint on the DSM.
 - a. If the GuardPoint is a manual device GuardPoint, you must first unguard it using the `secfsd -unguard` command on the CTE host before you unguard it on the DSM. If it is an automatic GuardPoint, you can skip this step and simply unguard the GuardPoint in the DSM.

The following example checks the guard status of `/dev/sdc1` and gets the current key name, then unguards the device.

```
# secfsd -status guard
GuardPoint  Policy                Type                ConfigState  Status  Reason
-----
/dev/sdc2   IDT_DEMO_POLICY_1  rawdevice          guarded      guarded  N/A
/dev/sdc3   IDT_DEMO_POLICY_1  rawdevice          guarded      guarded  N/A
/dev/sdc1   IDT_DEMO_POLICY_1  manualrawdevice    guarded      guarded  N/A

# voradmin idt status xform /dev/sdc1
Status:      Complete
Relocation Zone 0 (relocated = 0)
SegSpc 27, Xformation Range: 4294967295 ... 4294967295, SegIDs: none
KeyID:       2793    Key Name: IDT_DEMO_KEY_1
Old KeyID:   0       Old Key Name: clear_key

# secfsd -unguard /dev/sdc1
secfsd: Path is not guarded

# secfsd -status guard
GuardPoint  Policy                Type                ConfigState  Status  Reason
-----
/dev/sdc2   IDT_DEMO_POLICY_1  rawdevice          guarded      guarded  N/A
/dev/sdc3   IDT_DEMO_POLICY_1  rawdevice          guarded      guarded  N/A
/dev/sdc1   IDT_DEMO_POLICY_1  manualrawdevice    unguarded    not guarded  Inactive
```

- b. Return to the DSM Management Console, select the GuardPoint in the GuardPoints table, and click **Unguard** to unguard the device in the DSM.

Wait until the GuardPoint has been removed from the DSM.

5. Return to the device and run the `voradmin idt rekey` command. After you run the `voradmin` command, the IDT Device Header is temporarily removed from the device.

```
# voradmin idt rekey /dev/sdc1
Enter YES to prepare device /dev/sdc3 for rekey -> YES
# voradmin idt status /dev/sdc1
Device /dev/sdc1 is configured to guard as IDT-Capable GuardPoint
```

Note: For manual GuardPoints, you must unguard the device both using `secfsd -unguard` and the DSM Management Console before you can use the `voradmin idt rekey` command.

6. In the DSM, guard the device with the new **In-place Data Transformation - Device** policy you created earlier. If you selected a Manual GuardPoint, use `secfsd -guard` to activate the new policy and start the data transformation to the new key.

During the IDT process, user access to the GuardPoint is blocked until IDT completes the transformation process.

The following example shows how to use `secfsd -guard` on manual GuardPoint `/dev/sdc1`, and the status messages that occur during the rekey process. If you are using an automatic GuardPoint, you do not need to use the `secfsd -guard` command. Instead, the rekey process starts as soon as you push the new policy from the DSM.

```
# secfsd -guard /dev/sdc1
secfsd: Path is guarded
# secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
/dev/sdc2	IDT_DEMO_POLICY_1	rawdevice	guarded	guarded	N/A
/dev/sdc3	IDT_DEMO_POLICY_1	rawdevice	guarded	guarded	N/A
/dev/sdc1	IDT_DEMO_POLICY_2	manualrawdevice	guarded	guarded	Data transformation in progress

```
# voradmin idt status xform /dev/sdc1
Status: In-Progress
Relocation Zone 0 (relocated = 0)
SegSpc 27, Xformation Range: 3987 ... 3993, SegIDs: 3991 3987 3988 3992 3989 3990
3993
KeyID: 2921 Key Name: IDT_DEMO_KEY_2
Old KeyID: 2793 Old Key Name: IDT_DEMO_KEY_1
```

7. After the `xform` status shows as completed, you can restart all application workloads on the guarded device.

```
# voradmin idt status xform /dev/sdc1
Status: Complete
Relocation Zone 0 (relocated = 0)
SegSpc 27, Xformation Range: 4768 ... 4768, SegIDs: none
KeyID: 2921 Key Name: IDT_DEMO_KEY_2
Old KeyID: 2793 Old Key Name: IDT_DEMO_KEY_1
# secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
/dev/sdc2	IDT_DEMO_POLICY_1	rawdevice	guarded	guarded	N/A
/dev/sdc3	IDT_DEMO_POLICY_1	rawdevice	guarded	guarded	N/A
/dev/sdc1	IDT_DEMO_POLICY_2	manualrawdevice	guarded	guarded	N/A

Guarding an IDT-Capable Device with Multiple IO Paths on Linux

Each individual IO path from a server node to a storage controller is treated as a separate device on the host. DM-Multipath on a Linux host provides a management framework to group the individual IO paths to the same LUN into a single multipath device. If you use DM-Multipath to manage devices on the protected host, the individual devices that correspond to each IO path to the LUN cannot be configured for guarding as IDT-Capable, as those devices are under control of DM-Multipath. To guard such devices, you must guard the device mapper generated by DM-Multipath (multipathd) under the `/dev/mapper` directory.

Note

IDT and Efficient Storage are the only feature of CTE that exclusively support guarding of device mapper generated devices under DM-Multipath framework.

The following example illustrates the procedure for guarding a device mapper generated device with the alias name `/dev/mapper/mpathA`.

1. Create a **In-place Data Transformation - Device** policy using an XTS-AES 256 key as the key rule.
2. On the host, prepare the device to be configured as IDT-Capable using the `voradmin idt config [-external] new|xform [-c n] <mapper-alias-name>` command.
For example, if the disk is a new disk with no existing data, you would enter:

```
# voradmin idt config new /dev/mapper/mpathA
```


If the disk has existing data that you want to encrypt, you would enter:

```
# voradmin idt config xform /dev/mapper/mpathA
```
3. On the DSM, guard `/dev/mapper/mpathA` as Device GuardPoint using the policy created above. Be sure to check the **In-place Data Transformation - Device** check box.
4. For Manual Guard configuration, enable the GuardPoint using the `secfsd` command as follows:

```
# secfsd -guard /dev/mapper/mpathA
```
5. For Auto Guard, wait for the `/dev/mapper/mpathA` device to be guarded on the protected host.
6. Once the device is guarded, provide the pathname of the `secvm` device to applications and/or file system operations. For example, `/dev/secvm/dev/mapper/mpathA`.

Viewing Device Status and the IDT Device Header

After you guard a device, you can view the status of that device using the `voradmin idt [xform] status <device-name>` command, where:

- `xform` (optional). If you specify this option, CTE shows the status of any data transformation processes happening on the device. If you do not specify this option, CTE displays the IDT Device Header for the device.
- `<device-name>` (required). The standard Linux name of the device whose status you want to view. (For example, `/dev/sdc2`.)

For example, if you want to view the IDT Device Header for the Linux device `/dev/sdc2`, you would enter:

```
# voradmin idt status /dev/sdc2
IDT Header on /dev/secvm/dev/sdc2
      Version:                      1
      Change:                       0
Private Region Size:                129024 sectors
Exported Device Size:               9627648 sectors
      Key UUID:                    9cc3c8e4-7ea7-310f-85c7-6f911de1ab52
      Mount Path:                  None
```

If you want to view the data transformation status on `/dev/sdc2`, you would enter:

```
# voradmin idt status xform /dev/sdc3
Status:          In-Process
Relocation Zone  9764864 (relocated = 1)
SegSpc 27, Xformation Range: 3217 ... 4799, SegIDs: 4795 4796 4791 4792 4797 4798
4799
KeyID:           2793      Key Name:      IDT_DEMO_KEY_1
Old KeyID:       0        Old Key Name:  clear_key
```

The **Status** field displays **In-Progress** if a data transformation process is running, and **Completed** if the process has finished.

Linux System and IDT-Capable GuardPoint Administration

voradmin IDT Commands on Linux

The `voradmin` command is a command line utility for management of CTE specific configuration and status reporting. The `voradmin` command also supports configuration management related IDT-Capable GuardPoints (IDT).

For details about the Linux `voradmin idt` command options, see the man page for the `voradmin` command.

File System Mount Points on Linux

You can create and mount a file system on an IDT-Capable GuardPoint. CTE imposes one restriction on the mount point pathname selected for a device. Once you mount the device on a pathname, you cannot change the mount point to a different pathname. This restriction is enforced to allow the file system mount point to be guarded using a separate policy to enforce access control rules on the mounted file system namespace.

The following example shows the mount point of the IDT-Capable GuardPoint as the `/xfs` directory. The example also shows a failed attempt to mount the file system on a different directory pathname.

```
# voradmin idt status /dev/sdc1
IDT Header on /dev/secvm/dev/sdc1
Version:          1
Change:          0
Private Region Size: 129024 sectors
Exported Device Size: 9627648 sectors
Key UUID:         9cc3c8e4-7ea7-310f-85c7-6f911de1ab52
Mount Path:       /xfs
# umount /xfs
# mkdir /other-xfs
# mount -t xfs /dev/secvm/dev/sdc2 /other-xfs
mount: permission denied
# mount -t xfs /dev/secvm/dev/sdc2 /xfs
```

Auto Mount Options for File System Devices on Linux

IDT-Capable GuardPoints containing file systems can also be added to the `/etc/fstab` configuration file for auto mount at startup or unmount at shutdown. An entry can be for a GuardPoint configured for either Auto Guard or Manual Guard. For more information about Auto and Manual Guard options, see ["Guard the Linux Device with an IDT-Capable GuardPoint" on page 218](#).

Use the device path corresponding to an IDT-Capable GuardPoint device when specifying `fstab` entries, such as `/dev/secvm/dev/sdh`. Do not use the native device pathnames, such as `/dev/sdh`, or device mapper device names. You must also include several settings in the `fstab` entry for each IDT-Capable GuardPoint, as shown in the following table:

Option	Description
<code>x-systemd.requires=secvm-barrier.service</code>	Ensure that the IDT-Capable GuardPoint is enabled before the device is mounted at startup and disabled after the device is unmounted at shutdown. The <code>secvm-barrier.service</code> service is a proxy for all the services that make up CTE.
<code>nofail</code>	The system boot will proceed without waiting for the IDT-Capable device if it can't be mounted successfully.
<code>x-systemd.wanted-by=<idt device>.device</code>	Required for Linux distributions running <code>systemd</code> 242 or later. Instructs <code>systemd</code> to add a <code>Wants=</code> dependency on the IDT-Capable device to ensure that, when the device becomes available, this mount operation is executed. <code><idt device>.device</code> is the name of the device specified in <code>fstab</code> with the <code>'/'</code> replaced with <code>'.'</code> . For example, <code>/dev/secvm/dev/sdb</code> becomes <code>dev-secvm-dev-sdb.device</code> .

This is an example of an entry in `/etc/fstab` for an IDT-Capable GuardPoint with an xfs file system that is mounted on `/xfs`:

```
/dev/secvm/dev/sdh /xfs xfs x-systemd.requires=secvm-barrier.service, \
x-systemd.wanted-by=dev-secvm-dev-sdh.device,nofail 0 0
```

For information about configuring `systemd` for CTE, see [Chapter 6: "CTE and systemd" on page 76](#).

Linux System Utilities for Signing

The following table includes recommendations on the system and file system specific utilities for inclusion in the signature set to allow or deny root execution.

EXT Utilities	Deny/Allow	XFS	Deny/Allow	Generic Utilities	Deny/Allow
<code>badblock</code>	Allow	<code>fsck.xfs</code>	Allow	<code>mount</code>	Allow
<code>debugfs</code>	Deny	<code>mkfs.xfs</code>	Allow	<code>umount</code>	Allow
<code>e2freefrag</code>	Allow	<code>xfs_repair</code>	Allow	<code>dmsetup</code>	Allow
<code>e2fsck</code>	Allow	<code>xfs_admin</code>	Allow		
<code>e2image</code>	Allow	<code>xfs_bmap</code>	Allow		
<code>e2label</code>	Allow	<code>xfs_check</code>	Allow		
<code>e2undo</code>	Allow	<code>xfs_copy</code>	Deny		
<code>filefrag</code>	Allow	<code>xfs_db</code>	Deny		
<code>fsck.ext2</code>	Allow	<code>xfs_estimate</code>	Allow		
<code>fsck.ext3</code>	Allow	<code>xfs_freeze</code>	Allow		
<code>fsck.ext4</code>	Allow	<code>xfs_fsr</code>	Allow		
<code>logsave</code>	Allow	<code>xfs_growfs</code>	Allow		
<code>mke2fs</code>	Allow	<code>xfs_info</code>	Allow		
<code>mkfs.ext2</code>	Allow	<code>xfs_logprint</code>	Allow		

EXT Utilities	Deny/Allow	XFS	Deny/Allow	Generic Utilities	Deny/Allow
mkfs.ext3	Allow	xfs_mdrestore	Allow		
mkfs.ext4	Allow	xfs_metadump	Allow		
resize2fs	Allow	xfs_mkfile	Deny		
tune2fs	Allow	xfs_ncheck	Allow		

Resizing Guarded IDT Devices

Devices configured as IDT-Capable can be resized using the system-provided resizing utilities. If you are using a file system on the GuardPoint, you can mount the file system after resizing the device and then grow the file system to the new size using the appropriate utility such as `xfs_growfs` or `resize2fs`.



WARNING

Do not shrink IDT-Capable GuardPoints. Due to relocation of user data from the CTE Private Region, if you shrink the device, you may corrupt data on the device.

1. Stop applications from accessing the IDT-Capable GuardPoint.
 - Unmount the file system if the device is mounted.
 - Disable the IDT-Capable GuardPoint on the DSM if using Auto Guard or on the host with the `secfsd -unguard <device-name>` command if using Manual Guard.
2. Use the native disk management tools to resize the device.
3. After resizing the device, check the size of the device with the `fdisk -l` or similar command. Note that you cannot use the `voradmin idt status` command to verify the new size of the device at this point because the size information is not updated in CTE until the IDT-Capable GuardPoint is re-enabled.
4. If the reported size does not match what you expect, you may need to rescan your storage devices using the command appropriate for the device's connection type.
5. Once the expected size is achieved, enable the IDT-Capable GuardPoint and restart your applications.

This process is identical to resizing an ES GuardPoint. For an example of that process with CTE-Efficient Storage, see ["Example: Resizing a Linux Device" on page 195](#).

Use Cases Involving IDT-Capable GuardPoints

IDT-Capable GuardPoints support all of the use cases that apply to ES GuardPoints. For details, see ["Use Cases Involving Efficient Storage GuardPoints" on page 196](#).

Alerts and Errors on Linux

This section lists the alerts and errors that may be encountered during system operations.

Encryption key on device has not been made available

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the encryption key specified in the policy for the GuardPoint has not been made available to the protected host.

Solution: Check the host's connectivity with the DSM.

Specified policy disagrees with metadata set on the Guard Path

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the key specified in the policy for the GuardPoint does not match with the key stored in the IDT Device Header.

Solution: Un-guard the device and check the name and UUID of the key in the IDT Device Header using `voradmin idt status <device-name>` and `voradmin idt status xform <device-name>` commands and compare the name and UUID with the key name specified in the policy. Correct the discrepancy and re-guard the device.

Device has not been configured for IDT-Capable or Efficient Storage

This alert may appear as the reason for a GuardPoint not to have been enabled. The message appears in the output of `secfsd -status guard` command. The status indicates that the device has been properly guarded as an IDT-Capable GuardPoint on the DSM but the device has not been initialized for guarding as IDT-Capable.

Solution: The most probable cause of this error is that you did not initialize the device for guarding as IDT-Capable on protected host. It's also possible that the guarded device has already configured for guarding as Ean IDT-Capable GuardPoint. If the device needs to be initialized for guarding as IDT-Capable, see ["Initializing an IDT-Capable Device" on page 215](#).

Device not resized for guarding as IDT-Capable or Efficient Storage

This message appears in the output of `secfsd -status guard` command and indicates that the IDT-Capable GuardPoint was not successfully enabled. The status indicates that the newly guarded IDT-Capable GuardPoint, which has been initialized with `xform` option of `voradmin`, has not been resized to accommodate storage space for the CTE Private Region.

Solution: Unguard the IDT-Capable GuardPoint from the DSM, resize the LUN and verify that the host sees the expanded size, and then guard the IDT-Capable GuardPoint from the DSM.

Data transformation failed

This message appears in the output of `secfsd -status guard` command and indicates that the IDT-Capable GuardPoint was not successfully guarded. The status indicates that the protected host encountered an error while transforming the data on the device during IDT.

Solution: Consult with the system and/or storage admin to check on the health of the LUN in the storage array. You may contact Thales Support for troubleshooting and recovery if there has not been a report of any error on the LUN.

Data transformation in progress

This message appears in the output of `secfsd -status guard` command and indicates that the IDT-Capable GuardPoint was not successfully enabled. The status indicates that the protected host is transforming the data on the device.

Solution: You must wait for data transformation to complete. Check the status of transformation by running `voradmin idt status xform <device name>`. Access to the device is blocked until transformation completes.

Device <device-name> is configured to guard as Efficient Storage GuardPoint

This error message is reported by the `voradmin` command when initializing a device as an IDT-Capable GuardPoint that has already been initialized for guarding as an Efficient Storage GuardPoint.

Solution: The device has already been initialized for guarding as Efficient Storage and is probably waiting to be guarded as an ES GuardPoint. If you want to change the device to an IDT-Capable GuardPoint, you can remove the ES configuration by running `voradmin esg delete <device-name>` and then re-initializing the device as an IDT-Capable GuardPoint as described in ["Initializing an IDT-Capable Device" on page 215](#).

Device <device-name> is configured as Efficient Storage GuardPoint

This error message is reported by the `voradmin` command when initializing a device as IDT-Capable that is already being guarded as an Efficient Storage GuardPoint.

Solution: The device is already guarded by an Efficient Storage GuardPoint. If you want to change it to an IDT-Capable GuardPoint, you would need to decrypt the data, delete the Efficient Storage GuardPoint, then reinitialize the device as an IDT-Capable GuardPoint.

Device <device-name> is configured to guard as IDT-Capable GuardPoint

This error message is reported by the `voradmin` command when initializing a device as an IDT-Capable GuardPoint that has already been initialized for guarding as an IDT-Capable GuardPoint.

Solution: The device has already been initialized for guarding as IDT-Capable and is probably waiting to be guarded as an IDT-Capable GuardPoint through the DSM. Alternatively, if you want to remove the IDT-Capable configuration, use the `voradmin idt delete <device-name>` command.

Device <device-name> is configured as IDT-Capable GuardPoint

This error message is reported by the `voradmin` command when initializing a device that is already being guarded as an IDT-Capable GuardPoint.

Solution: The device is already guarded by an IDT-Capable GuardPoint.

GuardPoint for device <device-name> still guarded on DSM

This error message is reported by the `voradmin` command when attempting to initialize a device for rekey or removing the device as IDT-Capable.

Solution: Unguard the IDT-Capable GuardPoint from the DSM, wait for the protected host to process the update, and then rerun the `voradmin` command.

Failed to open device <device-name>, error Device or resource busy

This message occurs when `voradmin` detects that the target device is busy.

Solution: The device may already be in use by other application. Rerun the `voradmin` command when the device is no longer in use.

Device <device-name> is not configured as IDT-Capable

This error message is reported by the `voradmin` command when attempting to delete a device as an IDT-Capable GuardPoint.

Solution: This message indicates that the target device has been not initialized for guarding as IDT-Capable. The message may also be reported if the specified device has been initialized for guarding as IDT-Capable but it has not been guarded yet. In this case, it removes the preparation made by `voradmin`. You can remove the IDT-Capable configuration status on the device by running `voradmin idt delete <device-name>`. You may see the same error message again, and if you do, you can ignore it.

Abort! Error: Could not stop secfs, secvm device(s) busy

This error occurs during CTE shutdown when there is a busy CTE protected device.

Solution: Verify that all applications directly accessing `secvm` protected GuardPoints have been shut down. Ensure that all file systems on top of a `secvm` protected devices are under the control of `systemd` and have been unmounted before attempting to shut down the agent.

Abort! Error: Could not unmount file systems

This error occurs during CTE shutdown when a file system under the control of `systemd` fails to unmount.

Solution: Verify that file systems on top of an IDT-Capable GuardPoint devices are not busy and then rerun the agent shut down command.

A dependency job for idt.mount failed. See 'journalctl -xe' for details

This error occurs during CTE startup when system fails to mount a file system. This error message is typically accompanied by a long timeout during the CTE startup process.

Solution: Check that the underlying device is available and that the IDT-Capable GuardPoint was successfully applied on the device. Once the device is available, the file system will automatically finish mounting.

ESG/IDT-ALERT: IO error on header for [GuardPoint]

This is an alert message to the DSM. It occurs when CTE encounters a general error when attempting to access the private region on an IDT-Capable device.

Solution: An I/O error attempting to read or write to the device may have been caused by errors on the host or storage array. Consult with the system and/or storage admin to check on the health of the LUN in the storage array. You may contact Thales Support for troubleshooting and recovery if there has been no report of errors on the LUN.

ESG/IDT-ALERT: Data transformation failure on [GuardPoint]

This is an alert message to the DSM. It occurs when protected host encounters an error transforming the data on device during IDT process.

Solution: Please contact Thales Support for troubleshooting and recovery.

ESG/IDT-INFO: Data transformation complete on [GuardPoint]

This message is a notification to the DSM admin that the protected host has completed the data transformation of the specified IDT-Capable GuardPoint.

ESG/IDT-ALERT: Failed to resize <device-name>

This alert is a notification to the DSM admin that the protected host has failed to update the change to the device size in the IDT Device Header on the device.

Solution: Please contact Thales Support for troubleshooting and recovery.

FSADM-ALERT: ESG/IDT required Signature Set for system utilities may have to be resigned

This alert is a notification to the DSM admin that the recent system upgrade to the protected host may have updated the binary files listed in the signature set for restricting root access.

Solution: Upon this notification you must immediately re-sign the affected or all the binary files to prevent them from accessing protected data. See ["Linux System Utilities for Signing" on page 227](#).

File System is not automatically mounted after IDT completes

An IDT-Capable device with a file system that has been configured to automatically mount may fail to automatically mount while the device undergoes data transformation through IDT. Following is a sample log message in the kernel ring buffer that reports a failed attempt to access a device during IDT. You can ignore this message.

```
Vormetric SecVM: secvm_map during IDT ((dc 00000000c3537611))
```

When access to a device is to mount the file system, the kernel ring buffer may also report a second error message indicating that a file system failed to mount due to data corruption. You can ignore this message. This occurs because the mount command is issued after the device has been guarded but before data transformation through IDT is complete. While IDT is in progress, the device cannot be used, so any attempt to mount the file system will fail.

Solution: Manually mount the file system after IDT is complete.

Chapter 19: CTE with Teradata Database Appliances

CipherTrust Transparent Encryption (CTE) offers IDT-Capable GuardPoints on Linux for protecting data on raw devices. The IDT solution offers data encryption, data transformation, and access control on storage devices. The principles behind CTE's IDT-Capable GuardPoints can also be applied to protect Teradata Database Appliances. (For details about IDT, see [Chapter 18: "CipherTrust InPlace Data Transformation for Linux" on page 209](#).)

Note

Currently, this feature is only supported on the DSM. Support for this feature will be added to CipherTrust Manager in a future release.

This chapter contains the following sections:

IDT-Capable GuardPoints and Teradata Database Appliances	233
Requirements and Considerations	233
Guarding a Teradata Database Device	235
Changing the Encryption Key on Teradata Devices	243
Access Rules to Apply on the Teradata Database Appliance	244
Replication of IDT Metadata Files Across Members of a Clique	248
Best Practices	250
Uninstalling CTE from the Teradata Cluster	251
Alerts and Errors	252

IDT-Capable GuardPoints and Teradata Database Appliances

The Teradata Database Appliance must be protected by an IDT-Capable GuardPoint. The CipherTrust InPlace Data Transformation (CTE-IDT) feature offers capabilities such as initial data transformation and access control on protected raw devices. The transformation capability transforms existing clear-text data on a device to cipher-text, and allows for subsequent re-transformation using another encryption key.

You must be familiar with CTE and DSM support for IDT-Capable GuardPoints before you can configure CTE to work with Teradata. For details about CTE-IDT, see [Chapter 18: "CipherTrust InPlace Data Transformation for Linux" on page 209](#).

Requirements and Considerations

Location of the CTE Private Region

The CTE Private Region contains the metadata CTE requires in order to support initial transformation of data on the device and subsequent data transformation to other encryption keys. By default, CTE creates the CTE Private Region at the beginning of the guarded device. If data already exists on the device, CTE requires that the device to be expanded by 63 MB to make room for the CTE Private Region. The existing data in the first 63MB of the device is then migrated into the expanded space and the beginning of the device is reserved for the CTE metadata. This data relocation is totally transparent to applications and users.

With a Teradata Database Appliance, however, CTE cannot create the CTE Private Region at the beginning of the Teradata pdisk devices because the disks in the Appliance cannot be expanded. Therefore, for Teradata Databases, CTE stores the metadata in special directory called the CTE Metadata Directory located at

`/var/opt/teradata/vormetric/vte-metadata-dir`. This directory contains all of the metadata for every Teradata Database device that is protected by CTE.

While this does not affect the functionality of CTE, it does affect the way administrators need to back up the Teradata Database because both the Teradata Database and the metadata directory must be backed up together. You will not be able to restore a Teradata Database without access to the associated metadata in the CTE metadata directory.

Metadata File Access and Teradata Clusters

A Teradata *cluster* can contain multiple hosts. The members of a cluster that share access to pdisk devices belong to a *clique*. When you create an IDT-Capable GuardPoint on a pdisk, the metadata for that GuardPoint must be available to all members of the clique. CTE automatically replicates the metadata files across the members of a clique when the metadata is created or changed. For details, see ["Replication of IDT Metadata Files Across Members of a Clique" on page 248](#).

Additional Requirements and Considerations

- The Teradata kernel must be at minimum version 4.4.140-96.54.TDC-default on every node of the Teradata Database Appliance on which you plan to install CTE. Refer to the release notes document for CTE releases for compatibility requirements between the kernel releases from Teradata and CTE releases.



CAUTION

Be sure the version of the Teradata Database is fully compatible with CTE.

The Parallel Upgrade Tool (PUT) component of Teradata Database has been enhanced to discover CTE protected devices. The Parallel Upgrade Tool (PUT) component of Teradata (TDput) must be version `TDput-03.09.06.09` or higher. This capability in the PUT component must be available in your Teradata Database.

The Parallel Database Extensions (PDE) component of Teradata (ppde) must be version `ppde-16.20.53.07` or higher. This capability in the PDE component must be available in your Teradata Database.

The Teradata I/O Scheduler (tdsched) component must be version `01.04.02.02-1` or higher. This capability in the I/O Scheduler component must be available in your Teradata Database.

Contact your Teradata Customer Support Representative if you are unsure of the availability of this functionality in your Teradata cluster.

- The CTE Agent must be installed in `/opt/teradata/vormetric` on every node in the Teradata cluster. In order to specify this location, use the `-d` option when installing CTE. For example:

```
# ./vee-fs-7.0.0-47-sles12-x86_64.bin -d /opt/teradata/vormetric
```

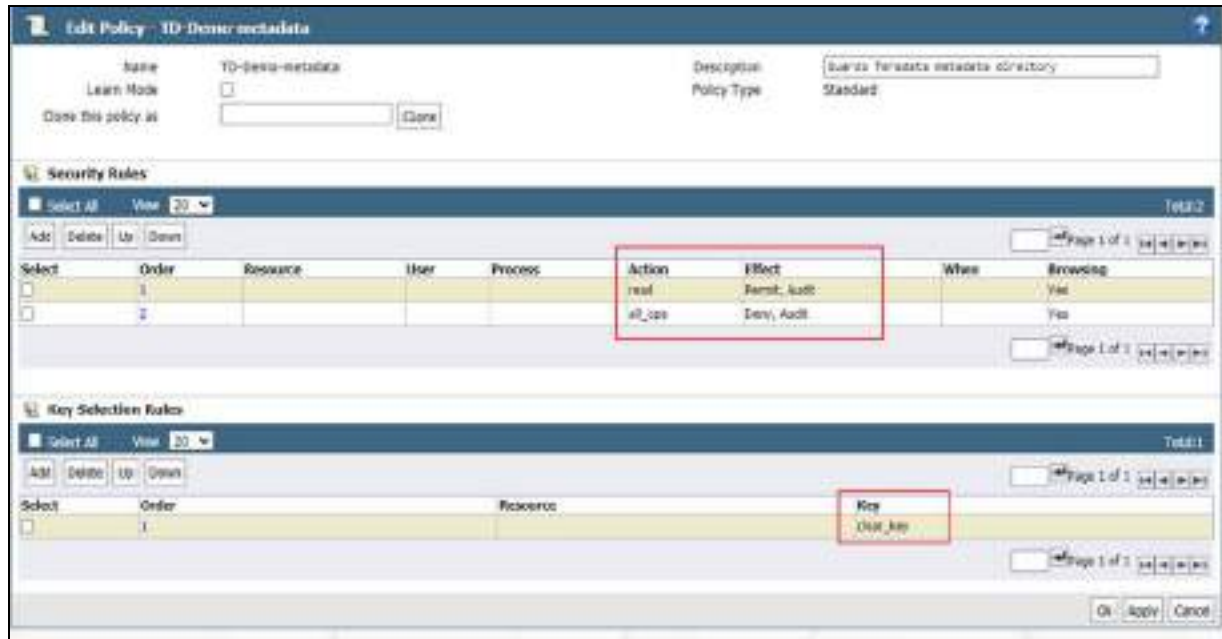
Note: The CTE Agent can be installed without stopping the Teradata Database service.

- The CTE metadata directory `/var/opt/teradata/vormetric/vte-metadata-dir` must be guarded by the DSM Administrator to prevent accidental modification or deletion of the CTE metadata files. If the CTE metadata directory is not guarded, any attempt to configure or enable an IDT-Capable GuardPoint on the Teradata appliance will be rejected.

The standard CTE policy associated with the metadata directory must:

- Deny all users (including the root user) the ability to modify or remove any files in the metadata directory.
- Specify the key `clear_key` in the key rule so that the metadata is stored in clear text.

The following figure shows a sample policy for guarding the CTE metadata directory:



- The Teradata Database service must be stopped in order to upgrade an existing CTE Agent installation. To stop the Teradata Database service, use the `tpareset -x Stopping Database` command.
- The Teradata Database service must be stopped before CTE can rekey any guarded devices, and the service must remain stopped until CTE has finished rekeying *all* guarded devices on the appliance.

Guarding a Teradata Database Device

In order to guard a Teradata Database device, you need to:

1. Install CTE on every node in your Teradata Database Appliance. During this procedure you will register each node (also called the 'protected host') with the DSM. For details, see ["Install CTE on the Teradata Database Appliance" below](#).
2. Identify the devices that you want to guard as IDT-Capable GuardPoints. For details, see ["Identify the Devices to Be Guarded" on the next page](#).
3. Select the initial configuration method that you want to use. For details, see ["Select the Initial Configuration Method" on page 237](#).
4. Initialize and guard the devices using the selected initialization method. For details, see ["Initialize and Guard the Database Devices Using the Standard Initialization Method" on page 237](#) or ["Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method" on page 240](#).

Note

You must use the "In-place Data Transformation - Device" policy type when guarding those devices.

Install CTE on the Teradata Database Appliance

CTE must be installed on every node in the Teradata cluster, including any Hot Standby Nodes. When you install CTE on every node in your Teradata cluster and register each node with the DSM, keep the following things in mind:

- You must have AES-NI available on the host.
- The Teradata kernel must be at version 4.4.140-96.54.TDC-default, or higher, on the Teradata Database Appliance on which you plan to install CTE. Refer to CTE release notes for compatibility between CTE and Teradata kernel releases.
- Your version of Teradata Database must be fully compatible with CTE for supporting the pdisk devices protected as IDT-Capable GuardPoints.
- The CTE Agent must be installed in `/opt/teradata/vormetric`. In order to specify this location, use the `-d` option when installing CTE. For example:

```
# ./vee-fs-7.0.0-47-sles12-x86_64.bin -d /opt/teradata/vormetric
```



WARNING

Before you install or upgrade CTE, you must stop the Teradata Database and any other applications that access the database devices directly or through the database service. Failure to stop the applications will result in a failure to install or upgrade CTE.



CAUTION

Be sure to install the CTE Agent in a file system with sufficient free storage space. The minimum available free space is the number of pdisks in your cluster multiplied by 63MB.

For details about installing the CTE Agent and registering it with the DSM, see ["Configuring CTE for Linux with a DSM" on page 39](#).

Identify the Devices to Be Guarded

Storage devices in Teradata clusters are known as pdisks. A pdisk is a slice of a LUN exported from the backend storage system attached to the nodes in a cluster. For example, the pdisk named `/dev/pdisk/dsk304` is a symbolic link to the slice on the LUN called `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`, as shown below:

```
# ls -l /dev/pdisk/dsk304
lrwxrwxrwx 1 root root 70 May 18 12:21 /dev/pdisk/dsk304 -> /dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

CTE guards the devices represented by the pdisks in the Teradata cluster. In the example above, the device that you must configure and guard as an IDT-Capable GuardPoint is `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`. You cannot use the symbolic link name when initializing or guarding the storage devices.

To identify the disks available to the Teradata cluster and require CTE protection, look in `/dev/pdisks` on each node in the cluster. Any symbolic links that point to a Linux device path are the disks that should be initialized.



CAUTION

Do *not* enter the path name of the pdisk device when initializing it for guarding or in the DSM when you actually guard the device.

Select the Initial Configuration Method

Thales supports two methods for the initial configuration of Teradata Database devices:

- **Standard Initialization Method.** This method configures devices for initial encryption of existing clear-text data on the database devices. The time required to encrypt may take hours or even days, depending on the volume of data, the number of database devices and nodes, and the bandwidth of the storage back-end of database devices. For details, see ["Initialize and Guard the Database Devices Using the Standard Initialization Method" below](#).
- **Backup/Restore Initialization Method.** This method skips the initial encryption step but requires a full backup of the database and the engagement of Teradata Customer Support to assist you with some configuration steps at the Teradata database level in preparation for the full restore of database after the database devices are protected. The length of time required for this method depends on the length of time it takes to back up, and then fully restore, your Teradata database. For details about using this method, see ["Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method" on page 240](#).

Initialize and Guard the Database Devices Using the Standard Initialization Method

The following procedure describes how to perform the initial configuration of your database devices using the Standard Initialization Method. This procedure encrypts the existing data in place and does not require you to backup your Teradata database when initially deploying CTE. It may, however, take several hours, or even days, to complete depending on the volume of data, the number of database devices and nodes, and the bandwidth of the storage back-end of database devices.



WARNING

For each device, you must designate *one and only one* of the nodes in the cluster as the node on which you plan to initialize and guard the device for the first time. The designated node must be the only one that guards the device until the entire initial data transformation process has completed. **DO NOT** initialize or guard any device on multiple nodes in the cluster simultaneously, because multiple nodes attempting to transform the same data can corrupt the data on the entire device.

1. Shut down the Teradata Database so that the devices you want to protect can be configured. You cannot initialize an online database device.
2. For each device, designate one of the nodes in the cluster as the node you will use for the initial data transformation when the device is guarded for the first time.
3. Log into the designated node in the Teradata Database Appliance and run the `voradmin idt config` `[-external] [new|xform] [-c <n>] <device-name>` command, where:
 - `[new|xform]` (required) indicates whether data already exists on the device. If the device contains no data (it is a new disk), specify `new`. If the device contains data that you want to keep, specify `xform`. Most installations of Teradata Appliance are expected to have `pdisk`s populated with data, therefore most often you will use the `xform` option. When you use `xform`, CTE will transform all existing data on the device from clear-text to cipher-text as soon as you guard the device on the Appliance. The device will be inaccessible until the transformation is complete, and the device must remain offline to the Teradata Database service during the entire transformation process. No user access will be permitted until all data has been transformed.
 - `-external` (required). You *must* use this option when initializing any Teradata device. With this option, CTE writes the CTE Private Region to a metadata file located in the CTE metadata directory. For details, see ["Location of the CTE Private Region" on page 233](#).

- `-c <n>` (optional). If you use this option, CTE sets the number of data transformation jobs to run in parallel to the number specified in `<n>`. `<n>` can be an integer between 1 and 60 (default: 8).

Each data transformation job transforms 1MB worth of data and requires CPU resources in addition to three I/O operations as part of data transformation. Each job reads 1MB of data from the device, preserves the data in the CTE private region, rekeys the data to cipher-text, and writes the transformed data to the device. If you increase the number of parallel jobs, the data transformation process will complete faster but there will be an increased performance impact on the system. Only increase the `-c` option if you are certain that the system resources are available to handle the additional load.

The value for the `-c` option you specify here remains in effect for all subsequent data transformations (such as any data rekeys) until you specify a new value.

- `<device-name>` (required). The name of the Teradata Database device that you want to initialize.

For example:

```
# voradmin idt config -external xform -c 20 \  
/dev/disk/by-id/tcmdp-360080e500043092c0000b46f5c34c018-part3
```

4. Repeat the `voradmin idt config` command for each device you want to initialize. If you want to distribute the processing load among all the nodes in the cluster, make sure that you run the `voradmin idt config` command for each device on the node you designated for the purpose. The node on which you run the `voradmin idt config` command must also be the node that performs the initial data transformation.
5. After you initialize the devices, you need to use the DSM Management Console to designate those devices as an IDT-Capable GuardPoints and assign the In-place Data Transformation - Device policy (or policies) you want to use on those devices as described in ["Guard the Devices as IDT-Capable GuardPoints" below](#).

Guard the Devices as IDT-Capable GuardPoints



WARNING

For each device, you must designate one and only one of the nodes in the cluster as the node on which you plan to initialize and guard the device for the first time. The designated node must be the only one that accesses the device until the entire initial data transformation process has completed. This requires guarding each device at the designated host level rather than at the host group level. **DO NOT** initialize or guard any device on multiple nodes in the cluster simultaneously, because multiple nodes attempting to transform the same data can corrupt the data on the entire device.

1. Log on to the Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.
2. Select **Hosts > Hosts** on the menu bar. The *Hosts* window opens.
3. Click the target host in the **Host Name** column. The Edit Host window opens to the General tab for the selected host.
4. In the **Policy** field, select a In-place Data Transformation - Device policy from the list of available policies. The policy must meet the requirements described in ["Policy Requirements for IDT-Capable GuardPoints" on page 213](#).

Note: For information about how to create a GuardPoint, see the chapter, "Managing GuardPoints", in the *DSM Administration Guide*.

5. In the *Type* field, select **Raw or Block Device (Auto Guard)**.

6. In the *Path* field, add the Linux device name for the device you want to guard. For example, `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`. Do *not* enter the symbolic `pdisk` device name for a Teradata disk.
7. Make sure the In-place Data Transformation - Device check box is selected. An example of this is shown below.



8. Click **OK**.

The DSM pushes the policy and the GuardPoint configuration to the node in the cluster and the CTE Agent on the node writes the IDT Device Header into the CTE Private Region in the local CTE metadata directory on the node.

If this is a new device, the status changes to guarded immediately. If there is existing data on the device, CTE begins transforming the data from clear-text to cipher-text as soon as the GuardPoint configuration is available and the device status changes to guarded. The device will remain inaccessible until this data transformation completes. The length of time required to transform the data depends on the amount of existing data and the number of parallel data transformation jobs specified on the `voradmin config` command. To see the data transformation progress, use the `voradmin idt xform status <device-name>` command, as described in ["Viewing Device and Data Transformation Status" on the next page](#).

Devices with existing data are transformed from clear-text to cipher-text using the encryption key specified in the selected policy through the CipherTrust InPlace Data Transformation (CTE-IDT) process. For details on how CTE does data transformation on IDT-Capable GuardPoints, see [Chapter 18: "CipherTrust InPlace Data Transformation for Linux" on page 209](#).



WARNING

The initial data transformation of each device must be executed on *one and only one* of the nodes in the cluster. DO NOT initialize or guard the device on multiple nodes in the cluster before the initial data transformation has completed, because doing so initiates the data transformation process on the device on multiple nodes. The simultaneous attempts to transform the data for the first time can cause data corruption of all data on the entire device.

After the device is initialized and guarded, the protected device must be accessed through the device pathname corresponding to the `secvm` device. For example, if you guard the Linux device `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`, the pathname becomes `/dev/secvm/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3` as soon as the process is complete.

9. After all the Teradata Database devices have been guarded, disable the guarded IDT-Capable GuardPoints on each designated node and then enable those GuardPoints at the Host Group level on all the nodes in the clique.
10. After guarding your devices and before starting your database, you must change the current configuration of your cluster to reflect the status of the pdisk devices guarded as IDT-Capable GuardPoints. See the **Rebuild Vconfig Only** option of the Teradata Parallel Upgrade Tool (PUT) service to apply the guarded status of the pdisk devices into your database configuration. The **Rebuild Vconfig** process applies the guarded configuration status of each pdisk and resets the pdisk symbolic link to the CTE `secdm` device.



WARNING

You must complete this step before starting your database. Failure to do so will result in database failures and potential corruption of your database.

For example, the pdisk `/dev/pdisk/dsk304` is linked to the `secdm` device after **Rebuild Vconfig Only** commits the guarded status of pdisk on each node:

```
# ls -l /dev/pdisk/dsk304 \
lrwxrwxrwx 1 root root 70 May 18 12:21 /dev/pdisk/dsk304 -> /dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part
```

11. After all the Teradata Database devices have been guarded in the clique and the **Rebuild Vconfig Only** on TDput has been executed, start the Teradata Database:

```
/etc/init.d/tpa start
```

Viewing Device and Data Transformation Status

After you guard a Teradata Database device, you can view the status of that device using the `voradmin idt status [xform] <device-name>` command, where:

- `xform` (optional). If you specify this option, CTE shows the status of any data transformation processes happening on the device. If you do not specify this option, CTE displays the IDT Device Header for the device.
- `<device-name>` (required). The name of the Teradata Database device that you want to initialize. This must be the actual device name and not the symbolic pdisk name.

For example, if you want to view the status of device `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`, you would enter:

```
# voradmin idt status /dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

If you want to check the data transformation progress on the device `/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3`, you would enter:

```
# voradmin idt status xform \
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

The **Status** field displays **In-Progress** if a data transformation process is running, and **Completed** if the process has finished.

Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method

The Standard Initialization Method encrypts the Teradata database devices using In-place data transformation. Because Teradata Appliance models range in both storage and node sizes within a cluster, the time it takes to encrypt the existing data in-place on these large scale models may exceed the desired timeframe.

To address this issue on an existing Teradata database, you can configure CTE on Teradata Appliances using the Backup and Restore method to retain existing data. The total time required to configure your Teradata Appliances with CTE using this method depends on how long your backup/restore application takes to restore the database.

To use this method, you must:

1. Backup the entire Teradata database, including all meta files required for a full restore of that database.
2. Install and configure CTE on the Teradata database devices.
3. Work with Teradata Customer Support to initialize a `sysinit` on the Teradata Appliance cluster in preparation for a full database restore.
4. Perform a full restore of the Teradata database from the backup to the CTE protected devices. CTE automatically encrypts the data as it is restored to each protected device.

Prerequisites

Before starting this process, the following prerequisites must be completed:

- Make sure you have met the requirements described in ["Requirements and Considerations" on page 233](#).
- Create or identify the XTS-AES 256 key that you will use for the In-place Data Transformation - Device policy you will apply to the IDT-Capable GuardPoints.
- Create a **Standard** policy that will be used to guard the CTE Metadata Directory (`/var/opt/teradata/vormetric/vte-metadata-dir`).
- Create an **In-place Data Transformation - Device** policy that will be used to guard the Teradata Database Devices. This policy must use an XTS-AES 256 key.
- Identify all of the devices that need to be guarded as described in ["Identify the Devices to Be Guarded" on page 236](#).

Procedure

1. Using a Teradata certified backup application, backup your *entire* Teradata database. The backup needs to include the Data Dictionary, the user database, and everything else that is required for a successful restore of your database. Contact your Teradata Customer Support representative for the requirements for a full backup.
2. After confirming that your backup of the Teradata database completed and successful, shutdown the Teradata database.

```
# tpareset -x -f "shutting down for CTE installation"
```
3. Install CTE in `/opt/teradata/vormetric` on all nodes in the Teradata cluster and register them to a DSM server as described in ["Install CTE on the Teradata Database Appliance" on page 235](#).

```
# ./vee-fs-7.0.0-47-sles12-x86_64.bin -d /opt/teradata/vormetric
```
4. Create the CTE metadata directory (`/var/opt/teradata/vormetric/vte-metadata-dir`) on all nodes in the cluster.

```
# . pcl -shell "mkdir -p /var/opt/teradata/vormetric/vte-metadata-dir"
```
5. If you are using the Teradata Intelibase model, do the following. If you are using the Teradata Inteliflex model, proceed to Step 6.
 - a. Log on to the DSM, click the **Hosts** tab, and set the GuardPoint to the CTE Metadata Directory (`/var/opt/teradata/vormetric/vte-metadata-dir`) using the Standard policy that was created for the metadata directory on all the nodes in the Teradata cluster.
 - b. On each node, identify the list of disks that will be configured and guarded as "new" devices as described in ["Identify the Devices to Be Guarded" on page 236](#).

- c. On each node, configure each disk to be guarded as a new IDT-Capable device using the `voradmin idt config -external new` command.

```
# voradmin idt config -external new \  
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

Note: Make sure that you configure each device using the `new` option. This option tells CTE to guard the device without transforming the data.

- d. Log on the DSM, click the **Hosts** tab, and select one of the host in the clique to set the GuardPoints for all the devices that have been initialized as new IDT-Capable devices using the In-place Data Transformation - Device policy that you created.

Repeat this step for all other hosts until all initialized devices have been guarded with an In-place Data Transformation - Device policy.

6. If you are using the Teradata Inteliflex model, do the following. Otherwise, proceed to Step 7.

- a. Designate one of the nodes in a clique as the node on which you will perform the first-time initialization and guarding procedures for each device. For example, if you have a 4 clique cluster, you must designate a total of 4 nodes, one from each clique.
- b. Log on to the DSM, click the **Host Groups** tab, and create a host group for each clique. For example, if your Inteliflex cluster has 4 cliques, you would create 4 host groups, one for each clique. For example, cluster-clique-1, cluster-clique-2, cluster-clique-3, and cluster-clique-4.

- c. On the **Host Groups** tab, click the name of one of the host groups you just created in the Host Group **Name** column. Click on the **Members** tab and add the designated node from the clique as a member of this host group.

For example, if you clicked on the host group clust-clique-1, you would add the designated node from clique 1 to this host group.

Repeat this step until all designated nodes have been added to the Host Group that matches their clique. In the previous example, you would have one designated node in each of the 4 host groups that you created.

- d. On the **Host Groups** tab, click the name of one of the host groups you just created in the Host Group **Name** column. Click on the **GuardPoints** tab and add a GuardPoint for the CTE Metadata Directory (`/var/opt/teradata/vormetric/vte-metadata-dir`) using the Standard policy that was created for the metadata directory on all the nodes in the Teradata cluster.

Repeat this step for each Host Group you created for your cliques. In the previous example, you would add the metadata directory GuardPoint in each of the 4 host groups that you created.

- e. On the designated node for each clique, identify the list of disks that will be configured and guarded as a "new" IDT device as described in ["Identify the Devices to Be Guarded" on page 236](#).

- f. Configure each disk device on the designated node to be guarded as a new IDT-Capable device using the `voradmin idt config -external new` command.

```
# voradmin idt config -external new \  
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

Note: Make sure that you configure each device using the `new` option. This option tells CTE to guard the device without transforming the data.

- g. For each of the other designated nodes you identified, identify the list of devices to be guarded and configure them using the `voradmin idt config -external new` command.

Repeat this configuration process until all devices on all designated nodes that you want to guard have been configured as new IDT-Capable devices.

- h. On the **Host Groups** tab, click the name of one of the host groups you just created in the Host Group **Name** column. Click on the **GuardPoints** tab and add a GuardPoint for each device that you initialized as a new IDT-Capable device using an In-place Data Transformation - Device policy.

Repeat this step on each one of the host groups you created.

The guarded devices will immediately be set as guarded on the designated node through the host group. However, as part of Teradata cluster support, each guarded device will have its metadata file replicated across all nodes in a clique as described in ["Replication of IDT Metadata Files Across Members of a Clique" on page 248](#). You must wait for metadata replication to complete for each clique in a cluster before continuing to the next step. This process takes approximately 1 second per disk that was guarded. So if you guarded 10 disks, you need to wait approximately 10 seconds. Verify that the number of metadata files on each clique matches with the designated node using the following command:

```
# pcl -shell "ls /var/opt/teradata/vormetric/vte-metadata-dir | wc -l"
```

The number of metadata files on each node in the clique should also match the number of devices in that clique. For example, if you have a clique with 10 devices in it, then the results of the above `pcl` command should show 10 metadata files on each node in the clique.

- i. After metadata replication is completed on all cliques, log on the DSM and click the **Hosts Group** tab, then click the name of one of the host groups you just created in the Host Group **Name** column. Click the **Members** tab and add the rest of the nodes that belong to that clique to the Host Group. After all the nodes have been added, the DSM automatically pushes the existing GuardPoints out to the newly added members.

Repeat this step for each one of the Host Groups that you created for your cliques.

7. Verify that all nodes in a clique shows all the devices as guarded.

```
# pcl -shell "secfsd -status guard"
```

8. Work with Teradata Customer Support to perform a `sysinit` of the Teradata appliances in preparation for the full database restore.
9. Restore your Teradata database from backup.

Changing the Encryption Key on Teradata Devices

To meet various compliance requirements, you may want to change the key that CTE has used to encrypt the Teradata Database devices. This process is called “Key rotation” or “Rekey”.

If you want to rekey a Teradata Database device, you can either:

- Follow the process for standard IDT-Capable GuardPoints. For details, see ["Changing the Encryption Key on Linux IDT-Capable Devices" on page 222](#).
- Use the Backup/Restore method as described in ["Initialize and Guard the Teradata Database Devices Using the Backup/Restore Method" on page 240](#). The only differences between the initial configuration described in that section and rekey process are:
 - You do not need to change the policy assigned to the CTE Metadata Directory.
 - You need to create a new In-place Data Transformation - Device policy that specifies a key rule with the existing key used to encrypt the Database devices in the **Current Key** field and the new XTS-AES 256 key you want to use to encrypt the data in the **New Key** field.
 - When you re-guard the designated node in each clique, make sure you use the new policy so that CTE knows it needs to re-encrypt the data with the new key after you restore the devices from the backup.

Note

Make sure you stop the Teradata database before you rekey the devices.



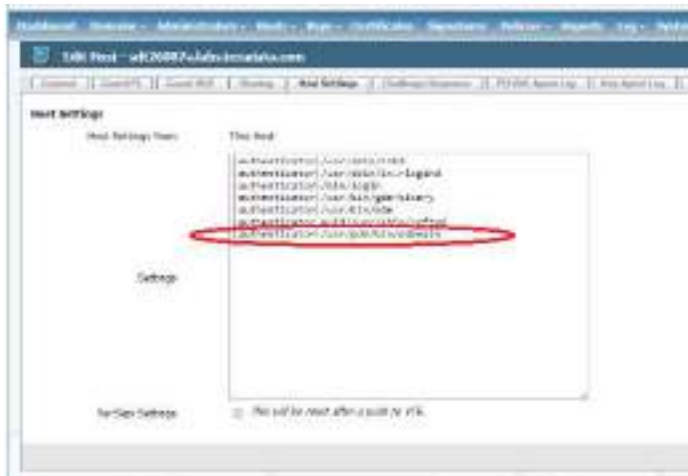
WARNING

Rekeying a device must be executed only on *one and only one* of the nodes in the cluster. DO NOT prepare the device for rekey or guard the device with the new rekey policy on multiple nodes in the cluster because doing so initiates the data transformation process on the device on multiple nodes. The simultaneous attempts to rekey the data can cause data corruption of all data on the entire device.

Access Rules to Apply on the Teradata Database Appliance

This section provides the instructions for creating a sample policy and signature sets specific to a Teradata Database Appliance to deny unprivileged users access to clear-text data on guarded devices. Such a policy requires the inclusion of specific security rules to restrict access to the Teradata Device GuardPoints for specific set of users, groups, and/or processes.

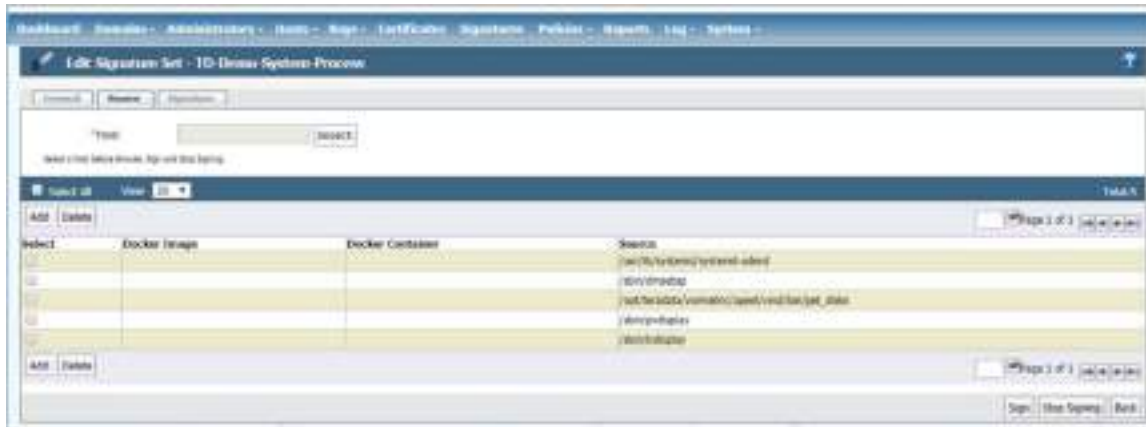
1. In the DSM Management Console, edit the host entry for the Teradata Database Appliance.
2. Go to the **Host Settings** tab and add `/usr/pde/bin/pdmain` to the list of binaries.



3. Create a signature set for system processes that require access to guarded devices. The following system processes on the Teradata Database Appliance *must* be permitted access:

- /usr/lib/systemd/systemd-udevd
- /sbin/dmsetup
- /opt/teradata/vormetric/agent/vmd/bin/get_disks
- /sbin/pvdisplay
- /sbin/lvdisplay

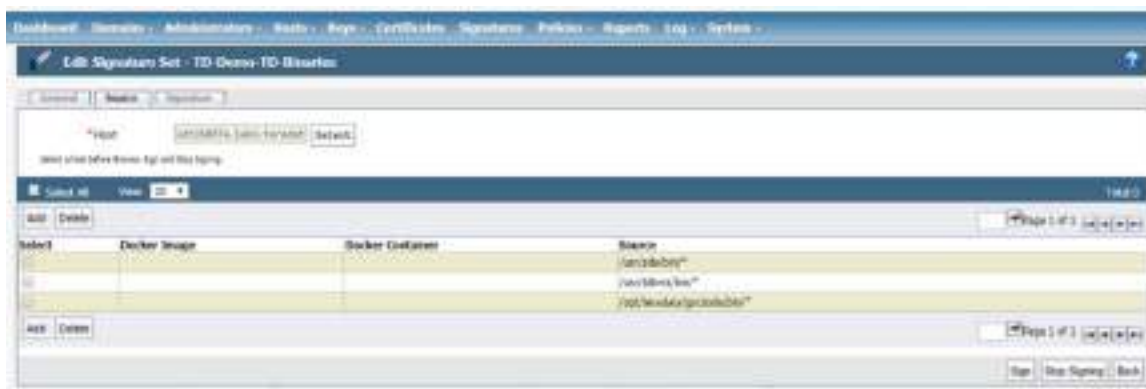
You can include additional processes as needed. In the following example, this signature set is called TD-Demo-System-Process.



4. Create a signature set for Teradata Database processes that require access to guarded devices. The following directories contain the Teradata binaries that require access:

- /usr/pde/bin/*
- /usr/tdbms/bin/*
- /opt/teradata/gsctools/bin/*

You can include additional processes as needed. In the following example, this signature set is called TD-Demo-TD-Binaries.



5. Create a system-level process set to associate the signature set created for the system-level processes in step 3. In the following example, this process set is called TD-Demo-system-process.



6. Create a Teradata Database process set to associate the signature set for the Teradata Database binaries created in step 4. In the following example, this process set is called TD-Demo-TD-process.



7. Create the user set for the Teradata trusted group on your appliance. In the example below, the trusted group name on the Teradata Appliance is `tdtrusted`.

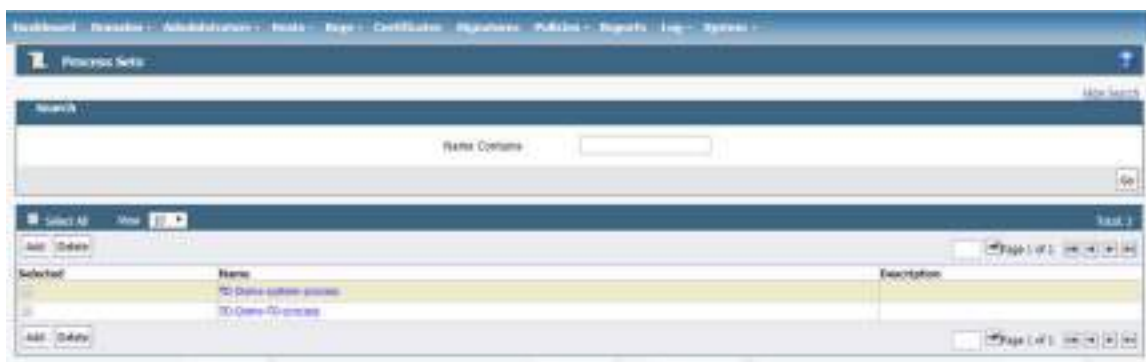


8. If you have any other trusted groups that you want to include in your security rule, add a user set for each one of those trusted groups. You can add as many user sets to the policy as you need.

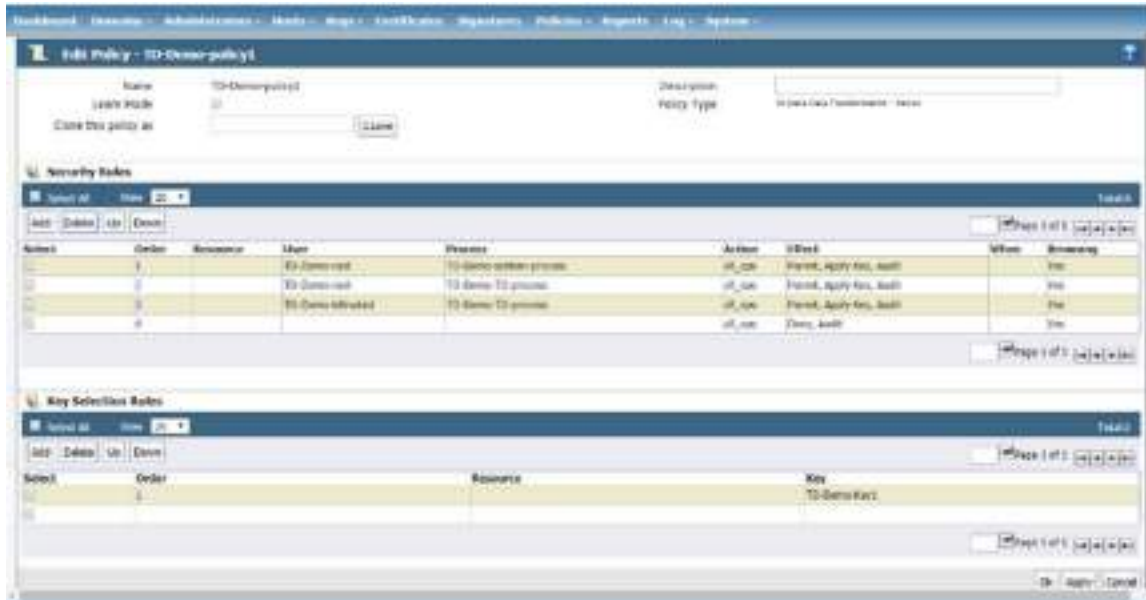
9. Create a user set for the root user and any other privileged users you want to add. In the example below, only the root user is trusted to access the guarded Teradata devices.



10. Verify that you have the complete signature sets, process sets, and user sets as shown in the examples below.



11. Apply the policy to the Teradata Device GuardPoints. For example:



Replication of IDT Metadata Files Across Members of a Clique

For Teradata, metadata for IDT-Capable GuardPoints is stored in external files in the CTE metadata directory. Because the Teradata appliance is a cluster of multiple hosts (or nodes) that share access to the same devices across multiple nodes, a metadata file must be replicated across the nodes that are in the same clique within the cluster, including Hot Standby nodes. Replication is required when the initial data transformation has been completed, and it is required again during subsequent rekeys. The availability of the metadata files on all members of the clique is critical for high availability of Teradata database in the event of a node failure because the data on the device cannot be accessed without the encryption key stored in the metadata.

Upon completion of data transformation on each device, the CTE Agent on that device automatically replicates the metadata file for that device to the other nodes in the clique using the Teradata `pcl` command. CTE uses `pcl` to both determine the other members of the clique and to replicate the metadata to those other members. When the metadata is replicated on the remote nodes, any existing metadata for the recently-transformed device already on those nodes is replaced with the updated metadata files sent by the CTE Agent. This replacement is achieved by sending the updated metadata file to all the remote nodes through `pcl` and replacing each existing metadata file on the remote nodes with the most recent metadata files.

Specific Issues to Consider

This section describes specific problems that may be encountered during data transformation and metadata replication. Manual user intervention will be required to recover from the reported issues. For troubleshooting and recovery steps, see ["Alerts and Errors" on page 252](#).

General PCL Error

If the `pcl` command fails during the replication process, a message indicating the error will be logged on the DSM. The messages on DSM are tagged with IDT-TD-ALERT. For example:

- IDT-TD-ALERT: Node <node name> did not respond to `pcl` command
- IDT-TD-ALERT: Failed to distribute IDT-Capable metadata file to remote nodes

These errors indicate that the node specified in the first error did not respond to a `pcl` command during metadata distribution and so the metadata distribution must be manually performed across the clique before access to the device is possible.

Offline Node in Clique During Data Transformation

If a node is offline during data transformation and metadata replication process, CTE will log a message on the DSM that metadata replication to the target node failed. The administrator will be required to manually replicate the metadata file to the offline node when the node comes online. The metadata file must be replicated before the database is brought up.

To do so, run the `voradmin td distribute <device name>` command to distribute the metadata file of each device. The command will copy or update the metadata file on the host that has come online. For example:

```
# voradmin td distribute \  
/dev/disk/by-id/tdmp-360080e500043092c0000b46f5c34c018-part3
```

Adding a New Node to a Clique

When you add a new node to an existing clique, the metadata files of all disks shared in the clique must be manually replicated to the newly added node before any of the guarded devices on the new node are enabled. This should be done manually using the `voradmin td distribute` command, as described above, by the Teradata administrator as part of joining the cluster.

Interoperability with Host Groups

For Teradata, when you create a new IDT-Capable GuardPoint using the `voradmin idt config xform` command, or when you subsequently rekey an existing IDT-Capable GuardPoint with the `voradmin idt rekey` command, the device must be initialized and guarded on one and only one of the nodes in the cluster. That means the IDT-Capable GuardPoint cannot be part of a Host Group when an IDT-Capable GuardPoint is created or rekeyed because membership in a Host Group means that any data transformation on any member of the Host Group is initiated for that member on all nodes in the Host Group simultaneously. In the case of a Teradata cluster, multiple nodes simultaneously trying to perform data transformation on a particular device can lead to data corruption of all data on the entire device.

After the device has been guarded or rekeyed and the metadata files have been replicated to other members of the Teradata clique, then you can then rejoin the host with the Host Group.

To configure a new device whose host is part of a host group:

1. In the DSM, make sure that there is no GuardPoint for the device at the Host Group level.
2. Designate one of the nodes in the cluster as the node you will use to initialize the GuardPoint and for the initial data transformation when the device is guarded for the first time.
3. On the designated node, initialize the device using the `voradmin idt config -external xform <device name>` command. For details, see ["Initialize and Guard the Database Devices Using the Standard Initialization Method" on page 237](#).
4. In the DSM, guard the device on the designated node using an In-place Data Transformation - Device policy. For details, see ["Guard the Devices as IDT-Capable GuardPoints" on page 238](#).
5. Wait for the data transformation to complete on the host and for CTE to replicate the metadata to the other members of the clique.
6. You can verify that the metadata file has been distributed to the other nodes in the clique by running `md5sum /var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata` on each node in

the clique.

7. In the DSM, remove the IDT-Capable GuardPoint you added earlier in this procedure.
8. Guard the device through the Host Group to make sure that all nodes in the cluster recognize it as guarded.

To rekey a new device whose host is part of a host group:

1. In the DSM, unguard the IDT-Capable GuardPoint through the Host Group and make sure that it has been removed from all nodes in the cluster.
2. Designate one of the nodes in the cluster as the node you will use to prepare the GuardPoint for rekeying and to perform the data transformation when the device is guarded with the new policy.
3. On the designated node, prepare the device for rekey using the `voradmin idt rekey <device name>` command.
4. On the other nodes in the clique, make sure that the device metadata has been renamed running `ls /var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata*` on each of the other nodes. On these other nodes, the metadata file for the device should be renamed to `/var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata_xforming`.
5. In the DSM, guard the device on the designated node with the In-place Data Transformation - Device policy that specifies the new key you want to use for the device.
6. Wait for the data transformation process to complete, and then make sure that the metadata for the device has been updated on the other nodes in the clique and the renamed metadata files have been removed. Each node should have identical copies of `/var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata` and `/var/opt/teradata/vormetric/vte-metadata-dir/vormetric/secvm_<device>_metadata_xforming` should *not* exist on any node.
7. In the DSM, remove the IDT-Capable GuardPoint you created earlier in this procedure on the designated node.
8. Guard the device through the Host Group to make sure that all nodes in the cluster recognize it as guarded.

Best Practices

Using a of Host Group to Guard Metadata Directories

Thales recommends that customers use a host group exclusively for guarding and management of the CTE external metadata directories across all nodes in Teradata cluster. (For details about the CTE metadata directory, see ["Location of the CTE Private Region" on page 233.](#))

By using a Host Group, the same DSM policy can be applied to the external metadata directory (`/opt/vte/vte-metadata-dir`) on all of the CTE protected nodes in the cluster.

Using a Host Group for Guarding Teradata Devices in a Clique

Thales recommend that customers use a Host Group on the DSM to guard and manage the devices shared by all CTE protected nodes in a clique. Each clique in the cluster should be associated with a separate Host Group. When configuring the Host Group, the members for that host group are the nodes that belong within a clique in the cluster.

Example 1: If you have a cluster consisting of 4 cliques where there are 2 nodes sharing disks in each clique, you would create 4 Host Groups, one for each clique. In each Host Group, you would add the 2 nodes that are associated with the clique.

Example 2: If you have a cluster consisting of 1 clique where there are 6 nodes sharing disks in the clique, you want to create 1 host group with all 6 members that belong within that clique.

Below is an example of the Host Groups for a cluster consisting of three cliques and one metadata group:



Name	Cluster Group	Description	Sharing
TD-clique1-clique-1		host group for cluster1-clique-1	
TD-clique1-clique-2		host group for cluster1-clique-2	
TD-clique1-clique-3		host group for cluster1-clique-3	
TD-clique1-metadata		host group for cluster1-metadata	

Best Practice for Preparation for Initial Data Transformation or Rekey

With large amount of data managed in Teradata clusters, duration of initial data transformation and/or subsequent rekey can be very long and challenging because the database must be stopped during the entire data transformation process. Although you cannot transform data without shutting down the database, you may be able to reduce the transformation time by distributing the transformation of the guarded devices across multiple nodes in your cluster.

Because multiple nodes in a cluster within a clique share access to the same devices, you can designate a subset of devices to each node within the clique for initial data transformation or subsequent rekey. This requires unguarding all of the IDT-Capable devices in the Host Group associated with the clique and re-enabling each IDT-Capable GuardPoint only on the node designated for the data transformation of that IDT-Capable GuardPoint. The device then remains unguarded on other nodes until the data transformation completes.

After the data transformation completes, you can then enable the guarded devices at the Host Group level. Enabling the guarded device at Host Group level enables the guarded devices on all the nodes within the clique to share access to the device.

After transforming data and guarding each device on all the nodes, you can then restart the database.

As described in ["Interoperability with Host Groups" on page 249](#), the metadata file for each device is replicated to the hosts in the cluster that share access to the device. As noted, replication of metadata files is automatic.

Uninstalling CTE from the Teradata Cluster

The following procedure describes how to remove CTE from your Teradata cluster. Note that uninstalling CTE will unprotect the pdisk devices that CTE is protecting/encrypting. Because the data on the pdisks remain encrypted after uninstalling CTE, the entire clear-text data must be restored to the pdisks from backup. Therefore, you must have a full backup of your database to restore to your cluster before you uninstall CTE. See the Teradata Administration Guide or your Teradata Customer Support Representative for information about backing up your database in full.

Note

You must be familiar with CTE operations for protecting Teradata clusters and IDT-Capable GuardPoints.

To uninstall CTE:

1. Make sure you have access to a full database backup so that you can restore your Teradata database after uninstalling CTE.
2. Shut down your Teradata database.

3. Use the `secfsd -status guard` command to view the full list of device GuardPoints guarded by CTE on each node of your cluster. From this information, create a consolidated list of GuardPoints with one entry per device in the consolidated list. Note that the devices accessed by the nodes in the same clique are shared devices on each node. The consolidated list must include all devices that are protected in your cluster.
4. Perform the following steps on the DSM:
 - a. Click on the host group name associated with your Teradata cluster and then click the **GuardPoints** tab.
 - b. Select the device names listed in GuardPoints table. The devices listed in GuardPoints table are the same devices listed in the consolidated list of devices compiled in step 3.
 - c. Click the **Disable** button to disable the selected device GuardPoints on all nodes in the cluster.
 - d. Wait for device status to change from green circle to red circle in the Status column for all the selected devices.
 - e. Select the same devices.
 - f. Click the **Unguard** button to remove the selected device GuardPoints on all nodes in the cluster.
5. Perform the following steps on one of the nodes of every clique in your cluster:
 - a. Run the `voradmin idt delete` command to delete the IDT-Capable GuardPoint configuration recorded for each device. This command automatically deletes the GuardPoint configuration across the nodes in the same clique.

```
# voradmin idt delete <device name>
```
 - b. Repeat the previous step on the other devices in your cluster, if any.
6. Go back to the DSM and do the following:
 - a. Select the Metadata Directory GuardPoint in the GuardPoints table of the same host group.
 - b. Click Disable to disable the Metadata GuardPoint directory on every node in the cluster.
 - c. Select the Metadata Directory GuardPoint in the GuardPoints table again and then click Unguard to remove the Metadata Directory GuardPoint on all the nodes in the cluster.
7. On every node in the cluster:
 - a. Run the following command to stop CTE service on each node

```
# /etc/vormetric/secfs stop
```
 - b. Run the following command to uninstall the CTE Agent on each node:

```
# /opt/teradata/vormetric/agent/vmd/bin/uninstall
```

To restore to the full backup of the database to your cluster, contact your Teradata Customer Support Representative (CSR) to perform System Initializer and do a full restore of the database from your backup.

Alerts and Errors

This section lists the alerts and errors that may be encountered during system operations on Teradata Appliance. Refer to Alerts and Errors listed in the chapter on IDT-Capable Device GuardPoints for additional Alerts and Errors.

General Errors

The errors in this section indicate what step failed during CTE system operations for Teradata clusters and will always be paired with an operation error which indicates which CTE system operation failed. For example:

- IDT-TD-ALERT: Node <node name> did not respond to pcl command
- IDT-TD-ALERT: Failed to complete rekey on remote nodes

This pairing of errors indicates that the steps after data transformation were unsuccessful and that the `voradmin` command `voradmin td rekeyed <device name>` is the one that failed.

For details about the `voradmin td rekeyed` command, see the `voradmin` manpage.

IDT-TD-ALERT: Node <node name> did not respond to pcl command

The node listed did not respond to a `pcl` command to perform an operation.

Solution: Check if the node is still online and responding. If it is, run the `voradmin` command to repeat the failed operation. This error message will always be accompanied by one of the other IDT-TD-ALERTS which will determine which `voradmin` command to run to correct the error.

IDT-TD-ALERT: Node <node name> failed to perform voradmin task

The node listed failed to perform a `voradmin` command invoked through `pcl`.

Solution: Correct the issue blocking `voradmin` and run the `voradmin` command to repeat the failed operation. This error message will always be accompanied by one of the other IDT-TD-ALERTS which will determine which `voradmin` command to run to correct the error.

IDT-TD-ALERT: Failed to find clique for disk <device>

CTE failed to locate the clique for the device specified.

Solution: Verify that `/usr/lib/tmpfiles.d/pdisk.conf` is properly configured on all nodes in the Teradata cluster.

IDT-TD-ALERT: Failed to move or rename IDT-Capable metadata file on remote nodes

This error can be due to two issues; one, metadata files that have been distributed to the remote nodes cannot be moved into the metadata directory, or two, metadata files on remote nodes cannot be renamed in preparation for rekey.

Solution: For the first issue, rerun `voradmin td distribute <node name> <device name>` command once any other problems have been resolved. For the second issue rerun `voradmin td rekey <device name>` to prepare for rekey again once any other problems have been resolved.

For details about the `voradmin td` commands, see the `voradmin` manpage.

IDT-TD-ALERT: Failed to get GuardPoint status on remote nodes

The GuardPoint for the device is still present on the DSM for remote nodes or CTE failed to ascertain the GuardPoint status for remote nodes.

Solution: Verify that the GuardPoint for the device has been removed from the DSM for remote nodes and then rerun the `voradmin` command. This error message will always be accompanied by one of the other IDT-TD-ALERTS which will determine which `voradmin` command to run to correct the error.

Operation Errors

These errors indicate which CTE system operation failed and what command should be run upon resolution of the issue that caused the error.

IDT-TD-ALERT: Failed to distribute IDT-Capable metadata file to remote nodes

CTE failed to copy the IDT-Capable metadata file from the current node to all nodes in the clique.

Solution: Correct any issues blocking `pcl` or `voradmin` and then run `voradmin td distribute <node name> <device name>` to attempt copying the metadata file over to the remote node.

For details about the `voradmin td distribute` command, see the `voradmin` manpage.

IDT-TD-WARNING: Failed to delete IDT-Capable metadata file on remote nodes

CTE was unable to remove the IDT-Capable metadata file for a device from a remote node.

Solution: Run `voradmin idt delete <device name>` on the remote node after correct issues impeding `voradmin`. Members of the clique that have successfully removed the metadata file will not be adversely affected if an attempt to remove an already de-configured device occurs.

IDT-TD-ALERT: Failed to complete rekey on remote nodes

CTE was unable to complete the rekey operation on remote nodes to make the device available for guarding again.

Solution: Correct the issue and run `voradmin td rekeyed <node name> <device name>` to signal the remote node that rekey is complete and provide an updated copy of the metadata file to that remote node.

Chapter 20: Upgrading CTE on Linux

This chapter describes how to upgrade an existing VTE for Linux host to CipherTrust Transparent Encryption (CTE) for Linux.

Note

Currently, you can only upgrade a VTE for Linux host to CTE version 7.0.0.47 if you continue to use the DSM as your key manager. You cannot upgrade a VTE host to CTE and then register the upgraded CTE host with CipherTrust Manager. The migration path to CipherTrust Manager will be available in a future release.

This chapter contains the following sections:

Upgrading CTE	255
Scheduled Upgrade Feature	256

Upgrading CTE

This section describes the generic instructions for interactively upgrading CTE. If there are any changes to this procedure for the current release of CTE, those changes will be documented in the CTE Release Notes.

If you want to schedule an upgrade to occur the next time the system boots, see ["Scheduled Upgrade Feature" on the next page](#).

1. Stop any application accessing files in the GuardPoint.
2. Log on to the host where you will upgrade CTE. You must have root access.
3. Copy or mount the installation file onto the host system.
4. Start the upgrade by executing the install program for the release to which you want to upgrade. If you want to automatically accept the CTE License Agreement, you can include the `-y` parameter.

For example, the following command upgrades the product to version 7.0.0.47 after the user manually reviews and accepts the CTE License Agreement:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin
```

The following command upgrades the product to version 7.0.0.47 but automatically accepts the CTE License Agreement:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -y
```

5. Follow the prompts. During an upgrade, the following message displays. Enter Y at the prompt:

```
Upgrade detected: this product will be stopped and restarted.
Do you wish to proceed with the upgrade? (Y/N) [Y]: Y
Installation success.
```

You will not do the registration steps since CTE is already registered with the DSM.

6. To verify that the upgrade was successful, use the `vmd -v` command:

```
$ vmd -v
Version 6, Service Pack 2
7.0.0.47
2020-09-20 09:45:20 (IST)
Copyright (c) 2009-2020, Thales. All rights reserved.
```

Scheduled Upgrade Feature

This section describes how to run the scheduled upgrade feature on CTE for Linux systems. This option is available for CTE version 6.1.3 or later.

Note

Scheduled upgrade on reboot is not supported on HDFS nodes.

Warnings for CTE for Linux

- As with prior CTE versions, DSM connectivity is required during upgrade.
- Yum updates or OS patches should be done prior to CTE upgrade on reboot.
- If you upgrade from a compatible kernel to an incompatible kernel, the `secfs` module will fail to load on the next reboot.
- You may see the following behavior if the upgrade on reboot fails due to crash or power failure (this is similar to a failure during a normal upgrade).
 - If a crash or power failure occurs before the upgrade executes, the upgrade will not take place, and the currently installed CTE version continues to run after the reboot. Restart the system to upgrade successfully.
 - If a crash or power failure occurs during the upgrade, CTE may enter an inconsistent state. The only way to restore is to enter single-user mode and delete all the files or directories related to CTE.
 - If a crash or power failure occurs after a successful upgrade, then the new version will run on the next reboot. No user intervention is required in this case.
- During reboot or shutdown, all applications and services dependent on CTE services must be stopped before a scheduled update takes place. Failure to stop these services can result in an aborted scheduled upgrade during the system reboot. Examples of situations that may cause an aborted upgrade are applications with open files in a CTE GuardPoint, or a third party anti-virus software doing periodic scans.

See the `systemd` chapter in the *CTE Agent for Linux Advanced Configuration and Integration Guide* for examples of how to set up CTE start/stop dependencies with other programs.

Using the Scheduled Upgrade Feature

The following procedure describes how to use `voradmin` to schedule an upgrade that will be applied the next time the machine reboots.

1. If you want to check which version of CTE for Linux you currently have installed, use the `vmd -v` command:

```
$ vmd -v
Version 6, Service Pack 2
6.3.1.38
2020-09-20 11:09:40 (IST)
Copyright (c) 2009-2020, Thales. All rights reserved.
```

2. To schedule an upgrade on reboot, use the `voradmin upgrade schedule <path to CTE installer> -y [-p <path to temp upgrade directory>]` command, where:
 - `<path to CTE installer>` is the full path to the CTE installation file for the release to which you want to upgrade. For example, `./vee-fs-7.0.0-47-rh8-x86_64.bin`.
 - `-y` is an optional parameter that automatically accepts the CTE License Agreement. If you do not specify this parameter, the installer displays the CTE License Agreement and you must manually accept it before the upgrade can be scheduled.

- `-p <path to temp upgrade directory>` is an optional parameter that specifies the path to a directory in which you want CTE to store the temporary files it needs during the upgrade. The default is `/var/tmp/`.

To use this option:

- The currently installed version of CTE must be 6.3.1 or later.
- The version of CTE to which you are upgrading must be version 6.3.1 or later.
- The specified path must not be inside a GuardPoint or be a symbolic link.

For example, if you are upgrading from version 6.3.1.38 to version 7.0.0.47 and you want to automatically accept the license agreement and use the temporary directory `/temp_dir/`, you would enter:

```
$ voradmin upgrade schedule ./vee-fs-7.0.0-47-rh8-x86_64 -y -p /temp_dir/
Linux Kernel 3.10.0-862.el7.x86_64 is supported with the CTE version 7.0.0.47 being
installed.
Created symlink from /etc/systemd/system/multi-user.target.wants/secfs-upgrade.service to
/usr/lib/systemd/system/secfs-upgrade.service.
Successfully scheduled upgrade on reboot to build 7.0.0.47.
```

If you want to manually accept the CTE License Agreement and let the installer use the default temporary directory `/var/tmp/`, you would enter:

```
$ voradmin upgrade schedule ./vee-fs-7.0.0-47-rh8-x86_64
```

The installation script runs and displays the license agreement. When prompted, enter “Y” to proceed with the installation, or “N” to cancel it.

```
Do you accept this license agreement? (Y/N) [N] Y
Linux Kernel 3.10.0-862.el7.x86_64 is supported with the CTE version 7.0.0.47 being
installed.
Upgrade on reboot detected: this product will be upgraded on shutdown/reboot.
Do you wish to proceed with the upgrade? (Y/N) [Y]: Y
Created symlink from /etc/systemd/system/multi-user.target.wants/secfs-upgrade.service to
/usr/lib/systemd/system/secfs-upgrade.service.
Successfully scheduled upgrade on reboot to build 7.0.0.47.
```

3. If you want to verify that the upgrade was successfully scheduled, use the `voradmin upgrade show` command:

```
$ voradmin upgrade show
Upgrade on reboot is currently scheduled.
Current CTE version is 6.3.1.38, upgrade on reboot scheduled for CTE 7.0.0.47.
```

4. Reboot the machine, then log in and verify that the upgrade was successful.

```
$ vmd -v
Version 6, Service Pack 2
7.0.0.47
2020-09-20 09:45:20 (IST)
Copyright (c) 2009-2020, Thales. All rights reserved.
```

Note

Appropriate logs will be logged in syslog.

Performing a Manual Upgrade When an Upgrade is Already Scheduled

If an administrator runs a manual upgrade after an upgrade has already been scheduled, the installer displays the following warning:

```
WARNING: upgrade on reboot is already scheduled for 7.0.0.47.
Do you want to cancel scheduled upgrade on reboot ? (Y/N) [Y] :
```

If the administrator does *not* cancel the scheduled upgrade, the scheduled upgrade takes precedence and the manual upgrade fails with the message:

```
Already scheduled upgrade on reboot remains intact.  
Installation failure.
```

If the administrator wants proceed with the manual upgrade immediately, they must enter Y at the prompt to cancel the scheduled upgrade:

```
WARNING: upgrade on reboot is already scheduled for 7.0.0.47.  
Do you want to cancel scheduled upgrade on reboot ? (Y/N) [Y] : Y  
Removed symlink /etc/systemd/system/multi-user.target.wants/secfs-upgrade.service.  
WARNING: upgrade on reboot is cancelled for 7.0.0.47. Proceeding with manual upgrade.  
Upgrade detected: this product will be stopped and restarted.  
Do you wish to proceed with the upgrade? (Y/N) [Y]: Y  
.....  
Upgrade success.
```

To verify that the upgrade succeeded, the administrator can use the `vmd -v` command:

```
$ vmd -v  
Version 6, Service Pack 2  
7.0.0.47  
2020-09-20 09:45:20 (IST)  
Copyright (c) 2009-2020, Thales. All rights reserved.
```

Voradmin Commands for the Scheduled Upgrade Feature

To view the current CTE version, use the `vmd -v` command:

```
$ vmd -v  
Version 6, Service Pack 2  
6.3.1.38  
2020-09-20 11:09:40 (IST)
```

To schedule an upgrade on reboot, use the `voradmin upgrade schedule <path to CTE installer> [-y] [-p <path to temp upgrade directory>]` command, where:

- `<path to CTE installer>` is the full path to the CTE installation file for the release to which you want to upgrade. For example, `./vee-fs-7.0.0-47-rh8-x86_64.bin`.
- `-y` is an optional parameter that automatically accepts the CTE License Agreement.
- `-p <path to temp upgrade directory>` is an optional parameter that specifies the path to a directory in which you want CTE to store the temporary files it needs during the upgrade. The default is `/var/tmp/`.

To use this option:

- The currently installed version of CTE must be 6.3.1 or later.
- The version of CTE to which you are upgrading must be version 6.3.1 or later.
- The specified path must not be inside a GuardPoint or be a symbolic link.

For example, to schedule an upgrade on reboot to version 7.0.0.47 and automatically accept the CTE License Agreement and use the temporary install directory `/temp_dir/`, you would enter:

```
$ voradmin upgrade schedule ./vee-fs-7.0.0-47-rh8-x86_64.bin -y -p /temp_dir/
```

To get information about a scheduled upgrade:

```
$ voradmin upgrade show  
Upgrade on reboot is currently scheduled.  
Current CTE version is 6.3.1.38, upgrade on reboot scheduled for CTE 7.0.0.47.
```

If no upgrade has been scheduled, this command displays the following:

```
$ voradmin upgrade show  
Upgrade on reboot has not been scheduled.
```

To cancel an existing scheduled upgrade on reboot:

```
$ voradmin upgrade cancel  
Removed symlink /etc/systemd/system/multi-user.target.wants/secfs-upgrade.service.  
Successfully cancelled upgrade on reboot
```

Chapter 21: Uninstalling CTE from Linux

Considerations

- The CTE Agent must be removed from the Linux host before the host is removed from the key manager with which it is registered.
- Database applications like DB2 and Oracle can lock the user space while they run. If the uninstall fails because a GuardPoint is in use, determine which applications are using the files in the GuardPoint and stop them. Then run the uninstall again.
- Commands like `fuser` and `lsof` might not reveal an active GuardPoint because they detect active usage, not locked states. Although it may appear that a GuardPoint is inactive, it may be in a locked state. Under this condition, software removal may fail with an error similar to the following:

```
/home: device is busy.
```

Procedure

1. Stop any application from accessing files in the GuardPoint.
2. In the key manager with which this host is registered, do the following:
 - Decrypt any data you want to use after uninstall. After the CTE Agent software is removed, access to data is no longer controlled. If data was encrypted, it will remain encrypted. If decrypted or copied out of the GuardPoint, the data is visible as clear text.

This decryption must be done on *every* GuardPoint on the host if you want to access all existing data on the host.

- Make sure the Agent and System locks have been disabled for the host.
- Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.

Do not remove the host from the key manager yet.

3. Log on to the host as `root`.
4. Change the directory to an unguarded location (for example, `/`).



CAUTION

Do not change (`cd`) into the `/opt/vormetric` directory or into any directory below `/opt/vormetric`. If you run the uninstaller from `/opt/vormetric` or any of its subdirectories, the package removal utility may fail and return the following message:

You are not allowed to uninstall from the `/opt/vormetric` directory or any of its sub-directories.

Agent uninstallation was unsuccessful.

5. Start the uninstall. Type:

```
# /opt/vormetric/DataSecurityExpert/agent/vmd/bin/uninstall
Would you like to uninstall the vee-fs package? (Y/N) [Y]: Y
.....
Success!
```

6. Remove the host record from the key manager.



Contact us

For office locations and contact information,
visit cpl.thalesgroup.com/contact-us

[> cpl.thalesgroup.com <](https://cpl.thalesgroup.com)



CipherTrust Transparent Encryption

CTE Agent for Windows Advanced Configuration and Integration Guide

Release 7.0.0

Document Version 1

September 22, 2020

The bottom half of the page features a dark blue background with abstract geometric shapes. On the left, there is a large, bright blue triangle pointing upwards. Below it, a smaller, darker blue triangle points upwards. In the bottom left corner, there is a blue circle with a dotted pattern. The right side of the page has a vertical gradient from dark blue at the top to a lighter blue at the bottom, with a dotted pattern at the very bottom.

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2009-2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Contents

Preface	10
The CTE Agent Documentation Set	10
Document Conventions	10
Typographical Conventions	10
Notes, tips, cautions, and warnings	11
Sales and Support	12
 Chapter 1: Overview of CTE	 13
CTE Terminology	13
CTE Components	13
How to Protect Data with CTE	14
 Chapter 2: Getting Started with CTE for Windows	 15
Installation Workflow	15
Installing CTE with No Key Manager Registration	15
Configuring CTE for Windows with CipherTrust Manager	16
Assumptions	16
Requirements	16
Installation Prerequisites	17
Installation Method Options	17
Network Setup Requirements	17
Port Configuration Requirements	17
Hardware Association Feature	17
CTE Windows Installation Checklist	18
Interactive Installation on Windows	18
Silent Installation on Windows	20
Silent Installation Using the exe File	21
Silent Installation Using the MSI File	23
Registering CTE After Installation is Complete	25
Guarding a Device with CipherTrust Manager	26
Access the CipherTrust Manager Domain	27
Create an Encryption Key	27
Create a Standard Policy	28
Create a GuardPoint	31
Configuring CTE for Windows with a DSM	32
Assumptions	32
Requirements	32
Installation and Registration Options and Prerequisites	33

Installation Method Options	33
CTE Registration Method Options	33
Host Name Resolution Requirements	33
Port Configuration Requirements	34
One-way Communication Option	34
Hardware Association (Cloning Prevention) Option	34
CTE Windows Installation Checklist	35
Interactive Installation on Windows	36
Installing CTE and Registering Using the Shared Secret Registration Method	36
Installing CTE and Registering Using the Certificate Fingerprint Method	38
Silent Installation on Windows	40
Silent Installation Using the exe File and Shared Secret Registration Method	41
Silent Installation Using the MSI File and Shared Secret Registration Method	43
Silent Installation Using the exe File and Fingerprint Registration Method	46
Silent Installation Using the MSI File and Fingerprint Registration Method	48
Windows Silent Install Command Line Options	50
Registering CTE with the Shared Secret Registration Method After Installation is Complete	52
Registering CTE with the Fingerprint Registration Method After Installation is Complete	54
Guarding a Device with the DSM	57
Access the DSM Domain	57
Create an Encryption Key	57
Create a Standard Policy	58
Create a GuardPoint	58

Chapter 3: Special Cases for CTE Policies 60

More Information About Configuring CTE Policies	60
Re-Signing Executable Files on Secfs GuardPoints	60
Restricting Access Overrides from Unauthorized Identities	61
Behavior of Hard Links Inside and Outside of GuardPoints (Windows)	61

Chapter 4: Concise Logging 63

Overview of Concise Logging	63
Using Concise Logging	63
Considerations	63
Configuring Concise Logging for CTE Clients or Client Groups with CipherTrust Manager	64
Configuring Global Concise Logging with the DSM	64
Configuring Concise Logging for a Registered Host with the DSM	64

Chapter 5: Enhanced Encryption Mode	65
Compatibility	65
Difference between AES-CBC and AES-CBC-CS1	66
Disk Space	66
Encryption Migration	66
File Systems Compatibility	66
Storing Metadata	67
Missing IV file	67
FileTable Support on Windows	67
Using the AES-CBC-CS1 Encryption Mode in DSM	67
Using the AES-CBC-CS1 Encryption Mode in CM	68
Exceptions and Caveats	68
Best Practices for AES-CBC CS1 Keys and Host Groups	68
 Chapter 6: Utilities for CTE Management	 69
voradmin secfs Commands	69
voradmin secfs List Commands	69
voradmin secfs status Commands	70
vmsec Utility	70
vmsec Syntax	70
Displaying the CTE Challenge String	71
agenthealth Utility	71
The Agent Health Check Script	71
agentinfo Utility	72
agentinfo Utility (Java version)	72
agentinfo Utility (PowerShell version)	72
PowerShell version agentinfo parameters	72
Examples for using agentinfo utility (PowerShell version)	72
 Chapter 7: Using CTE with Microsoft SQL	 74
Using CTE with SQL	74
Using LDT with SQL FILESTREAM	74
Using CTE with SQL FileTables	74
Considerations	74
Advantages	75
Supported FileTables Use Cases	75
CTE Data Transformation of existing files in FileTables	75
Protect files in SQL FileTables with CTE	75
Protect files with SQL AlwaysOn Availability Groups with CTE	76

Install CTE on remote systems and guard the SQL Server VNN names	76
Unsupported FileTables Use Cases	76
Installing CTE on Microsoft SQL AlwaysOn	76
Methods for Initial Encryption	77
Configuration 1	77
Configuration 2	77
Configuration 3	78
Configuration 4	78
Data Transformation (Encryption in place)	79
Copy/Restore	79
SQL Server Policy Tuning	79
Using LDT with SQL AlwaysOn	79

Chapter 8: Secure Start 81

Secure Start Overview	81
Prerequisites	81
Encrypt by Moving the AD Service into a Guarded Directory	82
Create the AD GuardPath directory	82
Apply Secure Start GuardPoints to a Directory with the DSM	82
Apply Secure Start GuardPoints to a Directory with CipherTrust Manager	83
Verify the Secure Start GuardPoint with CLI	83
Move the AD Database into the Secure Start GuardPoint	83
Encrypt Data in Place with Offline Transformation	84
Encrypt with an LDT Transformation Policy	84
Configure the Time Out Failure	84
Recover a Server After it Loses Connection to the DSM	85
DSRM Mode	85
Other Use Cases	86
Boot a Windows Server in Azure	86
Best Practices for Encrypting and Protecting the AD Service	86
Access Control with Secure Start	86
Creating a Minimal Policy Required for AD with Access Control	86
Creating a Restricted Policy in DSRM Mode	87
Guard Directories	88
Perform Subsequent System State Backups	88

Chapter 9: Exchange DAG 89

Exchange DAG Overview	89
Use Case tested and supported by Exchange DAG with CTE	89

Recommendations	90
Requirements	90
Preparing your Exchange DAG Environment for Encrypting/Decrypting with CTE	91
Encrypting with LDT in the Exchange DAG environment	92
Decrypting with LDT in the Exchange DAG environment	93
Encrypting with a Standard CTE Policy in the Exchange DAG Environment	94
Unsupported Use Cases	94
Chapter 10: Storage Spaces Direct	96
S2D Overview	96
Deployment Options	96
Supported Use Cases	97
Chapter 11: Using CTE with Quantum StorNext	98
Overview of using CTE with Quantum StorNext	98
CTE and Quantum StorNext Compatibility	98
Supported StorNext Server and Client Configurations	98
Supported GuardPoint and Key Settings for SNFS File Systems	99
Supported Concurrent Access Read/Write Scenarios	99
Setting up CTE and Quantum StorNext Integration	100
Integration Task Overview	100
Installing and Configuring a Quantum StorNext MDC Server for Use with CTE	101
Installing and configuring Quantum StorNext DLC Clients for Use with CTE	101
Choosing a Mounting Method	101
Installing the CTE Agent on Each StorNext LAN client	101
Chapter 12: CTE-Efficient Storage for Windows	102
Introduction to CTE-Efficient Storage	102
Requirements and Considerations	102
CTE-Efficient Storage Enhanced Storage Arrays	103
Storage Arrays Compatible with CTE-Efficient Storage	103
Sharing Encryption Keys	103
Storage Array Registration	104
Efficient Storage Device Header and CTE Private Region	104
Device Size	104
DSM Domain Enabled for KMIP	104
ES GuardPoint Encryption Keys	105
Key Attributes - Example	105
KMIP Key Object	106

Policy Requirements for ES GuardPoints	107
Guarding an Efficient Storage Device on Windows	108
Requirements for Efficient Storage GuardPoints on Windows	108
Limitations for ES GuardPoints on Windows	109
Register the Windows Host with DSM	110
Initialize Windows CTE-Efficient Storage Devices	111
Initialize New Windows Devices	111
Initialize and Resize Existing Windows Devices	113
Guard the Windows Device with an ES GuardPoint	115
Data Relocation on Existing Windows Devices	116
Data Transformation on Existing Windows Devices	117
CTE-IDT Recovery From Crash	117
Windows System and ES GuardPoint Administration	117
voradmin esg list disk	118
voradmin esg config	118
voradmin esg status	118
voradmin esg status [xform] <device-label>	118
voradmin esg delete	119
Changing the Encryption Key for a Windows ES GuardPoint	119
Requirements and Considerations	120
Creating a New DSM Policy for Key Rotation	120
Rekeying the Windows Device	120
Resizing Guarded Efficient Storage Devices	123
Use Cases involving Efficient Storage GuardPoints	124
Use Case 1: Single Encryption Key	124
Use Case 2: Device-Level GuardPoints	124
Use Case 3: Directory-Level GuardPoints	126
Use Case 4: Full Device Protection	129
Alerts and Errors on Windows	132
ESG-ALERT: Data transformation failure on [GuardPoint]	132
ESG-INFO: Data transformation complete on [GuardPoint]	132
Disk label validation failed. Check your disk label and run command again.	132
Failed to get disk information	132
Boot partition is present on the disk. Disk or LUN can not be protected using CTE agent.	133
The disk is dynamic disk. This disk or LUN can not be protected using CTE agent.	133
Failed to initialize disk	133
Disk is already initialized/guarded with CTE ESG protection	133
Failed to initialize disk with CTE ESG protection. Size must be greater than %xMB, Current size: %yMB	133
Disk is initialized successfully with CTE ESG protection.	133

Disk is initialized successfully with CTE ESG protection. Disk must be Resized to at least 128MB before guarding as Efficient Storage GuardPoint	133
Failed to initialize disk with CTE ESG protection. The specified disk does not exist or is not online.	133
Disk with specified label does not exist. Please select another disk.	134
Header deletion failed with error code	134
Disk is protected with CTE ESG. Please unguard the disk before deleting ESG header.	134
CTE ESG header deleted successfully.	134
CTE ESG header does not exist on the selected disk. Please select another disk	134
Chapter 13: Upgrading CTE on Windows	135
To Upgrade in Windows Silently	135
Verify the Windows Installation	135
Resolving Problems that Prevent Silent Install	136
CTE Scheduled Upgrade	136
Scheduling a CTE Upgrade on the Command Line	136
Scheduling a CTE Upgrade Interactively (self-extracting .exe only)	137
Show Scheduled CTE Upgrades	137
Cancel a Scheduled CTE Upgrade	137
Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades	137
Finding The Name Used For A Previous MSI Installation or Upgrade	138
MSI File Name Lookup Method 1: PowerShell	138
MSI File Name Lookup Method 2: Windows Registry	138
Chapter 14: Uninstalling CTE from Windows	139
Appendix 15: Troubleshooting and Best Practices	140

Preface

The CTE Agent for Windows Advanced Configuration and Integration Guide provides information about advanced installation, configuration, and integration options for CTE for Windows.

The CTE Agent Documentation Set

The following guides are available for CTE Agent:

- *CTE Agent for Linux Quick Start Guide*
- *CTE Agent for Linux Advanced Configuration and Integration Guide*
- *CTE Agent for Windows Quick Start Guide*
- *CTE Agent for Windows Advanced Configuration and Integration Guide*
- *CTE Agent for AIX Installation and Configuration Guide*
- *CTE-Live Data Transformation with Data Security Manager*
- *CTE-Live Data Transformation with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with Data Security Manager*
- *Compatibility Matrix for CTE Agent for AIX with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent for AIX with Data Security Manager*
- *Release Notes for CTE for Linux Version 7.0.0.47*
- *Release Notes for CTE for Windows Version 7.0.0.47*
- *Release Notes for CTE for AIX Version 7.0.0.11*

Document Conventions

The document conventions describe common typographical conventions and important notice and warning formats used in Thales technical publications.

Typographical Conventions

This section lists the common typographical conventions for Thales technical publications.

Table 3-1: Typographical Conventions

Convention	Usage	Example
bold regular font	GUI labels and options.	Click the System tab and select General Preferences.
<i>bold italic monospaced font</i>	variables or text to be replaced	https://<Token Server name>/admin/ Enter password: <Password>
regular monospaced font	Command and code examples XML examples	Example: session start iptarget=192.168.253.102

Table 3-1: Typographical Conventions (continued)

Convention	Usage	Example
<i>italic regular font</i>	GUI dialog box titles	The <i>General Preferences</i> window opens.
	File names, paths, and directories	<i>/usr/bin/</i>
	Emphasis	<i>Do not</i> resize the page.
	New terminology	<i>Key Management Interoperability Protocol (KMIP)</i>
	Document titles	See <i>CTE Agent for Windows Advanced Configuration and Integration Guide</i> for information about CipherTrust Transparent Encryption.
quotes	File extensions Attribute values Terms used in special senses	"js", ".ext" "true" "false", "0" "1+1" hot standby failover

Notes, tips, cautions, and warnings

Notes, tips, cautions, and warning statements may be used in this document.

A Note provides guidance or a recommendation, emphasizes important information, or provides a reference to related information. For example:

Note

It is recommended to keep tokenization keys separate from the other encryption/decryption keys.

A tip is used to highlight information that helps you complete a task more efficiently, such as a best practice or an alternate method of performing the task.

Tip

You can also use Ctrl+C to copy and Ctrl+P to paste.

Caution statements are used to alert you to important information that may help prevent unexpected results or data loss. For example:



CAUTION

Make a note of this passphrase. If you lose it, the card will be unusable.

A warning statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data. For example:



WARNING

Do not delete keys without first backing them up. All data that has been encrypted with deleted keys cannot be restored or accessed once the keys are gone.

Sales and Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

For support and troubleshooting issues:

- <https://supportportal.thalesgroup.com>
- (800) 545-6608

For Thales Sales:

- <https://cpl.thalesgroup.com/>
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

Chapter 1: Overview of CTE

CTE includes several unique utilities to help you encrypt and manage your data. It also integrates with several third-party platforms such as Oracle, Microsoft SQL, and Quantum StorNext.

This document describes the installation and advanced configuration options for CTE, as well as detailed information about how to integrate CTE with the supported third-party products.

CTE Terminology

The CTE documentation set uses the following terminology:

Term	Description
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. Note This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". For example, the default installation directory is C:\Program Files\Vormetric\DataSecurityExpert\agent\.
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.
key manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers two key managers for use with CTE, the Vormetric Data Security Manager (DSM) and CipherTrust Manager.
host / client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed. The difference comes from the key manager you are using. The DSM refers to the machines as hosts, while the CipherTrust Manager refers to them as clients.
GuardPoint	A device or directory to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.
After the CTE Agent has encrypted a device on a host, that device is called a *GuardPoint*. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.
- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Thales offers two key managers that work with CTE:

- CipherTrust Manager, Thales's next generation key manager that supports most CTE for Windows features.
- The *Vormetric Data Security Manager* (DSM), Thales's legacy key manager that supports all CTE for Windows features.

Both key managers can be set up as either a security-hardened physical appliance or a virtual appliance. Both provide access to the protected hosts through a browser-based, graphical user interface as well as an API and a CLI. Thales recommends that you use the CipherTrust Manager unless you need a feature that is only supported by the DSM, as described below.

The CipherTrust Manager currently supports all CTE for Windows features *except* for CTE-Efficient Storage. (For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.)

You must select one and only one key manager per host or host group. While you could have some hosts registered with a CipherTrust Manager and some registered with a DSM, you cannot have the same host registered to both a CipherTrust Manager and a DSM.

Note: For a list of CTE versions and supported operating systems, see the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.

How to Protect Data with CTE

CTE uses policies created in the associated key manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your protected hosts. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of GuardPoints.

Policies specify:

- Whether or not the resting files are encrypted.
- Who can access decrypted files and when.
- What level of file access auditing is applied when generating fine-grained audit trails.

A Security Administrator accesses the DSM or CipherTrust Manager through a web browser. You must have administrator privileges to create policies using either key manager. The CTE Agent then implements the policies once they are pushed to the protected host.

CTE can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

Chapter 2: Getting Started with CTE for Windows

This chapter describes how to install CTE for Windows, register it with your selected key manager, and then create a simple GuardPoint on the protected host. It contains the following sections:

Installation Workflow	15
Installing CTE with No Key Manager Registration	15
Configuring CTE for Windows with CipherTrust Manager	16
Configuring CTE for Windows with a DSM	32

Installation Workflow

In order to install and configure CTE, you need to perform the following high-level tasks:

1. Select which key manager you want to use. The Vormetric Data Security Manager and the CipherTrust Manager have different requirements and support different features, so you must make this decision first. For details, see ["CTE Components" on page 13](#).
2. If you want to install the CTE Agent without registering with a key manager, see ["Installing CTE with No Key Manager Registration" below](#). However, you cannot protect any data on the host until it has been registered. Otherwise, set up your systems according to the requirements of the selected key manager. For details, see one of the following:
 - [Chapter 1: "Configuring CTE for Windows with CipherTrust Manager" on page 1](#).
 - ["Configuring CTE for Windows with a DSM" on page 32](#).
3. Create your policies, encryption keys, and GuardPoints using the selected key manager. For details, see one of the following:
 - ["Guarding a Device with CipherTrust Manager" on page 26](#).
 - ["Guarding a Device with the DSM" on page 57](#).

Installing CTE with No Key Manager Registration

The following procedure installs the CTE Agent on the host but does not register it with a key manager. You cannot protect any data on the host until the CTE Agent is registered with one of the supported key managers. For a comparison of the available key managers, see ["CTE Components" on page 13](#).

If you want to register the CTE Agent immediately after installing it, see ["Configuring CTE for Windows with CipherTrust Manager" on the next page](#) or ["Configuring CTE for Windows with a DSM" on page 32](#).

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the *License Agreement* page, accept the License Agreement and click **Next**.

6. On the *Destination Folder* page, click **Next** to accept the default folder or click **Change** to select a different folder. When you are done, click **Next**.

Notes

- Thales recommends that you install CTE in the default installation directory, `C:\Program Files\Vormetric\DataSecurityExpert\agent\`
- You must install the CTE Agent on the same drive as Windows. For example, if Windows is installed on the `C:` drive, you must install the CTE Agent on the `C:` drive.

7. On the *Ready to Install* page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
8. To tell the installer that you want to register later, clear the check box for **Register CipherTrust File System now**, then click **Finish**.
9. Reboot the host system to complete the installation.

Configuring CTE for Windows with CipherTrust Manager

This section describes how to install and configure CTE on Windows systems that you plan to register with a CipherTrust Manager. If you want to register CTE with a Vormetric Data Security Manager (DSM), see ["Configuring CTE for Windows with a DSM" on page 32](#).

The installation and configuration process consists of three basic steps:

1. Gather the information needed for the install and set up your network as described in ["Installation Prerequisites" on the facing page](#).
2. Install CTE on the protected host as described in ["Interactive Installation on Windows" on page 18](#) or ["Silent Installation on Windows" on page 20](#).
3. Register the protected host with a key manager and make sure that they can communicate with each other. This process can be done as part of the initial installation or at any point after the CTE Agent has been installed.

Assumptions

- The IP addresses, routing configurations, and DNS addresses allow connectivity between the key manager and all hosts on which the CTE Agent is installed.
- If the protected host is a virtual machine, the VM is deployed and running.
- For all types of upgrades, including interactive (GUI-based) and scheduled upgrades, the protected host must be able to connect to the key manager that it is registered to or the upgrade will fail.

Requirements

- You must install CTE on the system drive. Do *not* install CTE on a network share volume.
- The host on which you want to install CTE *must* support AES-NI hardware encryption.

Installation Prerequisites

This section lists the installation requirements and options you should consider before installing CTE.

Installation Method Options

There are two methods for installing CTE:

- **Interactive installation:** This is the most common and recommended type of installation. Use this for installing CTE on one host at a time using a standard InstallShield installation and registration wizard. See ["Interactive Installation on Windows" on the next page](#).
- **Silent installation:** Create pre-packaged installations by providing information and answers to the installation questions. Use silent installations when installing on a large number of hosts. See ["Silent Installation on Windows" on page 20](#).

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the Windows system on which you plan to install CTE to the CipherTrust Manager. After the Windows system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.
- If the system is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

If a protected client must communicate with the CipherTrust Manager through a firewall, see the CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

The default port for communication between the CipherTrust Manager and the CTE Agent is 443. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

Hardware Association Feature

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware clients.

You can enable hardware association during CTE registration process. You can disable hardware association by re-running the registration program.

To verify if hardware association (cloning prevention) is enabled on the protected client, access the Windows command line and run the `vmsec.exe hwok` command. The default location of `vmsec.exe` is `C:\Program Files\Vormetric\DataSecurityExpert\agent\vm\bin`.

To change the status from enable to disable or vice versa:

1. Open the system tray and right-click on the CipherTrust Lock icon.
2. Select **Register Host**.
3. Follow the prompts to re-register CTE with the CipherTrust Manager.
4. Select **Enable hardware association** in the wizard.

CTE Windows Installation Checklist

Use this table to verify prerequisites and collect the information you need for the installation.

Checklist item	Status
Get the CTE installation binary from Thales support, either self-extracting .exe file or MSI. The format for the self-extracting executable CTE file name is: vee-fs-<release>-<build>-<system>.exe Example: vee-fs-7.0.0-47-win64.exe The format for MSI CTE file name is: vee-<agent_type-build-system>.msi For example: vee-fs-7.0.0-47-win64.msi	
Get the Fully Qualified Domain Name (FQDN) of the CipherTrust Manager.	
Get the registration token for the CipherTrust Manager.	
Determine if you want to do an interactive (InstallShield) or silent (command line) install.	
Determine the Administrator password for the client.	
Get the CipherTrust Manager client profile name to associate with this client, unless you want to use the default client profile.	
Determine if you will register the IP address or the FQDN of the client. If you want to use the FQDN, make sure that there is a communication channel between the client and the CipherTrust Manager as described in "Installation Prerequisites" on the previous page .	
Decide if your environment will only support client-initiated communication as described in "Installation Prerequisites" on the previous page . Note: Thales recommends that you only use this option if your environment will not allow two-way communication between the CTE Agent and the CipherTrust Manager.	
Open the appropriate ports as described in "Port Configuration Requirements" on the previous page . The default CTE Agent port is 7024 for two-way communication.	
Decide if you want to enable cloning prevention as described in "Hardware Association Feature" on the previous page .	
Synchronize the host clock to the CipherTrust Manager clock.	

Interactive Installation on Windows

The Windows interactive install uses a standard InstallShield wizard that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see ["Silent Installation on Windows" on page 20](#)).

After you install CTE, you are prompted to register it immediately with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

The following procedure describes how to install the CTE Agent on the host and then register the CTE Agent with a CipherTrust Manager. If you want to install CTE and register it with a Vormetric Data Security Manager, see ["Configuring CTE for Windows with a DSM" on page 32](#).

Prerequisites

Make sure you have the following information from the CM Administrator:

- The registration token for the CipherTrust Manager with which you plan to register the CTE Agent.
- The name of the profile you intend to assign to the client if you want to use a profile other than the default client profile.
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the *License Agreement* page, accept the License Agreement and click **Next**.
6. On the *Destination Folder* page, click **Next** to accept the default folder or click **Change** to select a different folder. When you are done, click **Next**.

Notes

- Thales recommends that you install CTE in the default installation directory, `C:\Program Files\Vormetric\DataSecurityExpert\agent\`
- You must install the CTE Agent on the same drive as Windows. For example, if Windows is installed on the `C:` drive, you must install the CTE Agent on the `C:` drive.

7. On the *Ready to Install* page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
8. On the *InstallShield Wizard Completed* page, make sure the **Register CipherTrust Transparent Encryption** **now** check box is selected and click **Finish**. The installer opens the Register Host wizard.
9. In the Register Host dialog box, verify the host's machine name and click **Next**.
10. On the *Gathering agent information* page, select the **File System** check box and click **Next**.
11. On the *Gathering Key Manager information* page, enter the FQDN or IP address of the primary CipherTrust Manager.

When you are done, click **Next**. CTE communicates with the selected CipherTrust Manager to validate what features have been licensed and are available to the CTE Agent.

12. On the *Gathering host name information* page:
 - Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
 - To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association Feature" on page 17](#).
 - If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the client, select the **Enable LDT Feature** check box. For details on CTE-LDT, see *CTE-Live Data Transformation with CipherTrust Manager*.

When you are done, click **Next**.

13. On the *Gathering registration information* page, enter the following:
- **Registration token:** The registration token for the CipherTrust Manager with which you want to register this host.
 - **Profile name:** The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
 - **Host group** (optional): The name of the client group to which the client will be added.
 - **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.



WARNING

The registration token, profile name, and client group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

When you are done, click **Register**. CTE contacts the CipherTrust Manager and attempts to register the client with the specified options. The Register Host dialog box displays a message with the results of the registration request.

If the registration completed successfully, click **Finish**.

14. Restart the client to complete the installation process on the client.
15. After the host has rebooted, you can verify the installation by checking CTE processes:
- a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
 - b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.
16. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Silent Installation on Windows

Silent install refers to using the command line to install CTE in a non-interactive session. Use silent install to roll out CTE installations or upgrades to large numbers of hosts or to reduce your time and interaction as an administrator. Thales provides two types of installation binaries for silent installation:

- Self-extracting .exe
- Windows Installer Package (MSI).

Note: Thales supports installing or upgrading CTE with Microsoft System Center Configuration Manager (SCCM) using MSI installation binaries. For details, see your SCCM documentation.

For details, see one of the following procedures:

- ["Silent Installation Using the exe File" on the facing page](#)
- ["Silent Installation Using the MSI File" on page 23](#)

Silent Installation Using the exe File

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a CipherTrust Manager using the exe file. To install silently using the MSI file or using the Microsoft System Center Configuration Manager (SCCM), see ["Silent Installation Using the MSI File" on page 23](#).

Prerequisites

Make sure you have the following information from the CM Administrator:

- The registration token for the CipherTrust Manager with which you plan to register the CTE Agent.
- The name of the profile you intend to assign to the client if you want to use a profile other than the default client profile.
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `exe` file onto the Windows system.
3. Run the installation exe file using the following syntax:

```
<Installation_executable> /s /v"/qn INSTALLDIR=\"install-dir\" REGISTERHOSTPTS=\"Options\"
```

where:

- `/s` (required) specifies that this is a silent install.
- `/v` (required) specifies that you want to pass command line options and values of public properties through to the installer.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR=\"install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTPTS=\"Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

Parameter	Description
<i>CipherTrust Manager host name</i>	Required if you want to register CTE with a CipherTrust Manager.
<code>-token</code>	The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.
<code>-profile</code>	Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.
<code>-domain=domain_name</code>	Specifies the domain name with which this CTE Agent will be associated.

Parameter	Description
<code>-hostgroup=clientgroup_name</code>	Specifies the optional client group with which this client will be associated.
<code>-agent=your.agent.name.com</code>	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
<code>-keyagentpwd</code>	The administrative password for the CTE Agent. Required if the CTE Agent is being registered with a CipherTrust Manager. This password allows users to access encrypted data on the client if it is disconnected from the CipherTrust Manager.
<code>-useip</code>	Use the IP address of the protected host instead of host name. Used when <code>-agent</code> is not supplied.
<code>-description="description"</code>	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
<code>-port=port</code>	Specifies the port number this CTE Agent should use.
<code>-usehwsig</code>	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
<code>-enableldt</code>	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.

Note: If you want to enter an option with spaces in any value, it must be surrounded in two double-quotes with an escape character (\) before each double-quote. If the syntax is incorrect, the installation will fail.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- CTE will be installed in the custom directory `C:\cte\custom dir`.
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The CipherTrust Manager registration token is `12345` (`-token` parameter).
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The host will be registered with the description `This host was silently installed` (`-description` parameter). Again, the spaces in the description require the same syntax as in the installation directory name. For example: `-description=\"\"This host was silently installed\"\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> vee-fs-7.0.0-47-win64.exe /s /v" /qn
INSTALLDIR=\"\"C:\cte\custom dir\"\"
registerhostopts=\"my-key-mgr.example.com -agent=my-host.example.com
-token=12345 -description=\"\"This host was silently installed\"\"\""
```

Example: CTE-LDT, Hardware Acceleration

The following example specifies that:

- The agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter) and hardware association (`-usehwsig` parameter) features are enabled.

```
C:\> vee-fs-7.0.0-47-win64.exe /s /v" /qn  
registerhostopts=\"my-key-mgr.example.com -token=12345 -useip -enableldt -usehwsig\""
```

Silent Installation Using the MSI File

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a CipherTrust Manager using the MSI file. To install silently using the exe file, see ["Silent Installation Using the exe File" on page 21](#).

Note

Thales supports installing or upgrading CTE agents with Microsoft System Center Configuration Manager (SCCM) using MSI installation binaries. For details on how to do that, see your SCCM documentation.

Prerequisites

Make sure you have the following information from the CM Administrator:

- The registration token for the CipherTrust Manager with which you plan to register the CTE Agent.
- The name of the profile you intend to assign to the client if you want to use a profile other than the default client profile.
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `MSI` file onto the Windows system.
3. Run the installation exe file using the following syntax:

```
msiexe.exe /i <Installation_executable> /qn INSTALLDIR=\"install-dir\"  
REGISTERHOSTOPTS=\"REGISTERHOSTOPTS_Options\"
```

where:

- `/i` (required) enables CTE installation.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR=\"install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTOPTS=\"Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

Parameter	Description
<i>CipherTrust Manager host name</i>	Required if you want to register CTE with a CipherTrust Manager.
-token	The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.
-profile	Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.
-agent= <i>your.agent.name.com</i>	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
-keyagentpwd	The administrative password for the CTE Agent. Required if the CTE Agent is being registered with a CipherTrust Manager. This password allows users to access encrypted data on the client if it is disconnected from the CipherTrust Manager.
-useip	Use the IP address of the protected host instead of host name. Used when -agent is not supplied.
-description=" <i>description</i> "	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
-port= <i>port</i>	Specifies the port number this CTE Agent should use.
-usehwsig	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
-enableldt	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- CTE will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be in double-quotes. For example: `INSTALLDIR="C:\cte\custom dir"`.
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The CipherTrust Manager registration token is `12345` (-token parameter).
- The host will be registered using the host name `my-host.example.com` (-agent parameter).
- The host will be registered with the description `This host was silently installed` (-description parameter). Because -description is inside a double-quoted string, you must escape the double-quotes `-description=\"This host was silently installed\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> msixexec.exe /i vee-fs-7.0.0-47-win64.exe /qn
INSTALLDIR="C:\cte\custom dir"
registerhostopts="my-key-mgr.example.com -agent=my-host.example.com -token=12345
-description=\"This host was silently installed\""
```

Example: CTE-LDT, Hardware Acceleration

The following example specifies that:

- The agent will be installed in the default installation directory (the INSTALLDIR parameter is omitted).
- The CipherTrust Manager host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter) and hardware association (`-usehwsig` parameter) features are enabled.

```
C:\> msixexec.exe /i vee-fs-7.0.0-47-win64.exe /qn
registerhostopts="my-key-mgr.example.com -token=12345 -useip -enableldt -usehwsig"
```

Registering CTE After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see ["Interactive Installation on Windows" on page 18](#).

1. Log on to the host as a Windows user with administrative privileges.
2. Launch the CTE Registration Wizard using one of the following methods:
 - In the system tray, right click the CipherTrust Lock icon and select **Register Host**.
 - Run `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.exe`.
 - Reboot the system. CTE automatically displays the registration wizard if CTE is not already registered.
3. In the Register Host dialog box, verify the host's machine name and click **Next**.
4. On the *Gathering agent information* page, select the **File System** check box and click **Next**.
5. On the *Gathering Key Manager information* page, enter the FQDN or IP address of the primary CipherTrust Manager.

When you are done, click **Next**. CTE communicates with the selected CipherTrust Manager to validate what features have been licensed and are available to the CTE Agent.

6. On the *Gathering host name information* page:
 - Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
 - To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association Feature" on page 17](#).
 - If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the client, select the **Enable LDT Feature** check box. For details on CTE-LDT, see *CTE-Live Data Transformation with CipherTrust Manager*.

When you are done, click Next.

7. On the *Gathering registration information* page, enter the following:
 - **Registration token:** The registration token for the CipherTrust Manager with which you want to register this host.
 - **Profile name:** The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
 - **Host group** (optional): The name of the client group to which the client will be added.
 - **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.



WARNING

The registration token, profile name, and client group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

When you are done, click **Register**. CTE contacts the CipherTrust Manager and attempts to register the client with the specified options. The Register Host dialog box displays a message with the results of the registration request.

If the registration completed successfully, click **Finish**.

8. Restart the client to complete the installation process on the client.
9. After the host has rebooted, you can verify the installation by checking CTE processes:
 - a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
 - b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.
10. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Guarding a Device with CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

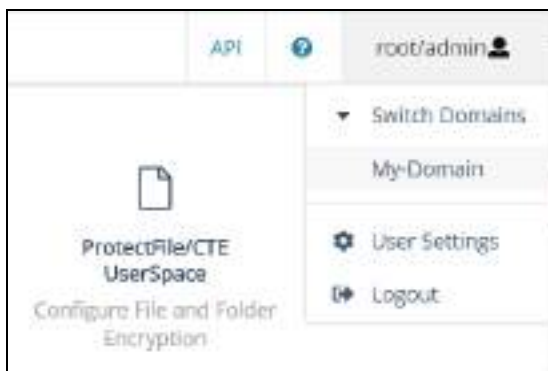
1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device or directory.
3. Identify or create a policy for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. Assign a GuardPoint to the device or directory.

The following example creates a simple policy and uses it to guard a directory on a registered client. For all of the following procedures, you must be logged into the CipherTrust Manager Console as a CipherTrust Manager Administrator, and you must be in the domain with which the client is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the CipherTrust Manager documentation.

Access the CipherTrust Manager Domain

1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to ["Create an Encryption Key" below](#). If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the user name **root/admin** on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.
 - c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

1. In the Applications page of the CipherTrust Manager Console, select **Keys & Access Management**.
2. Above the Key table, click **Create a New Key**.
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
4. In the **Key Metadata > Groups for Key sharing** section, do the following:
 - a. In the **Search** box, type "cte".
 - b. Add CTE Admins and CTE Clients to the key sharing groups by clicking the green **Add** button. The **Key Shared?** check box is automatically selected and the **Add** button changes to a **Remove** button.
 - c. Below the Groups table, click the **CTE Key Properties** check box.

CipherTrust Manager displays the following options for CTE keys:

- **CTE Versioned:** Specify whether the key is versioned. By default, the key is set as versioned.
For a standard policy, you should clear this check box. If you do not, the key will *not* appear in the keys list when you add the key rule to the standard policy.
- **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.
When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.
When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.

- **Encryption Mode:** Encryption mode of the key. The options are:
 - CBC
 - CBC CS1
 - XTS

Encryption using the XTS and CBC CS1 keys is known as enhanced encryption. For details, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.

5. In the Key Behaviors section at the bottom of the page, clear the **Prevent this key from being exported** check box. If the key cannot be exported, the key will not appear in the keys list when you add the key rule to the policy.

6. Click **Create**. The new key appears in the Keys table.

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
2. In the sidebar on the Clients page, click **Policies**.
3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
4. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a Standard policy.

Field	Description
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/CTE-LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.
Data Transformation	If you select Standard as the policy type, also select the the Data Transformation option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

When you are done, click **Next**.

5. On the Security Rules page, define the security rules you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of `key_op` and the effects `Permit` and `Apply Key`. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version. This rule is required by CTE-LDT, so you cannot edit it, move it, or delete it.

To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

For this example, click **Create Security Rule** and:

- Set Action to `all_ops`.
- Set Effect to **Permit** and **Audit**.

When you are done, click **Next**.

6. On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one. If the data has not yet been encrypted, select clear_key . Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select clear_key .
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

When you are done, click **Next**.

7. On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click Select to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in "Create an Encryption Key" on page 27 .

When you are done, click **Next**.

8. Click **Next**.

- On the confirmation page, review the information for the policy and click **Save**.

Create Policy

Review the provided policy details.

General info

Name: Create Policy
Policy Type: Standard
Description: Standard policy for new GuardPoints

Security Rules

Resource Set	User Set	Privilege Set	Action	Effect	Browsing
			key_op	perm_encrypt	yes
			all_ops	perm_decrypt	yes

Key Rules

Resource Set: _____ Current key name: clear-key

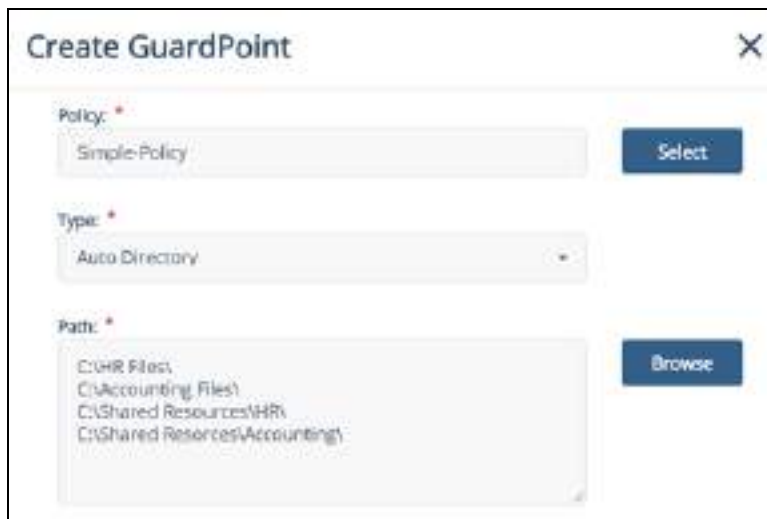
Data Transformation Rules

Resource Set: _____ Transformation Key Name: encrypt-key

Back Save

Create a GuardPoint

- Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
 - C:\HR Files\
 - C:\Accounting Files\
 - C:\Shared Resources\HR\
 - C:\Shared Resources\Accounting\
- Tip:** If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.
- In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
 - In the Clients table, click on the name of the client you want to protect.
 - Above the GuardPoints table, click **Create GuardPoint**.
 - In the Create GuardPoint page:
 - In the **Policy** field, select the policy you created earlier.
 - In the **Type** field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
 - In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a explorer window.
If you want to enter multiple paths, put each path on its own line. For example:



- d. Click **Create**.
- e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**. For this example, click No.

The CipherTrust Manager pushes the GuardPoint configuration to the client and CTE immediately begins transforming the data in the specified folders from clear-text to cipher-text.

6. When the data transformation has finished, applications can resume accessing the now-protected data.

Configuring CTE for Windows with a DSM

This section describes how to install and configure CTE on Windows computers and, optionally, registering CTE with a Vormetric Data Security Manager (DSM). If you want to register CTE with a CipherTrust Manager, see ["Configuring CTE for Windows with CipherTrust Manager" on page 16](#).

The installation and configuration process consists of three basic steps:

1. Gather the information needed for the install and set up your network as described in ["Installation and Registration Options and Prerequisites" on the facing page](#).
2. Install CTE on the protected host as described in ["Interactive Installation on Windows" on page 36](#) or ["Silent Installation on Windows" on page 40](#).
3. Register the protected host with the primary DSM and make sure that the CTE Agent and the DSM can communicate with each other. Registration can be done as part of the initial installation or at any point after the CTE Agent has been installed.

Assumptions

- The IP addresses, routing configurations, and DNS addresses allow connectivity between the key manager and all hosts on which the CTE Agent is installed.
- If the protected host is a virtual machine, the VM is deployed and running.

Requirements

- You must install CTE on the system drive. Do *not* install CTE on a network share volume.
- The host on which you want to install CTE *must* support AES-NI hardware encryption.

Installation and Registration Options and Prerequisites

CTE has the following installation prerequisites and provides the following installation and registration options. The options you choose determine the information you need to supply during the actual install procedure, so you should decide what options you want to use before you start the installation.

Installation Method Options

There are two methods for installing CTE:

- **Interactive installation:** This is the most common and recommended type of installation. Use this for installing CTE on one host at a time using a standard InstallShield installation and registration wizard. See ["Interactive Installation on Windows" on page 36](#).
- **Silent installation:** Create pre-packaged installations by providing information and answers to the installation questions. Use silent installations when installing on a large number of hosts. See ["Silent Installation on Windows" on page 40](#).

CTE Registration Method Options

You can register the protected hosts with a DSM using either the *Fingerprint method* or the *Shared Secret method*.

- **Fingerprint method** requires the DSM Administrator to add the FQDN, or IP address, of each protected host to the DSM before registering CTE.
During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. The security administrator must verify the fingerprint to make sure the certificate is valid.
- **Shared Secret method** requires the DSM Administrator to create a *shared secret* password—a case-sensitive string of characters—for auto-registering a domain or host group.
CTE installers use the shared secret to add and register protected hosts to the DSM for a domain or host group. The DSM Administrator can optionally add host names or IP addresses to the DSM. There is no need to verify that the protected host and DSM share valid certificates. You can add multiple protected hosts dynamically with a single shared secret password during CTE installation and registration.
After the DSM Administrator creates a shared secret for the domain or host group in which the new protected host will reside, obtain it and the validity period (one hour, day, week, or month) and register within that period.

Host Name Resolution Requirements

Host name resolution is the method of mapping a host name to an IP address. During this configuration process, enter either the FQDNs, or IP addresses, of your DSM and protected hosts. If you use FQDNs, your protected hosts must be able to resolve the DSM host names, and the DSM must be able to resolve its protected hosts.

Note

The exception to this requirement is if you plan to configure one-way communication between CTE and the DSM.

A Domain Name Service (DNS) server is the preferred method of host name resolution. If you use DNS, use the FQDNs for the DSM and hosts.

If you do *not* use a DNS, you can do one of the following:

- Use the IP addresses of the DSM and protected hosts.
- Add an entry for the DSM in the `C:\WINDOWS\system32\drivers\etc\hosts` file on each one of the Windows machines on which you want to install the CTE Agent.

- Add an entry in the `/etc/hosts` file on the DSM associated with the host. The administrator must use the CipherTrust CLI, and, in an HA environment, they must add an entry to *each* DSM in the cluster because entries in the `/etc/hosts` file are not replicated across the cluster.

Port Configuration Requirements

If a protected host must communicate with the DSM through a firewall, see the *DSM Administration Guide* to determine which of the ports must be opened through the firewall.

The default port for communication between the DSM and the CTE Agent is 7024. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

One-way Communication Option

In some deployments, CTE might not be visible to the DSM through normal network communications. For example, when the host on which CTE is installed:

- is behind NAT.
- is behind a firewall.
- is not permanently connected to a communication channel to the DSM.
- is unable to resolve the host name to an IP address.

In these situations, CTE can initiate CTE-only communication to the DSM. This feature is called one-way communication and works by having CTE poll the DSM for any policy messages or changes, then downloading changes as required.

The downside of one-way communication is that the DSM cannot issue any queries to CTE. For example, the DSM Administrator cannot browse host directories or User IDs. To enable the full functionality of both CTE and the CipherTrust Manager, Thales recommends that you use two-way communication between them whenever possible.

Port Usage in One-Way Communications Mode

By default, polling from the agent host to the DSM when running in one-way communications mode uses HTTP via port 8080. If the CTE Agent is configured to use secure polling, then polling is performed using HTTPS via port 8448 (in suite B mode) or port 8445.

Hardware Association (Cloning Prevention) Option

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware hosts.

You can enable hardware association during CTE registration process. You can disable hardware association by re-running the registration program.

To verify if hardware association (cloning prevention) is enabled on the protected host, access the Windows command line and run the `vmsec.exe hwok` command. The default location of `vmsec.exe` is `C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin`.

To change the status from enable to disable or vice versa:

1. Open the system tray and right-click on the CipherTrust Lock icon.
2. Select **Register Host**.
3. Follow the prompts to re-register CTE with the DSM.

4. Select **Enable hardware association** in the wizard.

To verify if hardware association (cloning prevention) is enabled on host, on the command line enter the following:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/access
```

If you see `usehw:true`, then hardware association is enabled. If you see `usehw:false`, it's disabled.

CTE Windows Installation Checklist

Use this table to verify prerequisites and collect the information you need for the installation.

Checklist item	Status
Get the CTE installation binary from Thales support, either self-extracting .exe file or MSI. The format for the self-extracting executable CTE file name is: vee-fs-<release>-<build>-<system>.exe Example: vee-fs-7.0.0-47-win64.exe The format for MSI CTE file name is: vee-<agent_type-build-system>.msi For example: vee-fs-7.0.0-47-win64.msi	
Get the Fully Qualified Domain Name (FQDN) of the DSM.	
Determine the Administrator password for the host.	
Determine if you want to do an interactive (InstallShield) or silent (command line) install.	
Determine if you want to register the CTE Agent with the DSM using the Shared Secret registration method or the Fingerprint registration method. For more information, see "CTE Registration Method Options" on page 33 .	
If using Shared Secret registration, obtain the following from the DSM Administrator: • Shared secret for the DSM. • The Domain in which this host should be registered. • (Optional) Host Group in which this host should be added.	
If using the Fingerprint registration, ask the DSM Administrator to add the host to the DSM with the Registration Allowed check box selected. After you verify the fingerprints, the DSM Administrator can select the Communication Enabled check box.	
Decide if you want to enable cloning prevention as described in "Hardware Association (Cloning Prevention) Option" on the previous page .	
Determine if you will register the IP address or the FQDN of the client. If you want to use the FQDN, make sure that there is a communication channel between the client and the DSM as described in "Host Name Resolution Requirements" on page 33 .	
Decide if your environment will only support client-initiated communication as described in "One-way Communication Option" on the previous page . Note: Thales recommends that you only use this option if your environment will not allow two-way communication between the CTE Agent and the CipherTrust Manager.	
Open the appropriate ports as described in "Port Configuration Requirements" on the previous page . The default CTE Agent port is 7024 for two-way communication.	
Synchronize host clock to DSM clock.	

Interactive Installation on Windows

The Windows typical install uses an interactive InstallShield wizard that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see ["Silent Installation on Windows" on page 40](#)).

After you install CTE, you are prompted to register it immediately with a DSM. CTE must be registered with a DSM before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

The procedure for installing CTE depends on the registration method you want to use. The available methods are described in ["CTE Registration Method Options" on page 33](#). After you have selected your registration method, you can use one of the following procedures:

- ["Installing CTE and Registering Using the Shared Secret Registration Method" below](#)
- ["Installing CTE and Registering Using the Certificate Fingerprint Method" on page 38](#)
- ["Installing CTE with No Key Manager Registration" on page 15](#)

Installing CTE and Registering Using the Shared Secret Registration Method

The following procedure describes how to install the CTE Agent on the host and then register the CTE Agent with a DSM using the Shared Secret registration method. For more information about the available registration methods, see ["CTE Registration Method Options" on page 33](#).

For other installation options, see ["Installing CTE and Registering Using the Certificate Fingerprint Method" on page 38](#) and ["Installing CTE with No Key Manager Registration" on page 15](#).

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the *License Agreement* page, accept the License Agreement and click **Next**.

6. On the *Destination Folder* page, click **Next** to accept the default folder or click **Change** to select a different folder. When you are done, click **Next**.

Notes

- Thales recommends that you install CTE in the default installation directory, `C:\Program Files\Vormetric\DataSecurityExpert\agent\`
- You must install the CTE Agent on the same drive as Windows. For example, if Windows is installed on the `C:` drive, you must install the CTE Agent on the `C:` drive.

7. On the *Ready to Install* page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
8. On the *InstallShield Wizard Completed* page, make sure the **Register CipherTrust Transparent Encryption** **now** check box is selected and click **Finish**. The installer opens the Register Host wizard.
9. In the Register Host dialog box, verify the host's machine name and click **Next**.
10. On the *Gathering agent information* page, select the **File System** check box and click **Next**.
11. On the *Gathering Key Manager information* page, enter the FQDN of the Primary DSM. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



When you are done, click **Next**. CTE communicates with the selected DSM to validate what features have been licensed and are available to the CTE Agent.

12. On the *Gathering host name information* page:
 - Specify the host name or IP address of the host. You can select the host name from the drop-down list or type it in the field. If you specify a host name, it must be resolvable by the DNS server (see ["Host Name Resolution Requirements" on page 33](#)).
 - To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association \(Cloning Prevention\) Option" on page 34](#).
 - If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the host, select the **Enable LDT Feature** check box. For details on CTE-LDT, see the *CTE-Live Data Transformation with Data Security Manager*.
 - If you want to have the CTE-Efficient Storage feature available on the host, select the **Enable ES Feature** check box. For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
 - Make sure the **Use Shared Secret Registration** check box is enabled.

When you are done, click **Next**.

Note: If you get the message "Only CTE-initiated communication is possible", make sure that the DSM and CTE can communicate over the network.

13. On the *Gathering shared secret registration information* page, enter the following:
 - **Shared secret:** The shared secret established for the domain in the DSM to which you intend to add this host. Contact the DSM Administrator for this value.
 - **Domain name:** The name of the DSM domain to which the host will be added. Contact the DSM Administrator for this information.
 - **Host group** (optional): The name of the host group to which the host will be added. Contact the DSM Administrator for this value.
 - **Host description** (optional): A user-defined description of the host to be registered.



WARNING

The shared secret, domain name, and host group are case-sensitive. If any of these are entered incorrectly, an error message displays. If you exceed the number of allowable login attempts to the DSM, you will be locked out of the DSM. For more information, talk to your DSM Administrator.

When you are done, click **Register**. CTE contacts the DSM and attempts to register the host with the specified options. The Register Host dialog box displays a message with the results of the registration request.

If the registration completed successfully, click **Finish**.

14. Restart the host to complete the installation process.
15. After the host has rebooted, you can verify the installation by checking CTE processes:
 - a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
 - b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.

Installing CTE and Registering Using the Certificate Fingerprint Method

The following procedure describes how to install the CTE Agent on the host and then register the CTE Agent with a DSM using the Fingerprint registration method. For more information about the available registration methods, see ["CTE Registration Method Options" on page 33](#).

For other installation options, see ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 36](#) and ["Installing CTE with No Key Manager Registration" on page 15](#).

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

On the *InstallShield Wizard Completed* page, make sure the **Register CipherTrust Transparent Encryption now** check box is selected and click **Finish**. The installer opens the Register Host wizard.

In the Register Host dialog box, verify the host's machine name and click **Next**.

Note: The machine name shown here does *not* need to match the one specified in the DSM. You will have an opportunity to select a different machine name later in this procedure.

On the *Gathering agent information* page, select the **File System** check box and click **Next**.

On the *Gathering Key Manager information* page, enter the FQDN of the Primary DSM. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



When you are done, click **Next**. CTE communicates with the selected DSM to validate what features have been licensed and are available to the CTE Agent.

On the *Gathering host name information* page:

- Specify the host name or IP address of the host. You can select the host name from the drop-down list or type it in the field. If you specify a host name, it must be resolvable by the DNS server (see ["Host Name Resolution Requirements" on page 33](#)).



WARNING

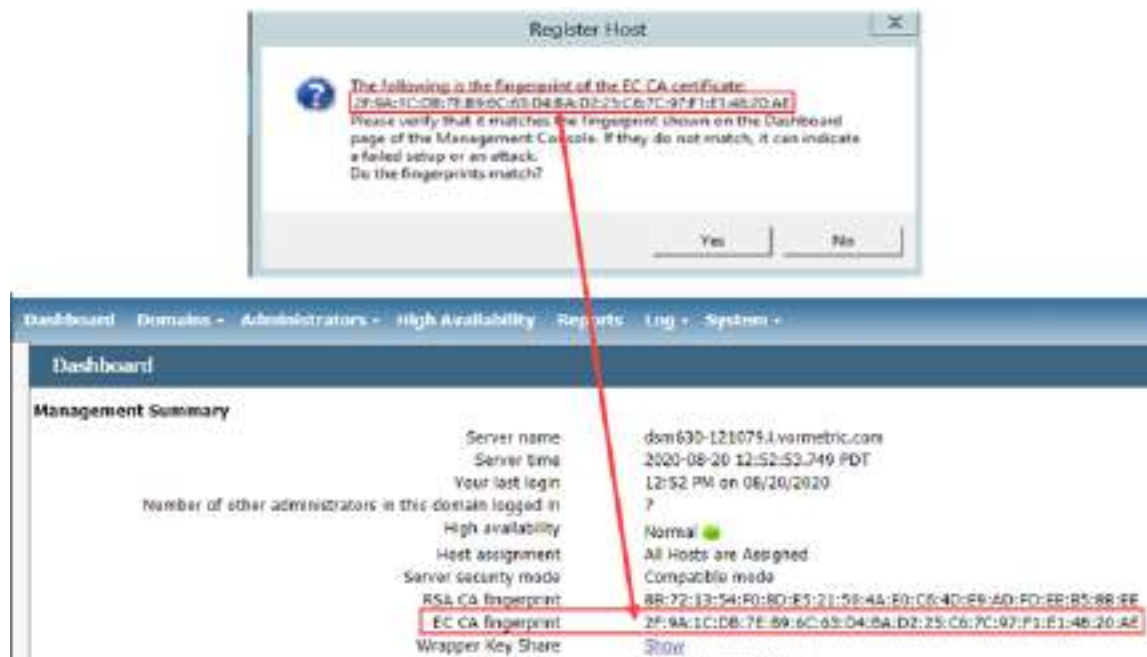
The host name specified here must exactly match the host name specified in the DSM in order for the fingerprints to match.

- To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association \(Cloning Prevention\) Option" on page 34](#).
- If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the host, select the **Enable LDT Feature** check box. For details on CTE-LDT, see the *CTE-Live Data Transformation with Data Security Manager*.
- If you want to have the CTE-Efficient Storage feature available on the host, select the **Enable ES Feature** check box. For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
- Clear the **Use Shared Secret Registration** check box so that CTE will use the Fingerprint Registration Method.

When you are done, click **Register**.

Note: If you get the message "Only CTE-initiated communication is possible", make sure that the DSM and CTE can communicate over the network.

CTE displays the Register host status page and displays the EC CA Certificate that it received from the DSM. This fingerprinting should exactly match the fingerprint displayed on the DSM Dashboard page. For example:



If the fingerprints match, click **Yes**.

Click **OK** when CTE displays the fingerprint for the host's certificate.

The *Register host status* page shows the two fingerprints and displays a message about the registration status. If the registration completed successfully, click **Finish**.

Restart the host to complete the installation process.

After the host has rebooted, you can verify the installation by checking CTE processes:

1. In the system tray of the protected host, right-click the CipherTrust Lock icon.
2. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.

Silent Installation on Windows

Silent install refers to using the command line to install CTE in a non-interactive session. Use silent install to roll out CTE installations or upgrades to large numbers of hosts or to reduce your time and interaction as an administrator.

Thales provides two types of installation binaries for silent installation:

- Self-extracting .exe
- Windows Installer Package (MSI).

Note: Thales supports installing or upgrading CTE agents with Microsoft System Center Configuration Manager (SCCM) using MSI installation binaries. For details, see your SCCM documentation.

For details, see one of the following procedures:

- "Silent Installation Using the exe File and Shared Secret Registration Method" on the facing page
- "Silent Installation Using the MSI File and Shared Secret Registration Method" on page 43
- "Silent Installation Using the exe File and Fingerprint Registration Method" on page 46

- ["Silent Installation Using the MSI File and Fingerprint Registration Method" on page 48](#)

For a combined list of all available silent install options for both the exe file and the MSI file, see ["Windows Silent Install Command Line Options" on page 50](#).

Silent Installation Using the exe File and Shared Secret Registration Method

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a DSM using the exe file and the shared secret registration method. For a list of other available methods, see ["Silent Installation on Windows" on the previous page](#).

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `exe` file onto the Windows system.
3. Run the installation exe file using the following syntax:

```
<Installation_executable> /s /v"/qn INSTALLDIR=\"install-dir\" REGISTERHOSTPTS=\"Options\"
```

where:

- `/s` (required) specifies that this is a silent install.
- `/v` (required) specifies that you want to pass command line options and values of public properties through to the installer.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR=\"install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTPTS=\"Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

Parameter	Description
<i>DSM host name</i>	Required if you want to register CTE with a DSM.

Parameter	Description
<code>-secret=shared-secret</code>	Specifies the shared secret for the DSM. This value is required for shared secret registration.
<code>-agent=your.agent.name.com</code>	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
<code>-keyagentpwd</code>	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
<code>-useip</code>	Use the IP address of the protected host instead of host name. Used when <code>-agent</code> is not supplied.
<code>-description="description"</code>	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
<code>-port=port</code>	Specifies the port number this CTE Agent should use.
<code>-usehwsig</code>	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
<code>-enableldt</code>	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.
<code>-enablees</code>	Specify this option automatically enable and register CTE-Efficient Storage during silent install.
<code>-log=%temp%\vor-agent-reg.log</code>	Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).
<code>-onewaycomms</code>	Specify this option when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

Note: If you want to enter an option with spaces in any value, it must be surrounded in two double-quotes with an escape character (\) before each double-quote. If the syntax is incorrect, the installation will fail.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- CTE will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be double-quoted, with each quote preceded by the escape character (\). For example:
`INSTALLDIR=\"\"C:\cte\custom dir\"\"`.
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).

- The host will be registered with the description `This host was silently installed` (`-description` parameter). Again, the spaces in the description require the same syntax as in the installation directory name. For example: `-description=\"\"This host was silently installed\"\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> vee-fs-7.0.0-47-win64.exe /s /v" /qn
INSTALLDIR=\"\"C:\cte\custom dir\"\"
registerhostopts=\"my-key-mgr.example.com -agent=my-host.example.com
-secret=MaCarena45# -domain=my-domain -description=\"\"This host was silently installed\"\""
```

Example: CTE-LDT, CTE-Efficient Storage, One-way Communication, Hardware Acceleration

The following example specifies that:

- The agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), CTE-Efficient Storage (`-enableees` parameter), one-way communication (`-onewaycomms` parameter) and hardware association (`-usehwsig` parameter) features are enabled.
- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).

```
C:\> vee-fs-7.0.0-47-win64.exe /s /v" /qn
registerhostopts=\"my-key-mgr.example.com -useip -enableldt -enableees
-onewaycomms -usehwsig -secret=MaCarena45# -domain=my-domain\""
```

Silent Installation Using the MSI File and Shared Secret Registration Method

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a DSM using the MSI file and the shared secret registration method. For a list of other available methods, see ["Silent Installation on Windows" on page 40](#).

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `MSI` file onto the Windows system.
3. Run the installation exe file using the following syntax:

```
msiexec.exe /i <Installation_executable> /qn INSTALLDIR=\"install-dir\"  
REGISTERHOSTOPTS=\"REGISTERHOSTOPTS_Options\"
```

where:

- `/i` (required) enables CTE installation.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR=\"install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTOPTS=\"Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

Parameter	Description
<i>DSM host name</i>	Required if you want to register CTE with a DSM.
<code>-secret=shared-secret</code>	Specifies the shared secret for the DSM. This value is required for shared secret registration.
<code>-agent=your.agent.name.com</code>	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
<code>-keyagentpwd</code>	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
<code>-useip</code>	Use the IP address of the protected host instead of host name. Used when <code>-agent</code> is not supplied.
<code>-description="description"</code>	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
<code>-port=port</code>	Specifies the port number this CTE Agent should use.
<code>-usehwsig</code>	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
<code>-enableldt</code>	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.
<code>-enablees</code>	Specify this option to automatically enable and register CTE-Efficient Storage during silent install.

Parameter	Description
-log=%temp%\vor-agent-reg.log	Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).
-onewaycomms	Specify this option when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- CTE will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be in double-quotes. For example: `INSTALLDIR="C:\cte\custom dir"`.
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).
- The host will be registered with the description `This host was silently installed` (`-description` parameter). Because `-description` is inside a double-quoted string, you must escape the double-quotes `-description=\"This host was silently installed\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> msixec.exe /i vee-fs-7.0.0-47-win64.exe /qn
INSTALLDIR="C:\cte\custom dir"
registerhostopts="my-key-mgr.example.com -agent=my-host.example.com -secret=MaCarena45#
-domain=my-domain -description=\"This host was silently installed\""
```

Example: CTE-LDT, CTE-Efficient Storage, One-way Communication, Hardware Acceleration

The following example specifies that:

- The agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), CTE-Efficient Storage (`-enableees` parameter), one-way communication (`-onewaycomms` parameter) and hardware association (`-usehwsig` parameter) features are enabled.
- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).

```
C:\> msixec.exe /i vee-fs-7.0.0-47-win64.exe /qn
registerhostopts="my-key-mgr.example.com -useip -enableldt -enableees -onewaycomms -usehwsig
-secret=MaCarena45# -domain=my-domain"
```

Silent Installation Using the exe File and Fingerprint Registration Method

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a DSM using the exe file and the fingerprint registration method. For a list of other available methods, see ["Silent Installation on Windows" on page 40](#).

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `exe` file onto the Windows system.
3. Run the installation exe file using the following syntax:

```
<Installation_executable> /s /v"/qn INSTALLDIR=\"install-dir\" REGISTERHOSTPTS=\"Options\"
```

where:

- `/s` (required) specifies that this is a silent install.
- `/v` (required) specifies that you want to pass command line options and values of public properties through to the installer.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR=\"install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this paramater, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTPTS=\"Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

Parameter	Description
<i>DSM host name</i>	Required if you want to register CTE with a DSM.
<i>-agent=your.agent.name.com</i>	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

Parameter	Description
-keyagentpwd	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
-useip	Use the IP address of the protected host instead of host name. Used when -agent is not supplied.
-description="description"	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
-port=port	Specifies the port number this CTE Agent should use.
-usehwsig	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
-enableldt	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.
-enablees	Specify this option automatically enable and register CTE-Efficient Storage during silent install.
-log=%temp%\vor-agent-reg.log	Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).
-onewaycomms	Specify this option when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

Note: If you want to enter an option with spaces in any value, it must be surrounded in two double-quotes with an escape character (\) before each double-quote. If the syntax is incorrect, the installation will fail.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- CTE will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be double-quoted, with each quote preceded by the escape character (\). For example:
`INSTALLDIR=\"\"C:\cte\custom dir\"\"`.
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using the host name `my-host.example.com` (-agent parameter).
- The host will be registered with the description `This host was silently installed` (-description parameter). Again, the spaces in the description require the same syntax as in the installation directory name. For example: `-description=\"\"This host was silently installed\"\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.


```
C:\> vee-fs-7.0.0-47-win64.exe /s /v" /qn
INSTALLDIR="\"C:\cte\custom dir\"\"
registerhostopts=\"my-key-mgr.example.com -agent=my-host.example.com
-description=\"\"This host was silently installed\"\"\""
```

Example: CTE-LDT, CTE-Efficient Storage, One-way Communication, Hardware Acceleration

The following example specifies that:

- The agent will be installed in the default installation directory (the INSTALLDIR parameter is omitted).
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), CTE-Efficient Storage (`-enableees` parameter), one-way communication (`-onewaycomms` parameter) and hardware association (`-usehwsig` parameter) features are enabled.

```
C:\> vee-fs-7.0.0-47-win64.exe /s /v" /qn
registerhostopts=\"my-key-mgr.example.com -useip -enableldt -enableees
-onewaycomms -usehwsig\""
```

Silent Installation Using the MSI File and Fingerprint Registration Method

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a DSM using the MSI file and the fingerprint registration method. For a list of other available methods, see ["Silent Installation on Windows" on page 40](#).

Note

Thales supports installing or upgrading CTE agents with Microsoft System Center Configuration Manager (SCCM) using MSI installation binaries. For details on how to do that, see your SCCM documentation.

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation MSI file onto the Windows system.
3. Run the installation exe file using the following syntax:

```
msiexe.exe /i <Installation_executable> /qn INSTALLDIR=\"install-dir\"
REGISTERHOSTOPTS=\"REGISTERHOSTOPTS_Options\"
```

where:

- `/i` (required) enables CTE installation.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR="install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\ Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTOPTS="Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

Parameter	Description
<i>DSM host name</i>	Required if you want to register CTE with a DSM.
<code>-agent=your.agent.name.com</code>	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
<code>-keyagentpwd</code>	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
<code>-useip</code>	Use the IP address of the protected host instead of host name. Used when <code>-agent</code> is not supplied.
<code>-description="description"</code>	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
<code>-port=port</code>	Specifies the port number this CTE Agent should use.
<code>-usehwsig</code>	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
<code>-enableldt</code>	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.
<code>-enablees</code>	Specify this option automatically enable and register CTE-Efficient Storage during silent install.
<code>-log=%temp%\vor-agent-reg.log</code>	Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).
<code>-onewaycomms</code>	Specify this option when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- CTE will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be in double-quotes. For example: `INSTALLDIR="C:\cte\custom dir"`.
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The host will be registered with the description `This host was silently installed` (`-description` parameter). Because `-description` is inside a double-quoted string, you must escape the double-quotes `-description=\"This host was silently installed\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> msixec.exe /i vee-fs-7.0.0-47-win64.exe /qn  
INSTALLDIR="C:\cte\custom dir"  
registerhostopts="my-key-mgr.example.com -agent=my-host.example.com -description=\"This host  
was silently installed\""
```

Example: CTE-LDT, CTE-Efficient Storage, One-way Communication, Hardware Acceleration

The following example specifies that:

- The agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), CTE-Efficient Storage (`-enablees` parameter), one-way communication (`-onewaycomms` parameter) and hardware association (`-usehwsig` parameter) features are enabled.

```
C:\> msixec.exe /i vee-fs-7.0.0-47-win64.exe /qn  
registerhostopts="my-key-mgr.example.com -useip -enableldt -enablees -onewaycomms -usehwsig"
```

Windows Silent Install Command Line Options

The MSI and self-extracting `.exe` silent install methods require different command line options to specify a silent installation. However, the parameters specific to CTE installation are the same for both MSI and self-extracting `.exe` install methods. See the following tables for required and optional command line options.

For a specific silent install procedure, see one the following:

- ["Silent Installation Using the exe File and Shared Secret Registration Method" on page 41](#)
- ["Silent Installation Using the MSI File and Shared Secret Registration Method" on page 43](#)
- ["Silent Installation Using the exe File and Fingerprint Registration Method" on page 46](#)
- ["Silent Installation Using the MSI File and Fingerprint Registration Method" on page 48](#)

General Format for Self-extracting .exe Silent Install Commands

For self-extracting `.exe` silent installations, be sure to escape the quotes surrounding the parameters passed in `REGISTERHOSTOPTS_Options` using a backslash (`\`) as shown:

```
<Installation_executable> /s /v"/qn REGISTERHOSTOPTS=\"REGISTERHOSTOPTS_Options\"
```

For example:

```
vee-fs-7.0.0-47-win64.exe /s /v"/qn REGISTERHOSTPTS=\"SecSrv.demo.com -useip\""
```

General Format for MSI Silent Install Commands

Use the following syntax for MSI silent installations:

```
msiexe.exe /i <Installation_executable> /qn REGISTERHOSTPTS="REGISTERHOSTPTS_Options"
```

For example:

```
msiexec.exe /i vee-fs-7.0.0-47-win64.msi /qn REGISTERHOSTPTS=" SecSrv.demo.com -useip"
```

Command Line Options for MSI and .exe Silent Installations

Refer to the following tables for required and optional command line options for MSI and self-extracting .exe CTE silent installations.

The following table lists the command line options for self-extracting .exe binary types.

Windows Attribute	Description	Required?
/s	Run the installation in silent mode.	Yes
/v	Pass command-line options and values of public properties through to the installer.	Yes

The following table lists the command line options for MSI binary types.

Windows Attribute	Description	Required?
/i	Enable installation/configuration	Yes, for installation
REINSTALLMODE=voums	Required REINSTALLMODE codes for upgrades	Yes, for upgrade
REINSTALL=ALL	Required REINSTALL setting for upgrades	Yes, for upgrade
/x	Required for uninstallation. See Chapter 14: "Uninstalling CTE from Windows" on page 139 .	Yes, for uninstall

The following table lists the command line options common to both MSI and self-extracting .exe binary types.

Windows Attribute	Description	Required?
/qn	Run the command in non-interactive mode (no GUI).	Yes
REGISTERHOSTPTS	Options for registering CTE with the DSM. The full set of options is specified below.	No
INSTALLDIR	Specifies an alternate location for installing CTE. Notes: • If syntax is incorrect, silent install will fail. See examples. • The alternate location must be on the system drive.	No
REBOOT=ReallySuppress	By default, the machine reboots after installation. Supplying this option prevents that. However, a reboot is still required to fully install CTE.	No

The following table lists the REGISTERHOSTOPTS parameters that determine log settings and CTE configuration settings. The REGISTERHOSTOPTS parameters are common to both MSI and self-extracting .exe binary types.

Parameter	Description
<i>DSM host name</i>	Required if you want to register CTE with a DSM.
<i>-secret=shared-secret</i>	Specifies the shared secret for the DSM. This value is required for shared secret registration.
<i>-agent=your.agent.name.com</i>	FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.
<i>-keyagentpwd</i>	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
<i>-useip</i>	Use the IP address of the protected host instead of host name. Used when <i>-agent</i> is not supplied.
<i>-description="description"</i>	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does <i>not</i> overwrite the existing description even if this option is specified.
<i>-port=port</i>	Specifies the port number this CTE Agent should use.
<i>-usehwsig</i>	Specify this option when you want to associate this installation with the machine hardware for cloning prevention.
<i>-enableldt</i>	Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) during silent install.
<i>-enableeas</i>	Specify this option automatically enable and register CTE-Efficient Storage during silent install.
<i>-log=%temp%\vor-agent-reg.log</i>	Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).
<i>-onewaycomms</i>	Specify this option when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

Registering CTE with the Shared Secret Registration Method After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see ["Installing CTE and Registering Using the Certificate Fingerprint Method" on page 38](#) or ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 36](#).

1. Log on to the host as a Windows user with administrative privileges.
2. Launch the CTE Registration Wizard using one of the following methods:
 - In the system tray, right click the CipherTrust Lock icon and select **Register Host**.
 - Run `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.exe`.

3. In the Register Host dialog box, verify the host's machine name and click **Next**.
4. On the *Gathering agent information* page, select the **File System** check box and click **Next**.
5. On the *Gathering Key Manager information* page, enter the FQDN of the Primary DSM. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



When you are done, click **Next**. CTE communicates with the selected DSM to validate what features have been licensed and are available to the CTE Agent.

6. On the *Gathering host name information* page:
 - Specify the host name or IP address of the host. You can select the host name from the drop-down list or type it in the field. If you specify a host name, it must be resolvable by the DNS server (see ["Host Name Resolution Requirements" on page 33](#)).
 - To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association \(Cloning Prevention\) Option" on page 34](#).
 - If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the host, select the **Enable LDT Feature** check box. For details on CTE-LDT, see the *CTE-Live Data Transformation with Data Security Manager*.
 - If you want to have the CTE-Efficient Storage feature available on the host, select the **Enable ES Feature** check box. For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
 - Make sure the **Use Shared Secret Registration** check box is enabled.

When you are done, click **Next**.

Note: If you get the message "Only CTE-initiated communication is possible", make sure that the DSM and CTE can communicate over the network.

7. On the *Gathering shared secret registration information* page, enter the following:
 - **Shared secret:** The shared secret established for the domain in the DSM to which you intend to add this host. Contact the DSM Administrator for this value.
 - **Domain name:** The name of the DSM domain to which the host will be added. Contact the DSM Administrator for this information.
 - **Host group** (optional): The name of the host group to which the host will be added. Contact the DSM Administrator for this value.
 - **Host description** (optional): A user-defined description of the host to be registered.



WARNING

The shared secret, domain name, and host group are case-sensitive. If any of these are entered incorrectly, an error message displays. If you exceed the number of allowable login attempts to the DSM, you will be locked out of the DSM. For more information, talk to your DSM Administrator.

When you are done, click **Register**. CTE contacts the DSM and attempts to register the host with the specified options. The Register Host dialog box displays a message with the results of the registration request.

If the registration completed successfully, click **Finish**.

8. Restart the host to complete the installation process.
9. After the host has rebooted, you can verify the installation by checking CTE processes:
 - a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
 - b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.

Registering CTE with the Fingerprint Registration Method After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see ["Installing CTE and Registering Using the Certificate Fingerprint Method" on page 38](#) or ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 36](#).

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host as a Windows user with administrative privileges.
2. Launch the CTE Registration Wizard using one of the following methods:
 - In the system tray, right click the CipherTrust Lock icon and select **Register Host**.
 - Run `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.exe`.
3. In the Register Host dialog box, verify the host's machine name and click **Next**.

Note: The machine name shown here does *not* need to match the one specified in the DSM. You will have an opportunity to select a different machine name later in this procedure.

4. On the *Gathering agent information* page, select the **File System** check box and click **Next**.
5. On the *Gathering Key Manager information* page, enter the FQDN of the Primary DSM. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



When you are done, click **Next**. CTE communicates with the selected DSM to validate what features have been licensed and are available to the CTE Agent.

6. On the *Gathering host name information* page:

- Specify the host name or IP address of the host. You can select the host name from the drop-down list or type it in the field. If you specify a host name, it must be resolvable by the DNS server (see ["Host Name Resolution Requirements" on page 33](#)).



WARNING

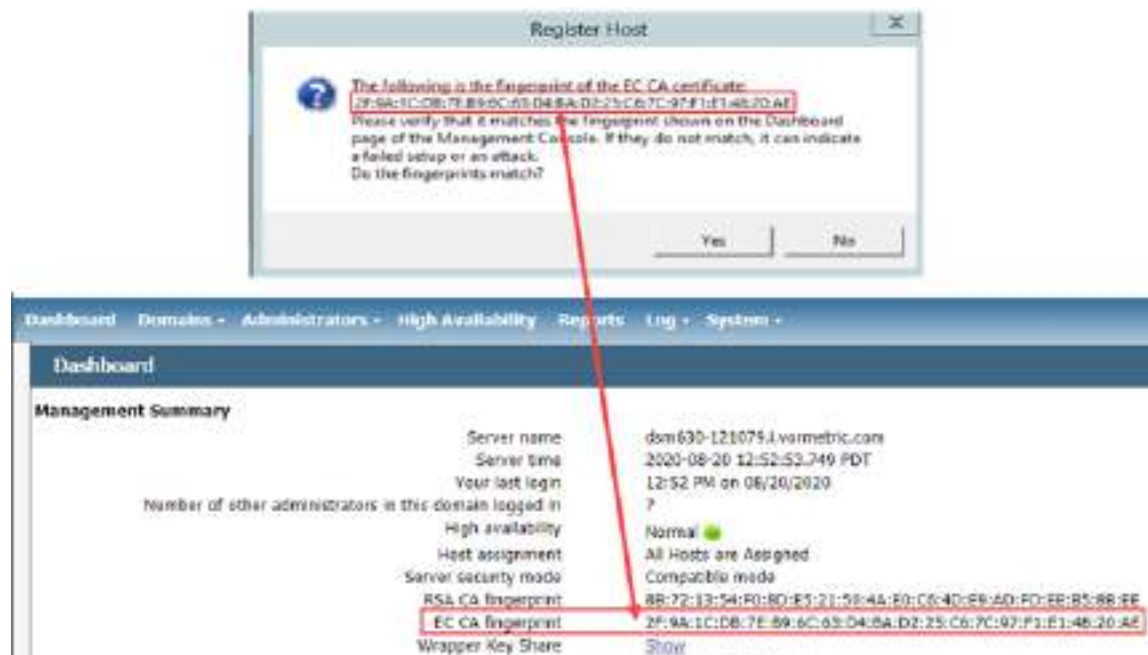
The host name specified here must exactly match the host name specified in the DSM in order for the fingerprints to match.

- To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association \(Cloning Prevention\) Option" on page 34](#).
- If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the host, select the **Enable LDT Feature** check box. For details on CTE-LDT, see the *CTE-Live Data Transformation with Data Security Manager*.
- If you want to have the CTE-Efficient Storage feature available on the host, select the **Enable ES Feature** check box. For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
- Clear the **Use Shared Secret Registration** check box so that CTE will use the Fingerprint Registration Method.

When you are done, click **Register**.

Note: If you get the message “Only CTE-initiated communication is possible”, make sure that the DSM and CTE can communicate over the network.

7. CTE displays the Register host status page and displays the EC CA Certificate that it received from the DSM. This fingerprinting should exactly match the fingerprint displayed on the DSM Dashboard page. For example:



If the fingerprints match, click **Yes**.

8. Click **OK** when CTE displays the fingerprint for the host's certificate.
The *Register host status* page shows the two fingerprints and displays a message about the registration status. If the registration completed successfully, click **Finish**.
9. Restart the host to complete the installation process.
10. After the host has rebooted, you can verify the installation by checking CTE processes:
 - a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
 - b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.

Guarding a Device with the DSM

After you register a device with a DSM, you can create as many GuardPoints on the device as you need. These GuardPoints can protect the entire device or individual directories or files.

In order to guard a device, you need to use the DSM Management Console to:

1. Access the DSM domain in which the host is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device.
3. Identify or create a policy for the device that specifies the access controls and the encryption keys to use for the device.
4. Create a GuardPoint for the device.

The following example creates a simple policy with a single key rule and no access controls and uses it to guard several directories on a registered host. For all of the following procedures, you must be logged into the DSM Management Console as a DSM Administrator, and you must be in the domain with which the host is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the *DSM Administration Guide*.

Access the DSM Domain

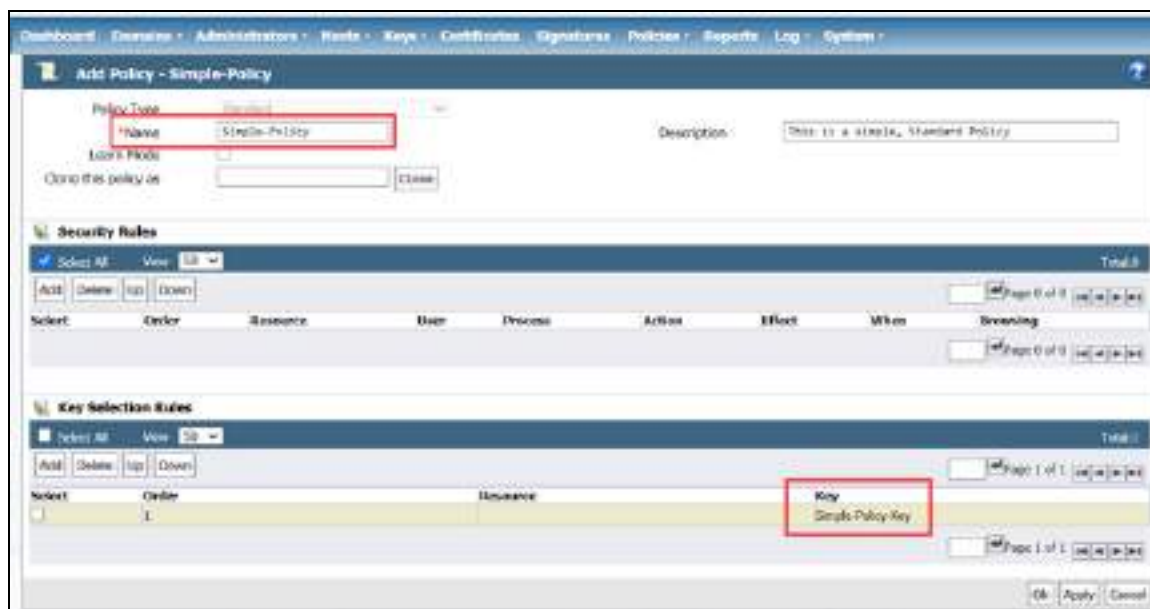
1. In a web browser, navigate to the URL of the DSM you want to use and log in with DSM Administrator credentials.
2. In the top menu bar of the DSM Management Console, select **Domains > Switch Domains**.
3. Select the domain with which the host you want to protect is registered and click **Switch to domain**.

Create an Encryption Key

1. In the top menu bar of the DSM Management Console, select **Keys**.
2. In the Key table, click **Add**
3. In the **Name** field, add a name for the key. This name must be unique. For example, Simple-Policy-Key.
4. Set any other desired options or use the defaults provided.
5. Click **Ok**.

Create a Standard Policy

1. In the top menu bar, select **Policies**.
2. In the Policy table, click **Add**.
3. In the Add Policy page:
 - a. Select a Policy Type. In this example, we will create a Standard policy.
 - b. Enter a name for the policy in the **Name** field. For example, Simple-Policy.
 - c. Enter a description for the policy in the **Description** field.
 - d. In the Key Selection Rules section, click **Add**.
 - e. In the Key field, click **Select**.
 - f. Select the key you created earlier and click **Select key**.
 - g. Click **Ok**.



4. Click **Ok** to create the policy.

Create a GuardPoint

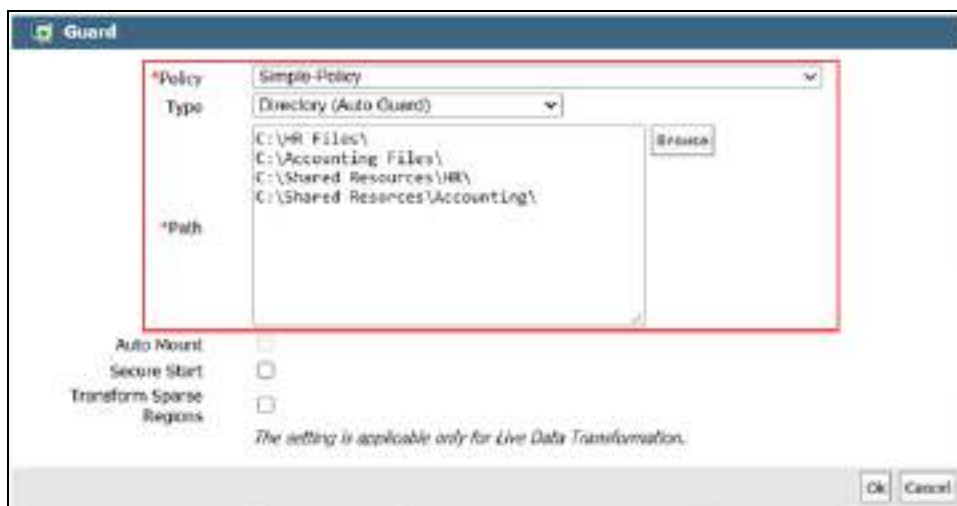
1. Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
 - C:\HR Files\
 - C:\Accounting Files\
 - C:\Shared Resources\HR\
 - C:\Shared Resources\Accounting\

Tip: If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

2. In the top menu bar, click **Hosts**.
3. In the Hosts table, click on the name of the host you want to protect.
4. Click the **GuardPoints** tab.

5. In the GuardPoints table, click **Guard**.
6. In the Guard page:
 - a. In the **Policy** field, select the policy you created earlier.
 - b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Directory (Auto Guard)**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a Windows-style explorer.

If you want to enter multiple paths, put each path on its own line. For example:



- d. Click **Ok**.

The DSM pushes the GuardPoint configuration to the host and CTE immediately begins transforming the data in the specified folders from clear-text to cipher-text.
7. When the data transformation has finished, applications can resume accessing the now-protected data.

Chapter 3: Special Cases for CTE Policies

This chapter describes some CTE-specific configuration tasks related to configuring policies in the DSM and contains the following sections:

More Information About Configuring CTE Policies	60
Re-Signing Executable Files on Secfs GuardPoints	60
Restricting Access Overrides from Unauthorized Identities	61
Behavior of Hard Links Inside and Outside of GuardPoints (Windows)	61

More Information About Configuring CTE Policies

This chapter describes some special cases that apply only to CTE agent policy configuration. See the DSM Administration Guide for general information about configuring policies. The following chapters in the *DSM Administration Guide* pertain specifically to the information in this chapter:

- “Creating and Configuring Signature Sets”
- “Configuring Hosts and Host Groups”
- “Configuring Policies”

Re-Signing Executable Files on Secfs GuardPoints

If any of your existing VTE for Windows hosts are running VTE versions prior to version 6.2.0, an issue affects signed executables in Live Data Transformation policies. In these older VTE versions, any executable that is part of either a host setting or a Signature set, and resides in a GuardPoint that uses a Live Data Transformation policy will have a different SHA signature after every LDT key rotation. After each LDT key rotation, the host settings executables will no longer be authenticated, or the Signature Set policy rules that include those executables will no longer match them as expected. This problem occurred because VTE generated an SHA signature of the encrypted executable which changes after each key rotation. To work around these issues on these older VTE versions, the DSM Security Administrator must manually re-sign each affected executable after each key rotation. This workaround is *not* needed for any VTE for Windows release version 6.2.0 or later.

The SHA signature is created from the unencrypted executable. This new SHA signature does not change with a key rotation.

If upgrading or installing a new machine using the same signature sets that you used previously, do the following:

1. Install the current release of the CTE Agent. The previous signatures will be used until the next key rotation.
2. Before the next key rotation, the security administrator must resign the binaries.
3. Do not remove the old signatures on the DSM or CipherTrust Manager until all agents have been upgraded to the latest CTE release. Refer to the *DSM Installation and Configuration Guide* for information on how to perform a manual re-sign.
4. After all agents have been upgraded, then you can remove the old signatures.

Note

In previous releases, if the executable was in a GuardPoint protected directory, but was the same as an unguarded executable, the administrator could restrict only the guarded executable. In the current release of CTE, the unguarded executable matches the guarded executable with regards to policies.

Restricting Access Overrides from Unauthorized Identities

In some setups, system administrators can use the host settings > `|authenticator|` feature with `su` to change identities and gain access to restricted data. Now, you can instruct CTE to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CTE can block from authenticating other processes.

Any executable path that is marked with a `|path_no_trust|` host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

CTE prevents overrides from other host settings authenticators, using the `|path_no_trust|` status. If a user runs the `su` command from a non-trusted shell, that new shell is still marked as `|path_no_trust|`, even if `|authenticator|/usr/bin/su` is specified in the host-settings. The `|path_no_trust|` feature overrides any and all authenticators under host settings.

To restrict access overrides in the DSM:

1. At the DSM Management Console, click **Hosts > Hosts**.
2. Click on an existing host name to edit the host.
3. Click **Host Settings** tab.
4. Add the following to the host settings:

```
|path_no_trust|<path of the binary>
```

For example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **OK**.

To restrict access overrides in CipherTrust Manager:

1. In the CipherTrust Manager Applications Page, click **CTE > Clients**.
2. Click on an existing client name to edit the client.
3. Click **Client Settings** tab.
4. Add the following to the client settings:

```
|path_no_trust|<path of the binary>
```

For example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **OK**.

Behavior of Hard Links Inside and Outside of GuardPoints (Windows)

When using hard links on Windows, all the hard links to a file must be within the boundary of a GuardPoint and must use the same key. The following scenarios provide additional details:

- If hard links to the same file are inside a GuardPoint and outside a GuardPoint, the effect on the file depends on what process accesses which hard link first. If the hard link within the GuardPoint is opened first, the file is transformed. If the hard link outside the GuardPoint is opened first, the file won't be transformed.

- If hard links to the same file exist in different GuardPoints with different keys, the file will be corrupted.
- If hard links to the same file exist in the same GuardPoint but with different keys, such as if folder-based rules are used, there will be a conflict in the key.

Chapter 4: Concise Logging

This chapter contains the following sections:

Overview of Concise Logging	63
Using Concise Logging	63

Overview of Concise Logging

Thales's standard operational logging sends audit messages for each file system operation. An audit message is sent each time a file is opened, read, updated, or written. Thales's standard logging can generate high volumes of log data. Most of these messages might not be useful or required by security administrators to monitor file system activity on the system.

Concise Logging allows you to focus on relevant audit messages and important actionable messages, such as errors and warnings. It can eliminate the repetitive and less important audit messages generated by read and write activity on a file, reading and writing directory attributes, and other file system activity.

Concise Logging eliminates the following types of messages:

- Duplicate audit messages for each and every block read by the user or application. With Concise Logging, CTE only sends an audit message the *first* time a user or application performs a read/write activity. Subsequent read/write activity by that user or application is not logged.
- Audit messages that read the attributes, read the basic information of file-set attributes, and other event-based messages.
- Audit messages for directory open, read directory attributes, and directory close.

Using Concise Logging

You can enable and disable the Concise Logging option from the DSM or CipherTrust Manager for the following:

- All registered hosts in all domains; see ["Configuring Global Concise Logging with the DSM" on the next page](#).
- A host that has registered with the DSM; see ["Configuring Concise Logging for a Registered Host with the DSM" on the next page](#).

Considerations

- Concise Logging changes the set of log messages that are sent to Security Information and Event Management (SIEM) software systems. If this results in loss of data required for customer reports, then disable Concise Logging.
- Concise Logging is only supported by CTE `secfs`.
- Enable and disable Concise Logging on the host. CTE applies it to all GuardPoints and for all users on the host for which it is selected. There is no finer-grained control, such as per GuardPoint, user, or message type.
- When you enable this setting at the DSM level, it applies to all hosts in all domains, that are added to the DSM, but does not apply to any existing hosts. Hosts added after this setting is enabled inherit this setting. The default global setting is off.
- Do not use Learn mode with Concise Logging.

Configuring Concise Logging for CTE Clients or Client Groups with CipherTrust Manager

In CipherTrust Manager, when you create a Client Profile, you can select to Enable Concise Logging. Then, you can apply that Client Profile to a specific client, or to all clients in a Client Group. To enable Concise Logging, see the chapter *Managing Profiles* in the *CTE Administrator Guide*.

Configuring Global Concise Logging with the DSM

You can enable or disable Concise Logging at any time. The DSM controls the function. Any change in the Concise Logging is reflected on any newly registered hosts and their domains.

To configure global Concise Logging:

1. Log in to the DSM with System Admin privileges.
2. Click **System > Log Preferences**. Your system may contain multiple log tabs.
3. Click on a **Log** tab.
4. In the Duplicate Message Suppression Settings field, click **Enable Concise Logging**.
5. Click **Apply**.
6. Repeat steps for any other logs, as appropriate.

The host sends the following message after the administrator has enabled Concise Logging for an individual host:

```
DAO00821: Administrator "voradmin" updated Security Server configuration "Concise Logging Enabled" from "true" to "false".
```

Configuring Concise Logging for a Registered Host with the DSM

You can enable Concise Logging for a host after you have registered it with the DSM. Hosts that are added to the DSM after enabling Concise Logging inherit the global settings from the DSM. This setting can be customized at any time.

To enable Concise Logging on the DSM for a registered host:

1. Log into your host with DSM Security Administrator privileges.
2. Select the host that you would like to customize.
3. Select a **Log** tab.
4. In the Duplicate Message Suppression Settings, click **Enable Concise Logging**.
5. Click **Apply**.

After you enable or disable Concise Logging, CTE generates a log message to record that event:

```
[CGA] [INFO] [CGA3201I] [11/11/2016 10:57:18] Concise logging enable  
[CGA] [INFO] [CGA3202I] [11/11/2016 10:57:27] Concise logging disabled
```

Chapter 5: Enhanced Encryption Mode

This chapter describes the enhanced AES-CBC-CS1 encryption mode for keys. It contains the following sections:

Compatibility	65
Disk Space	66
Encryption Migration	66
File Systems Compatibility	66
FileTable Support on Windows	67
Using the AES-CBC-CS1 Encryption Mode in DSM	67
Using the AES-CBC-CS1 Encryption Mode in CM	68
Exceptions and Caveats	68
Best Practices for AES-CBC CS1 Keys and Host Groups	68

The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

Note

AES-CBC-CS1 encryption does not require any additional license.

	AES-CBC	AES-CBC-CS1
Security Improvements		
Unique IV per-file	No	Yes
IV predictability	Yes	No
File System Support		
Local FS	NTFS/ReFS	NFS3/NFS4/CIFS
Remote FS	CIFS	CIFS (if the backend storage for the CIFS share is Windows-based storage).
Block Device Support (sevm)	Fully supported	No. When a policy contains a key with CBC-CS1 encryption mode, the guarding fails on the DSM, and an error message displays.

Compatibility

- Starting with VTE for Windows version 6.1.0, CTE is backward compatible with, and fully supports, the existing AES-CBC mode for both new and existing datasets.
- Starting with VTE for Windows version 6.1.0, CTE fully supports AES-CBC-CS1 encryption for LDT and offline data transformation on CTE Windows environments.
Versions of VTE prior to version 6.1.0 are *not* backwards compatible with AES-CBC-CS1 encryption. On these earlier versions, attempting to guard a device using a policy containing an AES-CBC-CS1 key will fail.
- Protected hosts supporting AES-CBC-CS1 encryption can be added to host groups.

Difference between AES-CBC and AES-CBC-CS1

The two encryption modes are completely different from a file format standpoint.

- AES-CBC-CS1 encryption only applies to file system directories; AES-CBC encryption applies to both files and block devices.

Notes

- If you attempt to use an AES-CBC-CS1 key to guard a block device or partition, the guarding fails with an error reported on the DSM or CipherTrust Manager, similar to: Raw or Block Device (Manual and Auto Guard) GuardPoints are incompatible with Policy "policy-xxx" that contains a key that uses the CBC-CS1 encryption mode."
 - While AES-CBC-CS1 encryption is supported on both Linux and Windows environments, the file formats are incompatible. An encrypted file created with a specific AES-CBC-CS1 key on Windows cannot be read on Linux, even if that specific key were to be used and vice versa.
- AES-CBC-CS1 uses cipher-text stealing to encrypt the last partial block of a file whose size is not aligned with 16 bytes.
 - Each file encrypted with an AES-CBC-CS1 key is associated with a unique and random base IV.
 - AES-CBC-CS1 implements a secure algorithm to tweak the IV used for each segment (512 bytes) of a file.

Disk Space

Files encrypted with AES-CBC-CS1 keys consume additional disk space in contrast to files encrypted with AES-CBC keys. This is because AES-CBC-CS1 encryption requires file IVs to be created and persistently stored in contrast to AES-CBC encryption which does not consume any additional disk storage.

Therefore, administrators need to plan and provision additional disk capacity prior to deploying AES-CBC-CS1 encryption.

	AES-CBC	AES-CBC-CS1
Local Windows FS	No change to file size. No ADS allocation.	Extra 4KB allocation (at minimum) in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.

Encryption Migration

You can use either LDT or offline dataxform to:

- Transform data encrypted by AES-CBC to AES-CBC-CS1 and vice versa.
- Transform AES-CBC-CS1 encrypted data to clear contents and vice versa.

File Systems Compatibility

On Windows, you can use AES-CBC-CS1 keys to guard currently supported file systems.

Note

The remote file system must have enough extra space to store the extra 4K bytes of the embedded header.

Storing Metadata

AES-CBC-CS1 encrypted files on Windows store the base IV of a file in a Windows ADS (Alternate Data Streams) associated with the file. The size required for saving the CS1 key depends on the allocation size of the file system. If the allocation size is set to 4k, then the new IV will require 4K of extra space on the disk. You can run the `fsutil fsinfo` tool to find out the allocation size of the file system.

The CS1 key is supported on following file systems:

- **NTFS**: Supported on all Windows platforms that are supported by CTE.
- **REFS**: Supported on Windows 2012 R2 and later.
- **CIFS**: Supported if the backend storage for the CIFS share is Windows-based storage.

Note

Some network storage servers do not support multiple ADS associated with a file.

To get the value of the base IV, type:

```
C:/>voradmin secfs iv get <file-name>
```

Note

The base IV of a file is protected. It cannot be set/modified/removed by commands and applications. However, if a GuardPoint is unguarded, the files in the GuardPoint are no longer protected. An adversary can then corrupt the content of the files, as well as the IVs.

AES-CBC-CS1 depends on the physical file system's support for extended attributes in a manner similar to the CipherTrust Transparent Encryption - Live Data Transformation feature.

Missing IV file

If the IV for a file is missing, or CTE is unable to read the IV, then CTE denies access to the file. This access denied message may trigger an application to display an error message. This message may vary from application to application.

	AES-CBC	AES-CBC-CS1
Local FS (Windows)	No change	Alternate Data Streams

FileTable Support on Windows

The CBC-CS1 key does not support FileTables. This is because FileTables do not support alternate data streams. The CS1 key requires the ability to write the per-file IV into an alternate data stream on each file.

Using the AES-CBC-CS1 Encryption Mode in DSM

Deploy AES-CBC-CS1 encryption by using a symmetric agent key type created in the DSM:

1. In the DSM, click **Keys > Agent Keys > Keys**.
2. Click **Add**.
3. In the Encryption Mode dropdown, select **CBC-CS1**.
4. In the Algorithm dropdown, select **AES128** or **AES256** to create an AES-CBC-CS1 key.

5. Edit or create a policy that will use the AES-CBC-CS1 key. In this policy:
 - If you are using NFS, in the **Security Rules** section, add a security rule that specifies:
Action: `f_rd_att`
Effect: `Permit, Apply Key`
This security rule allows CTE to read the base IV value in the file's embedded header over NFS. This rule is not needed if you are not using NFS.
 - In the **Key Selection Rules** section, click **Add** and select the AES-CBC-CS1 key.
6. Click **OK** to save the policy.
7. Push the policy to the GuardPoints that you want to use this encryption key.

Using the AES-CBC-CS1 Encryption Mode in CM

When you create a key in CTE, you enable Encryption Mode by selecting CTE Key Properties. See *Creating a New Key* in the "Managing Policies" chapter in the CTE Administrator Guide.

Exceptions and Caveats

Note the following when using AES-CBC-CS1 keys.

Guarding Existing Files Without Data Transformation

You must convert an existing file with clear text through offline data transformation or LDT. If you do not transform the file, then after you guard using an AES-CBC key, the file displays garbled characters.

If you use an AES-CBC-CS1 key, access to the file is blocked with an I/O error.

Best Practices for AES-CBC CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC CS1 keys unless all hosts are running VTE for Windows version 6.1.0 or CTE version 7.0.0 or later.

Chapter 6: Utilities for CTE Management

Thales provides a variety of utilities that augment the standard Windows utilities. This combination of tools helps administrators manage CTE. The following utilities are described in this chapter:

voradmin secfs Commands	69
vmsec Utility	70
agenthealth Utility	71
agentinfo Utility	72

voradmin secfs Commands

The `voradmin secfs list` and `voradmin secfs status` commands display GuardPoint and policy information on the host.

voradmin secfs List Commands

The `voradmin secfs list` command has the following options:

voradmin secfs list Options

guardpoints	Displays all the GuardPoints on the host.
policy	Displays all the policies used on the host.
logger	Displays the logging details on the host.
status	Displays the authentication settings on the host.

For example, to view all the GuardPoints on the host, you would enter:

```
C:\>voradmin secfs list guardpoints
Guard Point:      1
Policy ID:        16553
Policy name:      ES-Standard-Policy
Directory:        esg-disk1-demo
Type:             rawdevice
Status:           guarded

Guard Point:      2
Policy ID:        18857
Policy name:      Accounting-IT-Access-Policy
Directory:        G:\Data
Type:             local
Status:           guarded

Guard Point:      3
Policy ID:        18985
Policy name:      LDT-Policy
Directory:        C:\LDT-Folder
Type:             local
Status:           guarded
```

To view just the policies in use on the host, you would enter:

```
C:\>voradmin secfs list policy
Policy:           1
Policy name:      LDT-Policy
```

```
Type:                LDT

Policy:              2
Policy name:         ES-Standard-Policy
Type:                ONLINE

Policy:              3
Policy name:         Accounting-IT-Access-Policy
Type:                ONLINE
```

voradmin secfs status Commands

The `voradmin secfs status` command has the following options:

voradmin secfs status Options

keys	Displays the current status of the keys on the host.
lock	Displays the status of any system or agent locks on the host.

For example:

```
C:\>voradmin secfs status keys
Encryption keys are available

C:\>voradmin secfs status lock
FS Agent Lock: Disabled
System Lock: Disabled
```

vmsec Utility

The `vmsec` utility allows you to manage the security aspect of the CTE Agent on the host. On Windows the `vmsec` utility is `<windows-agent-install-dir>\vmd\bin\vmsec.exe`. The default path is:

```
C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmsec.exe
```

vmsec Syntax

check_install	Verifies that the kernel component is running. This command checks CTE services and reports if any of the services are not running.
challenge	Initiates challenge-response on the host. This command displays a File System Agent password challenge string and enter the response string when the DSM is not network accessible.
status	Displays kernel configuration.
vmdconfig	Displays the vmd configuration.
check_hwenc	Determines whether this system supports hardware crypto.
hwok	Reports status of hardware signature.
passwd [-p passwd]	Enters the host password when the DSM is not network accessible. User can unlock the GuardPoints with this password.
version	Displays the CTE version.

Displaying the CTE Challenge String

In addition to using `vmsec challenge` on Windows, you can also right-click the tray icon and select **Challenge...-> Response**. The *CTE Challenge/Response* window opens.

If no challenge string is displayed, the host password is static. If a challenge string displays, contact a DSM Administrator for the response string.

agenthealth Utility

The `agenthealth.ps` utility validates:

- Super-user privilege
- CTE Agent installation
- CTE registration to DSM Server
- CTE processes/modules that are running
- Available disk resources
- Current GuardPoints

Tests if the agent can reach the GuardPoints

- CTE log directory resource status

This directory contains pending CTE log files for upload. This utility reports the size and number of pending files for upload. These text files are logs that contain vmd/SecFS information. They are regenerated whenever secfs restarts. If the number of files is unexpectedly large, this can indicate a problem.

The Agent Health Check Script

The Agent health check script (`agenthealth.ps1`) is located in `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\`

To run the Agenthealth check script:

1. Run the power shell command to enable self-signing for the system.
Before running agent-health script make sure power shell command has enough privileges to execute the Powershell script. Some Windows operating systems have default execution policy set as `restricted`.
Use the Powershell command `Set- Execution-policy Remote Signed` to change the execution policy if needed.
2. Open the Powershell prompt as administrator.
3. Type:
`.\agenthealth.ps1`

For example:

```
.\agenthealth.ps1
Log file is at C:\Program
Files\Vormetric\DataSecurityExpert\agent\log\agent_health.log
Checking super user privilege..... OK
Vormetric Agent installation..... OK
Vormetric policy directory..... OK
Registration to server..... OK
Kernel drivers are loaded..... OK
VMD is running..... OK
SECFSD is running..... OK
```



```
rhat26130.qal.com is resolvable..... OK
rhat26130.qal.com port 8446 is reachable..... OK
rhat26130.qal.com port 8447 is reachable..... OK
Can communicate to at least one server..... OK
VMD is listening on port 7024..... OK
Time of last update from server 2016-12-01      14:39:49.038
Checking available disk space..... OK
Checking logging space ..... OK
    Log directory is "/var/log/vormetric"
    File system for log data is "/", 32G free (17% full)
    Log directory contains 2 of maximum 200 files (1% full)
    Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to C:\GP2..... OK
```

agentinfo Utility

The `agentinfo` utility collects system logs, CTE agent logs, CTE agent trace information, and system information for diagnostic purposes. All this information is saved in the destination path and compressed into a zip file. The `agentinfo` utility is available as an `agentinfo.js` Java command and as an `agentinfo.ps1` PowerShell command.

agentinfo Utility (Java version)

The `agentinfo.js` utility is a JavaScript file. You can open it in a text editor to see specific functions.

The `agentinfo.js` support collection scripts reside in the following path on systems where the CTE agent is installed.

To run the `agentinfo` script on Windows, navigate to one of the following folders:

```
C:\Program
Files\Vormetric\DataSecurityExpert\agent\vmd\bin

or

C:\Program
Files\Vormetric\DataSecurityExpert\agent\shared\bin
```

then run the following script:

```
agentinfo.js
```

agentinfo Utility (PowerShell version)

The PowerShell version of `agentinfo` supports several parameters.

PowerShell version agentinfo parameters

Directory - Specify the directory where all the collection information is saved. By default, this information is saved in the current directory.

ZipFile - Specify the name of the compressed file, where all the collected information will be archived. By default, this information is saved in the current directory.

Logfile - Specify the name of the files where verbose logs will be saved. By default, this information is saved in the current directory.

Examples for using agentinfo utility (PowerShell version)

To save all the collection information in “c:\AgentLogs” folder, run the following command:

```
.\agentinfo.ps1 -Directory 'C:\AgentLogs'
```

To save all the collected information in “c:\AgentLogs” folder and verbose logs in “c:\temp\AgentInfo.log”, run the following command:

```
.\agentinfo.ps1 -Directory 'C:\AgentLogs' -LogFile 'c:\temp\AgentInfo.log'
```

To save all the collected information in “c:\AgentLogs” folder, verbose logs in “c:\temp\AgentInfo.log”, and create the “AgentInfo.zip” archive file, run the following command:

```
.\agentinfo.ps1 -Directory 'c:\AgentLogs' -LogFile 'c:\temp\AgentInfo.log' -ZipFile  
'C:\temp\AgentInfo.zip'
```

Note

PowerShell 5.1 or later is required. Use the `$PSVersionTable.PSVersion` command to confirm which PowerShell version you are using.

Chapter 7: Using CTE with Microsoft SQL

This chapter discusses using CTE with Microsoft SQL AlwaysOn and SQL File Tables. It contains the following sections:

Using CTE with SQL	74
Using LDT with SQL FILESTREAM	74
Using CTE with SQL FileTables	74
Installing CTE on Microsoft SQL AlwaysOn	76
Data Transformation (Encryption in place)	79
Copy/Restore	79
SQL Server Policy Tuning	79
Using LDT with SQL AlwaysOn	79

Using CTE with SQL

You must stop the SQL service before guarding the SQL DB. When this occurs, the SQL Server replication may become unsynchronized. When restarting, it may take a brief period of time for the SQL Server replication to resynchronize with the other node. The SQL Server issues a warning against any attempted failovers during that brief period.

Note

Minimizing the duration for which the SQL Server service is stopped is beneficial for reducing the resynchronization period.

Using LDT with SQL FILESTREAM

When applying a Live Data Transformation (LDT) GuardPoint to SQL Server with FILESTREAM enabled, a rekey may be triggered which never finishes. This can occur if SQL Server is renaming files when the GuardPoint is applied, which causes the rekey to start the scan process again. If the rekey seems to be taking a long time, stop the SQL service until the rekey finishes and then restart the SQL service.

Using CTE with SQL FileTables

SQL FileTables allows you to store files and documents in special tables in the SQL Server called FileTables, but access them from Windows applications as if they were stored in the file system, without making any changes to your client applications. For some of the use cases, you can use FileTables with CTE.

Considerations

- The CTE Agent must be installed on the same server where the FileTables reside. If the FileTables reside on your SQL server, then you should install the CTE Agent on your SQL server.
- If multiple servers access the SQL FileTables:
 - Install CTE agent on all of the servers.
 - Protect all of the FileTable folders with the same CTE policy.

**CAUTION**

Accessing the FileTable without CTE may corrupt the data.

- When you create a new FileTable, alter, or drop FileTables, this may require applying a new GuardPoint.
- Every FileTable has a separate FileTable Folder so you must apply separate GuardPoints for each FileTable.
- You must apply a unique GuardPoint to each VNN path.
For example, if you configure two FileTables on an SQL Server, then the remote SQL administrator system must apply one GuardPoint to each configured VNN name.
- Guarding on a VNN name is similar to guarding a network path with CTE.
- If you want to access the FileTables from multiple remote systems, you must install CTE agent on those systems and apply the GuardPoints.

**CAUTION**

LDT is not supported with SQL FileTables. Only use offline Data Transformation to transform the initial SQL data.

Advantages

- System administrator cannot see the data locally on the SQL server because no CTE Agent is installed on the SQL server.
- The data transferring between servers is also encrypted.

Supported FileTables Use Cases

CTE supports the following FileTables use cases:

CTE Data Transformation of existing files in FileTables

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the FileTable folder for the existing FileTable.
3. Create an offline Data Transformation policy and apply to the GuardPoint on the FileTable folder.
4. Run the Dataxform utility to transform the data.

Protect files in SQL FileTables with CTE

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the FileTable folder for the existing FileTable.
3. Create a production policy and apply the GuardPoint on the FileTable folder.
4. Once the GuardPoint is active, you can use the file table to load and access files.

Protect files with SQL AlwaysOn Availability Groups with CTE

When the database that contains the FILESTREAM, or FileTable data, belongs to an AlwaysOn availability group, the FILESTREAM and FileTable functions accept or return virtual network names (VNNs) instead of computer names.

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the virtual network names (VNNs) for the existing FileTable.
3. Create a production policy and apply the GuardPoint to the VNN name
4. Once the GuardPoint is active, you can use the FileTable to load and access files.
5. When you enable FILESTREAM on an instance of SQL Server, it creates an instance-level share to provide access to the FILESTREAM data. Access this share by using the computer name in the following format:
`\\<computer_name>\<filestream_share_name>`
6. In an AlwaysOn availability group, the computer name is virtualized by using a Virtual Network Name, (VNN). When the computer is the primary replica in an availability group, and databases in the availability group contain FILESTREAM data, then SQL creates a VNN-scoped share to provide access to the FILESTREAM data. Applications that use the file system APIs have to use the VNN-scoped share, which has a path in the following format:

`\\<VNN>\<filestream_share_name>`

Install CTE on remote systems and guard the SQL Server VNN names

In this use case, CTE is installed on the SQL administrator system (a separate system from where the SQL Server resides) and a GuardPoint is applied to the VNN name.

Unsupported FileTables Use Cases

CTE does not support the following use cases:

1. Install CTE agent on the SQL Server and locally apply the GuardPoint on the SQL Server storage.
2. Access FileTables with Transact-SQL.
3. Access FileTables with File I/O APIs on the SQL server. Perform all file I/O on the remote system running the CTE agent.

Installing CTE on Microsoft SQL AlwaysOn

This section describes how to implement CTE with Microsoft SQL AlwaysOn in a variety of configurations for primary and secondary replica servers, and assumes that you have a basic understanding of Microsoft SQL database.

You may want to keep the primary server decrypted to serve all users, and use the secondary database for running reports or backups.

- If the database is encrypted, then the Volume Shadow copy-related backups will snapshot and backup encrypted protected data.
- Administrators with the `apply_key` permission can run a query and pull down reports from the secondary database server without affecting the performance of the primary database server.
- The secondary server could be in a remote Data Recovery location. You may want to secure it with encryption.
- LDT is supported with SQL AlwaysOn. See ["Using LDT with SQL AlwaysOn" on page 79](#) for more information.

Methods for Initial Encryption

There are multiple methods for performing the initial encryption of the databases. Decide on which of the following methods best fits your environment. For more information on transforming data, see the *CTE-Live Data Transformation with Data Security Manager*.

- Data Transformation – Encrypt data in place.
- Backup and Restore to a GuardPoint.
- Copy and paste the data into a GuardPoint.

Configuration 1

- Databases on primary server and secondary replica servers require encryption
- Database name and location of secondary replica server are the same as the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Change the primary database to offline mode.
3. Confirm the creation of a data transformation and/or operational policy.
4. Guard the folder containing the primary database files with that policy:
 - a. If using 'Encrypt data in place' as the selected method of encryption, execute the data transformation and then apply the operational policy.
 - b. If using the 'Copy/Restore' method of encryption, apply the operational policy on an empty folder/device.
5. On the secondary server, create a new folder to store the replicated database.

Note: The folder name and the path must be the same as the primary server.

6. Guard the folder with the operational policy.
7. Perform step 4 above for additional secondary server(s).
8. Put the primary database back into online mode.
9. Setup SQL AlwaysOn High Availability group to perform FULL Data Synchronization.
This copies the primary database and replicates it to secondary replica servers.
10. Verify that the databases in the secondary server are in “Synchronized” mode.

Configuration 2

- Database on the primary server does not require encryption, but the secondary replica database requires it
- Database names and locations for the secondary replica servers are the same as the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Confirm the creation of a data transformation and/or operational policy.
3. On the secondary server, create a new folder to store the replicated database.

Note: The folder name and the path must be the same as the primary server.

4. Guard the folder with the operational policy.
5. Perform step 3 & 4 above for additional secondary server(s).
6. Setup SQL AlwaysOn High Availability group to perform **FULL Data Synchronization**.
This copies the primary database and replicates it to secondary replica servers.
7. Verify that the databases in the secondary server are in “Synchronized” mode.

Configuration 3

- Databases on the primary and secondary replica servers require encryption
- Database name is the same, but the location of the secondary replica server is in a different location from that of the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Change the primary database to offline mode.
3. Confirm the creation of a data transformation and/or operational policy.
4. Guard the folder containing the primary database files with that policy:
 - a. If using 'Encrypt data in place' as the selected method of encryption, execute the data transformation and then apply the operational policy.
 - b. If using the 'Copy/Restore' method of encryption, apply the operational policy on an empty folder/device.
5. On the secondary server, create a new folder to store the replicated database.

Note: The folder name and the path must be the same as the primary server.

6. Guard the folder with the encryption policy.
7. From secondary server, perform the restore to the primary database.
 - a. Select the options **Restore with norecovery** and **Relocate all files to folder**.
 - b. Specify the path of the new folder from step 5.
8. Repeat steps 4 & 5 above for any additional secondary server(s).
9. Setup SQL AlwaysOn High Availability group to perform **JOIN ONLY Data Synchronization**.
This joins the secondary database to the SQL Always High Availability Group. It also establishes replication of new data and logs from the primary to the secondary replicated server.
10. Verify that the databases in the secondary server are in **Synchronized** mode.

Configuration 4

- Database on the primary server does not require encryption, but the secondary replica database requires encryption
- Database name is the same, but the location on the secondary replica server is in a different location than that of the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Confirm the creation of a data transformation and/or operational policy.
3. On the secondary server, create new folder to store the replicated database.
4. Guard the folder with the operational policy.
5. From secondary server, perform restore the primary database:
 - a. Select the options **Restore with norecovery** and **Relocate all files to folder**.
 - b. Specify the path of the new folder from step.
6. Setup SQL AlwaysOn High Availability group to perform **JOIN ONLY Data Synchronization**.
Joins the secondary database to the SQL Always HA Group. It also establishes replication of new data and logs from the primary to the secondary replicated server.
7. Verify that the databases in the secondary server are in **Synchronized** mode.

Data Transformation (Encryption in place)

For more information on transforming and encrypting data-in-place, see the *CTE-Live Data Transformation with Data Security Manager*.

Copy/Restore

For more information on transforming data using the copy and replace method, see the *CTE Data Transformation Guide*.

SQL Server Policy Tuning

In this section, you created and defined a process set for SQL Server that grants certain executables –in this case `sqlservr.exe`– unrestricted access to the database files. The need may arise to allow other executables, and/or users, access to the files.

You can grant this access by:

- Adding to the existing process set
- Creating a new one

The best option depends on the access requirements. The key decision is whether or not to select the **Apply Key** effect along with **Permit** or not. Omitting **Apply Key** on a security rule that still contains **Permit** allows the specified user or process to access to the data, but does not apply the encryption key, so therefore only shows them the data in its encrypted, cypher-text format. This is useful for anti-virus or backup software that may need to scan or copy the file, but does not necessarily need to see the contents.

Using LDT with SQL AlwaysOn

To guard a directory with an LDT (Live Data Transformation) policy, you must temporarily close all files in that directory. In a SQL Server AlwaysOn environment, this may entail temporarily stopping the SQL Server service on the node that is being guarded. Once the directory is guarded, then you can start the SQL Server service immediately.

It is important to remember the SQL Server AlwaysOn replication standard operating procedures.

- If one SQL Server service is taken offline for any reason, then once it is brought back on line, it takes the SQL Server a moment to re-synchronize the database nodes.
- The longer that secondary service was down, and the more inserts/updates and deletes that occurred on the still active node during that downtime, then the longer the synchronization period takes.
- During that synchronization period, any attempted fail over results in the SQL Server warning that data loss may occur if the fail over continues. However, once the SQL Server has completed re-synchronizing that secondary node, then any fail over is safe and does not result in loss of data.

Chapter 8: Secure Start

This chapter describes encrypting an Microsoft Active Directory (AD) with the Secure Start feature. It contains the following sections:

- Secure Start Overview 81
- Prerequisites 81
- Encrypt by Moving the AD Service into a Guarded Directory 82
- Encrypt Data in Place with Offline Transformation 84
- Encrypt with an LDT Transformation Policy 84
- Configure the Time Out Failure 84
- Recover a Server After it Loses Connection to the DSM 85
- Other Use Cases 86
- Best Practices for Encrypting and Protecting the AD Service 86

Secure Start Overview

Secure Start offers data protection for applications which start earlier in the boot sequence than VMD (Vormetric Daemon). For example, the Microsoft Active Directory system service starts very early in the boot sequence. To determine if another application qualifies, contact Thales technical support.

Notes

- Secure Start is included with CTE v6.0.2. You do not have to purchase it separately.
- Secure Start is supported on Windows Server 2008 R2 and later versions.

In CTE v6.0.1 and below, CTE cannot encrypt the AD system service because it boots earlier in the boot sequence than the VMD agent service. After it boots, VMD makes a secure connection with the DSM and retrieves the encryption keys from the DSM. Therefore, since AD boots before that, the AD system service is not encrypted.

CTE offers Secure Start through a new type of GuardPoint. A Secure Start GuardPoint starts before the AD services, and can, therefore, encrypt those services.

There are three methods for encrypting the directory:

- "Encrypt by Moving the AD Service into a Guarded Directory" on the next page
- "Encrypt Data in Place with Offline Transformation" on page 84
- "Encrypt with an LDT Transformation Policy" on page 84

Prerequisites

Prior to using Secure Start to guard your AD database:

1. Backup your AD database:
 - a. Navigate to **Administrative Tools**.
 - b. Click **Windows Server Backup**.
 - c. Click **Action > Backup Once**.
 - d. Follow the instructions in the Backup Wizard to create a backup of the server in a local drive.

Note: When the backup operation completes, it saves the server backup in `<backup drive>:\WindowsImageBackup\<BackupComputerName>`.

2. Perform a system state backup.
3. Obtain the Microsoft DSRM (Data Services Restore Mode) password.
4. Ensure that your AD database is not in `c:\Windows\NTDS`.



WARNING

Do not put your AD database in `c:\Windows` or `c:\Program files`. Secure Start cannot encrypt or decrypt any files in those folders.

Encrypt by Moving the AD Service into a Guarded Directory

You can move the AD service into a directory protected by a standard or LDT production policy. This method does not require the initial data transformation step. When you move the AD service into this directory, CTE immediately encrypts the data with either policy.

Note

This step occurs when the system is in DSRM mode, so users have no access to the AD service.

Create the AD GuardPath directory

Create the directory in which the AD service will reside.

1. Log in to the Active Directory Server in DSRM mode using the DSRM password. User ID is Administrator.
2. Create a folder to which you will move the AD database.

Apply Secure Start GuardPoints to a Directory with the DSM

Access to a Secure Start GuardPoint is only permitted during the boot sequence and for a short period of time. Once the VMD is up and running, it performs the normal agent initialization and communicates with the DSM to access files within a GuardPoint location.

To apply Secure Start GuardPoints in **DSM**:

1. In the DSM, click **Hosts > Hosts > <hostName>**
2. In the General host information section, select the option: **Secure Start GuardPoint**.
3. Click **GuardPoints**.
4. Select the directory and click **Guard**.
5. In the Policy field, select an **LDT** or **Standard Production** policy.
6. Set Type to **Directory (Auto Guard)**.
7. Click **Browse** and navigate to the folder that you just created for the AD database.
8. Select the option: **Secure Start**.
9. Click **OK**.
10. Select the GuardPoint and click **Secure Start On**.

Apply Secure Start GuardPoints to a Directory with CipherTrust Manager

To apply Secure Start GuardPoints in **CM**:

1. In the CipherTrust Manager Applications Page, click **CTE > Clients > <clientName>**.
2. Click **Create GuardPoint**.
3. In the Policy field, select a policy.
4. Set Type to **Auto Directory**.
5. Click **Browse**, navigate to, and select, the folder that you just created for the AD database.
6. Select the option: **Secure Start**.
7. Click **Create**.
8. Click **No** to the question, "Would you like to use these GuardPoint settings on another GuardPoint with a different path?" because you are only guarding the AD database.

Verify the Secure Start GuardPoint with CLI

After the policy is pushed to the Active Directory Server, verify the GuardPoints.

To verify the GuardPoints, type:

```
> voradmin ss verify <GuardPoint_path>
Successfully completed the command verify
Success from kernel -Successfully verified the secure start GP
```

Move the AD Database into the Secure Start GuardPoint

Move your AD database from the default location (c:\windows\NTDS) to this newly created protected folder.

To move the AD database:

1. In DSRM mode, login using the DSRM password. User ID is Administrator.
2. Start NTDSUTIL utility, type:

```
> activate instance ntds
```
3. Type:

```
> files
```
4. Type:

```
> move db to \<GuardPoint>
```
5. Type:

```
> move logs to \<GuardPoint>
```
6. Exit NTDSUTIL utility.
7. Reboot the system into normal mode. The Active Directory Services automatically starts after rebooting.

Note

This step occurs when the system is in DSRM mode, so users have no access to the AD service.

Encrypt Data in Place with Offline Transformation

Encrypting the AD database with a standard (production), or offline policy is very similar to encrypting other data with a standard (production), or offline policy.

The advantage to encrypting data in place is that it saves space. When you copy/move a directory into a guarded directory, you will need twice as much space to store the data because you leave a copy of the data in the original folder, as a precaution, until the original directory has been successfully moved and encrypted. Once the data is transformed, then you can delete the directory that contains the decrypted/clear data.

Using this method, you perform an Initial Data Transformation using the `dataxform` command line utility. During this transformation, access to the GuardPoint data is blocked. After initial transformation, you remove the initial policy, and then apply a production policy, so users can access the data.

Notes

- This step occurs when the system is in DSRM mode, so users have no access to the AD service.
- If your AD service is installed in the default directory, `C:\Windows\NTDS`, you must move it to another directory before you can encrypt it. See ["Encrypt by Moving the AD Service into a Guarded Directory" on page 82](#) for more information.

To encrypt the data:

1. In DSRM mode, login using the DSRM password. User ID is Administrator.
2. Create and apply a `dataxform` policy to the GuardPoint directory.
3. Run the `dataxform` command.
4. Remove the `dataxform` policy on the GuardPoint and replace it with a production policy.
5. Reboot out of DSRM mode.

Encrypt with an LDT Transformation Policy

Encrypting the AD database with an LDT policy uses the same steps as encrypting with a standard production policy. The only difference is that you select an LDT policy instead of a standard one. See ["Encrypt by Moving the AD Service into a Guarded Directory" on page 82](#) for more information.

Note

If your AD service is installed in the default directory, `C:\Windows\NTDS`, you must move it to another directory before you can encrypt it.

Configure the Time Out Failure

During the initial access to a Secure Start GuardPoint, the CTE agent sets a timer. The default duration is 120 seconds, but you can configure the duration. Minimum duration is one second, maximum duration is 300 seconds.

Data inside the GuardPoint is accessible without DSM connectivity until the timeout is reached. VMD service activates and makes a secure connection to the DSM. After the VMD makes a secure connection, the agent verifies that it is connected to correct DSM. If the VMD fails to connect to the DSM, the timeout is reached, and if AD is installed, the agent shuts down the system for data security purposes.

Note

In DSRM mode, when the timeout occurs, CTE removes the keys from memory. However, CTE does not shut down the system.

In normal mode, CTE shuts down the AD server. For any other application, or if AD is not installed, Secure Start does not shut down the server. However, the data inside the GuardPoint becomes inaccessible until DSM connectivity is restored, or you issue a challenge/response, or password. After the timer has expired, CTE denies any further access to the Secure Start GuardPoint.

1. To configure the timeout duration in seconds, type:

```
C:\> voradmin ss settimeout <timeout>
```

```
C:\> voradmin ss settimeout 220
```

Successfully completed the command settimeout

Successfully set the Secure Start timeout value to 220 seconds

2. To verify the timeout duration, type:

```
C:\> voradmin ss gettimeout
```

Successfully set the Secure Start timeout value to 220 seconds

Recover a Server After it Loses Connection to the DSM

User must unlock the GuardPoint by entering the Challenge/Response or password to restore the DSM connectivity. Once the GuardPoint is unlocked, you can start the AD services manually.

Note

The challenge response pop up dialog does not display in DSRM mode when the host loses DSM connectivity.

To activate the challenge/response:

1. Navigate to:

```
C:\Program
```

```
Files\Vormetric\DataSecurityExpert\agent\shared\bin
```

2. Double-click `etray.exe` to start it manually.

If the AD server does not connect to the DSM, then the AD system automatically shuts down. The Administrator must enter DSRM mode and restore the DSM connectivity to recover the server.

Prerequisites

Before rebooting your active directory servers, ensure that DSM connectivity is strong. If it is not strong, restore the DSM connectivity.

Note

When trying to fix a DSM connectivity issue, you can log in to DSRM mode. In DSRM mode, there is no requirement to increase the timeout, because in DSRM mode, the AD system does not shut down after timeout expires.

DSRM Mode

The first method for recovering a server relies on manual DSM connection troubleshooting:

1. Boot into DSRM mode.
2. Attempt to resolve why the server is not connecting to the DSM.
3. Fix that DSM connectivity issue.

4. Reboot into normal mode.

Other Use Cases

Using Secure Start GuardPoints, you can also secure an SQL Server on Microsoft Azure in certain scenarios. SQL system services in Azure also boot earlier in the boot sequence than the VMD (Vormetric Daemon) agent service.

Note

To determine if another application qualifies, contact Thales technical support.

Boot a Windows Server in Azure

To move and guard the AD database, you must boot the AD server into DSRM mode.

To boot a Windows Server 2012/2016 Domain Controller into DSRM remotely in Azure:

Note

The Windows Server 2012/2016 domain controller must be running and accessible through Windows Remote Desktop.

1. Establish a Remote Desktop session on the domain controller.
2. Open an command prompt as Administrator and type:

```
> bcdedit /set safeboot dsrepair
```
3. Reboot the domain controller. The Remote Desktop session disconnects.
4. Wait a few minutes, then establish a new Remote Desktop session. The domain controller will be running in DSRM.
5. To reboot into normal mode, open an command prompt as Administrator and type:

```
> bcdedit /deletevalue safeboot
```
6. Reboot the domain controller.

Best Practices for Encrypting and Protecting the AD Service

Thales recommends the following best practices when using Secure Start with an AD service.

Access Control with Secure Start

User can setup a restricted access control policy with encryption to prevent the unauthorized access of AD database files. The restricted policy with Secure Start:

- Prevents a rogue user from logging into the system, and moving or copying the AD database files to another directory and tampering with it.
- Denies permissions, after you setup and guard files, so that no one can move a file from the guarded directory. Plus it restricts any other unwanted/unnecessary process or users from tampering with AD files.
- Provides permission for an authorized user who needs access to AD services and files.

Creating a Minimal Policy Required for AD with Access Control

When creating a normal, strict policy for access control, you must allow access to the following processes and directories for Active Directory.

Processes

```
secfsd.exe (C:\Program
Files\Vormetric\DataSecurityExpert\agent\secfs\ sec\bin\)
lsass.exe (C:\Windows\System32\)
vds.exe (C:\Windows\System32\)
vssvc.exe (C:\Windows\System32\)
wbengine.exe (C:\Windows\System32\)
ntoskrnl.exe (C:\Windows\System32\)
```

Users

```
NT AUTHORITY\SYSTEM
```

To create a minimal policy:

1. Create a User Set named **AD_Minimum_User_Set** with the following parameters:

ID	uname	osDomains
1	SYSTEM	NT AUTHORITY

2. Create a Process Set named: **AD_Process_Set** with the following parameters:

ID	Directory	Base Name
1	C:\Program Files\Vormetric\DataSecurityExpert\agent\secfs\sec\bin	secfsd.exe
3	c:\Windows\System32\	ntoskrnl.exe
4	c:\Windows\System32\	vds.exe
5	c:\Windows\System32\	vssvc.exe
6	c:\Windows\System32\	wbengine.exe
7	c:\Windows\System32\	lsass.exe

3. Create a Security rule set with the following parameters:

Order	User	Process	Action	Effect	Browsing
1	AD_Minimum_User_ Set	AD_Process_Set	all_ops	Audit, Permit, Apply key	Yes
2				Audit, Deny	Yes

Creating a Restricted Policy in DSRM Mode

Create the following policy for the initial transformation of an AD database in DSRM mode. The policy allows access to the local administrator.

In DSRM mode, you use the `NTDSUTIL` utility to perform maintenance for an Active Directory.

To create a restricted policy:

1. Create a User Set named **AD_Minimum_User_Set** with the following parameters:

ID	uname	osDomains
1	SYSTEM	NT AUTHORITY
2	Administrator	localhost

2. Create a Process Set named: **AD_Process_Set** with the following parameters:

ID	Directory	Base Name
1	C:\Program Files\Vormetric\DataSecurityExpert\agent\secfs\sec\bin	secfsd.exe
2	c:\Windows\System32\	ntdsutil.exe
3	c:\Windows\System32\	ntoskrnl.exe
4	c:\Windows\System32\	vds.exe
5	c:\Windows\System32\	vssvc.exe
6	c:\Windows\System32\	wbengine.exe
7	c:\Windows\System32\	lsass.exe

3. Create a Security rule with with the following parameters:

Order	User	Process	Action	Effect	Browsing
1	AD_Minimum_User_Set	AD_Process_Set	all_ops	Audit, Permit, Apply key	Yes
2				Audit, Deny	Yes

Guard Directories

The best practice for guarding a directory with a Secure Start GuardPoint is to:

1. Create a directory.
2. Guard that directory with a standard production or LDT policy. Follow the steps in ["Apply Secure Start GuardPoints to a Directory with the DSM" on page 82](#).
3. Move the AD service into that directory.

Perform Subsequent System State Backups

After you move an AD service into a guarded directory, or out of a guarded directory:

1. Perform another system state backup.
2. Save this subsequent backup to a different location.

Chapter 9: Exchange DAG

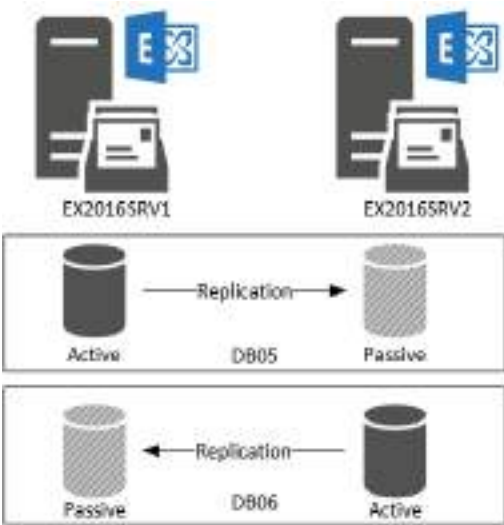
This chapter describes encrypting email databases using Microsoft Exchange database availability group (DAG). It contains the following sections:

- Exchange DAG Overview 89
- Recommendations 90
- Requirements 90
- Preparing your Exchange DAG Environment for Encrypting/Decrypting with CTE 91
- Encrypting with LDT in the Exchange DAG environment 92
- Decrypting with LDT in the Exchange DAG environment 93
- Encrypting with a Standard CTE Policy in the Exchange DAG Environment 94

Exchange DAG Overview

A DAG is a high-availability (HA) and data-recovery feature of the Microsoft Exchange Server. A DAG, which can consist of up to 16 Exchange mailbox servers, automates recovery at the database-level after a database, server or network failure. You can now use CTE for Windows to encrypt Exchange DAG mailboxes.

Figure 9-1: High Level Overview of Exchange DAG functions



You can encrypt the Exchange databases with a standard (offline) policy or an LDT policy. In an offline policy, users cannot access the database during initial data encryption. LDT is Live Data Transformation. It encrypts the data while users and applications are accessing files within it. LDT is used for Initial data transformation as well as transparent encryption/decryption.

Use Case tested and supported by Exchange DAG with CTE

Use CTE to encrypt Exchange DAGs in the following scenarios:

- Initial Data Transformation of Exchange Databases using:
 - Live Data Transformation
 - Standard Data Transformation

Note

For more information about LDT and Data Transform, request the guides for the software from Technical Support.

- Transparent Encryption/Decryption of the Exchange Database on DAG nodes
- Rotate the key using the Live Data Transformation policy

The following Exchange DAG operations were tested using the following use cases:

- Failover/Failback of databases from one node to another node and making both databases active on each node.
- Add new Databases to the existing nodes

Recommendations

To use Microsoft DAG Exchange:

1. Disable all antivirus software as suggested by Microsoft.
[https://technet.microsoft.com/en-us/library/bb332342\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/bb332342(v=exchg.160).aspx)
2. Disable Windows defender:
 - a. Type:
`> gpedit.msc`
 - b. Go to **Computer Configuration > Administrative Templates > Windows Components > Windows Defender**.
 - c. Double-click and then, in the context menu, click **Turn Off Windows Defender**.
For more information see <https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10>.
3. Only guard the Mailbox Database. Do not guard at a higher or lower directory.



State	Unapplied	Enabled	Disabled	Secure Start On	Secure Start Off	Transaction Support Required
Select Policy						
Database Mail - LDT/DTM Policy						
Host Group						
Protected Path						
End Group / Path						
Type						
Protect						
Secure Start						

4. Guard one host at a time. Do not apply GuardPoints to hostgroups.
5. Make sure that communication port 7024 is not blocked so that CTE agent can register with the host.

Requirements

The following is required for encrypting an Exchange DAG database with CTE :

- Windows Exchange Server 2016 Cumulative Patch 5
- Windows Server 2016 for Exchange Server nodes
- Windows 2016 Server as a file share witness
- Two nodes in the Exchange DAG configuration

- Both nodes on the same subnet

Note: Thales has not tested an environment with nodes on different subnets, but CTE supports this configuration. If you encounter any issues with different subnets, please contact Thales customer support.

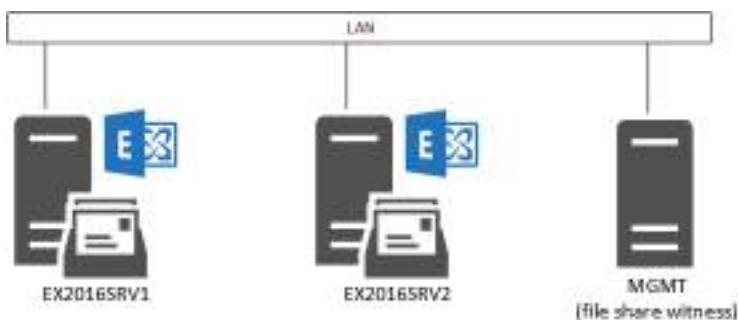
- Use the same CTE Policy and keys on both nodes.
- You must enable Secure Start on the GuardPoints.
- All users must be offline when applying the initial GuardPoint, (even for CTE-LDT).

Note: Alternatively, you can choose to make all of the DBs active on one node and perform data transformation on the other node.

- Prepare your environment for suspending databases:
 1. Suspend the Exchange Database to stop replication and access to data.
 2. Disable replication between the nodes.

Note: No file access can happen within the target directory

Figure 9-2: Proper Configuration for Exchange DAG



- Create Keys and Policies for the system

Note: You must use the same Keys and Policies on each node. For more information on Keys and Policies, see the *CTE-Live Data Transformation with Data Security Manager* and the *DSM Administration Guide*

- Install CTE agent on the systems
- Register the agent with the DSM and make sure LDT is enabled, (if they are planning to use LDT. For more information on LDT, see the *CTE-Live Data Transformation with Data Security Manager*.)

Preparing your Exchange DAG Environment for Encrypting/Decrypting with CTE

The following describes how to prepare your environment for encrypting with Exchange.

To use Microsoft DAG Exchange with LDT to encrypt data:

1. In the **Exchange Admin Center**, make Exchange node 1 the primary node.
Make node 1 the active node and move all of the databases to that node.



WARNING

Make sure that all of the Exchange services in node 2 are down and not accessing the Exchange databases. All Exchange Services must be stopped. All databases must be suspended.

2. Make all of the databases active on node 1.
3. Suspend all databases on node 2.

Note

Wait for 2-3 minutes for the database to finish with replication so the database will be suspended.

Encrypting with LDT in the Exchange DAG environment

You can use LDT for initial data transformation as well as transparent encryption/decryption.



WARNING

You must guard the databases with the same Key/Policy on both nodes.

1. Make sure that you have prepared your environment properly. See ["Preparing your Exchange DAG Environment for Encrypting/Decrypting with CTE" on the previous page](#).
2. Make sure that the GuardPoint is active on the host. Live Data Transformation starts on the server as soon as the GuardPoint is established.
3. Guard the Mailbox Database directory and apply the Live Data Transformation policy to the directory on node 2.
4. Select the GuardPoint and click **Secure Start On**.



WARNING

Only guard the Mailbox Database. Do not guard at a higher or lower directory.

[illegible]

WARNING

Guard one host at a time. Do not apply GuardPoints to both nodes using hostgroups.

5. In the **Exchange Admin Center**, go to the Exchange Database tab and **Resume** all Passive database copy on node 2.

Note: It may take a few minutes for the Exchange Service to resync. Monitor the Exchange logs on the system and make sure that replication is working. Make sure that database replication finishes and databases are in a healthy state before proceeding.

6. Wait for 10-15 minutes more for the server to move to the healthy state. If not, wait for some more time for the Content Index state to change to Healthy.

7. In the **Exchange Admin Center**, move all of the databases from node 1 to node 2.
Now the databases on node 1 are mounted as passive. All databases on node 2 are mounted as active.
8. Repeat these steps on node 1.

Decrypting with LDT in the Exchange DAG environment

To use an LDT policy:

1. Make sure that the LDT state is set to REKEYED before unguarding.
2. Make sure that all of the files inside the GuardPoint are at the same version of the key.
 - a. Run the LDT report to find the version:

```
> voradmin ldt report <GuardPoint path> [<logfile>]
```
 - b. Run the Key map report to find the version:

```
> voradmin ldt key [report|map] <key_name, version> <GuardPoint path>
```

To use Microsoft DAG Exchange with LDT to decrypt data:

1. Make sure that all of the Exchange services in node 2 are down and not accessing the Exchange databases.

Note: Suspension can take 2-3 Minutes.

2. In the **Exchange Admin Center**, make Exchange node 1 the primary node.
This means that node 1 is mounted as the active node and node 2 is mounted as the passive node.
3. Make all of the databases active on Exchange node 1.
4. Go to the Exchange Database tab and suspend all databases on node 2.
5. Unguard the database folders that you previously guarded on node 2.
6. Delete all of the metadata on all of the database folders on node 2, type:

```
> voradmin ldt attr delete [<file name path> | <guard path>]
```
7. Guard with an LDT policy set for Encryption to Clear on node 2.

Note: You must clone the current version of the encryption key to use as the current key in the new LDT policy and clear key as the transformation key.

8. Go to the Exchange Database tab and resume all databases on node 2.

Note: After a few minutes, the databases should become healthy automatically. If not wait for the LDT process to decrypt the data. Make sure that all of the data is transformed back to clear and that the LDT state is set to **REKEYED**.

9. Move the database from node 1 to node 2.
 10. Repeat this procedure for node 1.
- After both nodes are rekeyed and transformed from encryption to clear, you can unguard them.

1. In the **Exchange Admin Center**, make Exchange node 1 the primary node.
This means that node 1 is mounted as the active node and node 2 is mounted as the passive node.
2. Make all of the databases active on Exchange node 1.
3. Go to the Exchange Database tab and suspend all databases on node 2.

4. Unguard the database folders that you previously guarded on node 2.



WARNING

Always ensure that you are unguarding a passive node.

5. Repeat this procedure for Node 1.

Encrypting with a Standard CTE Policy in the Exchange DAG Environment

Refer to the following sections to prepare for encrypting in the Exchange environment.

To use Microsoft DAG Exchange with CTE:

1. In the **Exchange Admin Center**, make Exchange node 1 the primary node.

This means that node 1 is mounted as the active node and node 2 is mounted as the passive node.

2. Make all of the databases active on Exchange node 1.
3. Go to the Exchange Database tab and suspend all database on node 2.

Make sure that all of the exchange database services in node 2 are down and not accessing the Exchange databases.

Note

Suspension can take 2-3 Minutes.

4. Guard the mailbox database directory with a data transform policy.
5. Run `dataxform.exe`, type:

```
dataxform --rekey --print_stat --gp <directory>
```

6. After the data transformation is finished, unguard the directory and guard with a Production policy. Apply a standard production data transformation policy on only the node 2 database folders.

Note

Use the same Key/Policy on both nodes.

See “Remove the dataxform policy and apply production policy” in the *CTE Agent DataXform* guide for more information.

7. In the **Exchange Admin Center**, go to the Exchange Database tab and resume all databases on node 2.
After a few minutes, all nodes should become Healthy.
8. In the **Exchange Admin Center**, try to move a database from node 1 to node 2. If the data move is successful: this means that node 2 is mounted as the active node and node 1 is mounted as the passive node.
9. Repeat the previous steps for node 1.

Unsupported Use Cases

The following scenarios are not supported:

- Using different encryption keys on Exchange DAG nodes; both nodes must use the same encryption key
- Adding a new node to the Exchange DAG Environment

- Using the new CBC-CS1 key (not tested for this release)
- Encryption of Exchange Binaries
- Using nodes in a different subnet, data center or site, (Thales is not testing this scenario, but we do not believe it will cause any issues)

Chapter 10: Storage Spaces Direct

This chapter describes how CTE integrates with Windows Storage Spaces Direct (S2D) hyper-converged clusters. It contains the following sections:

S2D Overview 96

S2D Overview

S2D uses industry-standard servers with local-attached drives to create high-availability (HA) software-defined storage. SD2 is included in Windows Server 2019 Datacenter and Windows Server 2016 Datacenter, both of which are supported by CTE.

S2D extends the stack of usable storage devices to storage devices such as SATA and SAS HDD's, SSD's and NVMe (Non-Volatile Memory Express) disks to create shared disk volumes. S2D supports clusters of a minimum of two nodes, and a maximum of 16 nodes and 400 drives. S2D aggregates the available storage into a Storage Pool.

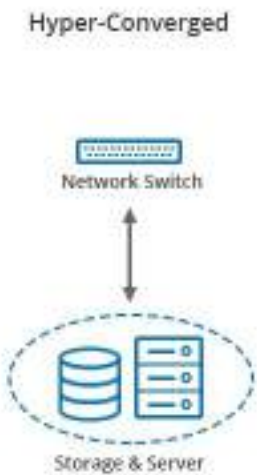
The hyper-converged deployment option runs virtual machines on the servers providing the storage.

A complete description of the S2D product, and instructions on how to set up the S2D environment is available on the Microsoft website at <https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/storage-spaces-direct-overview>

Deployment Options

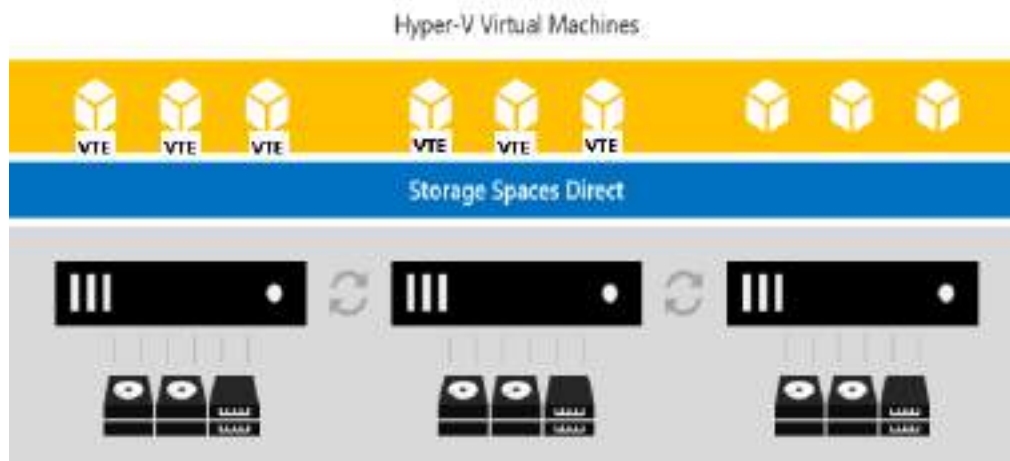
CTE supports S2D in a hyper-converged infrastructure where computing and storage components are in a single cluster as shown in the following figure.

Figure 10-1: Hyper-converged infrastructure



Hyper-converged with S2D and CTE virtual machines run on the servers providing the storage. In the following figure, CTE is installed inside 6 of the VMs to protect the data.

Figure 10-2: High-Level view of S2D



You can use all the capabilities of CTE to protect the data in the VMs in a S2D hyper-converged deployment. These capabilities are describe in ["Supported Use Cases" below](#).

Supported Use Cases

Thales tested only Hyper-converged deployments in the following scenarios.

- Initial Data Transformation of data using:
 - Live Data Transformation
 - Offline Data Transformation
- Transparent Encryption/Decryption of structure and unstructured data
- Key rotation using a Live Data Transformation policy

Chapter 11: Using CTE with Quantum StorNext

This chapter describes how to configure CTE and Quantum StorNext devices to interoperate to allow CTE policies to apply to storage managed by Quantum StorNext. This chapter contains the following sections:

Overview of using CTE with Quantum StorNext	98
CTE and Quantum StorNext Compatibility	98
Setting up CTE and Quantum StorNext Integration	100

Overview of using CTE with Quantum StorNext

Quantum StorNext Fibre Channel-connected devices provide shared file access to third party storage for workstation clients and are optimized for simultaneous access to very large files such as video files. The Quantum StorNext file system is known as SNFS or by its older name, CVFS.

You can encrypt and control access to SNFS files with DSM policies by installing CTE Agents on Windows clients that are configured for access to the SNFS file system. Some limitations apply to this integration, such as supported operating systems, supported SNFS features, concurrent read/write access by multiple clients, and GuardPoint settings (see the next section for more information about these limitations).

CTE and Quantum StorNext Compatibility

The following sections list the supported operating systems and CTE settings supported for use with Quantum StorNext file systems. Important unsupported configuration parameters are also listed.

Supported StorNext Server and Client Configurations

The CTE integration with SNFS file systems works only with certain SNFS versions, SNFS storage policies, and client operating systems.

Configuration parameter	Windows
StorNext (SNFS) operating system version	6.x
StorNext metadata controller (MDC) server OS type	Windows MDC supported
StorNext replication policy	Not supported
StorNext deduplication policy	Not supported
StorNext truncation	Supported
StorNext full and partial backup	Supported
StorNext expand filesystem	Supported
StorNext data migration	Supported
StorNext read-ahead cache	Disable for use with CTE
Client operating systems	Windows Server 2012 R2, Windows Server 2016
StorNext LAN client	DLC

Configuration parameter	Windows
StorNext mount method: locally mounted directory	Supported
StorNext mount method: Windows drive letter	Supported
StorNext mount method: CIFS	Not supported
StorNext mount method: NFS	Not supported

Supported GuardPoint and Key Settings for SNFS File Systems

When configuring CTE GuardPoints and keys for SNFS, keep in the mind the compatibility limitations listed in the following table.

Configuration element	Windows
Offline data transformation	Supported
Live Data Transformation (LDT)	Not supported
Key manager compatibility	See the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> or the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> for your CTE version
Guard unstructured data	Supported
Guard structured data	Not supported
GuardPoint type: Directory (including entire SNFS volume)	Supported
GuardPoint type: Raw device	Not supported
GuardPoint type: Block device	Not supported
GuardPoint mount option: manual guard	Not applicable
GuardPoint mount option: auto guard	Supported
GuardPoint mount option: automount	Not applicable
AES-CBC key type	Supported
AES-CBC-CS1 key type	Not supported

Supported Concurrent Access Read/Write Scenarios

If you want to allow access by multiple clients (users) to CTE-protected SNFS files under the same GuardPoint, just read-only access is supported. StorNext file locking is not implemented in CTE, so there is currently no way to prevent concurrent conflicting writes to the same file. As a result, Thales does not support write access to the same GuardPoint from multiple clients.

To enable read access to the same GuardPoint from multiple clients, ensure that all clients are configured to use the same policy and key.

Configuration parameter	Windows
Read/write access from a single LAN client to a GuardPoint	Supported
Read/write access from two or more LAN clients to the same GuardPoint	Not supported
Read-only access from one, two, or more LAN clients to the same GuardPoint	Supported

Setting up CTE and Quantum StorNext Integration

For the most part, CTE integration with Quantum StorNext is the same as for any standard file system. The next section provides an overview of the steps involved in making CTE work with SNFS. Later sections provide more information about the steps that are new or differ significantly from a typical CTE setup.

Integration Task Overview

The table below provides an overview of the steps involved in setting up SNFS and CTE to work together. As noted in the table, some of these tasks are described in the documentation for your selected key manager. Some of these steps may need to be performed by other staff members at your organization if you have divided the security administration duties as recommended by Thales and you don't have access to the key manager.

Task	Key configuration notes	For more information
Install and configure a Quantum StorNext MDC server for use with CTE	Disable the StorNext read-ahead cache. Only certain StorNext policies, features, and mount types are supported. See "Supported StorNext Server and Client Configurations" on page 98 .	See "Installing and Configuring a Quantum StorNext MDC Server for Use with CTE" on the next page .
Install and configure Quantum StorNext clients for use with CTE	Only certain operating systems are supported. See "Supported StorNext Server and Client Configurations" on page 98 .	See "Installing and configuring Quantum StorNext DLC Clients for Use with CTE" on the next page .
Create a domain for one or more SNFS hosts, or add them to an existing domain	No difference from standard CTE agent configuration.	See "Domain Management" in your key manager documentation.
Add the host to the key manager	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager documentation.
Install and register the CTE Agent on the host system	No difference in installation.	See Chapter 2: "Getting Started with CTE for Windows" on page 15
Create encryption keys (optional)	AES-CBC-CS1 keys are not supported on Windows. See the note in "Supported GuardPoint and Key Settings for SNFS File Systems" on the previous page .	See "Managing Keys" in your key manager documentation. For information about AES-CBC-CS1 keys, see Chapter 5: "Enhanced Encryption Mode" on page 65 .
Configure host groups containing one or more StorNext LAN clients (optional)	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager documentation.

Task	Key configuration notes	For more information
Configure policies (including user, process, and resource sets) to control access or enable encryption	No difference from standard CTE agent configuration.	See “Configuring Policies” in your key manager documentation.
Configure one or more GuardPoints	Some GuardPoint settings are not supported. See "Supported GuardPoint and Key Settings for SNFS File Systems" on page 99 .	See “Managing GuardPoints” in your key manager documentation

Installing and Configuring a Quantum StorNext MDC Server for Use with CTE

Install and configure a Quantum StorNext metadata controller (MDC) server using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Windows StorNext MDCs. Ensure that you configure the StorNext server to work with the settings supported by CTE as listed in ["Supported StorNext Server and Client Configurations" on page 98](#). For example, you must disable the StorNext read-ahead cache and only certain StorNext policies, features, and mount types are supported.

Installing and configuring Quantum StorNext DLC Clients for Use with CTE

Install and configure Quantum StorNext DLC clients using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Windows StorNext DLCs.

Ensure that you configure DLC clients to work with the settings supported by CTE as listed in ["Supported StorNext Server and Client Configurations" on page 98](#). For example, only certain operating systems are supported.

Note

Just read-only access is supported if multiple StorNext LAN clients will access files in the same GuardPoint. For more information, see ["Supported Concurrent Access Read/Write Scenarios" on page 99](#).

Choosing a Mounting Method

There are two methods for mounting a StorNext file system on Windows in the StorNext Client Configuration application:

- Map to Drive Letter
- Map to Directory

Both methods are supported in CTE. If you mount the StorNext file system using the Map to Directory method, you must create the directory on the Windows computer before assigning that directory in the Client Configuration application. For example, the default Map to Directory folder is `C:\Mount\snfs1`. If you use that default, you must create `C:\Mount\snfs1` before mounting the StorNext file system in the Client Configuration application.

If you change mounting methods (drive letter to directory or vice versa), you may need to close and reopen Windows Explorer or reboot the computer for the change to take effect.

Installing the CTE Agent on Each StorNext LAN client

Install a CTE Agent on each computer that is set up as a StorNext LAN client and for which you want to set policies. For supported operating systems, see the table in ["Supported StorNext Server and Client Configurations" on page 98](#).

Use any installation method supported for your operating system. For details, see [Chapter 2: "Getting Started with CTE for Windows" on page 15](#).

Chapter 12: CTE-Efficient Storage for Windows

Storage arrays offer features such as compression and deduplication for storage efficiency. They also provide simplistic encryption that fails to deliver the requisite levels of security. CipherTrust Transparent Encryption (CTE) offers a much higher level of security. However, in deployments where storage arrays receive encrypted data streams from hosts protected by a CTE instance (protected hosts), the encrypted data streams make the efficiency of storage array systems ineffective. This is because every block written by CTE is different resulting in zero deduplication and compression on these blocks.

CTE offers CTE-Efficient Storage as the solution to the storage efficiency challenge in storage arrays on Windows.

Note
Currently, this feature is only supported on the DSM. Support for this feature will be added to CipherTrust Manager in a future release.

This chapter contains the following sections:

Introduction to CTE-Efficient Storage	102
Guarding an Efficient Storage Device on Windows	108
Windows System and ES GuardPoint Administration	117
Changing the Encryption Key for a Windows ES GuardPoint	119
Resizing Guarded Efficient Storage Devices	123
Use Cases Involving Efficient Storage GuardPoints	124
Alerts and Errors on Windows	132

Introduction to CTE-Efficient Storage

CTE-Efficient Storage for Windows is a licensed feature available with CTE 7.0.0 or later. In addition, all CTE Agents must be registered with a Vormetric Data Security Manager (DSM) version 6.3 or later.

Note
All references to 'storage array' in this document assume storage array systems capable of supporting CTE-Efficient Storage functionality.

With CTE-Efficient Storage, CTE offers the same degree of security for the data stored on the arrays while offering a new type of encryption key and GuardPoint. The new type of key enables storage array systems to achieve storage efficiencies with encrypted data streams. The coordination between the storage array and CTE is essential for achieving storage efficiency with encrypted data.

In the context of this solution, a LUN exported from a storage array system to a CTE-managed host, is referred to as an *ES GuardPoint*. An ES GuardPoint is a guarded device configured with the CTE-Efficient Storage capability.

Requirements and Considerations

- CTE-Efficient Storage requires XTS-AES mode of the AES algorithm for encryption.
- CTE only supports CTE-Efficient Storage on servers with microprocessors integrated with Advanced Encryption Standard instruction set (AES-NI).
- CTE-Efficient Storage requires that the encryption keys be stored in the KMIP server on the DSM. Therefore, all hosts on which you want to create ES GuardPoints must be registered with a KMIP-enabled domain in the DSM.

CTE-Efficient Storage Enhanced Storage Arrays

CTE shares the encryption key associated with the LUN with a storage system that exports the LUN to a protected host. In this solution, the LUN is a device configured for CTE-Efficient Storage that can be guarded as an ES GuardPoint. When the device is guarded, the storage system and protected hosts coordinate operations for sharing the encryption key applied to the ES GuardPoint.

By sharing the key, the storage system decrypts the encrypted data streams that the protected host writes to the LUN, and then performs the data reduction process on the clear data before encrypting and storing the final encrypted data in the storage array system. The storage system does the reverse operations when the protected host reads data from Efficient Storage devices.

Storage Arrays Compatible with CTE-Efficient Storage

Currently, FlashArray from Pure Storage is the only storage system compatible with CTE-Efficient Storage ES GuardPoints.

FlashArray from Pure Storage is enhanced with CTE-Efficient Storage capabilities and inter-operates with CTE to provide CTE-Efficient Storage on Windows. The Pure Storage system is a client of the Vormetric Data Security Manager (DSM) and shares the encryption keys protecting the LUNs exported from the storage system to the protected hosts registered with the same DSM.

Note

See the EncryptReduce Installation Guide from Pure Storage for information on setting up interoperability with CTE.

Sharing Encryption Keys

CTE shares the encryption key for a LUN with the storage system using the KMIP protocol. In this solution, the DSM is the KMIP server, and the storage system is a KMIP client registered with the DSM. Any host accessing and protecting the LUNs from the storage system is a CTE managed host registered with the same DSM. The protected hosts register with the DSM using the `register_host` script executed on the protected hosts.

With the host and the storage system registered with the same DSM, the protected host continues enforcing policy and security rules on device and directory GuardPoints. The protected host stores an Efficient Storage Device Header, (ES Header) on each LUN configured as ES GuardPoint. The ES Header includes the UUID of the encryption key applied to the LUN and identifies the LUN as an ES GuardPoint to the storage array exporting the LUN. The storage array recognizes the ES Header on the LUN when the protected host writes the header, and then uses the UUID of the key from the header to retrieve the key attributes and material from the DSM (KMIP Server). This process enables the storage array and the protected host to share and apply the same key for encryption and decryption of data streams exchanged between them.

Note

The hosts accessing a shared LUN must be protected hosts registered with the same DSM as the storage array.

When the LUN is permanently de-configured as an ES GuardPoint, the ES Header must be removed. The storage array also detects the removal of the ES Header from the LUN and de-configures the LUN as an CTE-Efficient Storage device. Both the protected host and the storage array stop encryption and decryption of data streams exchanged between hosts and the storage array.

Storage Array Registration

The storage array administrator creates a certificate for the storage array and communicates the certificate to the DSM Administrator. The DSM Administrator produces a corresponding certificate specific to the array which is given to the storage array administrator. The DSM and the storage array system register both certificates and uses them each time they establish a secured session.

Note

See the EncryptReduce Installation Guide from Pure Storage for detailed instructions on registering the FlashArray as KMIP client with the DSM's KMIP server.

Efficient Storage Device Header and CTE Private Region

The key sharing aspect of an ES GuardPoint requires a small amount of disk space in the storage device reserved for CTE private use. The reserved space is where CTE shares information with the storage array that is exporting the device to the protected host. The reserved space starts the beginning of the device.

The protected host writes the ES Header to the device when the device is guarded for the first time. The storage array recognizes the header written to the LUN and begins the key sharing process and encrypting/decrypting data streams transferred between the protected host and the storage array on the LUN.

CTE allocates a small amount of storage space on each device configured as CTE-Efficient Storage. This region is reserved for exclusive use by CTE and is referred to as the CTE Private Region. The CTE Private Region is 64 megabytes.

CTE stores the ES Header and other metadata information to allow CTE and the storage array to exchange information. The ES Header occupies the first sector on the device. The method that CTE uses to claim the CTE Private Region on a device depends on whether the device is new (holds no data) or has existing data that you want to preserve. CTE writes the ES Header when guarding the device for the first time. The storage array recognizes the header written to the device and begins the key sharing process for exchange of encrypted data streams between the protected host and the storage array on the device.

Device Size

After you create the ES GuardPoint on the device, the device size reported to applications is the size of the device minus the space reserved for the CTE Private Region. This can lead to a discrepancy between the disk size reported by some applications versus the size reported by system utilities.



WARNING

Do not shrink ES GuardPoints. Due to relocation of user data from CTE Private Region, if you shrink the device, you may corrupt data on the device.

DSM Domain Enabled for KMIP

The KMIP protocol is the interface between the DSM and the storage arrays registered with the DSM. The Domain in the DSM for serving security requirements of storage arrays and protected hosts must be KMIP enabled. For deployment of CTE-Efficient Storage, you must create a new domain with the **Enable KMIP** option checked or modify an existing domain so that the **Enable KMIP** box is checked. This allows the DSM to make the keys for guarding CTE-Efficient Storage devices within the domain available to KMIP clients (storage arrays). Existing keys in a domain before checking **KMIP Enable** checkbox will not be accessible through KMIP.

A DSM domain can serve any number of FlashArrays as a KMIP client, but a FlashArray registered with a DSM domain *cannot* register with other domains in the DSM or with another DSM. This restriction forces the FlashArrays registered with a DSM domain to serve LUNs *only* to the CTE hosts registered with that specific DSM domain in that specific DSM.

Note

See the EncryptReduce Installation Guide from Pure Storage for detailed instructions on registering the FlashArray as KMIP client with the DSM's KMIP server.

ES GuardPoint Encryption Keys

ES GuardPoints must be encrypted using XTS-AES 256 keys. An XTS-AES 256 type key is a 512-bit key composed of two components:

- The first 256 bits of the key is the AES 256 encryption key component
- The second 256 bits is the tweak component

You create XTS keys on the DSM using the “Add Key” function, similar to non-XTS keys.

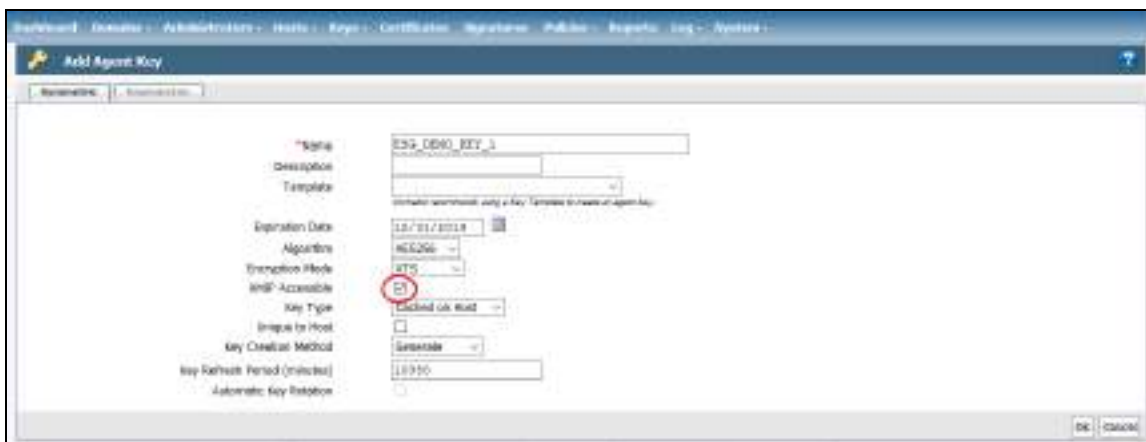
Note

You *must* check the **KMIP Accessible** check box on the “Add Agent Key” page to make the key available to KMIP clients through KMIP. If you do not check the **KMIP Accessible** option, storage arrays cannot get keys for CTE-Efficient Storage devices from the DSM (KMIP server) for sharing those keys with protected hosts.

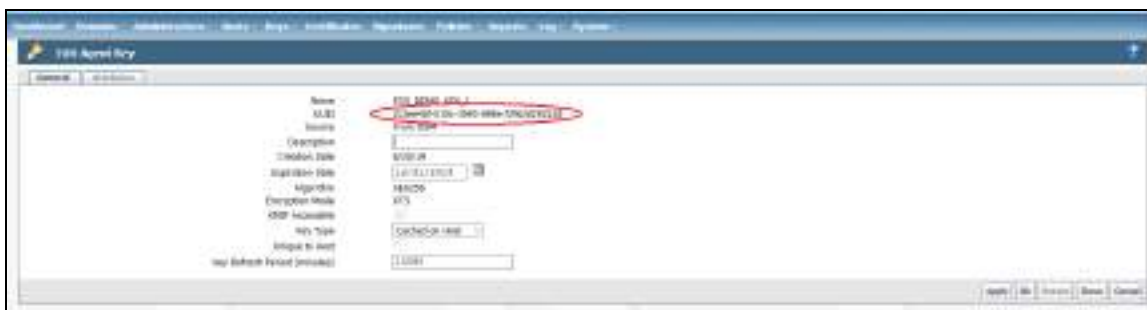
The DSM also generates a UUID for a newly added key. The DSM provides the key and its attributes to the protected hosts for guarding the CTE-Efficient Storage device. The protected host for the device writes the ES Header to the device, including the UUID of the key, before the initial attempt to enable an ES GuardPoint. The storage array recognizes the ES Header written to the device, retrieves the UUID from the ES Header, and retrieves information and attributes of the AES 256 component of the XTS-AES 256 key from the DSM using KMIP.

Key Attributes - Example

The following figure illustrates the parameters you should specify to add a new XTS-AES 256 key named ESG_DEMO_KEY_1. Note the key algorithm and encryption mode specified for the key and the checked “KMIP Accessible” option.



The following figure illustrates the general properties of ESG_DEMO_KEY_1 after adding the key. Note the UUID of the key.



The following figure illustrates the attributes of ESG_DEMO_KEY_1 after adding the key. Note that this tab displays both the UUID of the key and the UUID of the tweak component.



The attribute “x-deactivation-date” represents the date on which ESG_DEMO_KEY_1 expires. When the expiration date is reached, the key is no longer valid. It is important to choose an expiration date that exceeds any data retention period imposed on the data stored in the protected LUNs where the key is used. Note that any snapshot of a protected LUN inherits the same key protecting the primary LUN, therefore, if the key expires before reaching the end of retention period, the LUN and its snapshots will not be accessible. More importantly, do not delete the key before the data retention period expires on the LUN. The data on the LUN and its snapshots cannot be decrypted if the key is deleted prior to the data retention period.

KMIP Key Object

The following figure shows the attribute of the KMIP object for the specified UUID. The UUID specified in the example is the UUID of ESG_DEMO_KEY_1.



The following figure shows the KMIP attributes of the KMIP objects associated with ESG_DEMO_KEY_1.



The following figure shows the KMIP attributes of the KMIP object associated with the tweak component of ESG_DEMO_KEY_1.



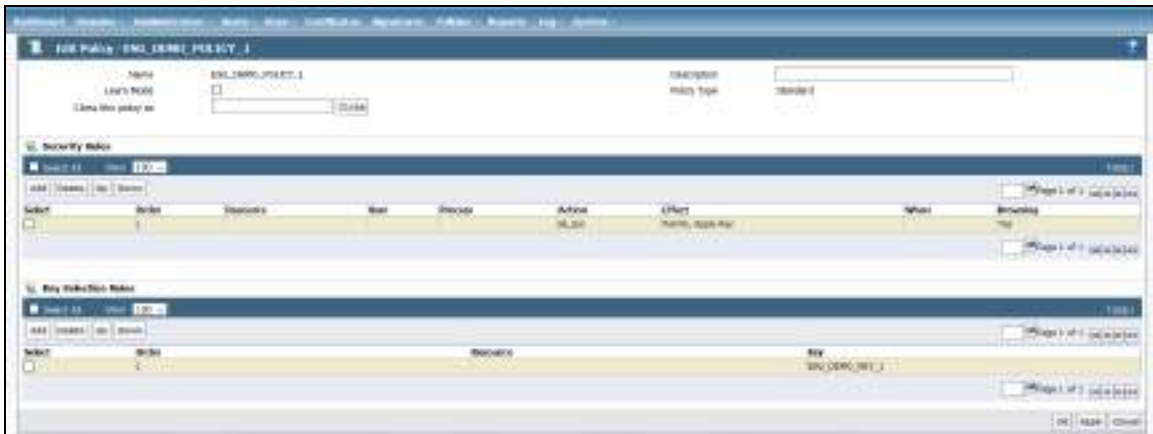
Policy Requirements for ES GuardPoints

Initializing an ES GuardPoint requires a Standard or In-place Data Transformation - Device policy with a KMIP-accessible XTS-AES 256 key as described in ["Initialize Windows CTE-Efficient Storage Devices" on page 111](#).

Rekeying an ES GuardPoint requires an In-place Data Transformation - Device policy with a KMIP-accessible XTS-AES 256 key as described in ["Changing the Encryption Key for a Windows ES GuardPoint" on page 119](#).

You may add security rules to restrict certain user/process access to protected devices. For suggestions about what security rules you may want to use, see ["Use Cases involving Efficient Storage GuardPoints" on page 124](#).

The following figure shows an example of a simple Standard policy that uses ESG_DEMO_KEY_1 key to guard devices.



Guarding an Efficient Storage Device on Windows

The following sections discuss how to guard an efficient storage device on Windows. If you want to guard an efficient storage Linux device, see the *CTE Agent for Linux Advanced Configuration and Integration Guide*.

In order to guard an efficient storage device, you need to:

1. Make sure the devices you intend to guard meet the requirements for Efficient Storage GuardPoints. For details, see ["Requirements for Efficient Storage GuardPoints on Windows" below](#).
2. Register the protected host with the DSM with Efficient Storage enabled. For details, see ["Register the Windows Host with DSM" on page 110](#).
3. Initialize the storage device to create a Private Region for the Efficient Storage Header. For details, see ["Initialize Windows CTE-Efficient Storage Devices" on page 111](#).
4. Log on to the DSM to apply the ES GuardPoint to the storage device. For details, see ["Guard the Windows Device with an ES GuardPoint" on page 115](#).

Requirements for Efficient Storage GuardPoints on Windows

Windows-specific requirements:

- The Windows host must be running one of the following:
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server 2019
- You can *only* protect data volumes with an ES GuardPoint. Protecting the boot volume with an ES GuardPoint is *not* supported.
- You must enable Secure Start on the protected host and in the ES GuardPoint in the DSM.

- Existing data LUNs must be increased in size by at least 128MB (64MB for the CTE private region plus an additional 64MB to allow enough space for the data to be shifted after the CTE private region has been created). For details, see ["Data Relocation on Existing Windows Devices" on page 116](#).

Note: If you create a new Windows device to be protected, do *not* initialize that device with the Windows Disk Manager until *after* you have created and assigned the ES GuardPoint. After the GuardPoint has been assigned through the DSM, you can manage the disk as normal using the standard Windows disk management tools.

A LUN must meet the following requirements before it can be protected as an ES GuardPoint:

- The storage array exporting the LUN to the protected host must be enhanced with the Efficient Storage capability. For details, see ["Storage Arrays Compatible with CTE-Efficient Storage" on page 103](#).
- The storage array exporting the LUN to the protected host must be a KMIP client registered with the same DSM as the protected host.
- The protected host must have direct physical access to the LUN through Fiber Channel Protocol (FCP) or iSCSI.
- The entire LUN must be protected as one and only one ES GuardPoint.
- In an ESXi environment, the LUN added to a virtual machine must be configured for Raw Device Mapping in physical mode, or:
 - The LUN must be part of a VVol datastore.
 - The LUN *cannot* be a VMDK or a disk in a datastore.
- In a HyperV environment, the LUN *cannot* be a virtual disk.

Limitations for ES GuardPoints on Windows

The current implementation of ES GuardPoints on Windows has the following limitations:

- CTE does not support dynamic disks or DFS/DFS-R.
- All applications that access the Pure Storage LUN directly must be shut down while the devices are being initialized, guarded, and encrypted. Once you begin this process, devices must not be accessed by any other applications until all data has been transformed. If other applications do access the device, CTE may not be able to successfully apply the ES GuardPoint and the user may have to reboot the device.
- If the disk is in a cluster:
 - The disk must be taken offline during the initial guarding process or while the disk is being rekeyed. You do *not* need to take any of the other disks in the cluster offline and you do *not* need to take the disk out of the cluster. But the disk itself must be offline.
 - Thales recommends that you do *not* include the disk in a host group because of the issues that can arise when CTE attempts to make changes to the same device through multiple hosts. These issues are compounded if you have multiple ES GuardPoints that are protected with different policies. In a cluster environment, it is better to manage each host individually through the DSM.
- Once the process has started, Administrators cannot use any Disk Management tools to manage the devices. All disk administration must wait until after the process is complete.
- When you unguard an ES GuardPoint, the files in that GuardPoint may still be accessible through the Windows File Explorer until Windows has updated the file cache. To update the cache immediately, you can do either of the following:
 - Issue the `voradmin esg status` command on the host.
 - Reboot the host.

Register the Windows Host with DSM

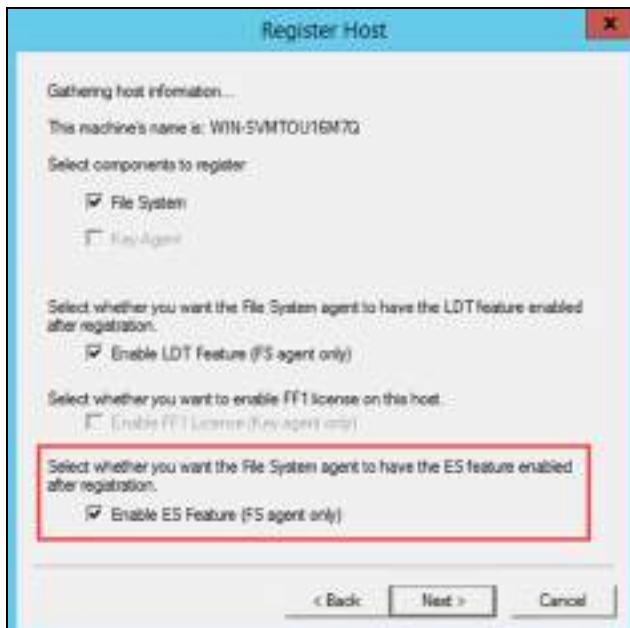
If the host is already registered with a DSM, you can initialize the devices you want to protect as ES GuardPoints as described in ["Initialize Windows CTE-Efficient Storage Devices" on the next page](#) as long as:

- The host is part of a DSM domain that has KMIP enabled.
- The DSM allows the host to register the File System component.
- A license for the CTE-Efficient Storage feature has been uploaded to the DSM.

To verify this, have the DSM Administrator check the host settings in the DSM.

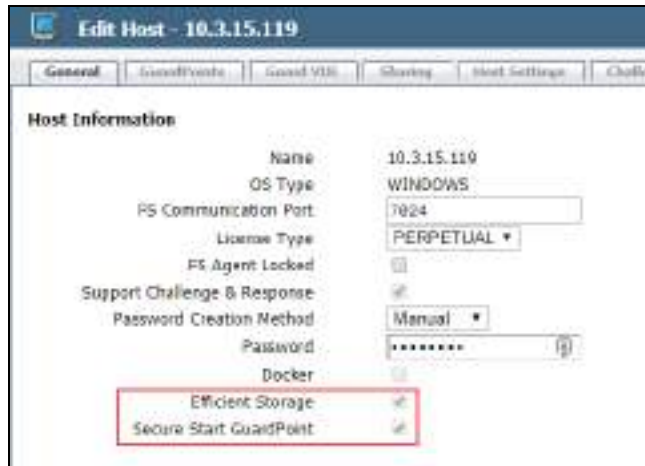
If the host is not already registered with a DSM, you need to register it before you can protect the devices on that host. When you register the host with the DSM, you must have AES-NI available on the host, a current license for registering host, and a current license for CTE-Efficient Storage. The following procedure describes how to register the host using the CTE Agent GUI. If you want to register the host silently, see the *CTE Agent for Windows Quick Start Guide*.

1. If you are planning to use the fingerprint registration method, make sure the DSM Security Administrator has added the host to the appropriate domain and enabled at least File system and KMIP as registration options.
2. If necessary, install CTE on the host. Follow the installation prompts as until you get to the registration portion of the installation. If CTE is already installed, you can start the registration process by running `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.exe`.
3. Follow the prompts to register the host with the DSM. During the registration process, make sure that you enable Efficient Storage support when you are selecting the features you want to register.



4. Complete the registration process as normal.
5. Reboot the machine after the registration process is complete.

- To verify that the host is properly registered with the Efficient Storage option enabled, have the DSM Administrator verify that **Efficient Storage** and **Secure Start GuardPoint** are checked for the host as shown below.



- After the host is registered with the DSM, initialize each device that you want to guard as described in the next section.

Initialize Windows CTE-Efficient Storage Devices

When you initialize a Windows CTE-Efficient Storage device, the process creates the CTE Private Region on the device so that CTE can write the Efficient Storage Device Header along with metadata that identifies the storage device as a guarded device. The CTE Private Region also contains the metadata for the initial transformation of clear-text data on device to cipher-text, and for the subsequent transformation of cipher-text on the device to another encryption key as needed. The initialization process also adds a user-defined label for the storage device that the DSM Administrator will use when referring to the device in the DSM.

Note

This user-defined label is maintained across system reboots, allowing CTE to always find the device regardless of any device name changes that may happen within Windows.

How you initialize the device depends on whether it is a new device or an existing device that already has data that needs to be transformed into cipher-text. For details, see:

- ["Initialize New Windows Devices" below](#)
- ["Initialize and Resize Existing Windows Devices" on page 113](#)

Initialize New Windows Devices

For each new device you want to initialize, run the `voradmin esg config new` command. The `new` option specifies that the device does not hold user data, and that CTE can reserve the first 64MB of storage on the device for the CTE Private Region. The remaining storage space is available for new user data. The device size reported to applications is the actual device size minus the CTE Private Region size.



WARNING

Do not use the `voradmin esg config new` command if the Windows disk has existing data that you want to keep. After you guard a device that has been initialized with this command, you will need to reformat the device and all existing data will be lost. To initialize a disk with existing data, see ["Initialize and Resize Existing Windows Devices" on the next page](#).

1. Log into the device as an Administrator and open PowerShell or Cmd (command prompt).
2. Close all applications, including any Windows disk management tools, that are using or mounting the device.
3. If this disk is part of a cluster, you must take the disk offline. You do *not* need to take any of the other disks in the cluster offline and you do *not* need to take the disk out of the cluster. But the disk itself must be offline during this procedure if it is part of cluster.
 - For an unstructured data cluster, open the Windows Failover Cluster Manager and go to **<cluster name> > Storage > Disks**, then select the disk and take it offline.
 - For a structured SQL database cluster, open the Windows Failover Cluster Manager and go to **Roles -SQL <cluster name> Role**. Stop the Role for the SQL instance or take the SQL server offline.
4. Make sure you know the Device Names of the devices that you want to protect.

To get a list of the Device Names for the available devices, use the `voradmin esg list disk` command and look in the **Device Name** column. Any new disk that is not a boot disk and that does not contain any data can be initialized by CTE as a new disk. For example:

C:\>`voradmin esg list disk`

Disk###	Device Name	Boot Disk	Size	Status	Partition	Read Only	SERIAL NUMBER
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	127.0 GB	Online	MBR	No	6000c29d241599...
Disk1	\Device\00000032	No	49.9 GB	Online	MBR	No	6000c29b1d5a4c...
Disk2	\Device\00000033	No	50.9 GB	Online	MBR	Yes	6000c290582227...
Disk3	\Device\00000034	No	50.9 GB	Online	MBR	No	6000c290fd627b...

In the example above, the available Device Names are `\Device\00000032`, `\Device\00000033`, and `\Device\00000034`.

5. Run the `voradmin esg config new <device-name>=<label>` command, where:
 - `new` (required) indicates that the device contains no data (it is a new disk). CTE will create the CTE private region at the beginning of the disk and the rest of the disk will be available for user data.
 - `<device-name>=<label>` (required) is the device name and a user-defined label for the device. This label will be the path the DSM Administrator uses to specify to the device in the DSM. (For example, `\Device\00000033=NewESDisk`.) The label can be 1 to 32 ASCII characters. Do not use spaces or special characters in the label.

Make sure that the device you select does *not* contain any existing data. When CTE applies the GuardPoint to a new device, it removes the existing file system information from the device. That means the device will need to be reformatted and all existing data will be unrecoverable as soon as the GuardPoint is applied.

For example, if you want to initialize a new disk Windows device named `00000033` with the label "NewESDisk", you would specify:

```
PS C:> voradmin esg config new \Device\00000033=NewESDisk
Disk is initialized successfully with CTE ESG protection.
```

- To verify that the disk has been initialized, run the `voradmin esg status` command.

This command shows that the device label has been set and the Xform Status has been set to NA (not applicable). For example:

C:\>**voradmin esg status**

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	unguarded	
Disk1	\Device\00000032	No		unguarded	
Disk2	\Device\00000033	No	NewESDisk	unguarded	NA
Disk3	\Device\00000034	No		unguarded	

- At this point the DSM Administrator can protect the device as an ES GuardPoint through the DSM Management Console as described in ["Guard the Windows Device with an ES GuardPoint" on page 115](#).

Note: The initialization process prepares the devices to be guarded but does not actually guard them. You need to assign an ES GuardPoint to each device through the DSM before the devices are actually protected. In addition, the initialization process is only kept in memory until the devices are guarded or rebooted. If a device is rebooted before you guard it, you will need to perform the initialization procedure again.

Initialize and Resize Existing Windows Devices

If a Windows device has existing data, you need to use the `voradmin esg config xform` command to initialize the disk for CTE. This command tells CTE that the data on the device needs to be encrypted after an ES GuardPoint is assigned to the device through the DSM. After the CTE initialization is complete, you then need to resize the device before you can guard it with an ES GuardPoint.

The following procedure describes how to initialize existing devices for CTE. Note that the existing data is not altered in any way until after you perform this procedure and you guard the data with an ES GuardPoint. CTE does *not* begin transforming the data from clear-text to cipher-text until the ES GuardPoint has been applied and the encryption key has been pushed to the device through the GuardPoint Policy.

- Log into the device as an Administrator and open PowerShell or Cmd (command prompt).
- Close all applications, including any Windows disk management tools, that are using or mounting the device.
- If this disk is part of a cluster, you must take the disk offline. You do *not* need to take any of the other disks in the cluster offline and you do *not* need to take the disk out of the cluster. But the disk itself must be offline during this procedure if it is part of cluster.
 - For an unstructured data cluster, open the Windows Failover Cluster Manager and go to **<cluster name> > Storage > Disks**, then select the disk and take it offline.
 - For a structured SQL database cluster, open the Windows Failover Cluster Manager and go to **Roles -SQL <cluster name> Role**. Stop the Role for the SQL instance or take the SQL server offline.
- Make sure you know the Device Names of the devices that you want to protect.

To get a list of available devices on Windows, use the `voradmin esg list disk` command. The Disk Name column shows the names of the available disks. In the list, existing disks must *not* be boot disks and they must *not* be Read Only. In the following example, \Device\00000032 and \Device\00000034 show **No** in the **Boot Disk** and **Read Only** columns:

C:\>**voradmin esg list disk**

Disk###	Device Name	Boot Disk	Size	Status	Partition	Read Only	SERIAL NUMBER
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	127.0 GB	Online	MBR	No	6000c29d241599...
Disk1	\Device\00000032	No	49.9 GB	Online	MBR	No	6000c29b1d5a4c...
Disk2	\Device\00000033	No	50.9 GB	Online	MBR	Yes	6000c290582227...
Disk3	\Device\00000034	No	50.9 GB	Online	MBR	No	6000c290fd627b...

- If you want to make sure the disk has not yet been initialized, used the `voradmin esg status` command. If the disk already has an ESG Device Label, then the disk has already been initialized. In the following example, Disk2 has already been initialized, but Disk1 and Disk3 have not:

C:\>**voradmin esg status**

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	unguarded	
Disk1	\Device\00000032	No		unguarded	
Disk2	\Device\00000033	No	NewESDisk	unguarded	NA
Disk3	\Device\00000034	No		unguarded	

- For each existing device you want to initialize, run the `voradmin esg config xform <device-name>=<label>` command, where:
 - `xform` (required) indicates that the device contains existing data. CTE will transform all existing data on the device from clear-text to cipher-text as soon as you guard the device. The device will be inaccessible until the transformation is complete, and the device must remain offline during the entire transformation process. No user access will be permitted until all data has been transformed.
 - `<device-name>=<label>` (required) is the device name and a user-defined label for the device. This label will be the path the DSM Administrator uses to specify to the device in the DSM. (For example, `\Device\00000032=ExistWinDisk1`.) The label can be 1 to 32 ASCII characters. Do not use spaces or special characters in the label.

For example, if you want to initialize a new disk Windows device named 00000032 with the label `ExistWinDisk1` and the device 00000034 with the label `ExistWinDisk2`, you would specify:

C:> **voradmin esg config xform \Device\00000032=ExistWinDisk1**

Disk is initialized successfully with CTE ESG protection. Disk must be Resized to at least 128MB before guarding as Efficient Storage GuardPoint

C:> **voradmin esg config xform \Device\00000034=ExistWinDisk2**

Disk is initialized successfully with CTE ESG protection. Disk must be Resized to at least 128MB before guarding as Efficient Storage GuardPoint

With Windows, you always need to increase the disk size on each device by at least 128MB, which provides enough space for the CTE Private Region as well as room to relocate the existing data. After you guard the disk, you can expand it again later but you cannot shrink it unless you remove the GuardPoint. For details about the data relocation, see ["Data Relocation on Existing Windows Devices" on page 116](#).

- To verify that the disks have been initialized, run the `voradmin esg status` command.

This command shows that the device labels have been set and the Xform Status has been set to Not Started. For example:

C:\>**voradmin esg status**

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	unguarded	
Disk1	\Device\00000032	No	ExistWinDisk1	unguarded	Not Started
Disk2	\Device\00000033	No	NewESDisk	unguarded	NA
Disk3	\Device\00000034	No	ExistWinDisk2	unguarded	Not Started

- At this point, you need to resize all initialized existing devices by increasing their volume size through the Pure Storage management interface. Make sure you increase the device size on each device by at least 128 MB. For details, see your Pure Storage documentation.

To verify that the disk size has been increased, use the `voradmin esg list disk` command.

C:\>**voradmin esg list disk**

Disk###	Device Name	Boot Disk	Size	Status	Partition	Read Only	SERIAL NUMBER
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	127.0 GB	Online	MBR	No	6000c29d241599...
Disk1	\Device\00000032	No	50.1 GB	Online	MBR	No	6000c29b1d5a4c...
Disk2	\Device\00000033	No	50.9 GB	Online	MBR	Yes	6000c290582227...
Disk3	\Device\00000034	No	51.1 GB	Online	MBR	No	6000c290fd627b...

You cannot assign an ES GuardPoint to the devices until it they have been resized. If you do not resize the devices, the GuardPoint assignment will fail.

- After the devices have been resized, the DSM Administrator can protect the devices as ES GuardPoints through the DSM Management Console as described in ["Guard the Windows Device with an ES GuardPoint"](#) below.

Note

The initialization process prepares the devices to be guarded but does not actually guard them. You need to assign an ES GuardPoint to each device through the DSM before the devices are actually protected. In addition, the initialization process is only kept in memory until the devices are guarded or rebooted. If a device is rebooted before you guard it, you will need to perform the initialization procedure again.

Guard the Windows Device with an ES GuardPoint

Note

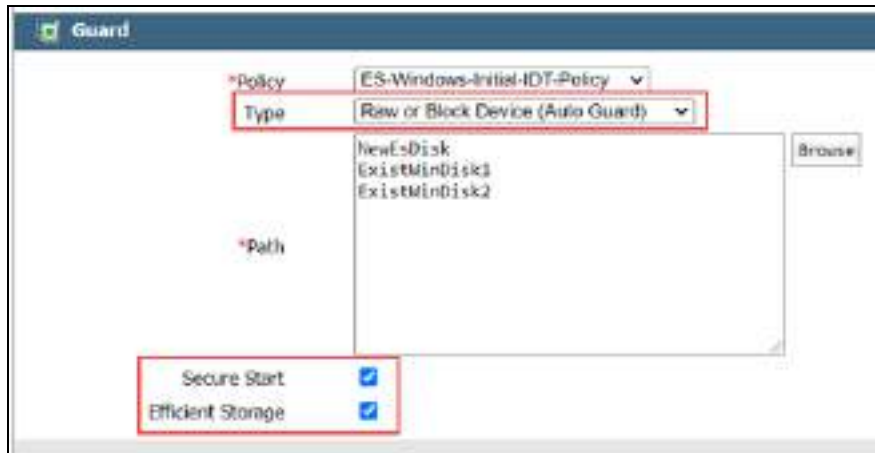
For details about how to create a GuardPoint, see the chapter, "Managing GuardPoints", in the *DSM Administration Guide*.

After the device has been initialized, you can guard the device as an ES GuardPoint from the DSM Management Console. For existing devices, as soon as the GuardPoint has been pushed to the host and the status changes to guarded, CTE begins transforming the data on the disk using the encryption key associated with the GuardPoint Policy.

- Log on to the DSM Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.
- Make sure that you know what Policy you want to associate with the GuardPoint or create a new policy if needed. The policy you use for CTE-Efficient Storage must be either a Standard policy or an In-place Data Transformation - Device policy, and it must use a KMIP-accessible XTS-AES 256 key in the key rule. For more information on key requirements, see ["ES GuardPoint Encryption Keys"](#) on page 105.
- Select **Hosts > Hosts** on the menu bar. The *Hosts* window opens.
- Click the target host in the **Host Name** column. The *Edit Host* window opens to the General tab for the selected host.
- Click the **GuardPoints** tab and then click **Guard**. The *Guard File System* window opens.
 - In the **Policy** field, select the Policy you identified or created earlier in this procedure. CTE will use the XTS-AES 256 key associated with this policy to encrypt the data on the device.
 - In the **Type** field, select **Raw or Block Device (Auto Guard)**.

When you select Auto Guard, CTE starts the guard process as soon as the policy is pushed to the host. You enable, disable, guard, and unguard the GuardPoint in the DSM.

- c. In the **Path** field, add the device label you assigned when you initialized the disk. For example, `ExistWinDisk1`.
If you specify multiple device labels in this field, all specified devices will be guarded and all will be encrypted with the encryption key specified in the selected policy.
- d. Make sure the **Secure Start** check box is checked.



6. When you are done, click **OK**.

The DSM pushes the policy and the GuardPoint configuration to the host and the CTE Agent on the host writes the ES Header into the CTE Private Region for the specified devices.

If this is a new device, the status changes to guarded and the disk is available for user access immediately. At this point you can use the Windows Disk Manager to perform any required disk management tasks and all data that gets written to the disk will be protected by CTE.

If there is existing data on the device, CTE begins transforming the data from clear-text to cipher-text as soon as the ES GuardPoint configuration is available and the device status changes to guarded. The device will remain inaccessible until this data transformation completes. The length of time required to transform the data depends on the size of the disk.

7. If this disk is part of a cluster, do the following:
 - a. If the disk has existing data, wait until the data transformation process has completed before you proceed. To verify the status of the process, use the `voradmin esg status` command.
 - b. After any required data transformation is complete, apply the same GuardPoint with the same policy to the disk on each one of the hosts that can access the disk. You must specify the same policy name and disk label on each host.

Tip: Thales recommends that you do *not* use a Host Group for clustered disks. Instead, you should apply the GuardPoint individually on each host.

- c. After you have created the GuardPoint on each host that can access the disk, you can bring the disk back online or restart the SQL Role/SQL server.

Data Relocation on Existing Windows Devices

When you add an ES GuardPoint to a device that has been initialized with the `xform` option, CTE shifts the existing data by 64MB, then it creates the CTE Private Region in the first 64MB on the device. This relocation occurs only once when the device is guarded for the first time.

Data Transformation on Existing Windows Devices

As the ES Header is written before data transformation begins, the data transformed to cipher-text and written back to the device during data transformation process is subject to data reduction process through the storage array.

Existing devices populated with data are transformed from clear-text to cipher-text using the encryption key applied to each device. Data transformation is also called CipherTrust InPlace Data Transformation (CTE-IDT).

CTE-IDT is not the same as the legacy offline data transformation. CTE-IDT is a block level data transformation with built-in resiliency to recover from system crashes during the data transformation process. CTE-IDT uses the CTE Private Region on the device to manage the entire transformation process. CTE-IDT partitions the data on a device in segments of 512KB in size and transforms one or multiple segments, up to 60 segments, in parallel. The CTE-IDT process preserves existing data in a segment during transformation in the private region of the device, and then transforms the data in-place. CTE-IDT also maintains the segments undergoing transformation in the private region. In the event of system crash, CTE-IDT will recover the segments undergoing transformation at the time of crash and then resume the transformation process.

Another advantage of CTE-IDT over legacy offline data transformation is that CTE-IDT does not require a separate policy for data transformation. With the same production policy applied to the device, CTE-IDT determines whether the device is in need of data transformation, per specification of `xform` option when device was initialized, and starts the CTE-IDT process when transformation is required. During the CTE-IDT process, access to the device is blocked until the CTE-IDT process completes.

To view the data transformation status, use the `voradmin esg status` command and look in the **Xform Status** column. In the following example:

- Disk1 has been guarded and the data transformation process has completed, so the device is guarded and ready to use.
- Disk2 was initialized as a new device, so no data transformation was required. The device is guarded and ready to use.
- Disk3 has been guarded but the data transformation process is still in progress. This device cannot be accessed until the data transformation process has completed.

```
C:\>voradmin esg status
```

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	unguarded	
Disk1	\Device\00000032	No	ExistWinDisk1	guarded	Completed
Disk2	\Device\00000033	No	NewESDisk	guarded	NA
Disk3	\Device\00000034	No	ExistWinDisk2	guarded	In-Progress

(18%)

CTE-IDT Recovery From Crash

CTE-IDT is fault tolerant in the event of system crashes. CTE-IDT keeps track of the transformation process over the entire device. In the event of a crash, CTE-IDT will automatically resume transformation from the point of failure as soon the GuardPoint is enabled after system startup.

If you find the transformation status set to **In-Progress** when the GuardPoint is not enabled, the **In-Progress** state reflects an earlier system crash after which the GuardPoint has not been enabled to recover from the interruption in the CTE-IDT process.

Windows System and ES GuardPoint Administration

The `voradmin` command is a command line utility for management of CTE specific configuration and status reporting. The `voradmin` command also supports configuration management related to ES GuardPoints (ESG).

Windows supports the following `voradmin esg` commands.

voradmin esg list disk

Command: `voradmin esg list disk`

Lists the disks available on the Windows host. The `Disk###` column matches the disk numbers in the Windows Disk Manager. The `Device Name` column shows the name of the disk that you need to use with other `voradmin` commands. In the following example, the `Device Name` for `Disk1` is `\Device\00000036`.

For example:

`C:\>voradmin esg list disk`

Disk###	Device Name	Boot Disk	Size	Status	Partition	Read Only	SERIAL NUMBER
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	127.0 GB	Online	MBR	No	6000c29d241599...
Disk1	\Device\00000032	No	49.9 GB	Online	MBR	No	6000c29b1d5a4c...
Disk2	\Device\00000033	No	50.9 GB	Online	MBR	Yes	6000c290582227...
Disk3	\Device\00000034	No	50.9 GB	Online	MBR	No	6000c290fd627b...

voradmin esg config

Command: `voradmin esg config [new|xform] <device-name>=<device-label>`

Initializes a new or existing Windows device so that it can be protected as an ES GuardPoint through the DSM. For details on using this command, see ["Initialize New Windows Devices" on page 111](#) and ["Initialize and Resize Existing Windows Devices" on page 113](#).

voradmin esg status

Command: `voradmin esg status`

Displays the status of the disks on the host. The `Disk###` column matches the disk numbers in the Windows Disk Manager. The `Device Name` column shows the name of the disk that you need to use with other `voradmin` commands. In the following example, the `Device Name` for `Disk1` is `\Device\00000032`.

If the device has been initialized, the user-defined disk label appears in the `ESG Device Label` column. If the device has been protected with an ES GuardPoint through the DSM, the `Guard Status` column displays “guarded”. The `Xform Status` column displays the status of any data transformation processes run on the disk. NA means it was a new disk, so no data transformation was needed. For existing disks, the `Xform Status` can be Not Started, In Progress, or Completed.

For example:

`C:\>voradmin esg status`

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	guarded	
Disk1	\Device\00000032	No	ExistWinDisk1	guarded	Completed
Disk2	\Device\00000033	No	NewESDisk	guarded	NA
Disk3	\Device\00000034	No	ExistWinDisk2	guarded	Completed

voradmin esg status [xform] <device-label>

Displays the details of the device specified in `<device-label>`, where `<device-label>` is the ESG Device Label assigned to the device. If you use the optional `xform` parameter, the command displays the status of any data transformation processes running on the device.

For example:

```
C:\> voradmin esg status NewESDisk
```

```
Disk###           Disk2
Device Name       \Device\00000033
Serial Number
Boot Disk        No
ESG Device label  NewESDisk
Guard Status      Guarded
Xform Status      NA
Key UUID         cf242f18-de61-3f72-ba57-0b28a94a4f21
```

```
C:\> voradmin esg status xform NewESDisk
```

```
ESG Rekey/Xform Status
```

```
-----
```

```
      Status      :NA
      Device Type  :New
```

Key Information:

```
      Key UUID     :cf242f18-de61-3f72-ba57-0b28a94a4f21
      KeyID        :48361
      KeyName       :ES-Key
      Old KeyID     :0
      Old KeyName   :clear_key
```

Block information:

```
      Transformed  :0
      Remaining    :0
      Total        :0
```

voradmin esg delete

Command: voradmin esg delete <disk-label>, where:

<disk-label> is the user-defined label that was specified when the device was initialized. To view a list of disk labels, use the voradmin esg status command.

Removes the ES Header from the specified device. The device *cannot* be protected as an ES GuardPoint or this command will fail.

For example:

```
# voradmin esg delete NewESDisk
ES disk header deleted successfully.
```

Changing the Encryption Key for a Windows ES GuardPoint

To meet various compliance requirements, you may want to change the key that CTE has used to encrypt an GuardPoint. Thales refers to this changing of encryption keys as “Key rotation” or “Rekey”. Unlike the CipherTrust Transparent Encryption - Live Data Transformation product offered by Thales for file systems on traditional storage devices, to change the encryption key on an ES GuardPoint, the device must be taken offline. The data on the device will be inaccessible during the key rotation process.

The key rotation process involves the following:

- Creating a new policy for key rotation
- Preparing the ESG device for key rotation
- Applying the new policy to the ESG device on the DSM

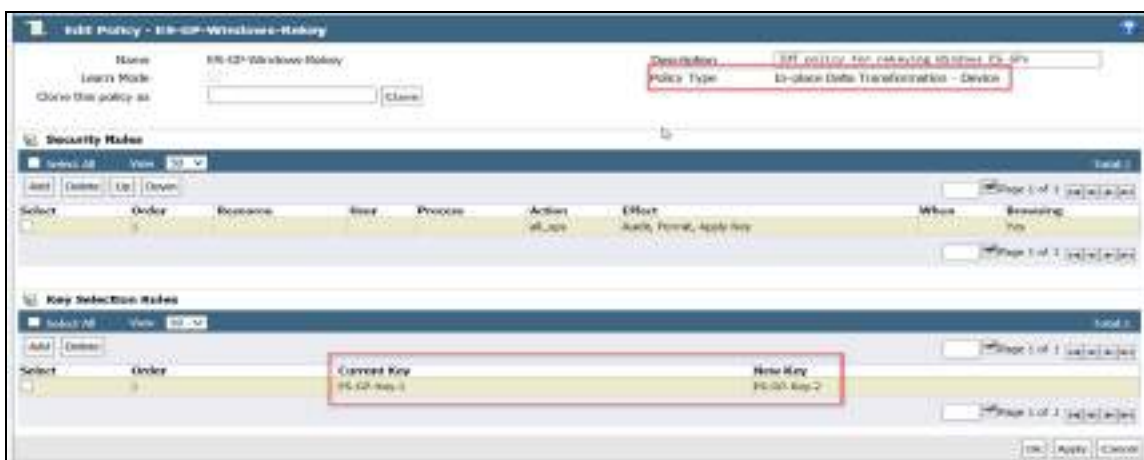
See the following sections for details of key rotation. If your organization has separated security duties, some of the steps below may need to be completed by different people.

Requirements and Considerations

Rekeying a Windows ES GuardPoint requires an In-place Data Transformation - Device policy, which is available with the DSM version 6.4.2 and later. If the Windows host is registered with an older version of the DSM, you must upgrade the DSM to at least version 6.4.2 if you want to rekey a Windows ES GuardPoint.

Creating a New DSM Policy for Key Rotation

As part of rekeying the data on an ESG device, you must create a new In-place Data Transformation - Device policy with a key rule specifying the current key and the new key. The screenshot below shows a policy named ES-GP-Windows-Rekey that specified the current key as ES-GP-Key-1 and the new key as ES-GP-Key-2:



When this policy is pushed to the host from the DSM, the CTE Agent will decrypt the data on the device using the key ES-GP-Key-1 and then will reencrypt it using the key ES-GP-Key-2.

Rekeying the Windows Device

1. Shutdown any applications accessing the GuardPoint. This also includes unmounting the file system if the GuardPoint is a device mounted as a file system.



WARNING

During this procedure, you will have to disable the GuardPoint while the device is being rekeyed. Therefore it is critical that no file changes occur during the rekey process or the data may become corrupted.

2. If this disk is part of a cluster, you must check the ownership of the disk and then take the disk offline. You do *not* need to take any of the other disks in the cluster offline and you do *not* need to take the disk out of the cluster. But the disk itself must be offline during this procedure if it is part of cluster.

During this procedure, you need to log into the host that owns the disk in order to run the `voradmin esg rekey` command. If you want to do that on a host other than the current owner, change the disk ownership in the Windows Failover Cluster Manager.

After you have set the correct owner, take the disk offline:

- For an unstructured data cluster, open the Windows Failover Cluster Manager and go to **<cluster name> > Storage > Disks**, then select the disk and take it offline.
- For a structured SQL database cluster, open the Windows Failover Cluster Manager and go to **Roles -SQL <cluster name> Role**. Stop the Role for the SQL instance or take the SQL server offline.

3. In the DSM Management Console, unguard the ES GuardPoint.

If this disk is part of cluster, unguard the disk on each one of the hosts that can access the disk.

4. Log into the host with System Administrator privileges.

If this disk is part of a cluster, you need to log into the host that is the current owner of the disk.

5. Make sure that the device you intend to rekey is no longer guarded using the `voradmin esg status` command. In the following example, we are about to rekey the device NewESDisk:

```
C:\>voradmin esg status
```

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	Unguarded	
Disk1	\Device\Ide\IdeDeviceP0T1L0-1	No	NewESDisk	Unguarded	NA
Disk2	\Device\Ide\IdeDeviceP1T1L0-3	No	ExistWinDisk1	Guarded	NA

6. Use the `voradmin esg rekey` command to prepare the device to be rekeyed. For example:

```
C:\>voradmin esg rekey NewESDisk
```

```
Disk is initialized successfully with CTE ESG protection.
```

7. In the DSM Management Console, guard the device with the new policy you created in ["Creating a New DSM Policy for Key Rotation"](#) on page 120. Make sure that:
- You select **Raw or Block Device (Auto Guard)**.
 - You check the **Secure Start** check box.

In the following example, NewESDisk is guarded with the In-place Data Transformation - Device policy ES-GP-Windows-Rekey:



When you click **OK**, the DSM pushes the new policy to the ES GuardPoint and the CTE Agent rekeys the device.

8. During the rekey process, you can use the `voradmin esg status` command to track the rekey progress.

C:\>**voradmin esg status**

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	Unguarded	
Disk1	\Device\Ide\IdeDeviceP0T1L0-1	Unknown	NewESDisk	Guarded	In Progress (80%)
Disk2	\Device\Ide\IdeDeviceP1T1L0-3	No	ExistWinDisk1	Guarded	NA

When the rekey process has finished, the status changes to Completed.

C:\>**voradmin esg status**

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	Unguarded	
Disk1	\Device\Ide\IdeDeviceP0T1L0-1	Unknown	NewESDisk	Guarded	Completed
Disk2	\Device\Ide\IdeDeviceP1T1L0-3	No	ExistWinDisk1	Guarded	NA

9. If you want to verify that the GuardPoint is using the new key, use the `voradmin esg status xform <device-label>` command. For example:

```
C:\> voradmin esg status xform NewESDisk
```

```
ESG Rekey/Xform Status
```

```
-----
```

```
      Status      :NA
      Device Type  :New
```

```
Key Information:
```

```
      Key UUID      :cf242f18-de61-3f72-ba57-0b28a94a4f21
      KeyID         :48361
      KeyName       :ES-Rekey
      Old KeyID     :0
      Old KeyName   :ES_Key
```

```
Block information:
```

```
      Transformed   :0
      Remaining     :0
      Total         :0
```

10. If the disk is *not* part of a cluster, you can restore access to the disk at this point. If it *is* part of a cluster, do the following:
- After any required data transformation is complete, apply the same GuardPoint with the same policy to the disk on each one of the hosts that can access the disk. You must specify the same policy name and disk label on each host.
 - After you have created the GuardPoint on each host that can access the disk, you can bring the disk back online or restart the SQL Role/SQL server.

Resizing Guarded Efficient Storage Devices

Devices configured for Efficient Storage can be resized using the system-provided resizing utilities. If you are using a file system on the GuardPoint, you can mount the file system after resizing the device and then grow the file system to the new size using the native Windows disk management tools.



WARNING

Do not shrink ES GuardPoints. Due to relocation of user data from CTE private region, if you shrink the device, you may corrupt data on the device.

- Stop applications from accessing the GuardPoint.
 - Unmount the file system if the device is mounted.
 - Disable GuardPoints: auto-guard if is enabled on the DSM, or manual-guard if is enabled on the protected host.
- Use the native disk management tools to resize the device.
- After resizing the device, check the size of the device. On Windows you can use the `voradmin esg list disk` command.
- If the reported size does not match what you expect, you may need to rescan your storage devices using the command appropriate for the device's connection type.
- Once the expected size is achieved, enable the GuardPoint and restart your applications.

Use Cases involving Efficient Storage GuardPoints

ES GuardPoints support three use cases for managing customer's data in GuardPoints. This section describes those potential use cases.

Use Case 1: Single Encryption Key

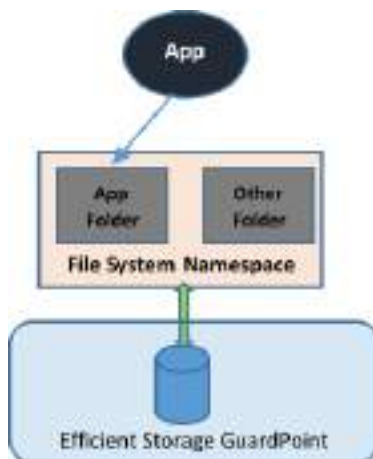
Applications, such as an Oracle Database, store structured data in one or multiple LUNs guarded as an ES GuardPoint. In this use case, a LUN may be an independent datastore or a member of a disk group managed by an application, for example an Oracle ASM disk group. In this use case, the policy applied to the GuardPoints specifies one key rule for encryption. The policy may include access rules for user or process level access control.



Use Case 2: Device-Level GuardPoints

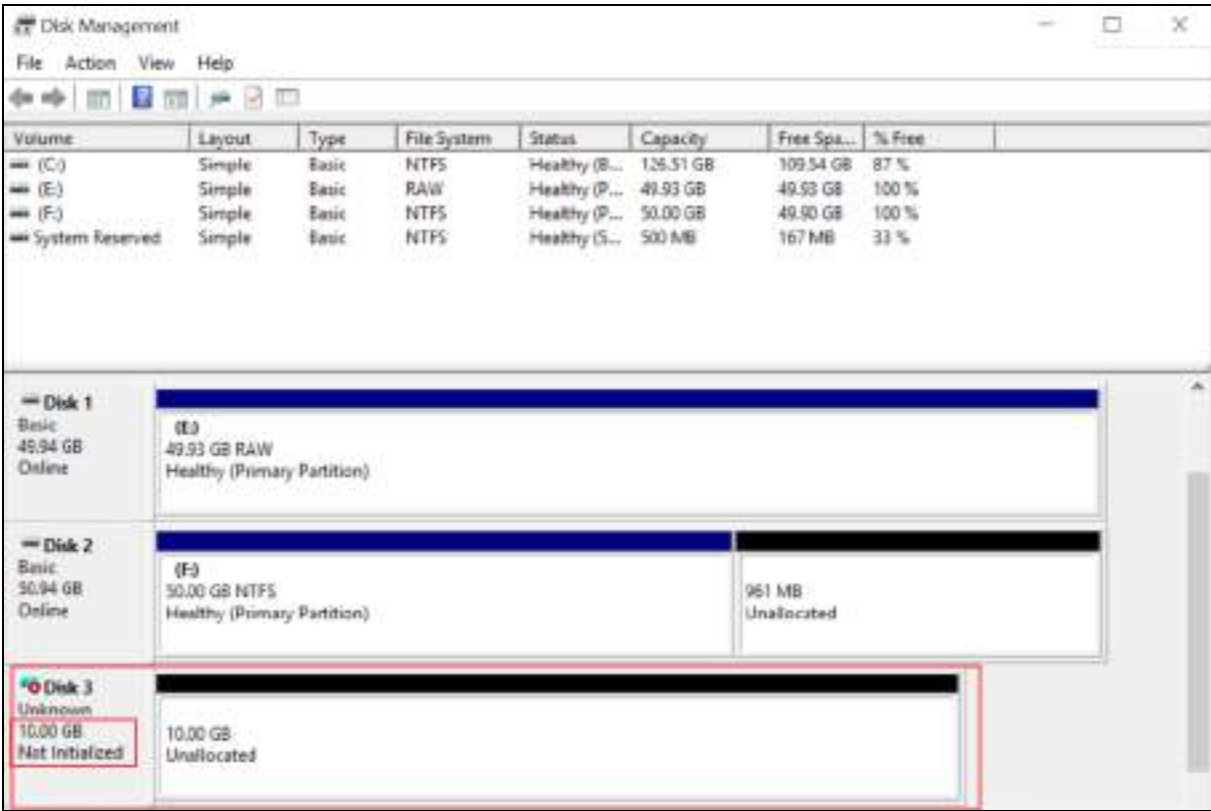
Protect structured or unstructured data stored in data files. The data files are organized inside one or more directories or folders within a file system namespace, such as NTFS or ReFS, without any protection on the folders or the file system namespace. In this use case, the file system resides in the device guarded as Efficient Storage using a policy with a key rule and *no user specified access rule*. Access rules are not applicable in this use case and should not be used.

Figure 12-1: File system resides in device guarded as ES GuardPoint



Example

In the following example, the Windows Administrator has created a new 10 MG VHD in the Windows Disk Management tool. This VHD is called Disk 3, and it has not yet been initialized.



The Windows Administrator then uses `voradmin esg list disk` to get the CTE device name for the new disk and initializes it using the `voradmin esg config new` command, as shown:

```
C:\>voradmin esg list disk
```

Disk###	Device Name	Boot Disk	Size	Status	Partition	Read Only	SERIAL NUMBER
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	127.0 GB	Online	MBR	No	
Disk1	\Device\00000032	No	49.9 GB	Online	MBR	No	
Disk2	\Device\00000033	No	50.9 GB	Online	MBR	No	
Disk3	\Device\00000051	No	10.0 GB	Online	MBR	No	

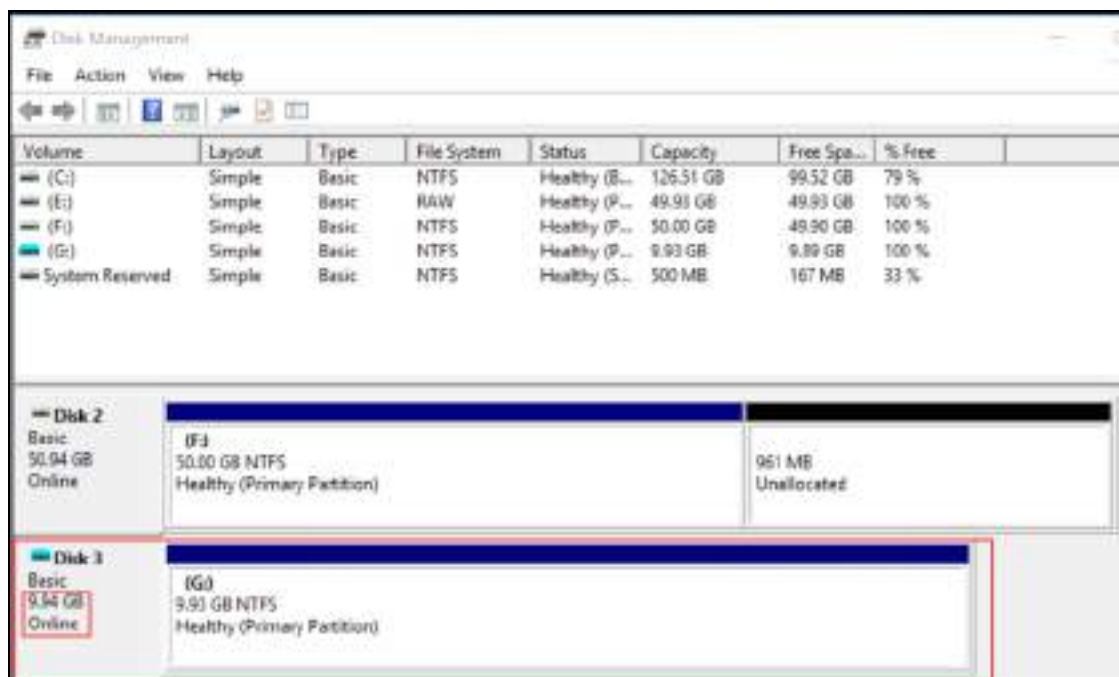
```
C:\>voradmin esg config new \Device\00000051=NewDisk3
Disk is initialized successfully with CTE ESG protection.
```

The Administrator guards the new disk through the DSM, and uses the `voradmin esg status` command to make sure the new disk has been successfully guarded.

```
C:\>voradmin esg status
```

Disk###	Device Name	Boot Disk	ESG Device label	Guard Status	Xform Status
Disk0	\Device\Ide\IdeDeviceP0T0L0-0	Yes	NA	unguarded	
Disk1	\Device\00000032	No	esg-disk1-demo	guarded	Completed
Disk2	\Device\00000033	No	esg-disk2-demo	guarded	Completed
Disk3	\Device\00000051	No	NewDisk3	guarded	NA

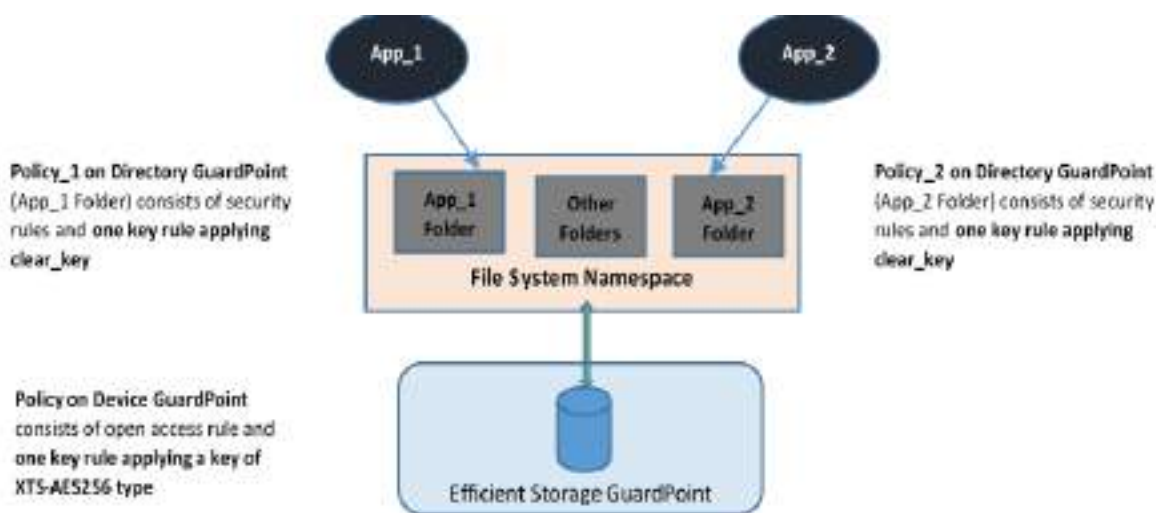
After the device has been guarded, the Administrator returns to the Windows Disk Manager and selects **Action > Rescan Disks** to make sure the Windows Disk Manager is synchronized with CTE. They then initialize the disk, create a new volume for it, and format it. Notice that the new volume size is slightly smaller than the original 10 GB because CTE has reserved room for the CTE Private Region.



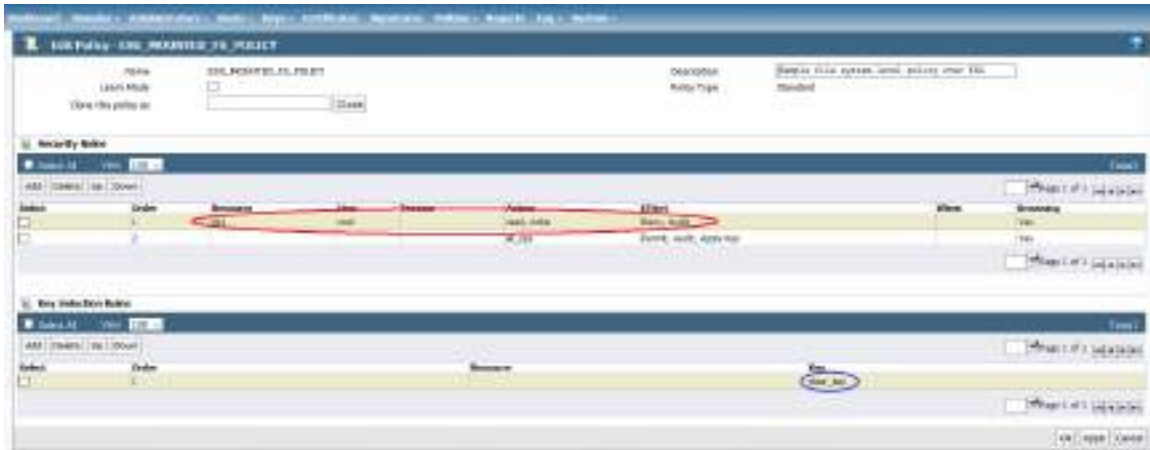
Use Case 3: Directory-Level GuardPoints

Protect structured or unstructured data stored in data files. The data files are organized inside one or multiple directories or folders within a file system namespace, such as NTFS or ReFS, where the entire file system namespace is guarded with one policy as a Directory GuardPoint. In this use case, the file system resides in a device guarded as ES GuardPoint.

Figure 12-2: All Data in file system Device Encrypted through an ES GuardPoint



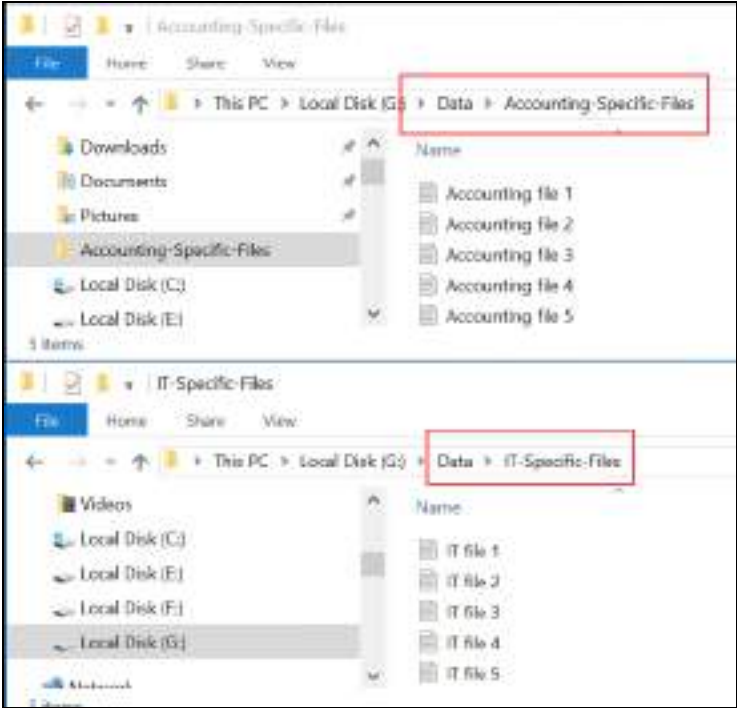
In this use case, two policies are enforced to protect the data in the device. As stated, one policy protects the entire file system namespace guarded under the Directory GuardPoint, and the guarded directory is the mount point pathname of the mounted file system. The policy on the mount point directory must specify *clear_key* in the key rule. Specifying a key other than *clear_key* must be avoided because all the data in the file system device is encrypted through the ES GuardPoint corresponding to the file system device. The screen shot below represents a sample Linux policy over the file system mount point where the policy blocks root access to read/write files under the subdirectory *dir1* in the mounted file system. For Windows, the policy would be the same as shown below except that the user name would be *Administrator* instead of root.



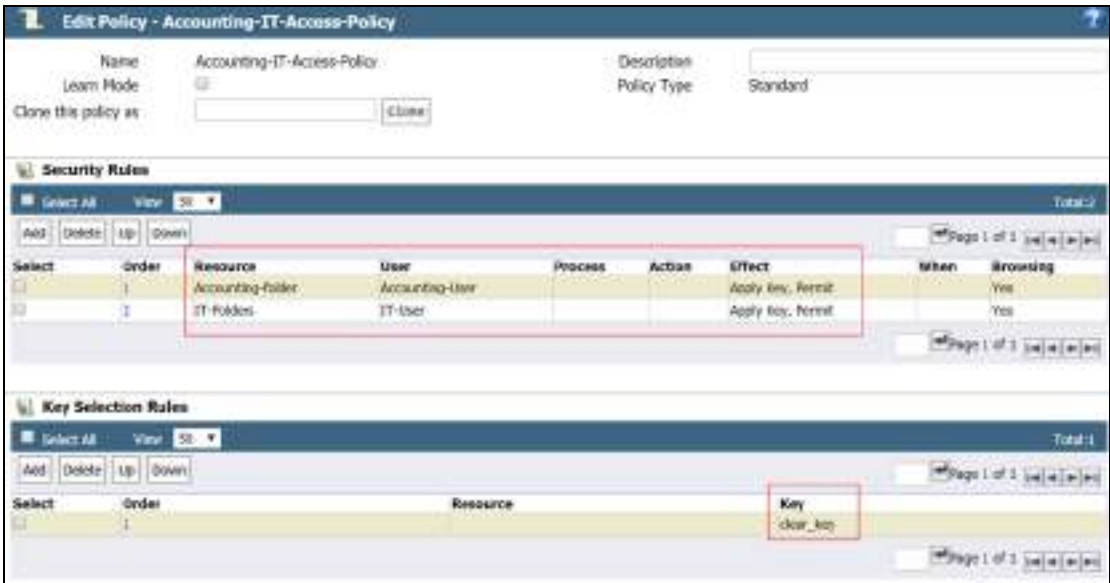
The second policy protecting the device is the same policy as use case 2.

Example

In this example, Jane Doe is a member of the Accounting team and John Fredricks is a member of the IT team. There are two folders on the guarded disk called `G:\Data\Accounting-Specific-Files` and `G:\Data\IT-Specific-Files`. Even though the disk is protected by an Efficient Storage GuardPoint, both Jane and John can see the files in either folder. For example:



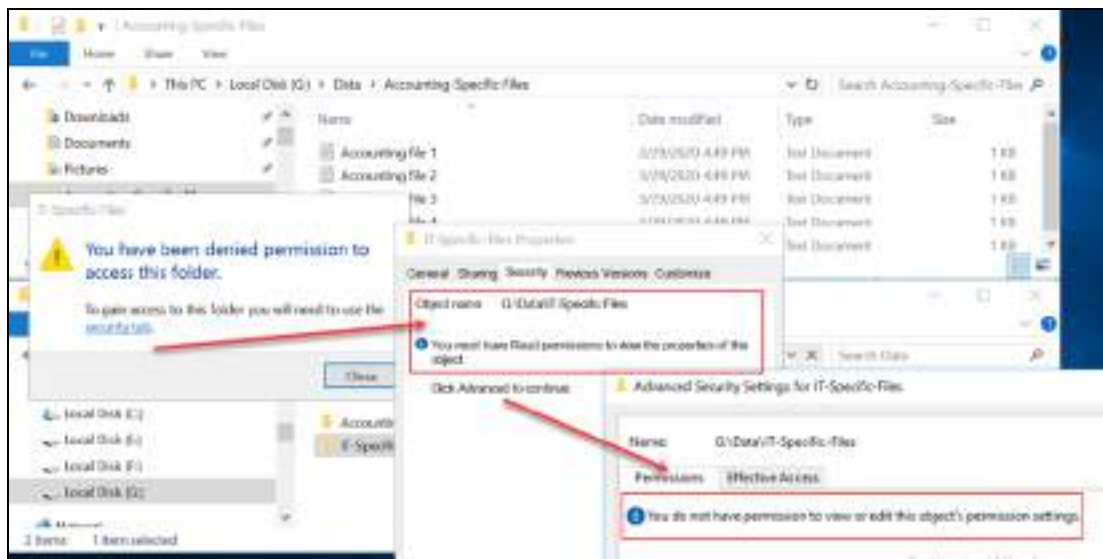
The DSM Administrator goes into the DSM and creates a standard policy that grants access to Jane Doe in the Accounting folder and grants access to John Fredricks in the IT folder. For the key rule, the policy must specify `clear_key`. For example:



Then the DSM Administrator applies the policy to `G:\Data`. For example:

Select All		View 50													
Guard		Unguard		Enable		Disable		Secure Start On		Secure Start Off		Transform Sparse Regions			
Select Policy		Host Group		Protected Path				Disk Group / Disk		Type		Domain		Auto Mount	
☐ ES-Standard-Policy				esg-disk1-demo						Raw or Block Device (Auto Guard)		ES		☐	
☐ ES-Standard-Policy				esg-disk2-demo						Raw or Block Device (Auto Guard)		ES		☐	
☐ ES-Standard-Policy				NewDisk3						Raw or Block Device (Auto Guard)		ES		☐	
☒ Accounting-IT-Access-Policy				G:\Data\						Directory (Auto Guard)		ES		☐	
Guard		Unguard		Enable		Disable		Secure Start On		Secure Start Off		Transform Sparse Regions			

Now when Jane Doe logs into the server, she can see the files in the Accounting-Specific-Files directory but she cannot access the files in the IT-Specific-Files directory, even if her account has Administrator-level access. For example:



Similarly, when John Fredricks logs in he will be able to access the files in the IT-Specific-Files directory but he will be unable to access the Accounting-Specific-Files directory.

Use Case 4: Full Device Protection

As shown in the previous use cases, administrators can add access control policies at the file system or directory level, thus controlling normal user access to the protected files. This does not, however, block users with Administrator privileges on the Windows machine from opening protected disks or volumes directly using Windows Administration tools such as DiskPart.

By opening the disks or volumes directly, Windows Administrators can read and write the clear text data from the device, bypassing any access controls. In order to prevent this, the DSM Security Administrator can include a *process set* in the policy associated with the device-level GuardPoint. The process set includes a white list of the processes that are allowed to run on the protected device. Any process not in the white list will be blocked by CTE.

Thales recommends adding at least the following system processes to your process set. These system processes are used to create snapshots and perform other standard disk management tasks. You can add other processes to your white list as required.

- Windows\System32\ntoskrnl.exe
- Windows\System32\svchost.exe
- Windows\System32\vds.exe

- Windows\System32\webm\WmiPrvSE.exe

For an additional layer of protection, you can create a *signature set* that contains the signature for each one of the processes that you want to add to your white list. If you include signature information in the process set, CTE uses that signature to verify the integrity of the process before it allows that process to access the protected data.

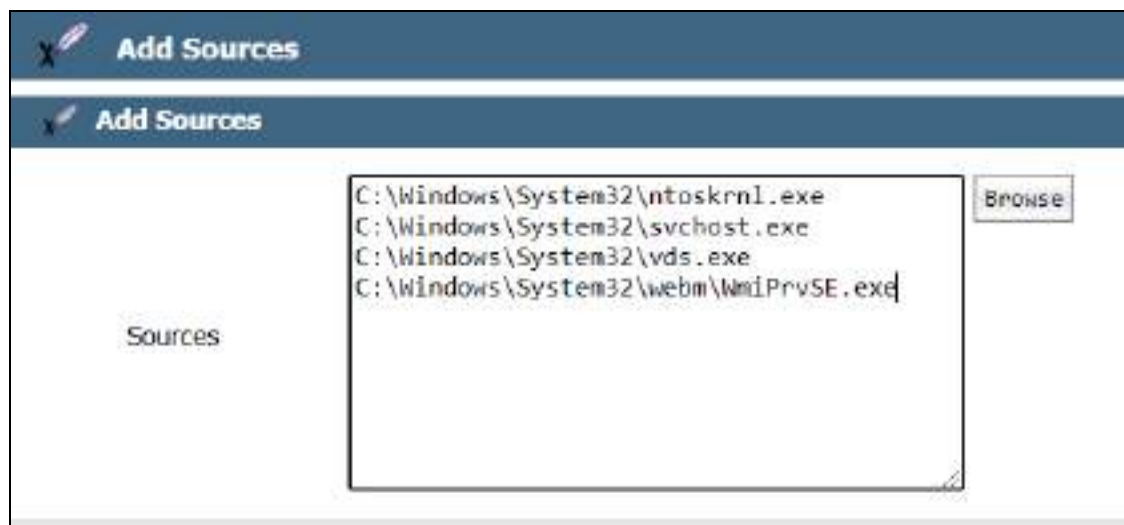
Note

Signature sets are host-specific, as the signature for a particular process may be different on different hosts. Therefore, if you add a signature set to a policy, you should only assign that policy to devices on the host associated with the signature set.

In the following example, we create a signature set that contains the four processes listed above, then we create a process set that references the signature set for each process. We then add the process set to a policy that we can use at the device level to protect the device.

1. Log into the DSM Management Console and switch to the appropriate domain.
2. To create the signature set:
 - a. In the top menu bar, click **Signatures**.
 - b. In the signature set table, click **Add**.
 - c. Enter a name for the signature set and click **OK**. For example, you could call the signature set "Win-WhiteList-Sigs".
 - d. Click on the name of the signature set you just created to edit the set.
 - e. Click the **Source** tab.
 - f. In the **Host** field, select the host whose processes you want to sign.
 - g. In the process table, click **Add**.
 - h. In the Add Sources dialog box, enter the processes you want to sign. You can either type the fully-qualified executable name or click **Browse** to select the process from an Explorer-styled interface. Make sure that each process is on its own line.

For example:



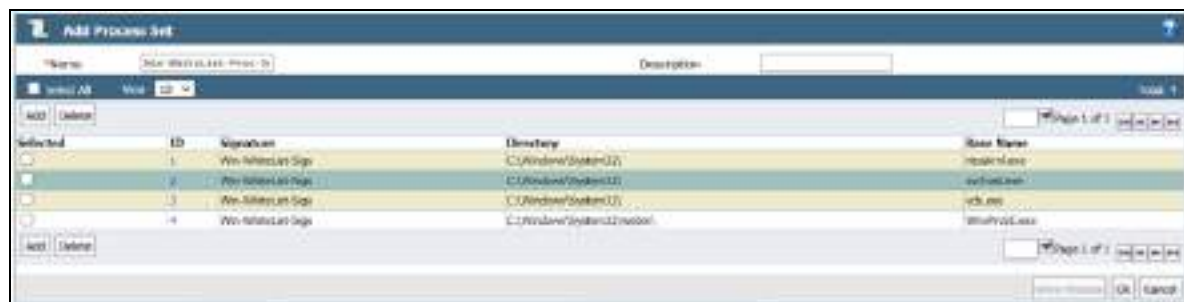
- i. Click **OK**.

- j. Click **Sign**.
- k. Click on the Signature tab to make sure that all processes now have a signature.



3. To create the process set:
 - a. In the DSM Management Console tool bar, select **Policies > Manage Policies > Process Sets**.
 - b. In the **Name** field, enter a name for the process set. For example, "Win-WhiteList-Proc-Set".
 - c. In the process set table, click **Add** and, for each process in the white list, fill out the following fields:
 - **Signature Set** — The name of the signature set you created in the previous step. For example, "Win-WhiteList-Sigs".
 - **Host** — The name of the host on which the process will run. You only need to specify the host if you want to **Browse** to the directory.
 - **Directory** — The directory in which the process resides. For example, "C:\Windows\System32\".
 - **File** — The process filename. For example, "vds.exe".

When you are done, there should be one entry for each process on the White List with the associated signature set.



- d. When you are done, click **OK**.

4. To add the process set to a policy:
 - a. Create a new policy or edit an existing policy.
 - b. In the **Security Rules** section, click **Add**.
 - c. In the Add Security Rule page, click the **Select** button associated with the **Process** field.
 - d. Select the process set you created in the previous step, then click **Select Process Set**.
 - e. Click the **Select** button associated with the **Action** field and select **all_ops**.
 - f. Click the **Select** button associated with the **Effect** field and select **Permit, Apply Key, and Audit**.
 - g. Click **OK**.
 - h. Add a second security rule with the effects **Audit** and **Deny**. Make sure that this rule comes *after* the process set rule.



- i. Save the policy.
5. Apply the policy to the appropriate device-level GuardPoints on the host associated with the signature set.

Alerts and Errors on Windows

ESG-ALERT: Data transformation failure on [GuardPoint]

This is an alert message to the DSM. It occurs when a protected host encounters an error transforming the data on the device during the IDT process.

Solution: Please contact Thales Support for troubleshooting and recovery.

ESG-INFO: Data transformation complete on [GuardPoint]

This message notifies the DSM Administrator that the protected host has completed the data transformation on the specified ES GuardPoint.

Disk label validation failed. Check your disk label and run command again.

This error occurs when you run the `voradmin esg config` command on an ESG device and you specify a disk label that is too long or that contains unsupported characters.

Solution: Check disk label and make sure that it meets the label name requirements.

Failed to get disk information

This error occurs when ESG found the device but cannot open it.

Solution: Please contact Thales Support for troubleshooting and recovery.

Boot partition is present on the disk. Disk or LUN can not be protected using CTE agent.

This message occurs when you run the `voradmin esg config` command on a disk that has a boot partition. ESG only supports protecting the data disks. You cannot use ESG to protect the system or boot disks.

The disk is dynamic disk. This disk or LUN can not be protected using CTE agent.

This message occurs when you run the `voradmin esg config` command on a dynamic disk. ESG does not support guarding dynamic disks.

Failed to initialize disk

This error message occurs when the `voradmin esg config` command fails to initialize the disk.

Solution: Please contact Thales Support for troubleshooting and recovery.

Disk is already initialized/guarded with CTE ESG protection

This message occurs when you run the `voradmin esg config` command on a disk is already protected by an ES GuardPoint or has already been initialized using the `voradmin esg config` command. The error message shows the disk label that was assigned to the device when it was initialized.

To determine the ESG status of all disks on the host, use the `voradmin esg status` command.

Failed to initialize disk with CTE ESG protection. Size must be greater than %xMB, Current size: %yMB

This error occurs when there is not enough free disk space to store the ES Header in the CTE private region on the disk.

Solution: Increase the disk size to at least the size shown in the error message.

Disk is initialized successfully with CTE ESG protection.

This notification indicates that CTE ESG protection has been successfully applied to the disk.

Disk is initialized successfully with CTE ESG protection. Disk must be Resized to at least 128MB before guarding as Efficient Storage GuardPoint

This message occurs after you use the `voradmin esg config xform` command on an existing disk. It indicates that the initialization was successful but that you must now increase the disk size by at least 128MB before you can apply the ES GuardPoint through the DSM.

Failed to initialize disk with CTE ESG protection. The specified disk does not exist or is not online.

This error message occurs when CTE cannot find the disk specified on the `voradmin esg config` command.

Solution: Check in the disk management utility to make sure the disk is available on the system. If it has gone offline, bring it back online and re-submit the `voradmin esg config` command. If the disk appears to be online and can be accessed by other applications but ESG still cannot find it, please contact Thales Support for troubleshooting and recovery.

Disk with specified label does not exist. Please select another disk.

This error occurs when the disk label specified on a `voradmin esg` command does not exist.

Solution: Check the disk label and resubmit the command. To see all available disk labels, use the `voradmin esg status` command.

Header deletion failed with error code

This error occurs when the Administrator enters the `voradmin esg delete <disk-label>` command for a valid ES disk but CTE cannot delete the ES Header from the specified disk.

Solution: Please contact Thales Support for troubleshooting and recovery.

Disk is protected with CTE ESG. Please unguard the disk before deleting ESG header.

This error occurs when the Administrator enters the `voradmin esg delete <disk-label>` command but there is still an ES GuardPoint assigned to the disk in the DSM.

Solution: Remove the ES GuardPoint through the DSM and then re-submit the `voradmin esg delete` command.

CTE ESG header deleted successfully.

This message indicates that CTE has successfully deleted the ESG header on the disk specified in the `voradmin esg delete <disk-label>` command.

CTE ESG header does not exist on the selected disk. Please select another disk

This message occurs when the Administrator enters the `voradmin esg delete <disk-label>` command but CTE cannot find an ES Header on the specified disk.

Solution: Check the disk label and resubmit the request. If the disk label is correct and the problem persists, please contact Thales Support for troubleshooting and recovery.

Chapter 13: Upgrading CTE on Windows

This chapter describes how to upgrade an existing VTE for Windows host to CipherTrust Transparent Encryption (CTE) for Windows.

Note

Currently, you can only upgrade a VTE for Windows host to CTE version 7.0.0.47 if you continue to use the DSM as your key manager. You cannot upgrade a VTE host to CTE and then register the upgraded CTE host with CipherTrust Manager. The migration path to CipherTrust Manager will be available in a future release.

This chapter contains the following sections:

- [To Upgrade in Windows Silently 135](#)
- [Verify the Windows Installation 135](#)
- [Resolving Problems that Prevent Silent Install 136](#)
- [CTE Scheduled Upgrade 136](#)
- [Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades 137](#)

To Upgrade in Windows Silently

If you have already installed CTE on a Windows computer and want to upgrade it silently, use the appropriate command below for the type of installation binary that you are using.

Note

The protected host must be able to connect to the DSM that it is registered to or the upgrade will fail.

Upgrade using self-extracting .exe

```
vee-fs-7.0.0-47-win64.exe /s /v" /qn"
```

Upgrade using MSI

```
msiexec.exe /i vee-fs-7.0.0-47-win64.msi /qn REINSTALLMODE=voums REINSTALL=ALL
```

Before upgrading using MSI, you must rename the installation file to the name of the previously used MSI installation file. See ["Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades" on page 137](#) for more information.

Note

For all types of upgrades, including interactive (GUI-based) and scheduled upgrades, the protected host must be able to connect to the DSM that it is registered to or the upgrade will fail.

Verify the Windows Installation

After running a silent install, verify the installation by checking CTE processes.

1. In the system tray, right-click the CipherTrust Lock icon.
2. Select **Status**. Review the information in the Status window to confirm the correct CTE are installed and registered.

Resolving Problems that Prevent Silent Install

If you encounter problems using MSI or self-extracting .exe silent install commands, first check the syntax of the command. To further investigate installation issues, you can use Microsoft diagnostics software:

- For desktop versions of Windows: [Microsoft Diagnostics Troubleshooting Wizard](#)
- For server versions of Windows: [Microsoft Automatic Troubleshooting Services](#) (MATS)

Refer to the Microsoft documentation on the linked pages for more information. See the *Compatibility Matrix for CTE Agent with Data Security Manager* for a list of versions of Windows that are supported for use with CTE.

CTE Scheduled Upgrade

Scheduled upgrade allows you schedule an upgrade of the CTE agent to occur after the next time the server hosting the agent reboots normally. Scheduled upgrade can minimize CTE service interruptions. Also, scheduled upgrade can reduce coordination issues in organizations where the security roles are separated.

Notes

- Install all Microsoft update patches before scheduling a CTE Agent upgrade. Otherwise, the upgrade will fail.
- The CTE scheduled upgrade feature is compatible with Windows Server 2008 R2 and higher versions.
- Currently, you can only upgrade a VTE for Windows host to CTE version 7.0.0.47 if you continue to use the DSM as your key manager. You cannot upgrade a VTE host to CTE and then register the upgraded CTE host with CipherTrust Manager. The migration path to CipherTrust Manager will be available in a future release.
- For all types of upgrades, including interactive (GUI-based) and scheduled upgrades, the protected host must be able to connect to the DSM that it is registered to or the upgrade will fail.

Scheduling a CTE Upgrade on the Command Line

To schedule CTE to upgrade the next time the system reboots, type:

```
> voradmin upgrade schedule <CTE setup executable path>
```

Self-extracting .exe Example

```
> voradmin upgrade schedule C:\6.0.3.15\vee-fs-7.0.0-47-win64.exe
```

MSI Example

```
> voradmin upgrade schedule C:\7.0.0.47\vee-fs-7.0.0-47-win64.msi
```

System Response

```
Creating and installing service to upgrade. CTE agent will be upgraded on next reboot.
```



WARNING

If you have scheduled an upgrade on reboot and the system crashes or is not shutdown gracefully, you must restart the system again to upgrade the agent.

Scheduling a CTE Upgrade Interactively (self-extracting .exe only)

When you open the self-extracting .exe CTE installation binary and a version of CTE is already installed, you have the option of upgrading immediately or initiating a scheduled upgrade. See the procedure below for details. This is an alternative to scheduling an update on the command line using `voradmin` (see ["Scheduling a CTE Upgrade on the Command Line" on the previous page](#)).

1. Move the self extracting .exe CTE installation binary to the computer on which you want to initiate the scheduled upgrade.
2. Double-click the self extracting .exe CTE installation binary to run it.
3. Click through the standard initial dialog boxes like the license dialog box.
4. On the **UPGRADE - Install now or Later** dialog box, click **Schedule Upgrade on next reboot** and then click **Next**.
5. Click **Schedule** on the confirmation dialog box.

The next time the computer reboots, the upgrade will occur.

This interactive method of scheduling an update is not available for MSI CTE installation binaries. You must use the `voradmin` command line scheduled upgrade method.

Show Scheduled CTE Upgrades

To display all scheduled CTE agent upgrades, type:

```
> voradmin upgrade show
```

System Response

```
Current version:      6.0.3.12
Target upgrade version: 6.0.3.15
Upgrade on reboot:    Enabled
```

Cancel a Scheduled CTE Upgrade

To cancel/cleanup a scheduled CTE agent upgrade, type:

```
> voradmin upgrade cancel
```

System Response

```
CTE agent upgrade canceled successfully.
```

Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades

When performing an upgrade, Windows Installer Package (MSI) expects the name of the installation binary to be the same as the binary that you used to install CTE. Because Thales includes the software version and build number in the binary file name, you must rename the installation binary to the name of the previously used MSI installation binary before upgrading using MSI. This applies to any MSI CTE upgrade method: typical (interactive), silent upgrade, and scheduled upgrade. If the name does not match the previous binary file name, the upgrade will fail with error code 1316.

For example, let's say that you installed the CTE Agent using the following installation file:

```
vee-fs-6.3.1.38-win64.msi
```

If you used this binary to install or upgrade CTE, the next time you want to upgrade CTE the installation binary that you download from Thales might have the following file name:

vee-fs-7.0.0.47-win64.msi

To upgrade successfully using MSI, you would need to rename the new installation binary to the previous file name of vee-fs-6.3.1.38-win64.msi before upgrading.

Finding The Name Used For A Previous MSI Installation or Upgrade

If you want to upgrade CTE using an MSI installation binary but don't know the file name that you used during the previous installation or upgrade, you can look it up by using one of the following methods on the computer where you installed CTE:

MSI File Name Lookup Method 1: PowerShell

Run the following command in PowerShell:

```
PS> (Get-WmiObject Win32_Product | where { $_.Name -match "CipherTrust Encryption Expert File System Agent" }).PackageName
```

Rename the new CTE setup installation binary to the file name output from the PowerShell command and proceed with the upgrade.

MSI File Name Lookup Method 2: Windows Registry

Find the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Product\  
905CB36BF7940894995701C86901D14F
```

Rename the new CTE installation binary to the file name in the registry and proceed with the upgrade.

Chapter 14: Uninstalling CTE from Windows

Considerations

- The CTE Agent must be removed from the Windows host before the host is removed from the key manager with which it is registered.
- Database applications like DB2 and Oracle can lock the user space while they run. If the uninstall fails because a GuardPoint is in use, determine which applications are using the files in the GuardPoint and stop them. Then run the uninstall again.

Procedure

1. Stop any application from accessing files in the GuardPoint.
2. In the key manager with which this host is registered, do the following:
 - Decrypt any data you want to use after uninstall. After the CTE Agent software is removed, access to data is no longer controlled. If data was encrypted, it will remain encrypted. If decrypted or copied out of the GuardPoint, the data is visible as clear text.

This decryption must be done on *every* GuardPoint on the host if you want to access all existing data on the host.
 - Make sure the Agent and System locks have been disabled for the host.
 - Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.*Do not* remove the host from the key manager yet.
3. Log on to the host as with system administrator privileges.
4. Use one of the following methods to uninstall the CTE Agent:
 - Use the standard Windows Add/Remove program utility from the Control Panel to remove the CTE software.
 - If you installed the CTE Agent using the MSI file, you can uninstall it using the command line with the `msiexec.exe /x Installation_executable /qn` command. For example:

`C:\> msiexec.exe /x vee-fs-7.0.0-47-win64.msi /qn`
5. Reboot the system when prompted.
6. Remove the host record from the key manager.

Appendix 15: Troubleshooting and Best Practices

Windows Systems

CTE will not register with the DSM

- If there is a firewall between the DSM and CTE, configure `vmd.exe` as a firewall exception on CTE for Windows. Otherwise, the DSM is unable to browse CTE.
- If using a Windows XP or Windows 2003 system Firewall, select **Control Panel > Windows Firewall > Exceptions > Add Program...** and browse for `vmd.exe`. The default location is
`C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmd.exe`
- If using a Windows 7 system Firewall, select **Control Panel > System and Security > Windows Firewall > Allowed Programs...** click **Change settings**, click **Allow another program** and browse for `vmd.exe`. The default location is
`C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmd.exe`

CTE with NFSv4: Permission denied error

You may see a permission denied error if you try to access files on an NFSv4 file system that is guarded by CTE.

CTE imposes a restriction on NFSv4 file systems to prevent write-only permissions from being set on individual files. You can work around this restriction by configuring read and write permissions on the same files.

You can also add a policy that allows write permissions.

This restriction applies only in the case of files resident in guarded NFSv4 file systems.

CipherTrust Transparent Encryption

CTE-Live Data Transformation with CipherTrust Manager

Release 7.0.0

Document Version 1

September 22, 2020

The bottom half of the page features a dark blue background with abstract geometric shapes. On the left, there is a large, bright blue triangle pointing upwards. Below it, a smaller, darker blue triangle points upwards. In the bottom left corner, there is a blue circular shape with a dotted pattern. The right side of the page has a vertical gradient from dark blue at the top to a lighter blue at the bottom, with a dotted pattern at the very bottom.

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2009-2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Contents

Preface	8
Intended Audience	8
Assumptions	8
The CTE Agent Documentation Set	8
Document Conventions	9
Typographical Conventions	9
Notes, tips, cautions, and warnings	9
Sales and Support	10
 Chapter 1: Introduction to CTE-LDT	 11
Overview of CTE-LDT	11
Use Cases	11
Keys in CTE-LDT (Versioned Keys)	12
Rekey Key Rotation	12
CTE-LDT Policies	12
CTE-LDT Runtime Flow	13
CTE-LDT Administrator Roles	14
Resiliency	15
 Chapter 2: Getting Started	 16
Using CTE-LDT	16
Backup/Restore	17
Restrictions	17
Windows Only Limitations	17
Linux Only Limitations	17
 Chapter 3: Setting Up CTE-LDT	 18
System Requirements	18
CipherTrust Software Requirements	18
CTE-LDT License Requirements	18
Host System Requirements	18
Backup Requirements	18
Linux-Specific Requirements	19
Supported Applications in Linux	19
Replication	19
SAP HANA Fibre Channel Systems	19
Installing the CTE-LDT License	19
Installing and Registering the CTE Agent Software	20

Setting the Linux Kernel Time Zone	22
Enabling CTE-LDT on a Protected Host	22
Chapter 4: Using CTE-LDT	24
Creating and Viewing Versioned Keys	24
Creating a Versioned Key	24
Viewing Versioned Key Information	26
Creating CTE-LDT Policies	26
Quality of Service	29
Purpose of QoS	29
Manage CTE-LDT Impact	29
Monitor and Control CPU Usage	29
Monitor and Control Rekey/Scan I/O Rate	29
QoS Scheduling During Backup/Restore	30
How to Set QoS	30
QoS Best Practices	32
General Best Practices for QoS	32
Select and Set Rekey I/O Rate	35
Create an CTE-LDT GuardPoint	37
Create an CTE-LDT GuardPoint for an Unguarded Directory	37
Converting a Non-CTE-LDT GuardPoint to an CTE-LDT GuardPoint	38
Rotating Encryption Keys (Rekey)	39
Manual Key Rotation	39
Creating a Key Rotation Schedule	39
Checking the Rekey Status	42
Obtaining Information About Keys Applied to Files	43
Key Report Option	43
Key Map Option	43
Showing GuardPoints During Rekey (Linux)	43
Suspending and Resuming Rekey and/or Scan Phase	44
Considerations	44
Automatic Suspend and Resume of CTE-LDT Operations Due to Insufficient Disk Space (Linux)	44
Behavior of Automatic Suspend and Resume of CTE-LDT Operations on ext4 File Systems	45
Rotating Encryption Keys While a Rekey is in Progress (Relaunch)	45
File System Operations	45
Renaming Files and Folders	46
Deleting a File	46
File Handling (Windows Only)	46
Enabling GuardPoints in Read-Only mounted file systems (Linux)	47
Copying Files Into a GuardPoint	47

Behavior of Hard Links Inside and Outside of GuardPoints (Windows)	48
Excluding Files or Directories from Rekey	48
Examples of Exclusion Key Rules	48
Encrypt Files With Exclusion Property a Non-Versioned Key	48
Exempt Excluded Files from Encryption (Set to clear_key)	49
Requirements for Exclusion Key Rules	50
Usage Notes and Limitations for Configuring Exclusion Key Rules	50
Adding an Exclusion Key Rule to an Existing Policy with Versioned Keys (Linux)	50
Adding an Exclusion Key Rule That is Part of an Active GuardPoint (Linux)	50
Changing an Exclusion Key Rule That is Part of an Active GuardPoint (Windows)	50
Conflicting Keys as the Result of Rename Operations	50
Overlapping Exclusion Key Rules	51
Caution About Applications That Create Temporary Files (Windows)	51
Rename Operations Crossing Key Rules (Linux)	51
Using Linked Files with Exclusion Key Rules (Linux)	51
Changing a Folder or Files from Versioned to Non-Versioned Key (Windows)	52
About the Exclusion Attribute for Files Matching an Exclusion Key Rule	53
The Exclusion Attribute is Persistent	53
Determining if a File is Included in an Exclusion Key Rule	53
Removing the Exclusion Attribute From a File	53
Rename and Restore Operations (Linux)	54
Listing All Files Included in an Exclusion Key Rule (Linux)	55
Listing All Files Included in an Exclusion Key Rule (Windows)	56
Using CTE-LDT with SAP HANA Fibre Channel Systems (Linux Only)	56
Chapter 5: CTE-LDT Administration	57
CTE-LDT Metadata in Extended Attributes	57
Listing Extended Attributes	58
MDS File (Linux)	59
Planning for CTE-LDT Attribute Storage	60
Using voradmin To Estimate Disk Space Required for CTE-LDT (Linux)	60
Displaying Metadata	61
Verifying Metadata (Windows only)	61
DFSR and Replication (Windows)	61
Multi-Node Configuration and Operation	62
CTE-LDT Behavior on Failover	62
Veritas Cluster Server	62
Backing Up and Restoring CTE-LDT GuardPoints	62
Clear Text Backup and Restore	62
Encrypted Backup and Restore	62

CTE-LDT Policy for Encrypted Backup and Restore	63
Backup/Restore of Metadata Store File (MDS) in GuardPoints Undergoing Rekey	64
Restoring a GuardPoint from a Backup	65
Potential Warnings During Restore Operation	66
Restore an Encrypted Backup	66
Restore a File Fully Rekeyed to the Latest Key Version	67
Restore a Partially Rekeyed/encrypted File	67
Restore a File Not Rekeyed/encrypted with an Older Key Version	67
Restoring Non-CTE-LDT Backup Data to an CTE-LDT GuardPoint	68
Using fsfreeze (Linux only)	69
CTE-LDT Backups Using a File System or Storage-Level Snapshot Tool	69
Windows Backup and Snapshots	70
CTE-LDT Backup and Restore Troubleshooting	70
Restored files to a GuardPoint protected with conflicting key rules	70
CTE-LDT Command-Line Administration: voradmin command	71
Moving a CTE-LDT GuardPoint from One CTE-LDT Policy to Another	72
Scenario	72
Removing CTE-LDT and Security Encryption	73
Migrating a GuardPoint Out of CTE-LDT	73
Converting a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy	73
Remove Protection from a GuardPoint	74
Deleting CTE-LDT Metadata (Linux)	76
Deleting CTE-LDT Metadata (Windows)	76
Removing CTE-LDT from a Host	77
Uninstalling the Agent while CTE-LDT is Rekeying GuardPoints	77
Chapter 6: Troubleshooting CTE-LDT	78
Monitoring and Statistics	78
Obtaining Statistics in the CipherTrust Manager with GuardPoint Status	78
Obtaining CTE-LDT Statistics at the Command Line	78
Obtaining a Rekey Report	79
About the rekey report	79
Manually generating a rekey report	79
Monitoring Ongoing CTE-LDT Operations at the Command Line (Windows only)	80
Protecting CTE-LDT GuardPoints against Failure in Underlying Filesystems (Linux)	80
CTE-LDT Recovery Challenges	80
CTE-LDT Recovery Enhancement	80
Recovery Alerts	81
Alerts Playbook	81
Failure to Suspend or Resume CTE-LDT Operation	81

Insufficient Resources	82
Failed to Update CTE-LDT Attribute	83
Rekey Stopped	83
Incomplete Key Rotation	83
Skipped Key Rotation	84
Failed to Update CTE-LDT Metadata During Scan Phase	84
File system inconsistencies after system crash	85
Error Messages	85
Failed to Transform File During Rekey	85
Failure to Suspend CTE-LDT	85
Failure to Start or Stop Transformation	86
Failure to Restart Transformation	86
Temporary Failure to Start Transformation on a File	86
Transient Condition while enabling GuardPoint	86
Failed to transform passthrough files for AD database files (Windows Only)	87
Warning and Info Messages	87
Stopping Transformation of a File on Volume Dismount (Windows only)	87
Issues with Policy or System Configuration	87
Failure to Enable GuardPoint During Cleanup	88
General CTE-LDT Operations	88
Missing CTE-LDT extended attribute	88
Locking Contention	88
Initiation and completion of CTE-LDT metadata cleanup	88
Recommendations and Considerations	88
All Platform Recommendations and Considerations	89
Binary Re-signing	89
Check for available disk space for CTE-LDT metadata	89
CTE-LDT Requirements for Backup	89
Learn Mode	89
Quality of Service (QoS)	90
Upgrade to CTE 7.0.0	90
Windows Recommendations and Considerations	90
File Handling	90
File Modification	90
CTE-LDT Limitations	91
Logical Sector Size	91
CTE-LDT Limitations on Linux	91

Preface

CTE-Live Data Transformation with CipherTrust Manager describes how to configure and use CipherTrust Transparent Encryption - Live Data Transformation (CTE-LDT) when the host is registered to CipherTrust Manager. If you want to use a Vormetric Data Security Manager (DSM) as your key manager, see the *CTE-Live Data Transformation with Data Security Manager* guide.

CTE-LDT is an optional, separately licensed feature of CipherTrust Transparent Encryption (CTE). With CTE-LDT, a CipherTrust Manager Administrator can change the encryption key and re-encrypt GuardPoint data without suspending user or application access to the data.

Intended Audience

CTE-Live Data Transformation with CipherTrust Manager is for security teams who want to rekey the existing GuardPoint data, or who need to perform an initial encryption of their GuardPoint data.

Assumptions

CipherTrust Transparent Encryption - Live Data Transformation is an enhancement to existing functionality. This documentation assumes the reader is familiar with the following CipherTrust products and processes:

- CipherTrust Manager
- CipherTrust Transparent Encryption (CTE)
- Key management
- Data encryption

The CTE Agent Documentation Set

The following guides are available for CTE Agent:

- *CTE Agent for Linux Quick Start Guide*
- *CTE Agent for Linux Advanced Configuration and Integration Guide*
- *CTE Agent for Windows Quick Start Guide*
- *CTE Agent for Windows Advanced Configuration and Integration Guide*
- *CTE Agent for AIX Installation and Configuration Guide*
- *CTE-Live Data Transformation with Data Security Manager*
- *CTE-Live Data Transformation with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with Data Security Manager*
- *Compatibility Matrix for CTE Agent for AIX with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent for AIX with Data Security Manager*
- *Release Notes for CTE for Linux Version 7.0.0.47*
- *Release Notes for CTE for Windows Version 7.0.0.47*
- *Release Notes for CTE for AIX Version 7.0.0.11*

Document Conventions

The document conventions describe common typographical conventions and important notice and warning formats used in Thales technical publications.

Typographical Conventions

This section lists the common typographical conventions for Thales technical publications.

Table 3-1: Typographical Conventions

Convention	Usage	Example
bold regular font	GUI labels and options.	Click the System tab and select General Preferences.
<i>bold italic monospaced font</i>	variables or text to be replaced	https://<Token Server name>/admin/ Enter password: <Password>
<code>regular monospaced font</code>	Command and code examples XML examples	Example: session start iptarget=192.168.253.102
<i>italic regular font</i>	GUI dialog box titles	The <i>General Preferences</i> window opens.
	File names, paths, and directories	/usr/bin/
	Emphasis	<i>Do not</i> resize the page.
	New terminology	<i>Key Management Interoperability Protocol (KMIP)</i>
	Document titles	See <i>CTE-Live Data Transformation with CipherTrust Manager</i> for information about CipherTrust Transparent Encryption.
quotes	File extensions Attribute values Terms used in special senses	“.js”, “.ext” “true” “false”, “0” “1+1” hot standby failover

Notes, tips, cautions, and warnings

Notes, tips, cautions, and warning statements may be used in this document.

A Note provides guidance or a recommendation, emphasizes important information, or provides a reference to related information. For example:

Note

It is recommended to keep tokenization keys separate from the other encryption/decryption keys.

A tip is used to highlight information that helps you complete a task more efficiently, such as a best practice or an alternate method of performing the task.

Tip

You can also use Ctrl+C to copy and Ctrl+P to paste.

Caution statements are used to alert you to important information that may help prevent unexpected results or data loss. For example:



CAUTION

Make a note of this passphrase. If you lose it, the card will be unusable.

A warning statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data. For example:



WARNING

Do not delete keys without first backing them up. All data that has been encrypted with deleted keys cannot be restored or accessed once the keys are gone.

Sales and Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

For support and troubleshooting issues:

- <https://supportportal.thalesgroup.com>
- (800) 545-6608

For Thales Sales:

- <https://cpl.thalesgroup.com/>
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

Chapter 1: Introduction to CTE-LDT

This chapter contains the following sections:

Overview of CTE-LDT	11
Keys in CTE-LDT (Versioned Keys)	12
CTE-LDT Policies	12
CTE-LDT Runtime Flow	13
CTE-LDT Administrator Roles	14
Resiliency	15

Overview of CTE-LDT

CipherTrust Transparent Encryption - Live Data Transformation (CTE-LDT) is an optional, separately licensed feature of CipherTrust Transparent Encryption (CTE). With CTE-LDT, after enabling a GuardPoint, a CipherTrust Manager Administrator can encrypt, or rekey, GuardPoint data without blocking user or application access to the data. In CTE-LDT, *rekey* means decrypting data with the current cryptographic key and then encrypting it with a new cryptographic key. The concept of rekey, and how CTE-LDT rekeys data, is described in this document.

After enabling GuardPoints, CTE-LDT performs *initial* encryption or rekeying in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block application and user access to data during encryption or rekey operations, which can seriously inconvenience users and affect operational efficiency.

With CTE-LDT, the CipherTrust Manager Administrator can create a single CTE-LDT policy for both initial encryption and subsequent rekeying. The same policy applies to production access and security rules without restricting user or application access to data. Applications have continuity of access to GuardPoint data during CTE-LDT.



WARNING

To prevent data loss or corruption, you must stop all applications and users that are accessing files inside a GuardPoint before enabling a Live Data Transformation encryption policy for that GuardPoint. Terminating the applications closes all files that are currently being accessed inside the GuardPoint.

Unlike non-Live Data Transformation policies, however, you do *not* need to keep the GuardPoint offline while data transformation takes place. Instead, you can restart all applications as soon as the GuardPoint has been applied to the host, and CTE will perform the data encryption in the background. This is the only application service downtime required when using CTE-LDT.

Use Cases

This section provides a summary of typical uses for CTE-LDT. The concepts mentioned in this section are described in more detail throughout the rest of this guide.

1. Encrypt unprotected data.

When protecting files in a directory, you must encrypt them. This process is called *initial data encryption*.

2. Convert non-CTE-LDT GuardPoints to CTE-LDT GuardPoints

Use when you have existing GuardPoints that are protected with policies created before you started using CTE-LDT.

3. Rekey process.

Changing the key from one version to another version of the same key provides more security. Using CTE-LDT, you can change the encryption keys to more secure keys.

4. Transform the encrypted data to clear data.

Keys in CTE-LDT (Versioned Keys)

CTE-LDT uses *versioned* keys. Each version of a particular versioned key has the same key name and encryption algorithm, but its own unique cryptographic material. That means that data encrypted with version 3 of a key named `LDT-Key` *cannot* be decrypted by *any* other version of `LDT-Key`, even though the key name remains the same.

Versioning allows you to add one key to your CTE-LDT encryption policy and then use different versions of that same key to periodically re-encrypt your data over time. CTE-LDT uses the new key material to transform data to the new key version, as part of the same Live Data Transformation policy that also protects the data. The process of re-encrypting data with a new version of the existing key is called *Key Rotation*.

In CipherTrust Manager, you can create a versioned key and then add that key to one or more Live Data Transformation policies. When you use CipherTrust Manager to create a new version of the key, CipherTrust Manager automatically pushes the new key version to any CTE clients associated with the Live Data Transformation policies that contain the key. As soon as the CTE Agent receives the new key, it begins transforming the data to the new key version in the background.

You can also create a Key Rotation Schedule in CipherTrust Manager that automatically rotates your keys periodically. When the scheduled rekey date is reached, CipherTrust Manager automatically creates a new key version and pushes it to any CTE clients that are associated with any policies that include the key. When CTE receives the new key version, it automatically starts the rekey process on the affected CTE-LDT GuardPoints.

Rekey | Key Rotation

In CTE-LDT, *rekeying* or *key rotation* means decrypting the data with a previous version of the key and re-encrypting it with a new version of the key. CTE-LDT allows users and applications to access data while CTE-LDT is rekeying the data. Rotating the key and re-encrypting the GuardPoint data with the new version of the key helps to maintain a high level of data security.

Most often, the rekey happens automatically based the Key Schedule defined in CipherTrust Manager, but you can also generate a new version of the key whenever you want to rekey the GuardPoints associated with that key.

CTE-LDT Policies

In CTE-LDT, you define a single policy for initial data encryption and subsequent rekeying. The policy specifies:

- **Current key**

Associated with data that you want to protect using CTE-LDT. This is either a non-versioned key from an earlier policy, or `clear_key`, which means that the data is not currently encrypted.

- **Transformation key**

The versioned key that CTE-LDT applies to transform the data from the key used for initial data transformation. When the transformation key rotates, it transforms the data from a previous version of the transformation key to a new version.

Note

Transformation key and versioned key are used interchangeably throughout this document.

As soon as CTE-LDT applies the policy to a GuardPoint and enables protection for it, CTE-LDT triggers an initial transformation from the current key to the transformation key.

When the transformation key expires, it generates the next version of the versioned key with new cryptographic material. The CipherTrust Manager then pushes the policy to the hosts. The policy now contains the new version of the key. This initiates a rekey process on the GuardPoint to transform data to the new version of the transformation key specified in the policy.

Users and applications can continue accessing data without any interruption during initial encryption and subsequent key transformations.

Note

During CTE-LDT policy creation, you must use the Apply Key effect in your policy. If you do not, then end users can see the clear text data until the file is transformed.

CTE-LDT Runtime Flow

This section presents an overview of how CTE-LDT works and what to expect when CTE-LDT is enabled and running in your environment. All of the tasks mentioned here are described in more detail later in this chapter.

First, the administrator completes CTE-LDT setup:

1. Upload the CTE-LDT license on the CipherTrust Manager.
2. Register CTE-LDT hosts with the CipherTrust Manager and be sure that the hosts are licensed for CTE-LDT.
3. Create one or more versioned keys.
4. Optionally create a Key Rotation Schedule or add your new keys to an existing schedule.
5. Define Live Data Transformation policies which use the versioned key(s) and contain rules governing CTE-LDT operations.
6. Optionally provide Quality of Service (QoS) settings for the CTE-LDT hosts. The QoS settings control the:
 - Window of time in which CTE-LDT operations are allowed to run.
 - Percentage of CPU resources that CTE-LDT can use, or the amount of data to transform according to the QoS setting per the CipherTrust Manager Administrator.

Note: Configuring the QoS settings is highly recommended as a best practice.

When these items are set up, CTE-LDT is ready to transform and encrypt data by applying policies to GuardPoints for live initial transformation and subsequent rekeys, as well as enforcement of security rules.

CTE-LDT goes through the following phases after the keys and Live Data Transformation policies are defined:

1. Initial data transformation starts

CTE-LDT begins when an Live Data Transformation policy is first applied to a GuardPoint or an LDT key is automatically rotated through a key rotation schedule in CipherTrust Manager. When a client that uses the associated policy contacts CipherTrust Manager, CipherTrust Manager sends the new policy, or the the key rotation notification, to the client. (If the same versioned key is used in multiple policies, *all* of the clients associated with the policies that contain the key are notified when the key changes.)

2. New key version triggers a rekey on the affected GuardPoints

On each client, CTE determines which GuardPoints are using the key that has just rotated to a new version. CTE starts an CTE-LDT rekey on each of those GuardPoints.

On Windows, you must wait for the current key rotation process to finish before you can launch another rekey request. On Linux, if another rekey is already underway on that GuardPoint, the new rekey is queued for later execution. For details, see ["Rotating Encryption Keys While a Rekey is in Progress \(Relaunch\)" on page 45](#).

3. Scan for files

On each GuardPoint where CTE has started a rekey, CTE-LDT determines which files to transform. CTE-LDT takes inventory of files encrypted with earlier versions of the rotated key and makes a persistent list of the files for transformation.

The scan phase might be interrupted, such as by a host reboot. In this case, when the host reboots and the GuardPoint is enabled again, the scan operation starts over from the beginning.

4. Rekey/Key Rotation

- a. Each file, from the persistent list of files, is decrypted using the old version of the key. The old key is applied to each file and then re-encrypted using the new version of the key. Note that new files created during the CTE-LDT process do not need to be rekeyed, as they inherit the new version of the key. Multiple files and multiple regions of files are rekeyed simultaneously.
- b. The CTE-LDT extended attribute of each file is updated. (For more about extended attributes, see ["CTE-LDT Metadata in Extended Attributes" on page 57](#).)
- c. You can suspend and resume the CTE-LDT rekey operation manually, or through the QoS schedule. This manages the impact CTE-LDT has on other applications and processes.

If system errors occur during rekeying, such as IO errors or crashes, CTE-LDT can manage and recover from them after the system error is fixed.

5. Finish

When all of the required files in the GuardPoint have been rekeyed, the system and storage resources used by CTE-LDT are released, except for the storage required for the extended attributes.

CTE-LDT creates a rekey report, listing all of the files that were rekeyed. For more information, see ["Obtaining a Rekey Report" on page 79](#).

Upon completion of rekey, the Rekey Status in the GuardPoint Status window of the CipherTrust Manager Console shows Rekeyed.

CTE-LDT Administrator Roles

Using CTE-LDT requires coordination and collaboration between several different administrators. Security, system, application performance and backup schedules are critical factors that affect planning. It is very important for the **CipherTrust Manager Administrator** to coordinate with the **system administrator** and the **backup administrators**. The following table describes the roles and responsibilities for these administrators.

CTE-LDT Administrators

Role	Responsibility	Actions
CipherTrust Manager Administrator	Administers CipherTrust Manager	Coordinates with system and backup administrators. Creates security policies, key rotation schedules, and rules for CTE-LDT. Defines Quality of Service settings for CTE-LDT, applications, and backups.

Role	Responsibility	Actions
System administrator	Administers servers on which CipherTrust Transparent Encryption (CTE) is deployed	Coordinates with the CipherTrust Manager Administrator to create Quality of Service schedule, taking into consideration the backup schedules.
Backup administrator	Manages data backups for data encrypted by CTE	Coordinates with the CipherTrust Manager Administrator to create Quality of Service schedule, taking into consideration the backup schedules.

Resiliency

CipherTrust Transparent Encryption - Live Data Transformation is resilient to many user actions and system occurrences. Since it is designed to run periodically without intervention, it includes various features to provide this resilience.

Before CTE-LDT enables a GuardPoint, it checks for any inconsistencies in files that were undergoing rekey at the time when system operations were interrupted. If it finds any inconsistencies, CTE-LDT corrects them before it enables the GuardPoint. It should only take a few seconds to identify and correct any inconsistency. On Windows, this process is delayed until applications access the affected files.

During rekey, if an issue such as an I/O problem or system crash occurs, the resiliency features of CTE-LDT ensures the consistency of user data. Such issues can cause an interruption in the middle of a rekey operation. When system operations resume, CTE-LDT corrects the problems and then resumes rekeying.

Chapter 2: Getting Started

This chapter contains the following sections:

Using CTE-LDT	16
Backup/Restore	17
Restrictions	17

Using CTE-LDT

Notes

- If you are new to CTE and CTE-LDT, read the CipherTrust Manager documentation first to familiarize yourself with the concepts of GuardPoints and Policies.
- Before installing CTE-LDT, see the *Compatibility Matrix for CTE Agent with CipherTrust Manager* to verify that your version of Linux is supported. Contact Thales Technical Support (<https://supportportal.thalesgroup.com>) for the matrix.

The following list contains the steps for successfully setting up and using CTE-LDT.

1. Install the CTE-LDT License on the CipherTrust Manager.
CipherTrust Transparent Encryption - Live Data Transformation is a separately-licensed feature of CTE. Before you can use it, you have to install the license to activate it. CTE-LDT is licensed for a specific number of hosts. For details about licensing, see the CipherTrust Manager documentation.
2. Install the CTE Agent and select the CTE-LDT feature during the install. For more information, see ["Installing and Registering the CTE Agent Software" on page 20](#).
If the client is already registered with CipherTrust Manager, you can enable CTE-LDT on the client through the CipherTrust Manager Console. For more information, see ["Enabling CTE-LDT on a Protected Host" on page 22](#).
3. Create Versioned Keys.
CTE-LDT uses *versioned keys*. A versioned key rotates to the next version of the key generating new key material automatically without policy change. CTE-LDT encrypts data with keys that use encryption standards like AES-256. This allows data to be re-encrypted without users having to edit the policy.
For more information, see ["Keys in CTE-LDT \(Versioned Keys\)" on page 12](#) and ["Creating and Viewing Versioned Keys" on page 24](#).
4. Optionally create a Key Rotation Schedule that will automatically rotate the versioned keys periodically. For more information, see ["Creating a Key Rotation Schedule" on page 39](#).
5. Create CTE-LDT Policies.
CTE-LDT uses a single Live Data Transformation policy to address both initial encryption and subsequent rekeying. The same policy applies to production access and security rules without restricting user or application access to data. Applications have continuity of access to GuardPoint data during CTE-LDT.
For more information, see ["Creating CTE-LDT Policies" on page 26](#).
6. Set QoS Settings.
QoS enables administrators to manage and control CTE-LDT impact to application workloads by monitoring and controlling the use of host system resources, such as memory or I/O utilization, during CipherTrust Transparent Encryption - Live Data Transformation. Administrators can also choose schedules for data transformation, or manually pause or resume transformation operations.
For more information, see ["Quality of Service" on page 29](#).

7. Create GuardPoints and Apply CTE-LDT policies to the GuardPoints

A GuardPoint is a directory in the file system hierarchy, where its contents have a CipherTrust data protection policy applied to it. The CTE Agent intercepts any attempt to access anything in the GuardPoint and uses the policies obtained from the CipherTrust Manager to grant or deny the access attempt. Typically data copied into a GuardPoint is encrypted, and only authorized users can decrypt and use that GuardPoint data.

For more information, see ["Create an CTE-LDT GuardPoint" on page 37](#).

Backup/Restore

Before you enable GP with CTE-LDT policies, make sure that you back up your data.

For more information, see ["Backing Up and Restoring CTE-LDT GuardPoints" on page 62](#).

Restrictions

Remember the following restrictions when using CTE-LDT:

- CTE-LDT does not support nested GuardPoints, where a GuardPoint is contained inside another GuardPoint.
- For HA clusters, CTE-LDT only supports the Asymmetric (active/passive) configuration. CTE-LDT does not support Symmetric (active/active) configuration.

Windows Only Limitations

CTE-LDT does not support GuardPoints on CIFS network shared directories.

Linux Only Limitations

- CTE-LDT does not support Linux automounted file systems.
- CTE-LDT does not support system hibernation (`pm-hibernate`) on Linux hosts where CTE-LDT is in use.
- CTE-LDT does not support GuardPoints on NFS shares and `secvm` configured devices.
- Do not use CTE-LDT on GuardPoints over XFS and VxFS file systems at the same time.
- You cannot use CTE-LDT and Docker container on the same host.
- You cannot use CTE-LDT and OpenShift container on the same host.

Chapter 3: Setting Up CTE-LDT

This chapter contains the following sections:

System Requirements	18
Installing the CTE-LDT License	19
Installing and Registering the CTE Agent Software	20
Setting the Linux Kernel Time Zone	22
Enabling CTE-LDT on a Protected Host	22

System Requirements

CipherTrust Transparent Encryption - Live Data Transformation (CTE-LDT) requires the following environment.

Note

See the latest *Compatibility Matrix for CTE Agent with Data Security Manager*, in the online support portal, for a list of CTE versions and supported operating systems.

CipherTrust Software Requirements

- CTE Agent version 7.0.0 or higher must be installed on every client that you want to protect.
- The CipherTrust Manager with which these clients are registered must be version 2.0.0 or higher.

CTE-LDT License Requirements

One CTE-LDT license is required for *each* protected host.

Host System Requirements

Memory requirements: Both Linux and Windows require a minimum of 8 GB memory on each protected host.

Disk space requirements: CTE-LDT requires a specific amount of disk space in the file system, over and above the space required for the guarded files themselves. CTE-LDT uses the additional space to store CTE-LDT metadata.

- For Linux, to estimate the amount of free file system disk space required by CTE-LDT on a Linux host, use the `voradmin ldt space` command.
- For Windows, the typical minimum space requirement for a GuardPoint is the number of files in the GuardPoint multiplied by 4K, plus 256MB. To estimate the amount of free space required for a GuardPoint, use the `voradmin ldt space <GuardPoint-name>` command.

Backup Requirements

The backup application must have the capability to back up user-extended attributes. For example, Thales tested CTE-LDT with NetBackup. You can also use other applications that can back up user-extended attributes.

Note

For Windows, the application must use Volume Shadow Copy service (VSS) for backup and restore.

Linux-Specific Requirements

To use CTE-LDT on an ext3 or ext4 file system, the block size **must** be 4K. Run `dumpe2fs` to determine the block size of the ext3 or ext4 file systems before using CTE-LDT. This limitation does not apply to XFS or VxFS file systems. You can use CTE-LDT on XFS with a block size of 1K or 2K.

For CTE-LDT to work properly, the underlying file system must support and enable user-extended attributes. All of the file systems supported by CTE-LDT support these attributes. If you are using CTE-LDT with ext3 or ext4 mount points, you must explicitly enable the extended attribute mount option by editing `/etc/fstab` and adding the `user_xattr` mount option. In the other file systems supported by CTE-LDT, user extended attributes are enabled by default, so you do not have to explicitly enable them.

Example `/etc/fstab` entry for ext3 on Red Hat 6 or SLES:

```
/dev/sdb1 /disk2 ext3 defaults,user_xattr 0 0
```

Example `/etc/fstab` entry for ext4 on Red Hat 6 or SLES 12 (ext4 is not supported on SLES 11):

```
/dev/sdc1 /disk3 ext4 auto,users,user_xattr,exec 0 0
```

For more information about extended attributes, see ["CTE-LDT Metadata in Extended Attributes" on page 57](#).

Supported Applications in Linux

For all of the supported operating systems for database applications, see the *Compatibility Matrix for CTE Agent with CipherTrust Manager*.

Replication

- `rsync`.
- Hardware/software based replication system.

SAP HANA Fibre Channel Systems

SAP HANA is compatible with CTE-LDT. See the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *CTE Agent for Linux Advanced Configuration and Integration Guide*.

Installing the CTE-LDT License

CTE-LDT installs with the CTE Agent software, but it is a separately-licensed CTE feature. Before you can use it, you have to install the license on the CipherTrust Manager to activate CTE-LDT on any CTE clients. CTE-LDT is licensed for a specific number of clients.

1. Obtain an CTE-LDT license from Thales. You can purchase CTE-LDT along with the CipherTrust Manager software or you can add CTE-LDT later.
2. Install the license on the CipherTrust Manager.
For details, see the CipherTrust Manager documentation.

To confirm that the CTE-LDT license is in effect:

1. In the CipherTrust Manager Applications Page, open the **Admin Settings** application.
2. Click **Licensing** in the left-hand menu bar.
3. Expand the entry for **CTE - Live Data Transformation** in the License table. CipherTrust Manager shows the total number of client licenses in the **Total Clients** field and the total number of licenses used in the **Used Clients** field.

Installing and Registering the CTE Agent Software

Install the CTE Agent software with the CTE-LDT feature on each client you want to protect. The following procedure describes how to use the interactive installer to install CTE and register CTE-LDT. For additional registration options, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide*.

Prerequisites

Make sure you have the following information from the CM Administrator:

- The registration token for the CipherTrust Manager with which you plan to register the CTE Agent.
- The name of the profile you intend to assign to the client if you want to use a profile other than the default client profile.
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note: If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type **y** and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.47
```

```
In order to register the CipherTrust Transparent Encryption File System Agent
with a Vormetric Data Security Manager
```

- 1) you must know the host name of the machine running the DSM (the host name is displayed on the Dashboard window of the Management Console), and
- 2) unless you intend to use the 'shared secret' registration method, the agent's host machine must be pre-configured on the DSM as a host with the 'Reg. Allowed' checkbox enabled for this agent type on the Hosts window of the Management Console.

```
In order to register with a CipherTrust Manager you need a valid registration
token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Enter **y** to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE. For example:

```
Do you want to continue with agent registration? (Y/N) [Y]: y
```

```
Please enter the primary key manager host name: 10.3.200.141
```

```
You entered the host name 10.3.200.141
Is this host name correct? (Y/N) [Y]: y
```

6. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the following
list.
```

```
[1] sys31186.qa.com
[2] 10.3.31.186
```

```
Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 2
You selected "10.3.31.186".
```

7. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
Please enter the profile name for this host: My-Profile
Please enter the host group name for this host, if any:
Please enter a description for this host: RHEL7 system West Coast Datacenter
```

```
Token           : 12345
Profile name     : My-Profile
Host Group       : (none)
Host description : RHEL7 system West Coast Datacenter
Are the above values correct? (Y/N) [Y]: y
```

- At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloning. The default is **y** (enabled):

```
It is possible to associate this installation with the hardware of this
machine.  If selected, the agent will not contact the key manager or use any
cryptographic keys if any of this machine's hardware is changed.  This
can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]: y
```

- At the LDT prompt, specify that you want this client to use CTE-LDT by typing **Y** and pressing Enter:

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]: y
```

- At the Cloud Object Storage (COS) prompt, specify whether you want this client to use CTE COS.

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

- CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.
Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption File System Agent with the
CipherTrust Manager on 10.3.200.141.
```

```
Installation success.
```

- In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Setting the Linux Kernel Time Zone

The Linux kernel contains an internal time structure that may or may not contain time zone information. On system configurations that do not contain time zone information, CTE-LDT stores and displays timestamps for rekey beginning and ending in UTC (Coordinated Universal Time) rather than the system's local time zone. If this occurs, the administrator can set the kernel's internal time zone to the local time zone if they desire timestamps in their local time zone.

To set the Linux Kernel time zone information, at boot time type:

```
# hwclock --systz
```

The command sets the kernel's time zone to the local time zone and resets the System Time based on the current time zone.

Note

On systems that do not set the time zone by default, existing timestamps for completed rekeys remain in UTC, even if you run `hwclock --systz`. Only timestamps for new rekeys display the local time zone.

Enabling CTE-LDT on a Protected Host

When you install CTE on a host, you can enable CTE-LDT during the registration process as described in "[Installing and Registering the CTE Agent Software](#)" on page 20. If you have already registered the host with CipherTrust Manager, you can enable CTE-LDT in the client entry in CipherTrust Manager.

Note

The CTE-LDT license is valid for a certain number of clients. Once you reach this limit, you can either purchase additional CTE-LDT licenses, or reclaim a license by removing a CTE-LDT client. For details, see ["Removing CTE-LDT and Security Encryption" on page 73](#).

You cannot disable CTE-LDT on a client once it has been enabled.

To enable CTE-LDT on an existing host:

1. In the CipherTrust Manager Applications Page, open the **CTE** application and click **Clients** in the left-hand menu bar.
2. Click on the name of the client on whom you want to enable CTE-LDT.
3. On the Client Details page, select the **Live Data Transformation** check box, then click **Apply** to enable CTE-LDT on the protected host.

Note: After CTE-LDT has been enabled for the host, the check box is greyed out because you cannot change this option once it has been set.

Chapter 4: Using CTE-LDT

Creating and Viewing Versioned Keys	24
Creating CTE-LDT Policies	26
Quality of Service	29
Create an CTE-LDT GuardPoint	37
Rotating Encryption Keys (Rekey)	39
File System Operations	45
Excluding Files or Directories from Rekey	48
Using CTE-LDT with SAP HANA Fibre Channel Systems (Linux Only)	56

Setting up keys, policies, and GuardPoints with CTE-LDT is very similar to performing the same tasks in CTE without CTE-LDT. However, there are some differences.

This chapter contains the steps, in order, for successfully setting up and using CTE-LDT.

Creating and Viewing Versioned Keys

For CTE-LDT, you create a versioned key that you can add to any number of Live Data Transformation policies. When you add a new key version, CipherTrust Manager pushes the new version to every CTE client that is associated with any of they Live Data Transformation policies that contain that key.

Use the **Keys & Access Management** application in the CipherTrust Manager Applications Page when creating or viewing versioned keys.



CAUTION

Make sure that all keys you create for CTE-LDT are Symmetric. CTE-LDT does not support asymmetric keys.

Creating a Versioned Key

1. Log into the CipherTrust Manager Console as an administrator.
2. Open the **Keys & Access Management** application.
3. Click **Create a New Key**.
4. Enter a Key Name so that you will be able to find this key easily when you want to rotate it. For example, LDT-Key-1.

Note

When CipherTrust Manager displays the list of available keys, you cannot filter the list by versioned vs. non-versioned. Therefore, it is especially important to name the key in such a way that you can easily search for it by name.

Using a standard naming convention will also help if you want to create an automatic key rotation schedule for all your CTE-LDT keys.

5. In the **Key Metadata > Groups for Key sharing** section, do the following:
 - a. In the **Search** box, type "cte".
 - b. Add CTE Admins and CTE Clients to the key sharing groups by clicking the green **Add** button. The **Key Shared?** check box is automatically selected and the **Add** button changes to a **Remove** button.

- c. Below the Groups table, click the **CTE Key Properties** check box.

CipherTrust Manager displays the following options for CTE keys:

- **CTE Versioned:** Specifies that this is a versioned key. Make sure this option is selected.
- **Persistent on Client:** Specifies whether the key is stored in persistent memory on the client.

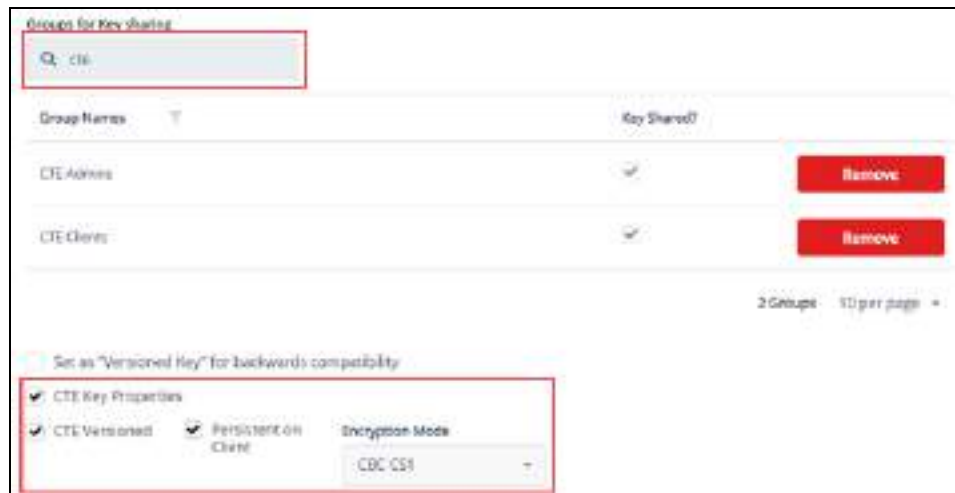
If this option is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.

If this option is *not* selected, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.

- **Encryption Mode:** Encryption mode of the key. Choose one of the following for CTE-LDT keys:
 - CBC
 - CBC CS1

Encryption using CBC CS1 keys is known as enhanced encryption. For details, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide*.

Note: XTS encryption is not supported for protecting directory-based GuardPoints. Do not select XTS as your encryption mode.



6. In the Key Behaviors section at the bottom of the page, clear the **Prevent this key from being exported** check box. If the key cannot be exported, the key will not appear in the keys list when you add the key rule to the policy. If you want the option to delete this key later on, clear the **Prevent this key from being deleted** check box. Use caution when deleting keys, as any data encrypted with that key will be inaccessible if you delete the encryption key.



7. Click **Create**. The new key appears in the Keys table.

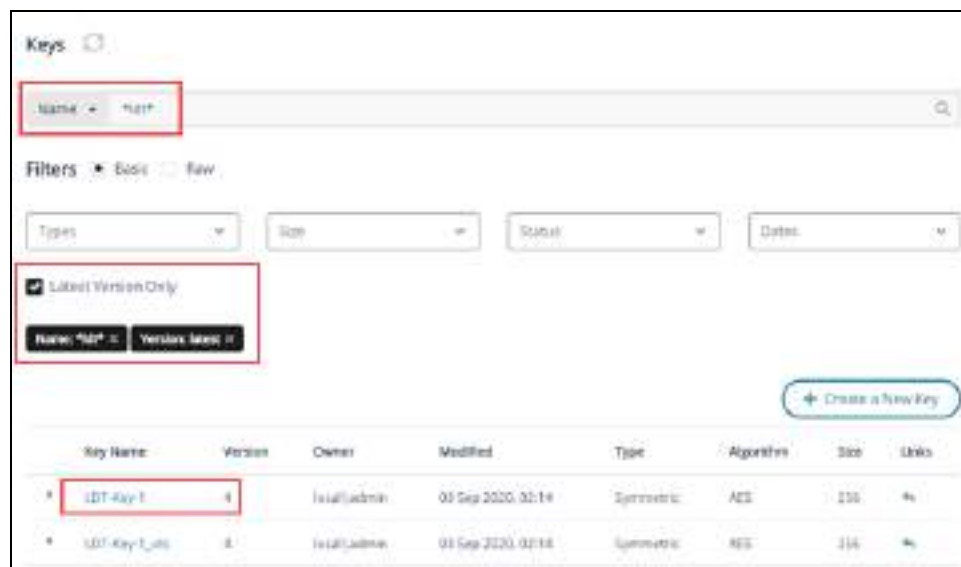
Viewing Versioned Key Information

1. Log into the CipherTrust Manager Console as an administrator.
2. Open the **Keys & Access Management** application.
3. Click the **Latest Version Only** check box to show only one entry for each versioned key.
4. Find the key in the Keys table.

Tip: You can filter the list by key name using wildcard searches. For example, if you know that the key name contains "LDT", you can search for *ldt*. The search is *not* case sensitive.

If the **Version** for a key is 0, then this is the first version of the key and no key rotation has taken place. If the **Version** is greater than 0, the key has been rotated.

Note: When you create a CBC CS1 key, CipherTrust Manager automatically makes a second key called <key-name>_xts. This key is maintained and used by CipherTrust Manager, and it can be ignored when you are looking at your CTE-LDT keys.



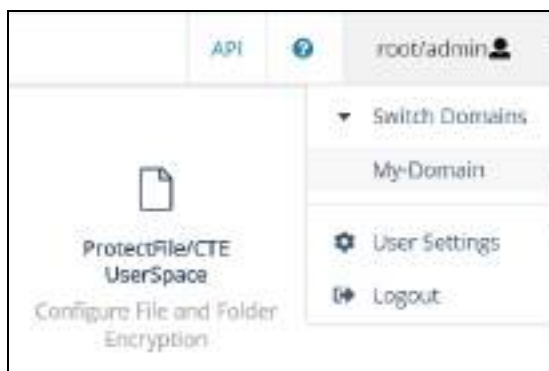
5. To find all versions of a key, click the name of the key in the **Key Name** column. CipherTrust Manager displays the ID, version number, state, and date created information for each version of the key.

Creating CTE-LDT Policies

CTE-LDT uses a single Live Data Transformation encryption policy to address both data transformation and ongoing protection. In contrast, if you do not use CTE-LDT, you need a separate policy for initial data transformation, or rekey, and another policy to protect the data while it is in production use. For more information about CTE-LDT policies, see ["CTE-LDT Policies" on page 12](#).

To create an Live Data Transformation encryption policy:

1. In a web browser, navigate to the URL of the CipherTrust Manager you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to the next step. If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the domain/user name (default: **root/admin**) on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.
 - c. The logged in user now shows the new domain name/user name.



3. In the CipherTrust Manager Applications Page, open the **CTE** application.
4. In the left-hand menu bar on the Clients page, click **Policies**.
5. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
6. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. For example: LDT-Policy-West
Policy Type	Select Live Data Transformation.
Description	A user-defined description to help you identify the policy later. For example: LDT policy for the West Coast Datacenter.
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/CTE-LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.

7. Click **Next**.

8. On the Security Rules page, define the security rules you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of `key_op` and the effects `Permit` and `Apply Key`. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version. This rule is required by CTE-LDT, so you cannot edit it, move it, or delete it.

To add additional security rules, click **Create Security Rule** and enter the requested information. If you want to grant user and application access to files at all times, including during initial CTE-LDT and subsequent key rotations, add a security rule with the action `all_ops` and the effects `Permit` and `Audit`.

For details about adding security rules, see the CipherTrust Manager documentation.

9. On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one. If the data has not yet been encrypted, select clear_key . Otherwise select the name of the non-versioned key that is currently being used to encrypt the data.
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

When you are done specifying key rules, click **Next**.

10. On the Confirmation page, review the information you entered and click **Save** when you are ready to save the policy.

The following example shows a simple CTE-LDT policy that encrypts clear-text files using a versioned key named LDT-Key-1. The `key_op` and `all_ops` actions in the Security Rules panel grant user and application access to files at all times, including during initial CTE-LDT and subsequent key rotations.

1 General Info

Name: LDT-Policy-West

Policy Type: Live Data Transformation

Description: LDT policy for the West Coast Datacenter

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*			key_op	permit,applykey	No
*			all_ops	permit,audit	Yes

3 Key Rules

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule
	clear_key	LDT-Key-1_v1	No

Quality of Service

CTE-LDT runs in real time, while users actively interact with applications. This could impact performance. However, CTE-LDT is designed to not adversely affect application or system performance.

Purpose of QoS

Quality of Service (QoS) provides tools for an administrator to minimize the effect of CTE-LDT on system and application performance. It provides a set of parameters that administrators can set to control CTE-LDT use of system resources, primarily CPU and I/O bandwidth. When the QoS parameters are set appropriately, CTE-LDT stays within the defined boundaries to ensure that critical user applications are not adversely affected by CTE-LDT operations.

Manage CTE-LDT Impact

Administrators can pause or resume CTE-LDT operations to manage and control CTE-LDT impact to application workload. When data transformation occurs, either during initial or subsequent transformations, it requires substantial host CPU and I/O resources. This can cause contention for resources between the applications simultaneously running on the protected host. The administrator specifies QoS settings on each host, or at a host group level, that is using CTE-LDT. When CTE-LDT is running, QoS monitors CPU or rekey/scan rate on the host and enforces the QoS settings. QoS can also monitor and enforce an administrator imposed limit on the volume of data undergoing rekey per second. The QoS settings enable you to strike a balance between completing an CTE-LDT process and not interfering with host application performance.

Monitor and Control CPU Usage

QoS monitors and controls the use of host system resources during CTE-LDT, specifically, CPU usage and rekey/scan rate.

Note

You can control CPU usage or rekey/scan I/O rate, but not both. The CPU usage and rekey/scan I/O rate options are mutually exclusive.

Monitor and Control Rekey/Scan I/O Rate

You can choose Rekey I/O Rate as a threshold to control the CTE-LDT processing rate. When this threshold is entered, the Quality of Service continuously monitors CTE-LDT transformation and enforces the specified amount of data during:

- **Rekeying**—CTE-LDT is transforming the data on active GuardPoints based on the new key version.
- **Scanning**—CTE-LDT is analyzing files in GuardPoints. Scanning occurs:
 - Before initial transformation (Linux only)
 - Before a rekey (Linux only)
 - Following an interrupted rekey, such as a reboot on Linux or Windows, and also a directory rename or directory deletion on Windows

You can set the Rekey I/O Rate or CPU Threshold for multiple clients through the QoS Settings section in a CipherTrust Manager client profile. All clients associated with a given client profile will use the QoS thresholds set in that profile unless the thresholds are overridden locally on the individual client. (The default setting for Rekey I/O Rate in the client profile is 0 (zero), which means QoS will run full throttle.)

To set the QoS thresholds locally on a particular client, use the `voradmin ldt ior <iorate>` command on that client. When you do so, the `voradmin` setting overrides the Rekey I/O Rate or CPU Threshold set in the CipherTrust Manager client profile. If QoS was already set locally on this client and you use `voradmin` to set the Rekey I/O Rate, CTE-LDT ignores any CPU threshold previously set.

To resume using the client profile QoS values for a client, use `voradmin ldt ior 0` to set the Rekey I/O Rate to 0 (zero). When you do so, CTE returns to using the Quality of Service settings in the client profile.

A tolerance level is associated with the Rekey I/O Rate. Together, the tolerance and Rekey I/O Rate specify a range for the CTE-LDT processing rate. The Quality of Service selects a proper tolerance for a Rekey I/O Rate provided through the `voradmin` command, and maintains the CTE-LDT processing rate at the specified Rekey I/O Rate plus or minus the tolerance. The tolerance is selected as follows:

- When the Rekey I/O Rate is less than or equal to 10MB/sec, the tolerance is 3MB/sec.
- When the Rekey I/O Rate is greater than 10MB/sec. and less than 50MB/sec, the tolerance is 4MB/sec.
- When the Rekey I/O Rate is at 50MB/sec or higher, the tolerance is 10% of the specified Rekey I/O Rate.

To set or reset Rekey I/O Rate on a single host, use the `voradmin` command as follows:

- To set the threshold of 50 MB/sec., use the following command:

```
# voradmin ldt ior 50
```

- To reset the current threshold:

```
# voradmin ldt ior 0
```

For more information about setting the Rekey I/O Rate using `voradmin`, see ["Select and Set Rekey I/O Rate" on page 35](#).

QoS Scheduling During Backup/Restore

QoS scheduling plays an important role when backing up/restoring data without the *Apply Key* rule applied to the backup/restore process. During backup/restore, you **must** pause CTE-LDT operations before taking backups. QoS scheduling allows the administrator to enter the schedule for QoS aligned with the backup schedule, and pause the CTE-LDT processes for the duration of the backup. The schedule specifies which days of the week, and what times of day, CTE-LDT is permitted to run. CTE-LDT cannot run at any time that is not permitted by the QoS schedule. QoS suspends CTE-LDT operations at all times outside of the schedule.

When setting a QoS schedule, consider your system and application peak demand periods during the day and week. Also consider your schedule for data backups. Schedule CTE-LDT to pause when you need all available system resources for other tasks, such as meeting peak user demand or performing data backups.

Note

On Windows, if your backup applications are using VSS, then you do not need to pause CTE-LDT on Windows.

How to Set QoS

To set QoS for a host to enforce a threshold on CTE-LDT based on CPU percentage:

1. Log into the CipherTrust Manager Console as an administrator.
2. Open the **CTE** application.
3. In the left-hand menu, select click **Profiles**.
4. If you want to add a new profile, click **Create Profile** and specify a profile name and description.

5. Click the profile name in the **Profiles** table.
6. Click the Quality of Service Configuration section heading to open the QoS options and select one of the following radio buttons:
 - **Rekey by Rate** — Specifies that you want to set a Rekey I/O Rate threshold. Enter a value between 0 and 100 in the associated **LDT QoS Rekey Rate** field. If you specify 0, CTE does not throttle the CTE-LDT rekey or scanning processes.
 - **Rekey by CPU**— Specifies that you want to set a CPU Rate threshold. Enter a value between 0 and 99 in the associated **CPU Percentage** field.

If you select this option, CTE-LDT applies a tolerance of +/- 2% on CPU threshold settings up to 7%. For threshold over 7%, CTE-LDT applies a tolerance of +/- 4%.

If CPU% is set to 0, QoS stops monitoring CPU usage and CTE-LDT operations run at maximum rekey rate within the available system resources. Setting CPU percentage to 0 does not affect CTE-LDT schedules, so CTE-LDT operations are suspended and resumed per QoS schedule.

If you do not enter CPU threshold percentage, CTE-LDT applies CPU threshold of 5% capped by default.

If CPU% is set to a very high value, such as 25%, the rekey process competes with other applications to use as many CPU cycles as it can. As a best practice, start with a setting of 10%, and increase or decrease it slowly by 5% until it reaches a reasonable level that does not adversely affect the performance of user applications. The higher the percentage, the more quickly CTE-LDT completes its processing. However, this speed causes increased competition for resources, which can significantly degrade the performance of other applications using this host.



CAUTION

Do not set CPU% to a very high value in an attempt to force faster data transformation. This can potentially exhaust other system resources.

When you select **Rekey by CPU**, the **Cap CPU Allocation** check box becomes available. Check this box to specify that the CPU allowance must never exceed the percentage set in CPU%. If **Cap CPU Allocation** is not checked, and additional CPU resources are available on the host, CTE-LDT consumes part of the available resources for rekey above the CPU threshold. Exceeding the threshold may impact your production workload as your production CPU resource consumption fluctuates over time.

For example, if CPU% is set to 10%, but **Cap CPU Allocation** is not set, the rekey process continues consuming available CPU cycles after reaching 10% CPU utilization, at which point the rekey process starts contending with applications for CPU cycles.

7. In the QoS Schedules section, select the schedule you want to use from the **LDT QoS Schedule** drop-down list. This list includes the following options:
 - ANYTIME
 - WEEKNIGHTS
 - WEEKENDS
 - CUSTOM

If you select anything other than CUSTOM, CipherTrust Manager displays the time ranges in which CTE-LDT can run in the **Time Ranges** column. If you select CUSTOM, you can then click the **Create New QoS Schedule** button to create a custom schedule. Add one custom schedule entry for each time range in which you want QoS to run.

By limiting CTE-LDT to periods of low application usage, you minimize the potential for resource contention between applications and CTE-LDT.

The following example shows a profile with the CPU threshold capped at 10%. The QoS schedule is set for 1 am to 4 am on Mondays, Wednesdays, and Fridays.

QUALITY OF SERVICE CONFIGURATION

☐ Rekey by Rate
LDT QoS Rekey Rate (MB/s)

☒ Rekey by CPU
☒ Cap CPU Allocation
CPU Percentage

QoS Schedules
LDT QoS Schedule: [Create New QoS Schedule](#)

Name	Time Ranges	
CUSTOM	Monday 1:00 AM - Monday 4:00 AM	...
CUSTOM	Wednesday 1:00 AM - Wednesday 4:00 AM	...
CUSTOM	Friday 1:00 AM - Friday 4:00 AM	...

QoS Best Practices

This section gives tips and examples to help you set QoS parameters for the best results.

General Best Practices for QoS

- Use Rekey I/O Rate threshold to limit CTE-LDT impact, if any, to your production workloads. Rekey I/O Rate approach is a simpler method for a CipherTrust Manager Administrator or system administrator to enforce a limit on the volume of data that CTE-LDT should rekey per second. You can choose a threshold, in units of MBs per second, which is a small percentage of peak IOPS from your production workload.
- You will see the effects of QoS settings only if the number and/or types of files in the GuardPoints stress the rekey or scan processes. On hosts with a relatively small number of files, the rekey or scan process may complete quickly without hitting a threshold and causing throttling to occur.

- Use QoS CPU parameters as an alternate method for controlling the effect CTE-LDT has on application performance.

Set limits on CTE-LDT CPU usage whenever runtime monitoring shows that user applications are affected by CTE-LDT. Start by setting the CPU parameter to 10%, then increase or decrease in 5% intervals, as needed, to tune the CPU allocation. When an acceptable level is reached, and CTE-LDT is not noticeably affecting user applications, leave the QoS CPU parameters at a constant setting.

- Use monitoring tools.

Monitor host CPU utilization with tools like `vmstat`, `top`, and `iotop` on Linux and `perfmon` on Windows.

You can also monitor and obtain statistics with the `voradmin ldt stats` command.

For more information about `voradmin ldt stats`, see ["Obtaining CTE-LDT Statistics at the Command Line" on page 78](#).

- Select CPU resource allocation for CTE-LDT from 1% to the available limit minus 5%.

If the monitoring tools indicate system CPU usage, without CTE-LDT, it is at N%, available CPU resource is M%, where $M = 100 - N$. Select a percentage within 1 - (M - 5) to allocate to CTE-LDT CPU usage. However, remember that QoS tolerates 2% - 4% leeway in the actual CPU usage, so adjust your selection by 2 - 4%.

- Do not set CPU resources to 0% or 99% in an attempt to minimize or stop CTE-LDT

A CPU% value of 0 or 99 is reserved for disabling the QoS CPU monitoring function. This does not stop CTE-LDT or minimize its resource usage; rather the opposite. It enables CTE-LDT to run with its maximum rekey rate. Note that when CPU % is not set, CTE-LDT clients enforce a 5% CPU threshold by default.

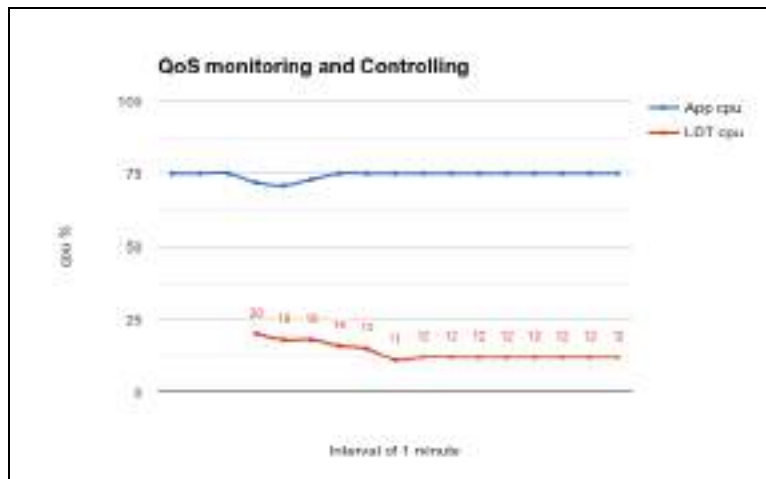
- Cap the CPU allocation.

QoS provides a **CAP CPU Allocation** parameter. Set this parameter to **True**. This ensures that CTE-LDT resource usage never exceeds the allocated percentage.

Example: Setting QoS before starting CTE-LDT

You can be proactive and set up QoS parameters before enabling GuardPoints that are protected with CTE-LDT policies. This ensures QoS starts monitoring and controlling CTE-LDT resource usage from the start. The following graph shows an example where 10% of the CPU is assigned to CTE-LDT. QoS makes sure that CTE-LDT is restricted to use only 10% of the CPU. There is a tolerance level of +/- 4%, so actual CTE-LDT usage can range between 5% and 15% of CPU. In the following example, applications use 75% of the CPU resources. As the graph shows, when CTE-LDT starts, application CPU utilization drops for a moment, because CTE-LDT exceeds the CPU threshold. QoS immediately reduces CTE-LDT's CPU usage to 12%, which is within tolerance levels for a 10% setting, and the application CPU share returns to normal.

Figure 4-1: QoS makes visible improvement immediately when CTE-LDT starts



The graph above was obtained on a Linux system running sysbench.

- To find the amount of CPU resources currently in use by applications, type:

```
# top -n 1 -b | grep sysbench | awk 'BEGIN {cpu=0} {cpu += $9} END {print cpu}'
```

- To find the amount of CPU currently in use by the CTE-LDT-protected host, type:

```
# top | grep Cpu
```

- To find the amount of CPU currently in use by CTE-LDT, type:

```
# voradmin ldt stats | grep CPU
```

Example: Monitoring and controlling resource usage during CTE-LDT

Suppose that CTE-LDT has started with CPU set to 25%, and users realize their applications are affected. For example, there might be a higher than expected level of CTE-LDT I/O operations. To return application performance to normal, reduce the CPU allocation for CTE-LDT.

1. Set the **CPU parameter** to a lower value, such as 10%.
2. Select the **Cap CPU Allocation** option.

QoS restricts CTE-LDT CPU usage to 10%. The application user should monitor their application. If the application's performance is still affected, reduce the CPU parameter further, such as to 5%. Repeat this procedure until application performance returns to a satisfactory level.

The following graph shows an example where QoS is not enabled to monitor and control CTE-LDT CPU usage from the start. When CTE-LDT starts, application CPU usage drops from 65% to 20%. By setting the QoS CPU parameter to 10%, application usage is greatly improved.

Figure 4-2: CPU usage allocation before and after QoS CPU parameter is set



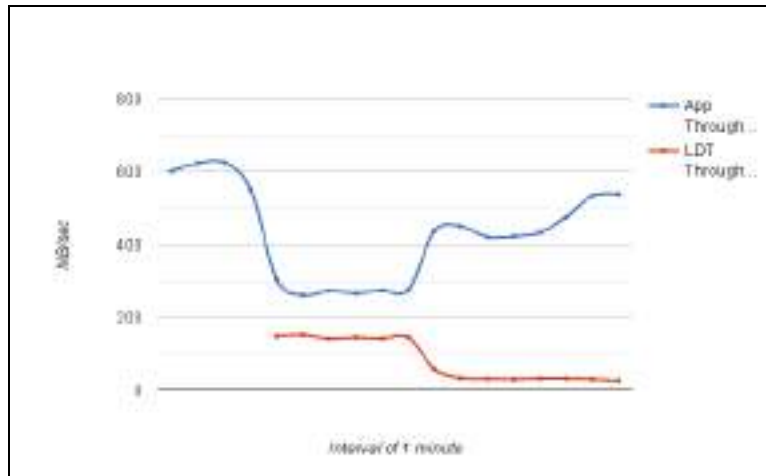
Example: How QoS CPU settings affect I/O bandwidth

Controlling CPU utilization indirectly controls I/O bandwidth. When CTE-LDT is consuming less CPU resources, it is usually performing fewer operations of all kinds, including input and output.

The following graph shows how an application's I/O throughput is affected by CTE-LDT, and how QoS can reduce this effect through monitoring and controlling the CTE-LDT CPU resource usage.

This graph is from the same system described in ["Example: Monitoring and controlling resource usage during CTE-LDT" above](#). No QoS parameters are set at first. When CTE-LDT starts, application I/O drops from more than 600 MB per second to below 30 MB per second. By setting the QoS CPU parameter to 10%, the CTE-LDT I/O operations drop to below the application's ability to perform so application I/O operations is greatly improved.

Figure 4-3: I/O operations before and after QoS CPU limit is set



To obtain the data for this graph:

- Use `iotop` and benchmarking tools on an RHEL system to obtain application I/O throughput.
- Use `voradmin ldt stats` to obtain the CTE-LDT I/O throughput and rekey rate.

Select and Set Rekey I/O Rate

You can choose to set the Rekey I/O Rate to control I/O operations from CTE-LDT to minimize CTE-LDT impact to your production workload. It's assumed that you already know the maximum IOPS on your host system during your production workload. With this information, you can choose a threshold for Rekey I/O Rate and enforce the selected threshold during CipherTrust Transparent Encryption - Live Data Transformation. The work flow is as follows:

1. Set **Rekey I/O Rate** threshold using `voradmin` or in the CipherTrust Manager Console.
2. QoS retrieves the threshold and starts monitoring and controlling CTE-LDT according to the specified threshold and the tolerance factor corresponding to the threshold.
3. The selected threshold will be in effect within 2 to 4 minutes after entering the threshold.

When Rekey I/O Rate and CPU or IOWAIT thresholds are set, QoS will monitor and control the CTE-LDT processing rate based on the Rekey I/O Rate threshold. The CPU threshold will be ignored.

Set Rekey I/O Rate Threshold

1. Set **Rekey I/O Rate** threshold by using `voradmin`:

```
# voradmin ldt ior 10
```

You can also set the Rekey I/O Rate for one or more managed hosts using the Quality of Service section in a client profiles. For more information about using this method, see ["How to Set QoS" on page 30](#).

In the `voradmin` example above, QoS enforces the threshold of 10MB/sec with the tolerance of +/- 3MB/second. Effectively, CTE-LDT attempts to rekey the amount of data in the range of 7MBs/second to 13MB/second.

On Linux and Windows, you can use `voradmin ldt ior` to report the current threshold setting without specifying a value for threshold:

```
# voradmin ldt ior
QoS Rekey I/O rate threshold: 10 MB/sec
QoS Rekey I/O tolerance: 3 MB/sec
```

2. Be sure the threshold you enter is appropriate for your production workload. To verify this:

- a. Observe the Rekey I/O Rate for a few minutes using `voradmin`.

On Linux, you can do this using:

```
# voradmin ldt stats
Host level statistics:
File stats: rekeyed=202390, passed=0, created=0, removed=0
Data stats: rekeyed=6.2GB, truncated=0.0MB
QoS: IOR threshold=10MB/sec, tolerance=3MB/sec
current_rekey_rate=2MB/sec, current_iow=0ms
load_factor=50, delay_factor=0, delay_scan=0
```

On Windows, you can do this using:

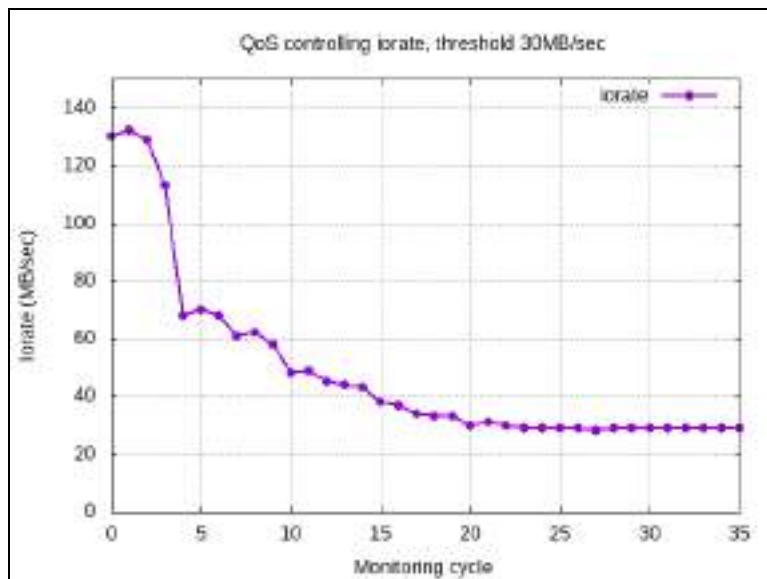
```
voradmin ldt monitor
Host Stats:
Total number of Guard Points      = 1
Rekey Status                      = Rekey done (Finished rekey on 1 out of 1 GP's)
Total files to be transformed     = 0
Total files transformed           = 0
Total files in progress           = 0
Total transformation threads      = 0

Current rekey rate                = 0 KB/s
Rekey IO rate threshold           = 1000 MB/s
Rekey IO rate tolerance           = 4 MB/s
```

- b. Set an appropriate threshold. Do not set the threshold value too high, as QoS might not be able to achieve it because of other resource bottlenecks.

3. Check the QoS controlling rekey rate.

QoS will monitor and control CTE-LDT utilization using the specified threshold. The following figure shows an example of how QoS monitors and controls CTE-LDT utilization. In this example, the threshold is 30 MB/sec. Throughput of CTE-LDT was nearly 130 MB/sec. QoS brings it down to within the range of 30 MB/second.



4. Disable QoS.

QoS will not monitor and control resources when all the thresholds, CPU, Rekey I/O rate, and IOWAIT are set to 0. When Rekey I/O Rate and IOWAIT are not explicitly set, it is considered to be set to 90 MB/second.

QoS continues to apply its schedules for suspending CTE-LDT operations at certain days and times regardless of what values are set for CPU, Rekey I/O Rate, and IOWAIT thresholds.

Summary of QoS Resources

The following table summarizes the available thresholds and the actions of QoS module to enforce the set thresholds:

Scenario	QoS Action
Only Rekey I/O Rate threshold is set	Monitor and control the CTE-LDT processing rate based on Rekey I/O Rate
Rekey I/O Rate and CPU threshold are set	Monitor and control the CTE-LDT processing rate based on Rekey I/O Rate. CPU threshold is ignored.

Create an CTE-LDT GuardPoint

After you have installed the license and registered the CTE-LDT host (see [Chapter 3: "Setting Up CTE-LDT" on page 18](#)), you can create an CTE-LDT GuardPoint on the host. When you create the CTE-LDT GuardPoint, you select a Live Data Transformation policy and apply that policy with its transformation keys to that GuardPoint. CTE automatically gets the Quality of Service settings from the associated Client Profile in CipherTrust Manager.

This section describes two scenarios:

- ["Create an CTE-LDT GuardPoint for an Unguarded Directory" below](#)
- ["Converting a Non-CTE-LDT GuardPoint to an CTE-LDT GuardPoint" on the facing page](#)

Create an CTE-LDT GuardPoint for an Unguarded Directory

To create an CTE-LDT GuardPoint on what was previously an unprotected/unguarded directory:

1. Create an Live Data Transformation policy that transforms data from clear text to a versioned key. In the policy, set Current Key to `clear_key` and Transformation Key to the versioned key. For details, see ["Creating CTE-LDT Policies" on page 26](#).
2. Set, or modify, the Quality of Service (QoS) parameters in the Client Profile associated with the CTE client to account for CTE-LDT on all GuardPoints on this client. For details see ["Quality of Service" on page 29](#).
3. In the CipherTrust Manager Applications Page, select the **CTE** application.
4. In the Clients table, click on the name of the client you want to protect.
5. Above the GuardPoints table, click **Create GuardPoint**.

6. In the Create GuardPoint page:
 - a. In the **Policy** field, select the CTE-LDT policy you created earlier.
 - b. In the **Type** field, select the type of device. For CTE-LDT, you can select **Auto Directory** or **Manual Directory**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a Windows-style explorer.

If you want to enter multiple paths, put each path on its own line.
 - d. Keep the **Preserve Sparse Regions** option selected if you want CTE to ignore sparse regions during data transformation.

A *sparse region* is a region within the file size that has not yet been written to. Therefore, it is not allocated with disk blocks. Any attempt to read a sparse region reads stream of zeros as data. A file may have one or more sparse regions, or an entire file may be sparse.

If you select **Preserve Sparse Regions**, CTE-LDT detects and skips transforming sparse regions. Therefore, it does not change the number of blocks utilized in the file system. This is the default.

If you disable **Preserve Sparse Regions**, CTE-LDT transforms a file without checking or skipping sparse regions, if they exist. Consequently, as CTE-LDT operations transform and fill sparse regions with encrypted stream of zeros, sparse regions are allocated with disk blocks. This increases the number of disk blocks utilized in the file system.
 - e. Click **Create**.
 - f. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**.

The CipherTrust Manager pushes the GuardPoint configuration to the client and CTE immediately begins transforming the data in the specified folders from clear-text to cipher-text.
7. When the data transformation has finished, applications can resume accessing the now-protected data.

Converting a Non-CTE-LDT GuardPoint to an CTE-LDT GuardPoint

After enabling CTE-LDT on a client, you can change a non-LDT GuardPoint to a CTE-LDT GuardPoint. CTE-LDT GuardPoints provide the advantage of allowing users to access all files in the GuardPoints while encryption is occurring. There is no downtime for the user except for the time needed to apply the GuardPoint.

1. Write a new CTE-LDT policy that transforms data from the non-CTE-LDT/non-versioned key used in the existing GuardPoint, to an CTE-LDT versioned key. See ["Creating CTE-LDT Policies" on page 26](#).
2. Make sure there is no application activity within the GuardPoint.



CAUTION

This step is critical. Do not skip it. Make sure there is no application activity within the GuardPoint.

3. Remove the current GuardPoint.
 - a. Open the **CTE** application and click **Clients** in the left-hand menu bar.
 - b. Click on the name of the client whose GuardPoint you want to change.
 - c. Find the GuardPoint you want to change in the GuardPoints table, then click the (...) button at the end of the row and select **Remove**.
4. Guard the directory again using the new CTE-LDT policy. Use the steps in ["Create an CTE-LDT GuardPoint for an Unguarded Directory" on the previous page](#), but choose the policy that starts from the non-versioned/non-LDT key rather than a policy that starts from `clear_key`.

Rotating Encryption Keys (Rekey)

The following sections describe procedures related to encrypting an existing GuardPoint with a new key (also called rekeying).

Manual Key Rotation

If you need to rekey your GuardPoint prior to the expiration of the current key version, you can manually start a rekey process.

On Windows, you cannot rotate a key until all current data transformations that use the same key have completed, whether those transformations are an initial data transformation or a rekey. On Linux, you can rotate the key at any time. For details, see ["Rotating Encryption Keys While a Rekey is in Progress \(Relaunch\)"](#) on page 45.

1. In the CipherTrust Manager Applications Page, open the **Keys & Access Management** application.
2. Click **Keys** in the left-hand menu bar.
3. In the Keys table, click on the name of the key that you want to rotate.
4. On the Key Detail page, click the Add button (+) above the table to add a new version.



The new version appears in the Versions table.



Creating a Key Rotation Schedule

In CipherTrust Manager, you can create an automatic key rotation schedule that will automatically rotate all of the keys included in the schedule on a periodic basis. As soon as CipherTrust Manager creates a new version of a key, it pushes the new version to any clients associated with the policies that use the key. If the policy is a Live Data Transformation policy, CTE automatically begins rekeying the data in the CTE-LDT GuardPoint with the new version of the key.

1. In the CipherTrust Manager Applications Page, open the **Admin Settings** application.
2. Click **Schedules** in the left-hand menu bar.

CipherTrust Manager displays the existing key rotation and backup schedules that have been defined in the system. Thales strongly recommends that you look at any existing key rotation schedules to make sure that the keys you want to rotate are *not* already included in one of those existing schedules.

If the existing key rotation schedules do not include the keys you want to rotate, continue with this procedure to create a new schedule.

3. On the **Schedules** page, click **Add Schedule**.
4. On the **Select Schedule Type** page, click **Key Rotation** and click **Next**.
5. Add a schedule name and description. Make sure you name the schedule as descriptively as possible so that other users can tell at a glance what keys that schedule includes. For example, you could name the schedule "Rotate-LDT-Keys" and use the description "Rotates all keys with "LDT" in their name on a yearly basis."

When you are done, click **Next**.

6. On the **Schedule Config** page, enter the following information:
 - **Duration**. Enter the day and time on which CipherTrust Manager should start using the key rotation schedule in the **Schedule Starts** field. When this day and time is reached, CipherTrust Manager looks at the date in the **Frequency** section and automatically creates a new version on that date.

Enter the day the schedule should end in the **Schedule Ends** field, or select the **Never** check box to tell CipherTrust Manager there is no end date for this key rotation schedule. If you select a date in this field, CipherTrust Manager automatically stops creating new key versions when that day and time are reached.

- **Frequency**. Select the **Basic** radio button to specify the frequency (daily, weekly, monthly, or yearly) and the UTC time at which CipherTrust Manager should automatically rotate the key after the schedule starts.

Select the **Raw (Cron)** radio button to create a cron job to control the key rotation schedule. Specify cron format in the following order:

minute, hour, day of month, month, and day of week

These five values indicate when the job should be executed. These values are mandatory and must be specified in the order given. The allowable values are:

Field	Allowed Values
minute	0-59 or * / , -
hour	0-23 or * / , -
day of month	1-31 or * / , -
month	1-12 or JAN-DEC or * / , - This field is case in-sensitive, so JAN, Jan, or jan are all equally valid.
day of week	0-6 or SUN-SAT or * / , - This field is case in-sensitive, so SAT, Sat, or sat are all equally valid.

Examples:

- December 31 at 2:35 AM UTC could be specified as: 35 2 31 Dec *
- On the 25th of every April, August, and December at midnight UTC could be specified as:
0 25 APR,Aug,dec *.
- Every Monday, Wednesday, and Friday at 8:00 PM UTC could be specified as: 0 20 * * 1,3,5

When you enter a **Duration** and a **Frequency**, CipherTrust Manager displays the next several times the key rotation will be run under the **Frequency** field. Make sure the key rotation will be done on the days you expect.

Note: While the specified time is in UTC, the scheduled run times are shown in your local time. Therefore there may not be an exact match between the time set in the **Frequency** field and the displayed run time.

When you are done, click **Next**.

7. On the **Key Rotation Page**, specify the selection criteria you want CipherTrust Manager to use when it selects the keys it will rotate.



CAUTION

Make sure you are extremely careful when you specify the selection criteria so that you do not accidentally rotate keys that should not be rotated using this schedule. Whenever a new key is added to CipherTrust Manager, CipherTrust Manager compares its name and details to the filters set in all key rotation schedules defined in the Admin Settings application, and it automatically adds the new key to ALL key rotation schedules where it matches the selection criteria.

If your selection criteria is too broad, you could accidentally rotate keys that should not be rotated by this key rotation schedule.

You can enter a key name in the **Name** field, or select any of the available filters from the drop-down lists. The Selected Keys table shows the keys that will be rotated by this schedule.

CipherTrust Manager displays the current list of keys that match this criteria in the **Selected Keys** table. Make sure you go through this list carefully so that you do not rotate keys you do not want to rotate.

For example, you can rotate all keys with "ldt" anywhere in their name by specifying `*ldt*` in the **Name** field:

Add Key Rotation Schedule

1 Select Schedule Type 2 General Info 3 Schedule Config 4 Key Rotation Query

A key rotation query is an object that specifies the keys that need to be rotated. All keys are rotated when it is not provided.

Name

Filters ☒ Basic ☐ Raw

Types Size Status Dates

☒ Latest Version Only

Name: *ldt* Version: latest

Selected Keys

Key Name	Ver	Modified	Type	Alg	Size
LDT-Key-West-Coast	2	08 Sep 2020, 10:10	Symmetric	AES	256
LDT-Key-East-Coast	3	08 Sep 2020, 10:10	Symmetric	AES	256
My_LDT_Key	0	08 Sep 2020, 10:07	Symmetric	AES	256

Back Save

If you only want to rotate the keys whose names begin with "ldt", use the query `ldt*` in the **Name** field. In the example above, that removes `My_LDT_Key` from the list of keys that will be rotated.

The search is case insensitive, so "ldt" will also match `LDT`, `ldT`, `ldT`, or any variation thereof.

When you are certain the list of keys to be rotated is accurate, click **Save**.

Checking the Rekey Status

During a rekey, you can check the progress in the CipherTrust Manager Console, however GuardPoint status is not relayed to the CipherTrust Manager in real time. A delay of several minutes before the CipherTrust Manager displays events on the client is likely. When the number of GuardPoints on the managed host is high, for example 100+, the delay in relaying GuardPoint status is due to delays in scheduling and the execution of CTE-LDT operations on the managed host for GuardPoints.

To see the progress of a rekey and the estimated completion time:

1. In the CipherTrust Manager Applications Page, open the **CTE** application.
2. Click **Clients** in the left-hand menu bar.
3. Click the **Client Name** of the client whose CTE-LDT status you want to check in the Clients table.

4. Find an active CTE-LDT GuardPoint and click **Active** in the **Status** column.

CipherTrust Manager displays the GuardPoint Health page, which includes transformation status information such as the basic status (Rekeyed or Rekeying), the last transformation completion time, the last transformation start time, and the estimated rekey completion time.

Obtaining Information About Keys Applied to Files

Key Report Option

In the following command, you can use the `report` option of the `voradmin` command to obtain information about all of the keys in use on the GuardPoint. The report lists all keys used in the GuardPoint. For each key, it gives the key name and key version number. It lists each unique key name and version combination only once, no matter how many files use the key.

The following example shows three keys used in the GuardPoint `/oxf-fs1/gp1`:

```
# voradmin ldt key report /oxf-fs1/gp1
LDT_KEY1,1
LDT_KEY2,2
LDT_KEY3,5
```

For an overview of `voradmin ldt`, see ["CTE-LDT Command-Line Administration: voradmin command" on page 71](#).

Key Map Option

In the `voradmin ldt key [report|map] <key_name> <guard_path>` command, you can use the `map` option to obtain information about which files in a GuardPoint were transformed with a specific key, where:

- `<key_name>` is the name of the key.
- `<guard_path>` is the path of the GuardPoint where the key was used.

For example, to view information about the key `LDT_KEY2` in the GuardPoint `/oxf-fs1/gp1`, you would enter:

```
# voradmin ldt key map LDT_KEY2 /oxf-fs1/gp1
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
```

Keys without a version number are used by files in an exclusion key rule or files that have yet to undergo initial key rotation. Use `voradmin ldt key map` in conjunction with `voradmin ldt attr get` to determine if a file using a key without a version number is part of an exclusion key rule or awaiting initial key rotation.

Showing GuardPoints During Rekey (Linux)

Use the following command to display a list of known CTE-LDT metadata stores and any associated GuardPoints currently undergoing transformation.

```
# voradmin ldt list all
MDS_1:  type=file, nguards=0, name=/disk2/::vorm:mds::
        Guard Table: version 1 nentries 0
MDS_2:  type=file, nguards=0, name=/disk3/::vorm:mds::
        Guard Table: version 1 nentries 0
MDS_3:  type=file, nguards=0, name=/disk4/::vorm:mds::
        Guard Table: version 1 nentries 0
```

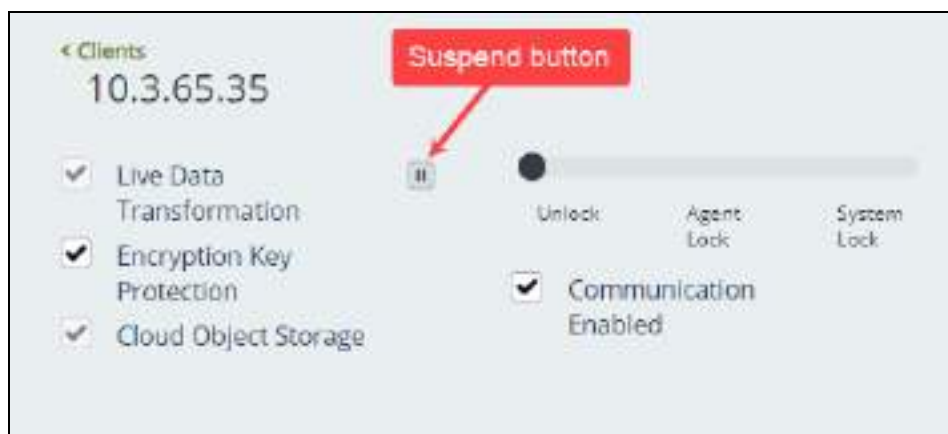

For an overview of `voradmin ldt` commands, see ["CTE-LDT Command-Line Administration: voradmin command" on page 71](#).

Suspending and Resuming Rekey and/or Scan Phase

The QoS schedule specifies certain time windows when CTE-LDT operations must be stopped temporarily. However, you can also suspend or resume CTE-LDT at the client level at any time.

To suspend CTE-LDT through the CipherTrust Manager Console:

1. Open the **CTE** application.
2. Click **Clients** in the left-hand menu bar.
3. Click the **Client Name** of the client on which you want to pause CTE-LDT in the Clients table.
4. In the Client Details area, click the **Suspend** button next to the Live Data Transformation field to suspend all CTE-LDT operations on the client.



After you pause CTE-LDT, the button turns into a Play button so that you can resume CTE-LDT operations when ready.

Considerations

- Disabling, or unguarding, an CTE-LDT GuardPoint where a rekey is in progress automatically suspends the CTE-LDT rekey operation.
- You can also use the `voradmin suspend/resume` command in Windows Powershell to suspend and resume the rekey. However, if you use the `voradmin ldt suspend` command to pause the rekey process, the CTE-LDT suspended state is not retained when the system reboots. If you want to retain the state after reboot, suspend the rekey from the CipherTrust Manager.
- On Linux, you can pause CTE-LDT during the scan phase of CTE-LDT. When paused during scan, CTE-LDT suspends operations that traverse through the namespace of GuardPoints in the scan phase of transformation. Suspending CTE-LDT during scan stops file lookup operations of CTE-LDT. This eliminates performance impact to I/O intensive production workloads, such as file serving type workloads, that access large number of files.

Automatic Suspend and Resume of CTE-LDT Operations Due to Insufficient Disk Space (Linux)

CTE-LDT requires adequate storage space headroom to perform CTE-LDT operations such as rekeying on GuardPoints. On Linux, if available storage space drops below the threshold required for CTE-LDT operations to continue, the CTE-LDT operations are automatically suspended. Once additional storage space is available in the file

system, CTE-LDT operations automatically resume.

As available space approaches the threshold for automatic suspension, CTE-LDT sends an alert to the CipherTrust Manager to notify you that you should free up more storage space before CTE-LDT operations are suspended. The alert on the CipherTrust Manager is:

Low space on guard point [GuardPoint], increase free space or CTE-LDT will be suspended.

Behavior of Automatic Suspend and Resume of CTE-LDT Operations on ext4 File Systems

By default, ext4 file systems reserve a portion of the storage space for use only by privileged processes to prevent running out of storage space in file systems. In this situation, non-privileged processes are automatically blocked from writing to the file system until the free disk space level reaches the minimum threshold. As CTE-LDT operates in privileged mode, CTE-LDT operations continue without blockage even if the free disk space threshold is low. Because of this ext4 feature, CTE-LDT operations on ext4 file systems may not be suspended due to low available storage space, even when the `df` command reports storage is 100% allocated.

Rotating Encryption Keys While a Rekey is in Progress (Relaunch)

On Linux, if a key is rotated (either manually or automatically when a key version expires) while CTE-LDT is in progress on a GuardPoint, the key rotation is processed and queued, and the GuardPoint is marked for relaunch. Relaunch indicates the need to restart CTE-LDT after the current transformation completes. If the GuardPoint has been rekeyed and is flagged for relaunch, CTE-LDT launches as soon as the GuardPoint is enabled.

Files already undergoing transformation at the time of the new key rotation complete rekey to the key version already in progress. Files that start transformation after the new key rotation request are rekeyed to the new key version. Once the current CTE-LDT of the GuardPoint is complete, CTE-LDT automatically relaunches to transform any files that are not rekeyed to the latest key version.

For example:

```
# voradmin ldt attr get /oxf-fs1/gp1
LDT stats: version=2, rekey_status=rekeying,relaunch
  Number of times rekeyed:          1 time
  Rekey start time:                 2020/03/18 16:54:00
  Last rekey completion time:       2020/03/18 16:53:38
  Estimated rekey completion time:  0 days 0 hours 6 minutes
  Policy key version:               344
  Data stats:
    total=9.8GB, rekeyed=0.0MB
    truncated=0.0MB, sparse=0.0MB
  File stats:
    total=1000, rekeyed=0, failed=0
    passed=0, skipped=0, created=0, removed=0, excluded=0
```

Note

Relaunch is supported on Linux only. It is not supported on Windows.

File System Operations

The following sections describe the file system operations that may require attention from the CipherTrust Manager Administrator.

Renaming Files and Folders

On both Linux and Windows hosts, you can rename files during initial transformation or rekey operations.

- On Linux, you cannot rename folders (directories) in a GuardPoint during a rekey operation. Any attempt to rename a directory is rejected with the error EAGAIN (try again) while CTE-LDT is in progress including the period during which transformation is suspended.
- On Windows, CTE-LDT stops if it is transforming the contents of a folder and a user attempts to rename/move that folder.

You can change the stopping behavior of CTE-LDT using the configuration parameter `oxf_stop_on_rename`.

Using the Registry Editor, or the Windows command line, add a registry entry in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Vmmgmt\Parameters` for `oxf_stop_on_rename`.

Registry Name	Values	Comments
<code>oxf_stop_on_rename</code>	0 - Disabled	CTE-LDT does not stop if there is contention.
	1 - Enabled	CTE-LDT stops if there is contention. Default: Enabled

For the target folder in rename operation, CTE-LDT is never stopped.

Deleting a File

When a file is removed before it is rekeyed, the file is not included in the total number of files transformed in the GuardPoint Health dialog box. Any discrepancy between total number of files to transform and those transformed is due to the removal of files from GuardPoints during CTE-LDT.

The `voradmin` command provides more detailed file level statistics related to rekey operations on the host. You can run `voradmin` to get file level statistics:

```
# voradmin ldt stats <guard_path>
```

File Handling (Windows Only)

It is critical that you understand how the CTE-LDT process handles read-only, binary (executable), NTFS encrypted and NTFS compressed files.

The CTE-LDT process is subjected to all of the File System policies and attributes set on the files. In some cases, this prevents CTE-LDT from encrypting a file. If users or applications are accessing files while CTE-LDT is in progress, CTE-LDT cannot change the attributes of the files and encrypt the file. It is critical that you understand how CTE-LDT handles various types of files:

- **NTFS Encryption and Compression**

If NTFS encryption and compression is enabled on a file or folder, the CTE-LDT process cannot encrypt these files. To maintain the data coherency, CTE-LDT skips the encryption of these files. These files display as “passthrough” files in the CTE-LDT statistics.

- **Read-Only Files**

When CTE-LDT encounters read-only files, it rekeys the file by resetting the read-only attribute and then setting the attributes back again when the rekey completes. If a file is open, CTE-LDT skips this file.

1. If the file is not opened, CTE-LDT changes the attributes of the file and stores the original attributes in the file metadata.
2. CTE-LDT starts Rekey on this file.
3. If a user requests to open a file for writing while rekey is in progress, access is denied. User can only open files for reading.
4. CTE-LDT restores the attributes once rekey is done.

- **Executable Files**

If an executable is running, or files are exclusively locked by the application, the CTE-LDT process cannot encrypt those files as it is unable to acquire the required locks on the files. CTE-LDT skips these files and changes to the INCOMPLETE state.

Enabling GuardPoints in Read-Only mounted file systems (Linux)

Access to a GuardPoint enabled in a read-only mounted file system is restricted to read operations. You cannot modify data in such file systems, therefore, you cannot perform CTE-LDT operations on GuardPoints in read-only file systems. For this reason, CTE-LDT automatically suspends operations when GuardPoints are enabled on read-only file systems. CTE-LDT ignores all attempts to resume CTE-LDT operations until the underlying file system is remounted with read/write access.



WARNING

You must disable a GuardPoint before changing the read/write mount options of the underlying file system. After changing the mount options, you can re-enable the GuardPoint. CTE-LDT operations adapt to the read/write options of the underlying file system when you enable the GuardPoint. Changing the mount options while a GuardPoint is enabled is unsupported and may result in unexpected errors.

Copying Files Into a GuardPoint

If you copy a file into a GuardPoint without an Apply Key rule, make sure that the file was previously copied from the same GuardPoint, or a GuardPoint protected with the same policy/versioned key. A copy operation, without an Apply Key rule, is the same as a backup or restore of a file from/to an CTE-LDT protected GuardPoint.

CTE enforces key rules of an CTE-LDT policy while a GuardPoint is enabled. CTE cannot enforce the key rules while a GuardPoint is disabled. Modifying or adding data/files inside a disabled GuardPoint is not only unsupported, but it also results in unrecoverable data corruption.



WARNING

Do not add new files or modify existing files inside CTE-LDT protected GuardPoints while the GuardPoint is not enabled. This results in unrecoverable data corruption and/or files that cannot be accessed when the GuardPoint is enabled.

Behavior of Hard Links Inside and Outside of GuardPoints (Windows)

When using hard links on Windows, all the hard links to a file must be within the boundary of a GuardPoint and must use the same key. The following scenarios provide additional details:

- If hard links to the same file are inside a GuardPoint and outside a GuardPoint, the effect on the file depends on what process accesses which hard link first. If the hard link within the GuardPoint is opened first, the file is transformed. If the hard link outside the GuardPoint is opened first, the file won't be transformed.
- If hard links to the same file exist in different GuardPoints with different keys, the file will be corrupted.
- If hard links to the same file exist in the same GuardPoint but with different keys, such as if folder-based rules are used, there will be a conflict in the key.

Excluding Files or Directories from Rekey

When you add a resource set to a key rule in a policy, you can select the **Exclude Rule** option. That tells CipherTrust Manager that the directories and/or files in the resource set should use a different key than the rest of the data in the CTE-LDT GuardPoint. If you specify `clear_key` for the key rule, then the directories and/or files in the resource set will be left unencrypted. Otherwise, you can select any non-versioned key to apply to those directories and/or files.

Examples of Exclusion Key Rules

This section describes some examples of how to use an exclusion key rule.

Encrypt Files With Exclusion Property a Non-Versioned Key

The following exclusion key rule applies the non-versioned key, `Key_TextFiles`, to any *new* files that are created with a `*.txt` extension.

Note

Existing `*.txt` files in the GuardPoint during the initial CTE-LDT data transformation process are assumed to be already encrypted with the same key that you specify in the exclusion key rule. These existing files are *not* transformed during the initial encryption or during any subsequent rekeys. The key you specify in the exclusion key rule is applied to new `*.txt` files only.

In the Policy, do the following:

1. Add a Key Rule.
2. In the **Resource Set** field, click **Select**.
3. Select a resource set that specifies *.txt in the **File** field and click the **Exclude Rule** option.



4. Click **Select**. CipherTrust Manager displays the resource set name in the Resource Set field with an icon indicating that this is an Exclusion Rule.
5. Select the `Key_TextFiles` key in the **Current Key Name** field.
6. Click **Add**.
7. Add any other key rules or exclusion key rules to the policy that you want. You must add at least one non-exclusion key rule that specifies the current encryption key and the versioned encryption key that you want to use with this Live Data Transformation policy.

For example, you could add another exclusion key rule that specifies all **.doc** files should be encrypted with the key `Key_DocFiles`, or one that specifies all **.zip** files should be left unencrypted by specifying the key `clear_key`.

Exempt Excluded Files from Encryption (Set to `clear_key`)

The following exclusion key rule sets all files in the resource set `/oxf-fs1/gp1/Clear_Files_Folder` (Linux) or `\oxf-fs1\gp1\Clear_Files_Folder` (Windows) to `clear_key` (in other words, not encrypted). Files in other directories that match other key rules in the same policy may be encrypted. This could allow unrestricted access to the files in `/oxf-fs1/gp1/Clear_Files_Folder` (Linux) or `\oxf-fs1\gp1\Clear_Files_Folder` (Windows) while access may be restricted to files in parallel directories.

- Linux Exclusion Key Rule: The Resource Set **Directory** field should contain `/oxf-fs1/gp1/Clear_Files_Folder`, and the **Key** should be `clear_key`.
- Windows Exclusion Key Rule: The Resource Set **Directory** field should contain `\oxf-fs1\gp1\Clear_Files_Folder`, and the **Key** should be `clear_key`.

Requirements for Exclusion Key Rules

Keep in mind the following requirements when configuring exclusion key rules:

- Before adding an exclusion key rule to an existing policy, you must disable all GuardPoints protected with the policy. Log on to the CipherTrust Manager to disable the GuardPoint.
- You cannot choose a versioned key for the key in an exclusion key rule. Only non-versioned keys or `clear_key` (no encryption) are valid for exclusion key rules.
- All exclusion key rules must be *above* all CTE-LDT transformation key rules in the **Key Rules** area in the policy.

Usage Notes and Limitations for Configuring Exclusion Key Rules

Keep in mind the information in the following sections when configuring an exclusion key rule.

Adding an Exclusion Key Rule to an Existing Policy with Versioned Keys (Linux)

When adding an exclusion key rule to an existing policy, the exclusion rule only applies to newly created files. Existing files that match the exclusion key rule remain encrypted with the same versioned key(s) specified in the non-exclusion key rule in the policy and will be rekeyed to the key in the exclusion key rule when the versioned key(s) rotates.

To force an existing file that matches an exclusion key rule to be transformed to the key in the exclusion key rule (non-versioned in this example), use one of the following methods:

- Rotate the versioned key specified in the policy to initiate rekey operations on the GuardPoint.
- Copy the existing file within the GuardPoint. The new file will be associated with the resource set in the exclusion key rule and will be encrypted with the non-versioned key. You can then delete the original file.

To perform a similar conversion on Windows, see ["Changing a Folder or Files from Versioned to Non-Versioned Key \(Windows\)" on page 52](#).

Adding an Exclusion Key Rule That is Part of an Active GuardPoint (Linux)

To edit and/or add an exclusion key rule to an CTE-LDT policy, all GuardPoints using the policy must first be disabled before the new key rule can be added.

Changing an Exclusion Key Rule That is Part of an Active GuardPoint (Windows)

Changes that you make to an exclusion key rule that is part of an existing policy in an active GuardPoint do not take effect until the GuardPoint that the exclusion key rule is part of is disabled and enabled again.

Conflicting Keys as the Result of Rename Operations

Do not attempt to move or rename a file encrypted with a versioned key to a name associated with an exclusion key rule with `clear_key`. If you attempt such a move or rename, the original file is unaffected but following error is output on Linux systems and a log entry is created:

```
<command name>: setting attribute 'user::secfs:xattr:' for 'user::secfs:xattr:': Invalid argument
<command name>: failed to close '<filename>': Invalid argument
```

No error is displayed on Windows systems. The target moved or renamed file is corrupted and should be deleted. The target file is also flagged with the `xattr_error` flag on Linux and `Rekey Status Excluded` on Windows. This flag prevents subsequent read/write access to the file. You can check the CTE-LDT attributes for the presence of this flag. See ["About the Exclusion Attribute for Files Matching an Exclusion Key Rule" on page 53](#).

Also, a log entry is sent to the CipherTrust Manager on Linux systems when this occurs. For example, if you moved the versioned file `/gp/foo.txt` into the GuardPoint `/gp/subdir/foo.txt` with an exclusion key rule that excludes matching files with the `clear_key`, the following log message would be created on the CipherTrust Manager:

```
[CGA] [WARN ] [29261] [CGS3268W] LDT-ALERT: encrypted data detected in filename [foo.txt] inode [35720037] in guard point [/gp] under clear exclusion key rule
```

Overlapping Exclusion Key Rules

Multiple exclusion key rules in the same policy may overlap each other. For example on Linux, if the non-versioned key `Key_A` is associated with resource `/oxf-fs1/gp1/Folder_Enc_With_KEY_A` and the non-versioned key `Key_B` is associated with resource `*.txt`, placement of the file `/oxf-fs1/gp1/Folder_Enc_With_KEY_A/foo.txt` overlaps the two key rules. In such a case, the first rule in the policy is enforced on `/oxf-fs1/gp1/Folder_Enc_With_KEY_A/foo.txt` when the file is created and in subsequent file access.

On Windows, if the non-versioned key `Key_A` is associated with resource `c:\oxf-fs1\gp1\Folder_Enc_With_KEY_A` and the non-versioned key `Key_B` is associated with resource `*.txt`, then they would overlap on the file `c:\oxf-fs1\gp1\Folder_Enc_With_KEY_A\foo.txt`. In such a case, the first rule in the policy is enforced on `c:\oxf-fs1\gp1\Folder_Enc_With_KEY_A\foo.txt` when the file is created and in subsequent file access.

Caution About Applications That Create Temporary Files (Windows)

Some applications on Windows create a temporary file version of the original file when you open and modify a file. This behavior can affect how you implement exclusion key rules.

If you have an exclusion key rule that uses a file extension to exclude files that may be opened and modified by such an application, exclude the temporary file name extension also. If you don't exclude the temporary file, the temporary file may be encrypted by another policy that matches the temporary file extension. Then the original file, which is copied from the temporary file, will be unreadable. Also keep in mind that other applications that may create temporary files with the same file extension and consider what policies should affect those temporary files.

This situation can happen with Microsoft Office files such as the `.docx` files used by Microsoft Word. When you open and modify a `.docx` file, Word creates a `.tmp` file version of that file. So for Microsoft Word you should add `*.tmp` to the exclusion key rule resource set if you add `*.docx`.

Rename Operations Crossing Key Rules (Linux)

On Linux, when a rename operation crosses key rules, the rename operation copies the source file to a new file using the new name and removes the original file. If the source file is flagged for exclusion key rule property, the target new file is disassociated with the exclusion key rule if the new name no longer matches the resource set associated with exclusion key rule. For more information, see ["About the Exclusion Attribute for Files Matching an Exclusion Key Rule" on page 53](#).

Using Linked Files with Exclusion Key Rules (Linux)

On Linux, do not create multiple hard links to the same target file such that the pathname of each hard link is associated with a resource set of an exclusion key and the key rules have different keys. Accessing the file through the pathname of each hard link results in a different key to be applied to the file resulting in data corruption in the target file due to application of multiple keys to the same data.

If you must create hard links, be sure the pathnames of hard links and the target file are within the same resource set.

Changing a Folder or Files from Versioned to Non-Versioned Key (Windows)

Exclusion key rules provide a way to convert a subset of guarded files or the contents of a folder from being encrypted by a versioned key to being encrypted by a non-versioned key. After this conversion, the excluded files or directory contents will be encrypted at the last version of the versioned key but the encryption keys for those items will not rotate to a new version when the keys for other non-excluded files are rotated. In other words, the excluded files or folder contents will be encrypted by a non-versioned key.

Follow these steps to change selected files or folder contents to a non-versioned key:

1. In the CipherTrust Manager, clone the versioned key that is used in the policy that you plan to edit. Cloning a key creates a non-versioned copy of the existing version of the versioned key.
2. In the CipherTrust Manager, disable the GuardPoint. Disabling the GuardPoint is required before modifying a policy applied in that GuardPoint.
3. Configure one or more resource sets to match the files that you want to exclude. For example, the resource set `star-dot-text` could contain `*.txt` and the resource set `sales-folder` could contain `\sales\*`.
4. Add one or more exclusion key rules to convert matching files to a non-versioned key. In the following example, files matching `*.txt` and files in the `sales` folder (as defined in resource sets) will be converted from the current version of the versioned key `AES256_versioned` to `AES256_clone`, assuming `AES256_clone` is a clone of `AES256_versioned`.

Order	Resource	Current Key	Transformation Key	Exclusion Rule
1	star-dot-txt	AES256_clone	AES256_clone	Y
2	sales-folder	AES256_clone	AES256_clone	Y
3		clear_key	AES256_versioned	N

Exclusion key rules must be ordered before other rules.

5. On the command line, run the following command to remove the CTE-LDT metadata from the files that you want to convert from versioned key to non-versioned key encryption:

```
voradmin ldt attr delete <path_to_files>
```

To recursively delete the CTE-LDT metadata from all files matching a pattern in all subfolders, use the following form, including `*` as a wildcard where needed:

```
voradmin ldt attr delete <path_to_files> -filter <filename>.<extension>
```

Note: Be careful when deleting the CTE-LDT metadata from files. If you delete the metadata from a file that does not match an exclusion key rule policy, the file will be unreadable after the next rekey.

Given the example exclusion key rule described in step 4, you would need to run this command on all files with the extension `.txt` (first example below) and on the files in `\sales` (second example below).

```
voradmin ldt attr delete c:\gp1 -filter *.txt  
voradmin ldt attr delete c:\gp1\sales
```

For more information about using `voradmin` on CTE-LDT metadata, run `voradmin ldt attr /?` on the command line.

6. In the CipherTrust Manager, re-enable the GuardPoint that includes the new exclusion key rule.
7. In the CipherTrust Manager, rotate the key for the policy that includes the new exclusion key rule.

Using the example exclusion key rule in step 4, after completing this procedure, files matching `*.txt` and files in the `sales` folder will have the exclusion attribute set and will be excluded from rekeying (see ["About the Exclusion Attribute for Files Matching an Exclusion Key Rule" on the next page](#)). Files not matching the exclusion key rule will be rekeyed to the next version of the `AES256_versioned` key.

To perform a similar conversion on Linux, see ["Adding an Exclusion Key Rule to an Existing Policy with Versioned Keys \(Linux\)" on page 50](#).

About the Exclusion Attribute for Files Matching an Exclusion Key Rule

Files matching an exclusion key rule have the status `rekey_excluded` in the CTE-LDT attribute. For more information about CTE-LDT attributes, see ["CTE-LDT Metadata in Extended Attributes" on page 57](#). To check for the exclusion attribute on a file, see ["Determining if a File is Included in an Exclusion Key Rule" below](#).

The Exclusion Attribute is Persistent

Exclusion from rekey is a persistent property. A file excluded from rekey is not rekeyed regardless of changes that may seem to disassociate the file from the exclusion key rule. For example, if you rename a file to a new name within the same GuardPoint that no longer matches the exclusion key rule that the original name matched, the file with the new name retains the encryption type (non-versioned key or `clear_key`) of the exclusion key rule. To remove the exclusion attribute from a file you must copy the file rather than move or rename it (see ["Removing the Exclusion Attribute From a File" below](#)).

Determining if a File is Included in an Exclusion Key Rule

Use the `voradmin ldt attr get <path to file>` command to check whether a file is associated with an exclusion key rule.

- On Linux, an excluded file will include the status `rekey_excluded` in the `voradmin` output. For example:

```
# voradmin ldt attr get /oxf-fs1/gp1/foo.txt
CTE-LDT attributes: rekeyed_size=0, rekey_status=rekey_excluded
```

- On Windows, an excluded file will include the attribute `Rekey Status Excluded` in the `voradmin` output. For example:

```
C:\> voradmin ldt attr get c:\gp1\foo.txt
CTE-LDT attributes:
Rekey Status Excluded
Initial Rekeyed Size 9 Bytes
Data Transformed 0 Bytes

Key:
Current Key Name/Version (Clear_Key)
New Key Name/Version (Clear_Key)
```

Removing the Exclusion Attribute From a File

To disassociate a file from an exclusion key rule, you must copy the file to a new file not associated with the resource set of the same or another exclusion key rule as the source file. You can then remove the original file. The new file is created under the default key rule of whatever policy applies to the new file. Moving or renaming a file does not disassociate a file from an exclusion key rule (see ["The Exclusion Attribute is Persistent" above](#)).

For example, assume the following exclusion key rule where `Key_TextFiles` is a non-versioned key:

Exclusion Key Rule: Resource set = *.txt, Key = `Key_TextFiles`

If you copy the file `test1.txt` to `test1.foo`, `test1.foo` is created with whatever key is specified in the policy that matches the new file. The key for the new file could be a non-versioned key, versioned key, `clear_key`, or, no key at all if the new file is outside of a GuardPoint. The original file `test1.txt` remains unchanged and encrypted with the `Key_TextFiles` non-versioned key because the file remains in the exclusion key rule.

Rename and Restore Operations (Linux)

The effect of rename or backup/restore operations involving files associated or not associated with exclusion key rules is mixed and somewhat confusing. In some cases, the operations to restore or rename cause conflicts between the key associated with the source file and the key associated with the target file. For example, the result of a rename operation involving a source file not associated with an exclusion key rule and target file name associated with a resource set of an exclusion key rule is different from the result of the same operation when target file name is associated with the resource set of an exclusion key rule with clear_key.

Note

Be sure to review the effect of the operations below and avoid administrative operations that cross associations of files across multiple resource sets with conflicting key rules.

Backup/Restore

The table below illustrates the status and the key effect of restore operations involving mixed keys associated with source files from backup image and existing target files inside GuardPoint.

Key Applied to File in Backup	Key Applied to existing file in GuardPoint	Key Effect of Restore Operation on Existing file
Versioned	Versioned	Versioned
Versioned	Exclusion key	xattr_error (failed)
Versioned	Exclusion clear key	xattr_error (failed)
Exclusion key	Versioned	Exclusion key
Exclusion key	Exclusion key	Exclusion key
Exclusion key	Exclusion clear key	xattr_error (failed)
Exclusion clear key	Versioned	Exclusion clear key
Exclusion clear key	Exclusion key	xattr_error (failed)
Exclusion clear key	Exclusion clear key	Exclusion clear key

The table below illustrates the status and the key effect of restore operations involving mixed keys associated with source files from backup image and new target files not present inside GuardPoint.

Key Applied to File in Backup	Key Applied to existing file in GuardPoint	Key Effect of Restore Operation on Existing file
Versioned	Versioned	Versioned
Versioned	Exclusion key	xattr_error (failed)
Versioned	Exclusion clear key	xattr_error (failed)
Exclusion key	Versioned	Exclusion key
Exclusion key	Exclusion key	Exclusion key
Exclusion key	Exclusion clear key	xattr_error (failed)
Exclusion clear key	Versioned	Exclusion clear key

Key Applied to File in Backup	Key Applied to existing file in GuardPoint	Key Effect of Restore Operation on Existing file
Exclusion clear key	Exclusion key	xattr_error (failed)
Exclusion clear key	Exclusion clear key	Exclusion clear key

Rename Operation

The table below illustrates the status and the key effect of rename operations for different combinations of versioned, exclusion key, and exclusion clear key.

Key Applied to File in Backup	Key Applied to existing file in GuardPoint	Key Effect of Restore Operation on Existing file
Versioned	Versioned	Versioned
Versioned	Exclusion key	Exclusion key
Versioned	Exclusion clear key	xattr_error (failed)
Exclusion key	Versioned	Exclusion key
Exclusion key	Exclusion key	Exclusion key
Exclusion key	Exclusion clear key	Exclusion key
Exclusion clear key	Versioned	Exclusion clear key
Exclusion clear key	Exclusion key	Exclusion clear key
Exclusion clear key	Exclusion clear key	Exclusion clear key

Listing All Files Included in an Exclusion Key Rule (Linux)

Determining the files that match an exclusion key rule involves two steps. You list all the keys in a GuardPoint, choose the key that you're interested in, and then run a command to list the files that match that key. This process works for both standard key rules and exclusion key rules.

1. Decide on the GuardPoint that you want to check for excluded files. For example, for the GuardPoint `/oxf-fs1/gp1`, type the following on the command line:

```
# voradmin ldt key report /oxf-fs1/gp1
LDT_KEY1,1
LDT_KEY2,2
LDT_KEY3,5
NON_VERSIONED_KEY
```

The number after the comma is the key version number. See ["Key Report Option" on page 43](#) for more information about the `voradmin` key report.

2. From the key report output, choose the key rule for which you want to list matching files. For example, to see the files associated with the NON_VERSIONED_KEY in the previous step, you would type:

```
# voradmin ldt key map NON_VERSIONED_KEY /oxf-fs1/gp1
/oxf-fs1/gp1/file1.dat10
/oxf-fs1/gp1/file2.dat10
/oxf-fs1/gp1/file3.dat10
/oxf-fs1/gp1/file4.dat10
/oxf-fs1/gp1/file5.dat10
```

See ["Key Map Option" on page 43](#) for more information about the `voradmin` key map report.

Listing All Files Included in an Exclusion Key Rule (Windows)

Determining the files that match an exclusion key rule involves two steps. You list all the keys in a GuardPoint, choose the key that you're interested in, and then run a command to list the files that match that key. This process works for both standard key rules and exclusion key rules.

1. Decide on the GuardPoint that you want to check for excluded files. For example, for the GuardPoint `c:\gp1`, type the following on the command line:

```
C:\> voradmin ldt key report c:\gp1
Keys used for GP, c:\gp1 :
clear_key,0
CS1-CTE-LDT-AES256,11
```

The number after the comma is the key version number. The `clear_key` key is not versioned, so the version number is 0.

2. From the key report output, choose the key rule for which you want to list matching files. For example, to show the files associated with the `clear_key` listed above, you would type:

```
C:\> voradmin ldt key map c:\gp1 clear_key,0
Files rekey with key (clear_key,0)-
c:\gp1\file1.txt
c:\gp1\file2.txt
c:\gp1\file3.txt
c:\gp1\file4.txt
c:\gp1\file5.txt
```

Using CTE-LDT with SAP HANA Fibre Channel Systems (Linux Only)

You must add additional CTE commands to the HANA administrator entry. To do so, edit the `/etc/sudoers` with a text editor and add entries for `/usr/bin/voradmin` and `/usr/bin/vmsec`. For example:

```
# hanadm ALL=NOPASSWD:
/usr/bin/secfsd,/usr/bin/voradmin,/usr/bin/vmsec,/sbin/multipath,/sbin/multipathd,/etc/init.d/m
ultipathd,/usr/bin/sq_
persist,/bin/mount,/bin/umount,/bin/kill,/usr/bin/lsof,/sbin/vgchange,/sbin/vgscan
```

If you are using an ext3 file system, you must mount it with extended attributes. To do so, edit the storage section of the `global.ini` file using a text editor and add the following lines:

```
partition_*_data__mountOptions = -o user_xattr
partition_*_log__mountOptions = -o user_xattr
```

Note

See the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide* for more information about SAP HANA.

Chapter 5: CTE-LDT Administration

This chapter contains the following sections:

CTE-LDT Metadata in Extended Attributes	57
DFSR and Replication (Windows)	61
Multi-Node Configuration and Operation	62
Backing Up and Restoring CTE-LDT GuardPoints	62
CTE-LDT Command-Line Administration: voradmin command	71
Moving a CTE-LDT GuardPoint from One CTE-LDT Policy to Another	72
Removing CTE-LDT and Security Encryption	73
Uninstalling the Agent while CTE-LDT is Rekeying GuardPoints	77

CTE-LDT Metadata in Extended Attributes

An *extended attribute* is a name/value pair permanently associated with a file or directory stored in a file system. CipherTrust Transparent Encryption (CTE) creates and maintains its own user extended attributes on CTE-LDT GuardPoint directories and files. The extended attributes are used to store metadata related to each file or directory that is protected using an CTE-LDT policy.

On Linux, CTE-LDT sets extended attributes on GuardPoint directories. The CTE-LDT attribute of an CTE-LDT GuardPoint stores the following metadata:

- Current key version.
- Rekey status.
- Rekey start and end times.
- Estimated completion time.
- Total amount of data transformed.
- Total number of files transformed.
- Current key signature and applied key signature.

On both Linux and Windows, CTE-LDT sets extended attributes on files. The CTE-LDT attribute of a file stores the following metadata:

- Name of the current key.
- Name of the versioned key.
Also referred to in the CipherTrust Manager Console and product documentation as the new key or the transformation key.
- Version number of the versioned key.
- CTE-LDT rekey status of the file.

In most cases, the current and new key names are the same. The exception is during initial transformation from a legacy policy to an CTE-LDT policy, when the file has been encrypted with the current key and is being transformed to the current version of the transformation key.

Note

Before you set up a GuardPoint for CTE-LDT, ensure that there is sufficient disk space available in your file system for CTE-LDT metadata. The amount of disk space you need depends on the number of files in your GuardPoint. For more information about the disk space requirement, see ["Planning for CTE-LDT Attribute Storage" on page 60](#).

The state of a file changes during CTE-LDT operations. The extended attributes are continually updated to reflect the current file status, which falls into one of the following categories:

- Rekeyed to the current version of the key.
- Rekeyed to the previous version of the key, or the initial key state (before the first CTE-LDT rekey has been performed).
- Partially rekeyed, where some regions of the file are rekeyed to the new key version and other regions are still keyed to the previous key version or the initial key.

Listing Extended Attributes

You can list extended attributes by using native operating system commands, or system calls. As part of GuardPoint administration, CTE can modify or delete extended attributes.

In Linux, CTE-LDT attributes are set on GuardPoint directories and regular files in GuardPoint directories protected with CTE-LDT policies. The CTE extended attribute name is `::secfs:xattr:.`

The following example uses the native Linux operating system command `attr` to display the CTE-LDT attribute for the GuardPoint `/oxf-fs1/gp1` and the file `/oxf-fs1/gp1/File_1.txt`.

Example 1:

```
# attr -l /oxf-fs1/gp1/File_1.txt
Attribute "::secfs:xattr:" has a 1044 byte value for /oxf-fs1/gp1/File_1.txt
Attribute "selinux" has a 37 byte value for /oxf-fs1/gp1/File_1.txt
```

Example 2:

```
# attr -l /oxf-fs1/gp1
Attribute "::secfs:xattr:" has a 1044 byte value for /oxf-fs1/gp1
Attribute "selinux" has a 37 byte value for /oxf-fs1/gp1
```

Example 3:

In the following example, the file `/oxf-fs1/gp1/File_1.txt` has the same name for current and new keys at the same key version. In the following example, if the versioned key `LDT_KEY` is at version 755, the file is rekeyed to the latest key version under the CTE-LDT policy.

```
# voradmin ldt attr get /oxf-fs1/gp1/File_1.txt
CTE-LDT attributes: rekeyed_size=4096, rekey_status=none
Key:    name=LDT_KEY, version=755
```

Example 4: (Linux)

The following is example of an CTE-LDT attribute on a GuardPoint directory on Linux:

```
# voradmin ldt attr get /oxf-fs1/gp1
LDT stats: version=1, rekey_status=rekeying
  Number of times rekeyed:      3 times
  Rekey start time:             2018/08/04 16:24:45
  Last rekey completion time:   2018/07/04 16:24:04
  Estimated rekey completion time: N/A
  Policy key version:           2043
```

```
Data stats:
    total=3.3GB, rekeyed=1.5GB, truncated=0.0MB
File stats:
    total=4307, rekeyed=1181,
    passed=2, skipped=0, created=0, removed=0
```

Example 5: (Windows)

The attribute for the GuardPoint `c:\GP 1` contains the status (rekeyed) and statistics specific to the GuardPoint and CTE-LDT. Following is sample output of `voradmin` command on Windows for statistics on a file:

```
C:\> voradmin ldt attr get c:\GP\Test.txt
LDT attributes:
    Rekey Status          Rekeyed
    Initial Rekeyed Size  10 Bytes
Key:
    Key Name/Version      (LDT_KEY, 28)
```

The attribute for GuardPoint `C:\GP` contains the status (rekeyed) and statistics specific to the GuardPoint and CTE-LDT:

```
C:\> voradmin ldt attr get c:\gp\
LDT Stats
-----
    Rekey Status          LDT_ST_REKEYED
    Last rekey completion time    10/2/2017 4:26:50
    Rekey Start time            10/2/2017 4:26:17
    Estimated rekey completion time    000:00:00

File Stats:
    Total      444
    Rekeyed    444
    Skipped    0
    Errored    0
    Passed     0
    Removed    0

Data Stats:
    Total      11 GB (12649143417 Bytes)
    Rekeyed    11 GB (12649143417 Bytes)
    Truncated  0 Bytes
```

MDS File (Linux)

In addition to CTE-LDT attributes, the CTE-LDT process on Linux requires persistent storage for additional metadata related to encrypting, or rekeying, files in GuardPoints. CTE-LDT allocates the storage space as soon as the CTE-LDT process starts on a GuardPoint. It maintains this storage space during the entire transformation process, until the GuardPoint is completely transformed.

Storage for this metadata is allocated and managed in a special file, called the MDS (metadata store) file. The MDS file resides inside a GuardPoint directory so each GuardPoint has its own MDS file.

The MDS file is a CTE protected file with the name `::vorm:mds::`. For example:

```
# ls -l /oxf-fs1/gp1/::vorm:mds::
-rwxr-xr-x. 1 root  root 31754474496 Dec  8 09:09 /oxf-fs1/::vorm:mds::
# du -B 1024 /oxf-fs1/gp1/::vorm:mds::
25056    /oxf-fs1/::vorm:mds::
```


As shown above, the MDS file is sparse. In the example, the file size is approximately 30GB, however the file is allocated with approximately 25MB of disk storage. CTE-LDT automatically creates the MDS file the first time the CTE-LDT process starts on any GuardPoint in the file system namespace. It populates the MDS file with all of the metadata for the GuardPoint at the beginning of the CTE-LDT process. Disk space allocated to the MDS file is freed and the MDS file in the GuardPoint directory is removed when the CTE-LDT process completes on the GuardPoint.



WARNING

The MDS file is protected. You cannot remove it unless the administrator runs the `voradmin` command to manually remove the MDS file once it is no longer needed. See ["Deleting CTE-LDT Metadata \(Linux\)" on page 76](#) for more information.

CTE-LDT automatically allocates and deallocates disk space for the MDS file as part of the CTE-LDT process. Deallocation of disk space for a GuardPoint does not change the MDS file size, although it frees the disk blocks. MDS files are sparse and very large in size. With no GuardPoint undergoing CTE-LDT, the minimum allocation of an MDS file is approximately 25MB.

Planning for CTE-LDT Attribute Storage

Before a GuardPoint is enabled for CTE-LDT, make sure that there is sufficient free disk space in the file system to which the GuardPoint belongs. Free space is required for CTE-LDT attributes (CTE extended attributes) and (in Linux) metadata in the MDS file. CTE-LDT attributes are created during initial encryption and are never freed until the GuardPoint is permanently unguarded and removed from the protection of an CTE-LDT policy. In contrast, disk space for metadata in the MDS file is temporary, kept only during the live transformation process.

When planning how much free disk space to reserve for CTE-LDT on a GuardPoint, consider the following:

- Number of files in the GuardPoint
- (Linux) Average length of absolute pathnames of files in the GuardPoint

The CTE-LDT process pre-allocates disk space for the Linux MDS file based on a minimum of 200K files with an average pathname of 1024 bytes per GuardPoint. The minimum space amounts to 325MB of disk space for the MDS file for each GuardPoint, even if file count is very low. (In Windows, CTE-LDT reserves the space when the file is rekeyed.)

Using `voradmin` To Estimate Disk Space Required for CTE-LDT (Linux)

In Linux, you can use the `voradmin ldt space` command to estimate the amount of disk space required for CTE-LDT attributes and the MDS file. The result is rounded to the nearest MB. The syntax of the command is:

```
# voradmin ldt space <guard path>
```

The following example shows how to estimate the required disk space to perform CipherTrust Transparent Encryption - Live Data Transformation on 1501 files in the GuardPoint `/oxf-fs1/gp1`. Estimate the disk space before protecting `/oxf-fs1/gp1` using an CTE-LDT policy. For example:

```
# voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 1501 files without CTE-LDT extended attributes
CTE-LDT disk space requirements: total 169MB (CTE-LDT attributes=6MB, MDS=163MB)
```

The `voradmin` command reports that 1501 files in `/oxf-fs1/gp1` without CTE-LDT attributes. These files are new to CTE-LDT. 6MB of space is required for the CTE-LDT extended attributes and 163MB for metadata in the MDS file.

The following example shows the output of the same command after encryption completes. This estimates the additional disk space needed for the next CTE-LDT rekey operation. For example:

```
# voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 0 files without CTE-LDT extended attributes
CTE-LDT disk space requirements: total 163MB (CTE-LDT attributes=0MB, MDS=163MB)
```

The voradmin command still reports on the same 1501 files, but because encryption has occurred using CTE-LDT, the files all have their CTE-LDT attributes. No additional space is required for CTE-LDT extended attributes on the next run. However, since the MDS file is transient and deletes after it finishes encrypting the GuardPoint, it requires additional space for the next key rotation.

Note

Windows estimates space using the following equations:

- Permanent Space = Number of Files * 4K
- Temporary Space = 128K * (Number of CPU * 2)

Displaying Metadata

Use the following command to see CTE-LDT file attributes or GuardPoint attributes:

```
# voradmin ldt attr get [<file name path> | <guard path>]
```

For an overview of voradmin ldt, see ["CTE-LDT Command-Line Administration: voradmin command" on page 71](#).

Verifying Metadata (Windows only)

Use the following command to verify if the metadata is corrupt:

```
# voradmin ldt attr verify [<file name path> | <guard path>]
```

For an overview of voradmin ldt, see ["CTE-LDT Command-Line Administration: voradmin command" on page 71](#).

DFSR and Replication (Windows)

The Distributed File System Replication (DFSR) service is a multi-master replication engine used to maintain synchronized folders on multiple servers. Replicating data to multiple servers increases data availability and provides users in remote sites with fast, reliable access to files.

If you are creating GuardPoints in a DFSR environment, you must first add the DFSR private folder guard path to the exclusion list in the Windows Registry. CTE-LDT should not attempt data transformation on this read-only directory.

1. Using the Registry Editor, or the Windows command line, add a registry entry in: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Vmmgmt\Parameters` named "LDTEExclusionGPList" of type REG_MULTI_SZ.
2. Add the `DfsrPrivate` directory path to the `LDTEExclusionGPList`.
For example, if the DFSR private directory path is `D:\data\DfsrPrivate`, add this string in `LDTEExclusionGPList`.
3. Reboot the system to make the change take effect.

Note

CTE-LDT does not perform a rekey on the DFSR private directory. Its rekey status is always "N/A".

If an application, or user, is performing a rename or a delete folder operation inside a GuardPoint with an CTE-LDT policy, this may restart the rekey process. Files which are already rekeyed will not be rekeyed again.

- If a rename or a delete operation is already performed on rekeyed files/folder, then the rekey process does not restart.
- If a rename or delete operation is performed in a folder where a rekey is in progress, CTE-LDT needs to stop the rekey process and restart the rekey again.

Multi-Node Configuration and Operation

This section describes what to expect at runtime when CTE-LDT operates in a multi-node cluster environment.

CTE-LDT Behavior on Failover

In a multi-node cluster, CTE-LDT runs in active-passive mode. A GuardPoint is only enabled on the active node, and CTE-LDT only runs on the active node. On the CipherTrust Manager Console, you can only view statistics for the active host.

If the active host fails over, and the standby host takes control, CTE-LDT also fails over to the second host. On the CipherTrust Manager Console, CTE-LDT statistics now appear on the other host.

Veritas Cluster Server

In an HA environment with Veritas Cluster Server, manual failover of service to a stand-by host may require manual intervention. If any GuardPoint is in the scan phase at the time of the manual failover, the failover process fails with the error "UNABLE to OFFLINE". The reason for the failure may be the scan state of a GuardPoint that cannot be suspended. CTE-LDT suspends CTE-LDT operations during the rekey state of transformation. Because CTE-LDT scan operations cannot be suspended, the Veritas Cluster Server fails to suspend CTE-LDT on GuardPoints in the scan phase of CTE-LDT operation. This state of CTE-LDT operation prevents Veritas Cluster Server to manually offline the service for fail-over.

Backing Up and Restoring CTE-LDT GuardPoints

This section describes procedures and considerations related to backing up and restoring data in CTE-LDT GuardPoints.

In addition to the files in a GuardPoint, CTE-LDT stores metadata in extended file attributes. These CTE-LDT attributes contain information that is required for decrypting the files and for the proper operation of CTE-LDT. Therefore, it is critical that your backup application also backs up the extended attributes of the files along with file data.

Clear Text Backup and Restore

A policy that applies a Security Rule with the Apply Key effect on backup/restore operations does not require any special rules for data access by backup applications. Under such a policy, backup applications always read clear data and store clear data in backup media. The backup application is not required to back up the CTE-LDT extended attributes, and a QoS schedule is not required to suspend CTE-LDT during backups.

Encrypted Backup and Restore

When a policy does not enforce a Security Rule with the Apply Key effect on backup/restore operations, the policy does not decrypt data on I/O operations from that backup application. Under such a policy, the backup application stores encrypted data and the CTE-LDT extended attributes of the file on the backup media.

In Linux, CTE-LDT operations must be suspended during backup. Suspending CTE-LDT completes the ongoing rekey operations on regions of files before starting the backup. During live transformation, CTE-LDT first preserves those regions of a file to be rekeyed in the MDS file. Then it updates some of the metadata in order to update the status of the data preserved in the MDS file in preparation for the rekey. Then it starts rekeying and updating those regions in the underlying file.

Suspending CTE-LDT waits for ongoing rekey operations to complete, and saves the metadata in the CTE-LDT extended attribute section of the MDS file. Suspending CTE-LDT ensures that the rekey status stored in the CTE-LDT extended attribute accurately reflects the rekey status of the data in the entire file during backup.

Note

This requirement does not apply to CTE-LDT for Windows.

The following table summarizes the state of the data in files in backup media:

CTE-LDT State of File	Security Policy	Backup Metadata or Alternate Data Streams Along with File data	Effect
Not rekeyed	Permit	Yes	Data in backup may be in clear format or encrypted with older key version.
Rekey in progress	Permit	Yes	File in backup storage is partially rekeyed. Some parts are in clear format or encrypted with older key version, and other parts are encrypted with current key version.
Rekey complete	Permit	Yes	File in backup storage is in the encrypted format with new key version.

CTE-LDT Policy for Encrypted Backup and Restore

Suppose you have an CTE-LDT policy allowing a backup user, or a backup process, to perform an encrypted backup. The backup user, or the backup process, reads encrypted data from files and stores the same encrypted data in backup media.

For example, suppose you wanted to back up GuardPoint `/oxf-fs1/gp1` protected by `My_LDT_Policy_1`. The key version before the key rotation is 8. The following steps occur:

1. Key version 8 expires and is rotated to version 9.
2. Rotating the encryption key triggers CTE-LDT to start running on the data under the GuardPoint.
3. The QoS schedule suspends CTE-LDT because a backup process is running.
4. The backup process begins, runs and later ends.
5. The QoS schedule resumes CTE-LDT.
6. CTE-LDT on the GuardPoint completes.

Note

Although the backup/restore scenarios and examples described in the rest of this section are specific to CTE-LDT on Linux platform, the concepts also apply to CTE-LDT on the Windows platform.

Consider the state of the three files in the GuardPoint during the CTE-LDT process, right after CTE-LDT is suspended in preparation for the backup. You can obtain the state of each file through the `voradmin ldt attr get` command, which examines the CTE-LDT state of each file captured in the CTE-LDT extended attributes of those files. (For an overview of `voradmin CTE-LDT`, see ["CTE-LDT Command-Line Administration: voradmin command" on page 71](#)).

- **File_1.dat** is rekeyed/encrypted to completion. The applied and new key versions are at version 9 of the key.

```
# voradmin ldt attr get /oxf-fs1/gp1/data_files/file_1.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9
```

- **File_2.dat** is partially rekeyed/encrypted. The applied key version is at version 8 and the transformation key is at version 9.

```
# voradmin ldt attr get /oxf-fs1/gp1/data_files/file_2.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=rekeying,state_saved
Current Key:      name=LDT_AES256_KEY, version=8
New Key:          name=LDT_AES256_KEY, version=9
```

- **File_3.dat** has not been rekeyed/encrypted. The applied key and transformation key are both at version 8, which is the version before the current key rotation.

```
# voradmin ldt attr get /oxf-fs1/gp1/data_files/file_3.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=8
```

While CTE-LDT is suspended on the GuardPoint, the backup process starts and archives these three files, including extended attributes, in the backup media.

```
# my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_1.dat \
    /backup-media/oxf-fs1/gp1/data_files/file_1.dat
# my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_2.dat \
    /backup-media/oxf-fs1/gp1/data_files/file_2.dat
# my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_3.dat \
    /backup-media/oxf-fs1/gp1/data_files/file_3.dat
```

Notes

- On Linux platforms, you must perform backups on a GuardPoint during periods when CTE-LDT is not actively transforming data in the GuardPoint. You must schedule backups in conjunction with CTE-LDT schedules or during periods when CTE-LDT is paused. Make sure to coordinate with the backup administrator and schedule accordingly.
- If the preferred method of backup is to create device level snapshots of the file system on the managed host or in the storage array subsystem, you must ensure that the schedule for creating snapshots pauses CTE-LDT before a snapshot is created.

Backup/Restore of Metadata Store File (MDS) in GuardPoints Undergoing Rekey

Backing up an entire GuardPoint using commands such as `cp`, `tar`, or `rsync`, or even commercial backup products that sweep the file system namespace for backing up files is supported. This method of backup performed while live transformation is in progress over GuardPoint poses some challenges when files in GuardPoint are backed up in encrypted format. The challenge with this method of backup is existence of the CTE-LDT Metadata Store file (MDS) in GuardPoint during backup or restore process and strict protection enforced on MDS files preventing deletion or modification to MDS files. Second, your backup utility must backup and restore extended attributes of files, and because CTE-LDT extended attributes are also protected similar to MDS files, your backup must be enabled to restore extended attribute of files. To overcome both restrictions, your policy on GuardPoint must include a security rule without Apply Key Effect to enable your backup utility to replace MDS file and CTE-LDT extended attribute of files as

part of backup/restore operations. Additionally, your backup utility must be signed with a signature set from the CipherTrust Manager for added security, and be executed with the option to preserve extended attribute options available with the standard Linux utilities.

The following table lists the supported backup utilities, required options to preserve extended attributes, and supported versions of the utilities.

Command	Required options	Supported version
cp	--preserve=all	OS default
tar	--xattrs	OS default
rsync	-vapIXWP --inplace	OS default
netbackup	overwrite existing files	v7.6.1 and v7.7.3

You can also backup and restore GuardPoint data, including the MDS file, if the requirements listed above on the backup utility are satisfied. GuardPoints associated with an MDS file located outside of GuardPoint namespace cannot be backed up or restore using this method of backup.

Note

You must suspend CTE-LDT on GuardPoint before performing backup or restore.

You can check your GuardPoint to determine if you can use this method of backup. If the directory of your GuardPoint is a mount point, MDS files reside inside your GuardPoint and this method of backup can be used for backing up or restoring your GuardPoint. However, GuardPoint directories below file system mount points must be checked and verified to use this method of backup. To verify, you can run the `voradmin` command to determine the MDS file associated your GuardPoint.

For example:

```
# voradmin ldt list all
MDS_1:  type=file, nguards=1, name=/oxf-fs1/gp1/:vorm:mds::

Guard Table: version 1 nentries 1
Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/oxf-fs1/gp1
File List: count 4308
```

The report on `/oxf-fs1/gp1` GuardPoint indicates association of the MDS file `/oxf-fs1/gp1/:vorm:mds::` with the GuardPoint. As the MDS file resides inside the GuardPoint directory, you can use this method of backup to backup and restore this GuardPoint.

Before restoring the GuardPoint, you must suspend CTE-LDT operations on the GuardPoint if live transformation is in progress. Failure to do so will fail to restore the MDS file in the backup image. Failure to restore MDS file affects partially rekeyed files restored to the GuardPoint. In such a situation the restored data is invalid, and you must remove all the files restored to the GuardPoint and repeat the restore operation after suspending CTE-LDT.

Restoring a GuardPoint from a Backup

To properly restore GuardPoint along with the MDS file, the following steps must be done in order:

1. Verify if live transformation is in progress on the GuardPoint and suspend the CTE-LDT operations. (Skip this step if no live transformation is occurring.)
2. With the same tool that was used for backup, restore to the GuardPoint.

3. Once restore is complete, GuardPoint needs to be disabled and enabled again. Run the `voradmin` command as shown below to determine how the GuardPoint was suspended at the time of backup. For manual GuardPoint, run the `secfsd` command as shown below. For auto-guards, disable and enable GuardPoints on CipherTrust Manager.

```
# secfsd -unguard <GuardPoint>
# secfsd -guard <GuardPoint>
```

4. Since GuardPoint was in suspended state during the time of backup, it will be restored in suspended state. You must resume CTE-LDT to complete CTE-LDT on the restored GuardPoint. You must resume CTE-LDT on the CipherTrust Manager if CTE-LDT was suspended on the CipherTrust Manager at the time of backup, otherwise you will resume CTE-LDT using `voradmin` command.

Run the `voradmin` command below to determine if CTE-LDT must be resumed on CipherTrust Manager or through `voradmin`. If the tag string next to SUSPENDED state of GuardPoint is `vadm`, run `voradmin` command to resume CTE-LDT, otherwise the tag value is `qos` and CTE-LDT must be resumed on CipherTrust Manager. In the example below, GuardPoint `/oxf-fs1/gp1` was suspended using `voradmin`, and it must be resumed after restore using `voradmin` command.

```
# voradmin ldt list all
MDS_1: type=file, nguards=1, name=/oxf-fs1/gp1::vorm:mds::
Guard Table: version 1 nentries 1
Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/oxf-fs1/gp1
File List: count 4308
# voradmin ldt resume /oxf-fs1/gp1
```

5. Wait for CTE-LDT completion on GuardPoint.
6. We strongly recommend that you disable and re-enable the GuardPoint once more.

The restore is now complete and files in your GuardPoint can be accessed.

The CTE Agent sends the following alert message to CipherTrust Manager if the restore operation is rejected:

```
LDT-ALERT: Restore of LDT protected file <GuardPoint> not allowed by policy
```

Potential Warnings During Restore Operation

When using `cp` for backup/restore, the `cp` command may report a failed attempt to preserve permissions on the Metadata Store File (MDS) during a restore. If you encounter the below message, continue to proceed with the restore steps since this will not affect the MDS file or dataset that is being restored.

```
cp: preserving permissions for '/oxf-fs1/gp1::vorm:mds::': Permission denied
```

When using `rsync` for backup/restore, the `rsync` command may report a failed attempt to set extended attribute when restoring the MDS file on system with selinux configured in enforced mode. If user encounters the below message, continue to proceed with the restore steps since this will not affect the MDS file or dataset that is being restored.

```
rsync: copy_xattrs: lsetxattr("/oxf-fs1/gp1::vorm:mds::", "security.selinux") failed:
Permission denied (13)
rsync: rsync_xal_set: lsetxattr("/oxf-fs1/gp1::vorm:mds::", "security.selinux") failed:
Permission denied (13)
```

Restore an Encrypted Backup

This section illustrates restoration of the three files from the backup media to the same GuardPoint, `/oxf-fs1/gp1`. The files are restored to a different directory under the GuardPoint.

Restore a File Fully Rekeyed to the Latest Key Version

Recall that *file_1.dat* was archived in the backup media when it was fully rekeyed to version 9 of the key. As the current version of the key is also 9, *file_1.dat* is restored from backup without any changes. After restoring the file, the state of the restored file and its applied and current key versions remain unchanged, as compared to the original file that was backed up.

```
# my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files \ /file_1.dat /oxf-fs1/gp1/restored_files/file_1.dat

# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_1.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9

# voradmin ldt attr get /oxf-fs1/gp1/data_files/file_1.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9
```

Restore a Partially Rekeyed/encrypted File

Recall that *file_2.dat*, archived in the backup media, was partially rekeyed between versions 8 and 9. As the current version of the key was 9 at the time of backup, *file_2.dat* is restored to the GuardPoint with the same version of the key from the time of backup. The file is flagged for *lazy rekey*, meaning that a background rekey operation is scheduled to transform the file to the latest key version the next time an application tries to access the file.

At the completion of restoration, the file is fully transformed to the key version (v9). The key version is also the latest one in the policy. Although the file is flagged for lazy rekey (LAZY_RK), the file does not need to be transformed to the latest key version because it's already there. Had the file been partially rekeyed from version 7 to version 8 of the key at the time of backup, the restored file would have completed rekeying to version 8 at the end of the restoration. Therefore, the LAZY_RK flag would initiate a background transformation to update the key version to the latest key version when the file is accessed.

If this file is not accessed by any application, the file remains unchanged in the GuardPoint. It is not transformed to the latest key version. To trigger a rekey, either re-push the CTE-LDT policy from the CipherTrust Manager, or access the file with an application, such as a file explorer.

```
# my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files/\ file_1.dat /oxf-fs1/gp1/restored_files/file_2.dat

# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_2.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=lazy_rekey
Key:      name=LDT_AES256_KEY, version=9

# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_2.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9
```

Restore a File Not Rekeyed/encrypted with an Older Key Version

Recall *file_3.dat* was archived in the backup media when it was keyed to version 8 of the key, one version below the latest version at the time of backup. At completion of the restoration, *file_3.dat* is restored from backup to the same version, version 8, that it was keyed to when it was backed up.

However, the file is flagged for lazy rekey. After restoring the file, it is keyed to version 8 and flagged for lazy rekey (LAZY_RK). The file is rekeyed to the latest key version, version 9, as soon as an application accesses the file. If this file is not accessed by any application, the file remains unchanged in the GuardPoint.


```
# my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files \ /file_3.dat /oxf-  
fs1/gp1/restored_files/file_3.dat  
  
# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_3.dat  
LDT attributes: rekeyed_size=1440743424, rekey_status=lazy_rekey  
Key:      name=LDT_AES256_KEY, version=8  
  
# sum /oxf-fs1/gp1/restored_files/file_3.dat  
39994 1406976  
  
# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_3.dat  
LDT attributes: rekeyed_size=1440743424, rekey_status=none  
Key:      name=LDT_AES256_KEY, version=9
```

Restoring Non-CTE-LDT Backup Data to an CTE-LDT GuardPoint

This section describes how to restore data encrypted with a non-versioned key to an CTE-LDT GuardPoint.

If the backup was performed with the Apply Key effect, the backup files are in clear text. Simply restore the clear text files to the CTE-LDT GuardPoint with the Apply Key effect. All files will be encrypted with the versioned key.

If the backup of the non-CTE-LDT GuardPoint was performed without the Apply Key effect, the backup is encrypted, and you must do the following:

Note

The following example is for a manual guarding. The steps may differ slightly if your GuardPoint is configured for auto guard.

1. Create a temporary directory for restoring the files, type:

```
# mkdir -p /oxf-fs1/tmp_restore
```
2. Restore the encrypted backup files into the temporary directory, type:

```
# cp -pr /backup-media/oxf-fs1/gp1/data_files/* /oxf-fs1/tmp_restore
```
3. Create a Standard Policy with the Apply Key effect for all operations, using the same key as the policy applied on the GuardPoint at the time of backup.
4. Create and enable a new GuardPoint for the temporary directory using the Standard Policy just created.

```
# secfsd -guard /oxf-fs1/tmp_restore
```
5. Ensure that the temporary GuardPoint and CTE-LDT GuardPoint are both enabled.

```
# secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/oxf-fs1/gp1	LDT_AES256	manual	guarded	guarded	N/A
/oxf-fs1/tmp_restore	AES256	manual	guarded	guarded	N/A
6. Move the restored files from the temporary folder to the GuardPoint enabled with the CTE-LDT policy. The CTE agent encrypts the files in the CTE-LDT GuardPoint using the current key version in effect for the CTE-LDT policy.

```
# mv /oxf-fs1/tmp_restore/* /oxf-fs1/gp1
```
7. Disable the temporary GuardPoint and remove the temporary restore directory.

```
# secfsd -unguard /oxf-fs1/tmp_restore  
# rm -fr /oxf-fs1/tmp_restore
```
8. Delete the temporary GuardPoint on the CipherTrust Manager.

Using fsfreeze (Linux only)

If you use the `fsfreeze` command to quiesce access to the file system before creating a snapshot, refer to the `fsfreeze` section in CTE Admin Guide in the Linux Utilities chapter on how to run the `fsfreeze` command to quiesce access to both the file system and the GuardPoint(s).



WARNING

Do not use CTE-LDT schedules and do not pause CTE-LDT to align backup schedules with CTE-LDT. Instead, use the `fsfreeze` command.

- Running `fsfreeze -f` on the GuardPoint directory pauses CTE-LDT operations in-progress and freezes access to both the GuardPoint and the underlying file system.
- Running `freeze -u` reverses `freeze -f`, allowing access to underlying file system and resuming CTE-LDT operations.

CTE-LDT Backups Using a File System or Storage-Level Snapshot Tool

You can make a file system snapshot using a Logical Volume Manager service or mirroring/splitting storage level LUNs of a file system inside the storage subsystem. CTE-LDT does not have requirements for where and how you create a file system snapshot. However, it is required that you **suspend CTE-LDT processes before you take the file system snapshot**. Suspending CTE-LDT ensures data and metadata consistency between files and CTE-LDT extended attributes.

You may choose to suspend CTE-LDT manually on the managed host using `voradmin ldt suspend` command or `fsfreeze -f`, or suspend CTE-LDT on the CipherTrust Manager.

Note

Be aware that suspending CTE-LDT on the CipherTrust Manager suspends CTE-LDT on the entire host.

After creating a file system snapshot, you can resume CTE-LDT processes on the GuardPoint using `voradmin ldt resume`, or `fsfreeze -u`, or resuming CTE-LDT on the CipherTrust Manager. Do not mix the use of `fsfreeze` and `voradmin ldt suspend` to pause and resume CTE-LDT. CTE suspends or resumes CTE-LDT processes during live transformation when freezing or unfreezing GuardPoint access using `fsfreeze -f` or `-u` option. See the *CTE Agent for Linux Advanced Configuration and Integration Guide* on the use of the `fsfreeze` command on a GuardPoint.

Note

You can make sure CTE-LDT is suspended at backup time by setting the QoS schedule.

You can mount a file system snapshot for data recovery. Configuration for GuardPoints must be duplicated over the mount point of the snapshot file system. Make sure to use the same CTE-LDT policy. Enabling GuardPoints over or under the snapshot mount point provides access to the protected files for recovery. You can choose to manually resume key rotation on the GuardPoints of the snapshot file system, although this is not necessary.

Following is an example of the `fsfreeze` command used to freeze access to the file system `/oxf-fs1` in order to create a snapshot of the file system device. This examples illustrates three GuardPoints enabled inside the file system namespace, `/oxf-fs1/gp-1`, `/oxf-fs1/gp-2`, and `/oxf-fs1/gp-3`. Executing the command `fsfreeze -f` targets any of the GuardPoints in the `/oxf-fs1` mount point and suspends CTE-LDT processes on all of the GuardPoints. Then it freezes access to the file system.

```
# fsfreeze -f /oxf-fs1/gp-1
# voradmin ldt list all
MDS_1:  type=file, nguards=1, name=/oxf-fs1/gp-3/:vorm:mds::
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED,
```

fs1/gp-3

File List: count 4308

MDS_2: type=file, nguards=1, name=/oxf-fs1/gp-2/::vorm:mds::

Guard Table: version 1 nentries 1

Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-2

File List: count 4308

MDS_3: type=file, nguards=1, name=/oxf-fs1/gp-1/::vorm:mds::

Guard Table: version 1 nentries 1

Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/oxf-fs1/gp-1

File List: count 4308

After the file system snapshot is created, executing the `fsfreeze -u` command on any of the GuardPoints in the file system namespace unfreezes access to the file system and resumes CTE-LDT processes on all of the GuardPoints.

```
# fsfreeze -u /oxf-fs1/gp-1
```

```
# voradmin ldt list all
```

MDS_1: type=file, nguards=1, name=/oxf-fs1/gp-3/::vorm:mds::

Guard Table: version 1 nentries 1

Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-3

File List: count 4308

MDS_2: type=file, nguards=1, name=/oxf-fs1/gp-2/::vorm:mds::

Guard Table: version 1 nentries 1

Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-2

File List: count 4308

MDS_3: type=file, nguards=1, name=/oxf-fs1/gp-1/::vorm:mds::

Guard Table: version 1 nentries 1

Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-1

File List: count 4308

Windows Backup and Snapshots

On Windows, most backup applications use Volume Snapshot Service (VSS) for the backup. Using VSS is required for backing up files in CTE-LDT GuardPoints. VSS service provides a consistent view of the data to backup and restore applications by taking a snapshot of the volume. Windows Backup uses the snapshot volume, while other applications can continue using the original volume for normal I/O operations. VSS snapshot volume uses a “Copy on write” mechanism to provide a consistent view of the data. Some of the high-level steps of the Windows backup process are:

1. Backup application takes a snapshot of the volume using the VSS service.
2. Backup application mounts this VSS volume to read the data to be backed up.
3. The CTE Agent uses the same policy as that of the original volume to protect these snapshots.
4. The CTE Agent applies the policy and rules to all the I/O requests coming from the backup and restore applications.

CTE-LDT Backup and Restore Troubleshooting

Restored files to a GuardPoint protected with conflicting key rules

When restoring an encrypted file from backup media to an CTE-LDT protected GuardPoint without the Apply Key effect, and the file in the backup media does not have an CTE-LDT extended attribute, the file restored to the GuardPoint is set with an CTE-LDT extended attribute that specifies the current key version of the key in the policy

associated with the data in the restored file. As the key and key version in the policy do not match the key that was applied to the data at the time of backup, the file restored to the CTE-LDT protected GuardPoint is unreadable.

When restoring an encrypted file from backup media to an CTE-LDT protected GuardPoint without Apply Key effect, and the key specified in the CTE-LDT extended attribute of the file in backup media conflicts with the key rules of the policy on the GuardPoint, the restore operation fails and flags the restored file in error. You can only remove the file, or truncate it, to clear the error status on the file. Access to such files, except remove or truncate, fail with an EINVAL error.

CTE-LDT Command-Line Administration: voradmin command

Use the `voradmin` utility to gather statistics and administer CTE-LDT on a client. It has slightly different syntax and command capabilities depending on whether the client is running Linux or Windows.

Note

Refer to the `voradmin` man page for `voradmin` usage in Linux.

To use `voradmin`:

1. Log in to the host running the CTE Agent with CTE-LDT enabled.
2. At the command line, type `voradmin`.
3. Follow the usage outputs onscreen to find the available commands and their syntax. The general syntax is:

```
# voradmin ldt <command> [args]
```

Command	Description
<code>voradmin ldt attr get delete <guard path> <object path></code>	Get or delete attributes for a GuardPoint or Object path.
<code>voradmin ldt key <report map <key> > <guard path></code>	Creates a report, or map, containing statistics after each key rotation on a GuardPoint.
<code>voradmin ldt list all</code>	(Linux only) List all MDS files and GuardPoints undergoing CTE-LDT processing.
<code>voradmin ldt monitor [interval]</code>	(Windows only) Monitor CTE-LDT progress. If an interval is specified (in units of seconds), it continually updates the monitoring output at the specified interval.
<code>voradmin ldt rekey report <guard path> [output file]</code>	Generate a rekey report manually for a Guardpath.
<code>voradmin ldt resume <guard path> all</code>	Resume guarding the GuardPoint directory.
<code>voradmin ldt space <guard path></code>	Estimates disk space needed for metadata and mds store information.
<code>voradmin ldt stats [<guard path>] [<interval>]</code>	Obtains transformation CTE-LDT statistics such as: • Current rekey status • Start time • Estimated completion time • Percentage completed • Total data • Amount of data transformed • Total files • Number of files transformed • Number of files skipped • Number of files remaining for rekey

Moving a CTE-LDT GuardPoint from One CTE-LDT Policy to Another

To change the CTE-LDT policy that an CTE-LDT GuardPoint uses, complete the following steps to ensure that the GuardPoint is migrated properly from one CTE-LDT policy to another CTE-LDT policy.

Scenario

The GuardPoint is currently attached to LDT-Policy-1, which rekeys from `clear_key` to `LDT-Key-1`. The objective is to migrate the data in the GuardPoint to another versioned key, `LDT-Key-2`. Migration to `LDT-Key-2` requires detaching the GuardPoint from `LDT-Policy-1`, and then attaching it to `LDT-Policy-2`, assuming `LDT-Key-2` is the versioned key specified in `LDT-Policy-2`. This is a two step migration:

1. Migrate a GuardPoint out of the CTE-LDT policy to protection under a standard policy.
The step requires cloning `LDT-Key-1` to a non-versioned key, and migrating the GuardPoint out of the CTE-LDT policy. Because the cloned key and the the current version of `LDT-Key-1` have the same key material, the data in the GuardPoint directory remains encrypted to the same key after migration of the GuardPoint out of CTE-LDT.
2. Migrate a GuardPoint protected under a standard policy to protection with an CTE-LDT policy.

Note that you may set the transformation key to `clear_key` instead of `LDT-Key-2` in the second policy (`LDT-Policy-2`). The effect of `clear_key` is transformation of the data in the GuardPoint directory to clear text. Although the transformation key in CTE-LDT policies must be a versioned key, `clear_key` is an exception. It allows CTE-LDT GuardPoints to be transformed to clear using the CTE-LDT process.

To properly move the GuardPoint from LDT-Policy-1 to LDT-Policy-2:

Note

Ensure that no active processes or users are accessing files in the GuardPoint, or its subdirectories, until all steps have been completed.

1. Follow the instructions for, ["Converting a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy" on the facing page](#).
2. Assuming the current version of the `LDT-Key-1` is version 5, then clone version 5 of the key to `Cloned-LDT-Key-1v5`.
 - a. In the CipherTrust Manager Applications Page, open the **Keys & Access Management** application.
 - b. Click the name of the versioned key that you want to clone.
 - c. In the Key Details area, find the version that you want to clone.
 - d. Click the (...) button at the end of the row and select **Clone** to clone the selected version of the key.
3. Follow the instructions for ["Using voradmin To Estimate Disk Space Required for CTE-LDT \(Linux\)" on page 60](#).
4. Follow instructions for ["Converting a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy" on the facing page](#) using the cloned key (`Cloned-LDT-Key-1v5`) as the Initial Key and `LDT-Key-2` as the key for the new CTE-LDT policy. The files are now rekeyed from `Cloned-LDT-Key-1v5` to `LDT-Key-2`.

Removing CTE-LDT and Security Encryption

If you want to stop using CTE-LDT on a GuardPoint or on a whole client, follow the instructions in the following sections.

Migrating a GuardPoint Out of CTE-LDT

Migrating a GuardPoint from CTE-LDT removes the security encryption. It also provides a CipherTrust Manager Administrator with the flexibility to relax the compliance requirement, when strict compliance for frequent key rotation on specific data is no longer mandatory. The following sections describe how to migrate a GuardPoint from CTE-LDT to a non-CTE-LDT policy, or to remove encryption protection from it.

Converting a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy

If you want to do more than just change the policy on a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy, see ["Deleting CTE-LDT Metadata \(Linux\)" on page 76](#) or ["Deleting CTE-LDT Metadata \(Windows\)" on page 76](#).

1. Clone the versioned key associated with the CTE-LDT GuardPoint to a non-versioned key.
The clone function creates a new key with the same cryptographic encryption material as the current version of the cloned versioned key.
This allows CTE-LDT to use the cloned key in a non-CTE-LDT policy to convert the GuardPoint from an CTE-LDT to a non-CTE-LDT managed policy.
 - a. In the CipherTrust Manager Applications Page, open the **Keys & Access Management** application.
 - b. Click the name of the versioned key that you want to clone.
 - c. In the Key Details area, click the (...) button at the end of the row showing the current version of the key and select **Clone** to clone the current version.
 - d. Enter a new name for the key in the **Key Name** field. Do *not* select the **CTE Versioned** option for the clone.
 - e. Click **Clone**.
2. Open the **CTE** application and click **Clients** in the left-hand menu bar.
3. Click on the name of the client whose GuardPoint you want to migrate.
4. Find the GuardPoint you want to migrate in the GuardPoints table, then click the (...) button at the end of the row and select **Disable**.
5. After CTE-LDT disables the GuardPoint, click the (...) button at the end of the row and select **Remove**.
6. (Linux only) Ensure that the GuardPoint is removed on the managed host:

```
# secfsd -status guard
No GuardPoints configured
```
7. CTE-LDT creates extended attributes for every file under the GuardPoint as well as the GuardPoint directory. Now that the CTE-LDT policy does not manage the GuardPoint, you must remove the extended attributes for every file in the GuardPoint, type:

```
# voradmin ldt attr delete /<GuardPoint>
```
8. The command may take some time depending on the number of files in the GuardPoint.

Note: For all of the file system mount points that contain an CTE-LDT protected GuardPoint, you must clean up the metadata first. See ["Deleting CTE-LDT Metadata \(Linux\)" on page 76](#).

9. Create a non-CTE-LDT policy using the cloned key you created earlier in this procedure.
 - a. In the **CTE** application, click **Policies** in the left-hand menu bar and then click **Create Policy**.
 - b. Enter a name for the policy in the **Name** field.
 - c. In **Policy Type**, choose **Standard**.
 - d. Click **Next**.
 - e. On the Security Rules page, click **Next** to skip adding a security rule.
 - f. On the Key Selection Rules, click **Create Key Rule**.
 - g. In the **Key Name** field, select the cloned key you created earlier.
 - h. Click **Add**.
 - i. Click **Next**.
 - j. Confirm that the key rule is correct and click **Save**.
10. Apply the non-CTE-LDT policy to the GuardPoint.



CAUTION

Make sure that you have removed all of the CTE-LDT metadata from the GuardPoint before applying the non-CTE-LDT policy.

- a. Open the **CTE** application and click **Clients** in the left-hand menu bar.
- b. Click on the name of the client whose GuardPoint you want to migrate.
- c. Click **Create GuardPoint**.
- d. In the *Create GuardPoint* dialog box, select the Policy that you just created in the **Policy** field.
- e. Select the **Type: Auto Directory** or **Manual Directory**.
- f. In the **Path** field, and enter or browse to the directory to protect.
- g. When you are done, click **Create**.

Remove Protection from a GuardPoint

When compliance may no longer require protecting data in a GuardPoint, you may choose to unprotect/decrypt it. Before removing protection from your GuardPoint, you must decrypt the data in your GuardPoint by setting it to clear. You have two options to decrypt your data:

- While a GuardPoint is protected and enabled under an CTE-LDT policy, you can use copy or backup/restore commands to save files in your GuardPoint to a location outside of your GuardPoint.
- Use the `dataxform` command to transform your GuardPoint to clear in an offline transformation process.

Copying Files to Decrypt Them

If you choose to copy your files, you must create a directory outside of the GuardPoint and then copy the files into the GuardPoint directory. After finishing copying, complete the following steps:

1. Open the **CTE** application and click **Clients** in the left-hand menu bar.
2. Click on the name of the client whose GuardPoint you want to remove.
3. Find the GuardPoint you want to remove in the GuardPoints table, then click the (...) button at the end of the row and select **Disable**.
4. After CTE-LDT disables the GuardPoint, click the (...) button at the end of the row and select **Remove**.

5. (Linux only) Ensure that the GuardPoint is removed on the managed host:

```
# secfsd -status guard  
No GuardPoints configured
```

This completes removal of the GuardPoint under an CTE-LDT policy. You can now remove the original files and data within the GuardPoint namespace.

Using Dataxform Command to Transform the Files

If you choose to use the dataxform command to transform data in your GuardPoint to clear, use the `voradmin` command to verify that earlier versions of the versioned key are not in use on your GuardPoint. Complete the following steps to clear all metadata in your GuardPoint. Then, transform your GuardPoint to clear.

1. Clone the versioned key associated with the CTE-LDT GuardPoint to a non-versioned key.
 - a. In the CipherTrust Manager Applications Page, open the **Keys & Access Management** application.
 - b. Click the name of the versioned key that you want to clone.
 - c. In the Key Details area, click the (...) button at the end of the row showing the current version of the key and select **Clone** to clone the current version.
 - d. Enter a new name for the key in the **Key Name** field. Do *not* select the **CTE Versioned** option for the clone.
 - e. Click **Clone**.
2. Create a Standard policy using the cloned key you just created.
 - a. In the **CTE** application, click **Policies** in the left-hand menu bar and then click **Create Policy**.
 - b. Enter a name for the policy in the **Name** field.
 - c. In **Policy Type**, choose **Standard**.
 - d. Enable the **Data Transformation** option.
 - e. Click **Next**.
 - f. On the Security Rules page, click **Next** to skip adding a security rule.
 - g. On the Key Selection Rules, click **Create Key Rule**.
 - h. In the **Key Name** field, select the cloned key you created earlier.
 - i. Click **Add**, then click **Next**.
 - j. On the Data Transformation page, click **Create Data Transformation Rule**.
 - k. In the **Transformation Key Name** field, select `clear_key`.
 - l. Click **Add**, then click **Next**.
 - m. Confirm that the key rule and data transformation rule are correct and click **Save**.
3. Click **Clients** in the left-hand menu bar.
4. In the Clients table, click on the name of the client whose GuardPoint you want to remove.
5. Find the GuardPoint you want to remove in the GuardPoints table, then click the (...) button at the end of the row and select **Disable**.
6. After CTE-LDT disables the GuardPoint, click the (...) button at the end of the row and select **Remove**.

Before you apply the offline data transformation policy to your GuardPoint, you must clean up the CTE-LDT metadata from your GuardPoint. CTE-LDT creates extended attributes for every file under the GuardPoint, as well as the GuardPoint directory. Now that the CTE-LDT policy does not manage the GuardPoint, you can remove the extended attributes for every file in the GuardPoint.

7. Remove the extended attributes of files in a GuardPoint, type:

```
# voradmin ldt attr delete <GuardPoint>
```

The command may take some time depending on the number of files in the GuardPoint. After metadata deletion is complete, you can apply the offline transformation policy on the GuardPoint.

8. CipherTrust Manager, guard and enable the GuardPoint with the Standard policy you created earlier.
9. After enabling your GuardPoint, run the `dataxform` command on the managed host to transform the GuardPoint to a `clear_key`, type:

```
# dataxform --rekey --gp /<GuardPoint>/ --preserve_modified_time --preserve_access_time --cleanup_on_success
```
10. After completion of `dataxform`, unguard the GuardPoint.
11. Remove the GuardPoint from the `dataxform` policy in CipherTrust Manager.

Deleting CTE-LDT Metadata (Linux)

To remove the metadata associated with the GuardPoint, you must run the `voradmin` command on the managed host to remove the CTE-LDT metadata associated with the GuardPoint.



WARNING

Before you attempt to remove an MDS file, make sure that no CTE-LDT-protected GuardPoints remain configured under the file system mount point.

In the following example:

- `/oxf-fs1` is the mount point
- `/oxf-fs1/gp1` is the CTE-LDT-protected GuardPoint

To delete the metadata associated with the GuardPoint:

1. Ensure that the GuardPoint is not enabled on the host. Run the command below and verify that the GuardPoint pathname does not appear in the output of the `secfsd` command, type:

```
# secfsd -status guard
```

2. Run the `voradmin` command to remove CTE-LDT attributes on the GuardPoint, type:

```
# voradmin ldt attr delete <GuardPoint path>
```

For example:

```
# voradmin ldt attr delete /oxf-fs1/gp1  
LDT metadata has been removed from all files in GuardPoint /oxf-fs1/gp1
```

Deleting CTE-LDT Metadata (Windows)

Use the following command to delete the CTE extended attribute for a file or a GuardPoint. This is useful when removing a GuardPoint from under an CTE-LDT policy (see ["Migrating a GuardPoint Out of CTE-LDT" on page 73](#)).

```
# voradmin ldt attr delete [<file name path> | <guard path>]
```

For an overview of `voradmin ldt`, see ["CTE-LDT Command-Line Administration: voradmin command" on page 71](#).

Removing CTE-LDT from a Host

Once you have registered a host and enabled CTE-LDT, you cannot disable the CTE-LDT feature by unchecking the CTE-LDT box. You must unregister the host from the CipherTrust Manager, then register it again without CTE-LDT. When you remove the CTE-LDT feature from a host entirely, the host's CTE-LDT license becomes available for use on another host.

1. Stop all applications from accessing data in CTE-LDT GuardPoints on the host.
2. Migrate data in every CTE-LDT GuardPoint using the steps described in the section ["Remove Protection from a GuardPoint" on page 74](#).



WARNING

Potential data loss. Ensure that you have decrypted the data and, optionally, copied it out of the GuardPoint. Once the CTE Agent software is removed, access to data is no longer controlled by CTE. If the data was encrypted, it remains encrypted, and there is no way to read it.

3. Remove the GuardPoints on the host from the CipherTrust Manager.
 - a. Remove the CTE-LDT metadata from those GuardPoints.
 - b. Remove the MDS files associated with those GuardPoints, if necessary. See ["Deleting CTE-LDT Metadata \(Linux\)" on the previous page](#) for more information.
4. Remove the host from the CipherTrust Manager. For details, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
5. Re-install the agent on the host.
6. Register the host with the CipherTrust Manager. This time, do not select the CipherTrust Transparent Encryption - Live Data Transformation option. See ["Enabling CTE-LDT on a Protected Host" on page 22](#).

Uninstalling the Agent while CTE-LDT is Rekeying GuardPoints

You cannot uninstall the CTE Agent if CTE-LDT is rekeying any GuardPoints on that client.

If you want to uninstall the CTE Agent from a client that contains CTE-LDT GuardPoints, you must first unencrypt the files on each CTE-LDT GuardPoint using the steps noted in the previous sections.

Chapter 6: Troubleshooting CTE-LDT

Monitoring and Statistics	78
Protecting CTE-LDT GuardPoints against Failure in Underlying Filesystems (Linux)	80
Alerts Playbook	81
Error Messages	85
Warning and Info Messages	87
Recommendations and Considerations	88

The CTE-LDT administrator needs to monitor and respond to runtime statistics and alerts.

Monitoring and Statistics

This section describes how to find the runtime status of CTE-LDT and how to get statistics about its operation.

Note

When you check GuardPoint status on the CipherTrust Manager, be aware that the status is not relayed in real time. There can be a delay of several minutes before the CipherTrust Manager becomes aware of events on the host. When you configure the host and v for one-way communication, the delay is longer, up to an hour, because CTE-LDT sends statistics to the CipherTrust Manager only once per hour.

To find out when the CipherTrust Manager last received a status update from the host, check the Last Status Update timestamp in the GuardPoint Health dialog (for information about how to display this dialog, see ["Obtaining Statistics in the CipherTrust Manager with GuardPoint Status" below](#)). For the most up-to-date statistics, inspect the client. Run the `voradmin` command on the managed hosts to retrieve status and statistics pertaining to GuardPoints.

Obtaining Statistics in the CipherTrust Manager with GuardPoint Status

During and after data transformation, you can view statistics about any GuardPoint on any client in your system. Either use the CipherTrust Manager, as described in this section, or use the `voradmin` command, as described in ["Obtaining CTE-LDT Statistics at the Command Line" below](#).

To display the GuardPoint status in CipherTrust Manager:

1. Open the **CTE** application and click **Clients** in the left-hand menu bar.
2. Click on the name of the client whose GuardPoint you want to view.
3. Click the Status of the GuardPoint you want to view in the GuardPoints table.
CipherTrust Manager displays the GuardPoint Health dialog box with various statistics about the GuardPoint.

Obtaining CTE-LDT Statistics at the Command Line

You can obtain CTE-LDT statistics from the command line using the following command:

```
# voradmin ldt stats <guard path> [interval]
```

This command displays transformation statistics for a GuardPoint, or for all GuardPoints, if none are specified. If you specify an interval (in units of seconds), the command continually updates the statistics on the given interval. If no GuardPoint is specified, the command returns the aggregate statistics at the host level, including specific statistics related to QoS. If a GuardPoint is specified, statistics include:

- Current rekey status
- Rekey Start time
- Last rekey completion time
- Estimated Rekey completion time
- Data Statistics including the amount of data transformed
- File statistics including:
 - Number of files transformed
 - Number of files skipped
 - Number of files remaining for rekey

Obtaining a Rekey Report

CTE-LDT generates a report automatically after completion of a key rotation. The report lists the files in the GuardPoint and the key and version of the key applied to each file. This kind of report may be a common compliance requirement.

The administrator can also request a rekey report during rekey, if the need to see the partial transformation results so far.

About the rekey report

On Linux hosts, CTE-LDT writes rekey reports to a local file on the agent host in `/var/log/vormetric/`. The file name begins with `ldaudit-log-`. It is followed by the file system directory name, GuardPoint directory name, and a timestamp. For example, for a GuardPoint at `/oxf-fs2/gp2` with rekey completed on November 19, 2016, just after 2:00 p.m. (hour 14), the rekey report file name would be `ldaudit-log-_oxf-fs2_gp2-2016111914917`.

The report includes:

- Total number of files in the GuardPoint
- Number of files transformed
- Rekey start and end times
- List of all files transformed
- Applied key and key version for each file (for example, files in different resource sets might have used different keys)

Manually generating a rekey report

To generate a rekey report manually, use the following command:

```
# voradmin ldt rekey report <GuardPoint> [<logfile>]
```

In `<GuardPoint>`, type the GuardPoint path. In `<logfile>`, you can optionally direct the output to a file. If no logfile is specified, the report displays on `stdout`.

Monitoring Ongoing CTE-LDT Operations at the Command Line (Windows only)

Use the following syntax to monitor CTE-LDT progress. If an interval is specified (in units of seconds), it continually updates the monitoring output at the specified interval.

```
C:\> voradmin ldt monitor [interval]
```

For an overview of `voradmin ldt`, see ["CTE-LDT Command-Line Administration: voradmin command" on page 71](#).

Protecting CTE-LDT GuardPoints against Failure in Underlying Filesystems (Linux)

CTE-LDT Recovery Challenges

The main challenge with CTE-LDT recovery is a failure to access files or specific blocks in files inside a GuardPoint. Before CTE-LDT runs the recovery process on a GuardPoint, the underlying file system was recovered before file system was mounted. File system recovery may create orphan files in the `lost+found` directory inside the mount point. If an orphan file belongs to the GuardPoint, CTE-LDT cannot recover the file as the file is no longer in the same directory as it was prior to the crash while it was undergoing rekey.

CTE-LDT Recovery Enhancement

CTE-LDT has been improved for handling inconsistencies in the underlying file system during execution of CTE-LDT recovery. When enabling a GuardPoint after a system crash, CTE-LDT performs consistency checks on the files undergoing rekey at the time of crash before enabling GuardPoint. If the CTE-LDT recovery process is unable to recover any of the affected files, the GuardPoint will not be enabled and CTE-LDT will send the following alert to the CipherTrust Manager:

```
[CGS3266E] LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in
underlying file system encountered during LDT recovery.
```

You can check the status of a GuardPoint and the reason for failing to enable a GuardPoint using the `seccfsd -status guard` command. For example, the GuardPoint `/mnt/gp` failed to guard because Guard point needs LDT recovery as reported in the `Reason` column for the following example GuardPoint.

GuardPoint	Policy	Type	ConfigState	Status	Reason
/mnt/gp	LDT220	manual	guarded	not guarded	Guard point needs LDT recovery

Details on the specific issues encountered, including any files that could not be recovered, are reported to a log file in the `/var/log/vormetric` directory. The log file name is in the format:

```
ldt_recovery_log:<guardpoint_name>:<timestamp>.txt
```

The log file name starts with `ldt_recovery_log`, followed by the GuardPoint pathname and the date and time of the recovery attempt. The GuardPoint pathname and date and time are separated with `:"`. For example:

```
/var/log/vormetric/ldt_recovery_log:_mnt_gp:2018-12-08-14:6:12.txt
```

Refer to the issues listed in the log file, and resolve those issues before enabling the GuardPoint again. A GuardPoint cannot be enabled in subsequent guard attempts until those issues are resolved. Each attempt generates a new log file. Check the CTE-LDT log file for missing files whose inode numbers match inode numbers of orphan files in `lost+found`. If there is a match, restore the file from `lost+found` to the pathname specified in the CTE-LDT recovery log file. Be sure to run the `mv` command to restore the file to the original location, do not run the `cp` command. After resolving all or some of the reported issues, you must run the command `voradmin ldt recover <GuardPoint>` to repeat the recovery process.

```
voradmin ldt recover <GuardPoint>
```

Running this command resolves the problems that can be corrected and clears the failed recovery status on the GuardPoint, allowing the GuardPoint to enable automatically within 30 seconds. If the GuardPoint does not enable, you can enable it using `secfsd -guard` command, if manual guard, or enable it on the CipherTrust Manager, if auto-guard. Note that if you are unable to resolve all of the reported issues, you accept the loss of some data or files, as reported in the latest recovery log file for the GuardPoint, when you run the command `voradmin ldt recover <GuardPoint>`.

Recovery Alerts

CTE-LDT sends two alerts to CipherTrust Manager if CTE-LDT fails to resolve the issues encountered during recovery.

The alert below is an error report sent to the CipherTrust Manager whenever CTE-LDT encounters failure during recovery prior to enabling GuardPoint. This alert also reports the GuardPoint specified in the message is not enabled:

```
[CGS3266E] LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in  
underlying file system encountered during LDT recovery.
```

The alert below is a warning report sent to the CipherTrust Manager only if `voradmin ldt recover` encounters errors and continues anyway. This alert reports the GuardPoint specified in the message has been enabled with some files in error status.

```
[CGS3267W] LDT-ALERT: LDT manual recovery on guard point [GuardPoint] completed with [#]  
errors.
```

The full message body does not currently appear in the logs on the CipherTrust Manager. At this time, the CipherTrust Manager shows the message ID without the message body.

Alerts Playbook

This section lists the CTE-LDT alerts and describes what to do in each case. CTE-LDT generates alerts when issues arise that require attention from the CipherTrust Manager Administrator. Without prompt attention, alerts can delay the rekey process or cause the process to remain incomplete.

Failure to Suspend or Resume CTE-LDT Operation

- **LDT-ALERT: Failed to suspend rekey on GuardPoint [GuardPoint]**

Solution: An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, you must fix the problem at the host OS or storage level.

The appropriate corrective action depends on when this problem occurs and the reason for the suspension. If the suspend request was at the host level as part of a QoS schedule, or it was initiated by a user on the CipherTrust Manager, the failure occurred at the host level rather than the specified GuardPoint.

Otherwise, the source is probably the initiation of a suspension on a specific GuardPoint before backup. If the backup operation is in progress when this alert message occurs, you must fix the cause of the suspension failure and then restart the backup. If the backup has already completed when the alert message occurs, the backup image on the GuardPoint may have inconsistent data and CTE-LDT metadata. Discard this backup image and do a fresh backup.

If you cannot find and fix the host OS or storage issue, contact Thales Support for troubleshooting and recovery.

- **LDT-ALERT: Failed to resume rekey on GuardPoint [GuardPoint]**

- **LDT-ALERT: Failed to resume rekey on all GuardPoints**

Solution: An I/O error is the most common cause of failure when updating persistent state of a GuardPoint. For I/O errors, you must fix the problem at the host OS or storage level.

The appropriate corrective action depends on when this problem occurs and the source of the problem. If the resume request was at the host level as part of a QoS schedule, or the resume request was initiated by a user on the CipherTrust Manager, the failure occurred at the host level rather than the specified GuardPoint.

Otherwise, the source is probably initiation of a resume operation on a specific GuardPoint after a backup is completed.

If you cannot find and fix the host OS or storage issue, contact Thales Support for troubleshooting and recovery.

Insufficient Resources

The following alerts trigger when there are not enough resources for CTE-LDT operations.

- **LDT-ALERT: Aborting rekey of file [FileName] due to insufficient disk space**

The key rotation process was stopped on a GuardPoint because there was not enough available disk space.

Solution: Resize or free up space in the file system where the PathName resides. Key rotation automatically starts again when sufficient free space becomes available.

- **LDT-ALERT: Failed to launch transformation on [GuardPoint]**

CTE-LDT failed to launch the data transformation process on the specified GuardPoint.

Solution: The most common causes of this failure are:

- Low amount of system resources, such as free disk space.
- Check the system logs for insufficient free space in underlying file systems. You can free up space by removing older files or resizing your underlying file system. You may resize the file system on-line or off-line.

For other issues, contact Customer Support.

- **LDT-ALERT: QoS failed to start**

The Quality of Service subsystem failed to launch QoS services due to lack of system resources.

Solution: A low amount of available memory is the most common cause of this failure.

Contact Customer Support.

- **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint] due to insufficient disk space**

- **LDT-ALERT: MDS file [PathName] exceeded disk space quota on gp [GuardPoint]**

There was not enough storage space in one or more file systems containing GuardPoints undergoing rekey.

Solution: Check the file systems where your GuardPoints reside to see how much space it is using. Add more storage space as needed. After the condition is corrected and disk space is available, CTE-LDT operations resume automatically.

- **LDT-ALERT: Low space on guard point [GuardPoint], increase free space or LDT will be suspended.**

Available storage space in the file system containing the GuardPoint is nearing the threshold below which CTE-LDT rekeying cannot continue. If available space does drop below that threshold, rekeying will be automatically suspended.

Solution: Check the file system where your GuardPoint resides to see how much space is available. Make more free space available if necessary. After the condition is corrected and storage space is available, rekeying resumes automatically.

Failed to Update CTE-LDT Attribute

The following alerts trigger when CTE-LDT extended attributes are not properly updated.

- **LDT-ALERT: Failed to update LDT attribute on GuardPoint [GuardPoint]. Error: [ErrorNumber]**

Solution: I/O error is the most common cause of failure when updating CTE-LDT extended attributes. For I/O errors, fix the problems at the host OS or storage level. In Linux, if you experience an I/O error, identify the file that had the error, and restore it from backup. See ["Backing Up and Restoring CTE-LDT GuardPoints" on page 62](#).

In Windows, you can recover a file that has corrupt metadata as follows:

- If the file is fully encrypted, remove the metadata. Type:

```
# voradmin ldt attr delete <file name path>
```

Then apply the same policy that was used to encrypt the data.

- If the file was only partially rekeyed, restore the file from a backup.

If you cannot find and fix the underlying host OS or storage issue that is causing corrupt metadata, contact Customer Support for troubleshooting and recovery.

- **LDT-ALERT: Failed to update LDT attribute**

CTE-LDT failed to create or update an CTE-LDT extended attribute of a file in a GuardPoint.

Solution: An I/O error is the most common cause of failure when updating an CTE-LDT extended attribute. For I/O errors, fix the problem at the host OS or storage level.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

Rekey Stopped

The following alert is specific to Windows and is triggered when rekey is stopped before it completes normally.

LDT-ALERT: Suspending rekey of binary file [PathName] during its execution

CTE-LDT operations encountered an executable file that is running.

CTE-LDT cannot rekey a running executable file until the execution of the binary file stops.

Solution (Windows)

1. Obtain the name of the executable file from the alert message.
2. Stop execution of the binary file.

Incomplete Key Rotation

- **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint]. Another rekey operation is already in progress** (Windows only)
- **LDT-ALERT: Key rotation failed on GuardPoint [GuardPoint]**

CTE-LDT failed to complete the key rotation process on the specified GuardPoint. On Windows, this may occur if a key rotation process is already in progress on the GuardPoint. This pre-existing rekey operation could be active, or it could be in a suspended state, either because of the QoS schedule or a manual pause initiated by the administrator. See ["Suspending and Resuming Rekey and/or Scan Phase" on page 44](#).

Solution

1. On Linux, you can run the following command to see whether key rotation is in progress on the GuardPoint.

```
# voradmin ldt list all
```
2. On Linux or Windows, check the rekey status of GuardPoints in the CipherTrust Manager Console.
3. If key rotation is already in progress on a Windows GuardPoint, wait for the key rotation to complete.

Contact Customer Support if this error occurs on Linux or if the cause of key rotation failure on Windows is not a key rotation in progress.

Skipped Key Rotation

The following alerts trigger when CTE-LDT skips key rotation.

- **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint]. It is on a read-only file system**

Key rotation is skipped on a specified GuardPoint because the mount point where the GuardPoint resides does not permit write operations.

Solution:

1. Remount the file system where the GuardPoint resides, and change the mount option to read/write.
 2. On the GuardPoint page on the CipherTrust Manager, press **Re-push Policies** to manually re-push the policies to the host to initiate key rotation on GuardPoints ready for key rotation.
- **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint] during pre-commit**
 - **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint] during commit**
 - **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint]. Error: [ErrorNumber]**
 - **LDT-ALERT: Failed to update LDT attribute on GuardPoint [GuardPoint]. Error: [ErrorNumber]**

CTE-LDT failed to start a key rotation process on a GuardPoint during a guard operation or when processing a key rotation notification from the CipherTrust Manager. For [ErrorNumber], a Linux error number is substituted, such as `errorcode 17`.

Solution: The host returns error code 17 during CTE-LDT key rotation if it cannot perform the key rotation because there is already a rekey in progress. This pre-existing rekey operation could be active, or it could be in a suspended state, either because of the QoS schedule or a manual pause initiated by the administrator. See ["Suspending and Resuming Rekey and/or Scan Phase" on page 44](#).

An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, fix the problem at the host OS or storage level.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

Failed to Update CTE-LDT Metadata During Scan Phase

CTE-LDT triggers the following alerts when CTE-LDT cannot properly update metadata during the scan phase. (See ["CTE-LDT Runtime Flow" on page 13](#) for information about the scan phase.)

- **LDT-ALERT: Scan error on [GuardPoint] removing MDS guard for relaunching dataxform**

CTE-LDT failed to update metadata when restarting a scan on the specified GuardPoint.

Solution: An I/O error is the most common cause of failure when updating CTE-LDT metadata. For I/O errors, fix the problem at the host OS or storage level and then restart operations.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Thales Support for troubleshooting and recovery.

- **LDT-ALERT: Online Dataform failed during post scan stage on [GuardPoint]**

CTE-LDT failed to update metadata when transitioning from scan to rekey phase on the specified GuardPoint.

Solution: An I/O error is the most common cause of failure when updating CTE-LDT metadata. For I/O errors, the problem must be fixed at the host OS or storage level and the operation restarted.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

File system inconsistencies after system crash

CTE-LDT sends two alerts to the CipherTrust Manager if CTE-LDT fails to resolve the issues encountered during recovery.

The alert below is an error report sent to the CipherTrust Manager whenever CTE-LDT encounters failure during recovery prior to enabling GuardPoint. This alert also reports the GuardPoint specified in the message is not enabled:

- **LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in underlying file system encountered during LDT recovery**

The alert below is a warning report sent to the CipherTrust Manager only if `voradmin ldt recover` encounters errors and continues anyway. This alert reports the GuardPoint specified in the message has been enabled with some files in error status.

- **LDT-ALERT: LDT manual recovery on guard point [GuardPoint] completed with [#] errors.**

Solution: See ["Protecting CTE-LDT GuardPoints against Failure in Underlying Filesystems \(Linux\)" on page 80](#).

Error Messages

This section describes runtime error messages. For information about other types of runtime messages, see ["Alerts Playbook" on page 81](#) and ["Warning and Info Messages" on page 87](#).

Failed to Transform File During Rekey

CTE-LDT could not complete transformation on a file.

Related Messages:

- **LDT: Rekey failed for file [PathName] on GuardPoint [GuardPoint]**
- **LDT: Extended attribute of inode [InodeNumber] is corrupted under GuardPoint [GuardPoint]**

Solution: An I/O error is the most common cause of failure when updating CTE-LDT metadata. For I/O errors, fix the problem at the host OS or storage level, and then restore the file from a backup.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

Failure to Suspend CTE-LDT

A request to stop CTE-LDT processing did not succeed. The suspend request was at the host level as part of a QoS schedule, or the suspend request was initiated by a user on the CipherTrust Manager.

Related Messages:

- **LDT: Failed to suspend rekey on all GuardPoints**
- **LDT operations could not be suspended on the host**

Solution: An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, fix the problem at the host OS or storage level.

If a backup operation is in progress when this message occurs, you must fix the cause of the suspend failure and then restart the backup. If the backup has already completed when the alert message occurs, the backup image on the GuardPoint may have inconsistent data and CTE-LDT metadata. Discard this backup image and do a fresh backup.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

Failure to Start or Stop Transformation

The following general messages are recorded when there are errors attempting to start or stop CTE-LDT:

- **LDT: Failed to abort key rotation on GuardPoint [GuardPoint]**
- **LDT: Failed to start**
- **LDT: Failed to stop**
- **LDT: Failed to exit**

Solution: Examine system logs for additional information as to the cause. If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

Failure to Restart Transformation

The following message is recorded when an attempt to restart transformation after a system reboot fails because the file system is mounted as read-only. Transformation on the specified GuardPoint cannot continue until the file system is mounted with write permission.

- **LDT: Skipped LDT recovery on read-only file system [GuardPoint]**

Solution: Re-mount the file system with write permissions.

Temporary Failure to Start Transformation on a File

The following messages are recorded when there are communication issues or lack of resources on the host. Once the condition is corrected, transformation of the file continues automatically:

- **LDT: Insufficient memory condition encountered during LDT on GuardPoint [GuardPoint]**
- **LDT: Encryption key for file [PathName] unavailable for LDT, possibly due to loss of communication to CipherTrust Manager**
- **LDT: Aborting rekey of file [PathName] due to lack of free memory. Try closing other application to resolve the issue**

Solution: Resolve the communication issues or increase the available resources, then verify that CTE-LDT has resumed processing.

Transient Condition while enabling GuardPoint

The following messages are recorded when a request is made to guard an CTE-LDT GuardPoint when GuardPoint initialization is already in progress. During the GuardPoint initialization, the system initializes MDS file associated with the GuardPoint in preparation for CTE-LDT. Initialization of the MDS file can take a few minutes. During this time, if

the system retries the guard operation, one of the following messages displays.

Related Messages:

- **Not re-guarding path *[path]* (Reason: GuardPoint initialization already in progress)**
- **Not re-guarding path *[path]* from container *[container]* (Reason: GuardPoint initialization already in progress)**

Solution: Wait for the current GuardPoint initialization to complete and then resubmit the new GuardPoint initialization request if desired.

Failed to transform passthrough files for AD database files (Windows Only)

CTE-LDT skipped the transformation of passthrough files for all AD database files. The problem occurs when the AD database remains in the default folder location.

Related Messages:

- **Skipping transformation of passthrough file *[filename]*. The file resides in the boot directory. CTE cannot encrypt boot directory files.**
- **Skipping transformation of passthrough file *[filename]*. CTE cannot encrypt these files. They are already encrypted using NTFS encryption or compressed.**
- **Skipping transformation of passthrough file *[filename]*. File is not in a GuardPoint directory.**

Solution: To fix this issue, move the AD database to any folder other than `c:\windows` or `c:\program files`.

Warning and Info Messages

This section describes runtime error messages. For information about other types of runtime messages, see ["Alerts Playbook" on page 81](#) and ["Error Messages" on page 85](#).

Stopping Transformation of a File on Volume Dismount (Windows only)

The following warning message is recorded when transformation of a file is stopped because the containing volume is dismounted.

- **LDT: Volume dismounted. Aborting transformation at file *[PathName]***

Issues with Policy or System Configuration

The following warning messages are recorded when CTE cannot perform CTE-LDT on the GuardPoint, because there are errors in the policy associated with the GuardPoint, or the file system containing the GuardPoint is not supported by CTE-LDT. Files in the GuardPoint can still be accessed, but no CTE-LDT encryption occurs.

- **LDT: The GuardPoint *[GuardPoint]* does not have a valid transformation policy, there is no new key rule**
- **LDT: The GuardPoint *[GuardPoint]* does not have a valid transformation policy, there is no key_op rule**
- **LDT: The GuardPoint *[GuardPoint]* does not support online rekey, only file operations from the offline data transform process will be allowed**

Failure to Enable GuardPoint During Cleanup

CTE-LDT records the following informational message when a user attempts to enable a newly added GuardPoint. This message displays if the GuardPoint directory was previously guarded with an CTE-LDT policy and the CTE-LDT metadata cleanup is in progress when user is guarding under the new policy.

- **LDT: Cannot enable GuardPoint [GuardPoint] during LDT clean-up process**

Solution: Retry the operation once the cleanup completes.

General CTE-LDT Operations

The following informational messages are recorded during various CTE-LDT operations. No action is required.

- **LDT: Successfully suspended rekey on GuardPoint [GuardPoint]**
- **LDT: Successfully suspended rekey on all GuardPoints**
- **LDT: Successfully resumed rekey on GuardPoint [GuardPoint]**
- **LDT: Successfully resumed rekey on all GuardPoints**
- **LDT: Rekey operation completed on GuardPoint [GuardPoint]**

Missing CTE-LDT extended attribute

The following warning message reports that the file with the specified inode number in the specified GuardPoint directory does not have an CTE-LDT extended attribute, therefore, access to the file is denied.

- **LDT: Extended attribute of inode [InodeNumber] is missing under GuardPoint [GuardPoint]**

Solution: CTE-LDT cannot determine the encryption key associated with the data in the file, therefore, you can only remove the file.

Locking Contention

The following messages are recorded during the rekey process on a file. When user access to the file is very high, it causes a high degree of locking contention between the rekey process and user access. The second message reports when the contention is no longer in effect and the rekey process has resumed accessing file to rekey.

- **LDT: Exclusive access for rekey delayed on inode [InodeNumber]**
- **LDT: Exclusive access for rekey granted after delay on inode [InodeNumber]**

Initiation and completion of CTE-LDT metadata cleanup

The following messages are recorded at the beginning and completion of CTE-LDT metadata cleanup through voradmin command.

- **LDT: Metadata will start getting removed from all files in GuardPoint [GuardPoint]**
- **LDT: Metadata has been removed from all files in GuardPoint [GuardPoint]**

Recommendations and Considerations

The following information provides guidance for a better user experience.

All Platform Recommendations and Considerations

Binary Re-signing

Any executable that is part of either a Signature set or a Host setting, and that resides in a GuardPoint that uses an CTE-LDT policy, will use different signatures for an CTE-LDT key rotation. The result is that the Host Settings binaries will no longer be authenticated, or that the Signature Set policy rules will no longer trigger for those binaries.

To prevent these issues, the Security Administrator must manually re-sign each affected binary after each key rotation.

Alternatively, CTE can generate unencrypted signatures of binaries inside GuardPoints to avoid these problems. For details, see the CipherTrust Manager documentation.

Check for available disk space for CTE-LDT metadata

Before launching CTE-LDT on a GuardPoint:

1. Check the available free disk space in the file system where your GuardPoint resides.
2. Type the following command to check the disk space requirement of CTE-LDT on a target GuardPoint:

```
# voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 1501 files without LDT extended attributes
LDT disk space requirements: total 169MB (LDT attributes=6MB, MDS=163MB)
```

In this example, the output shows that CTE-LDT requires 169MB of available disk space to launch and execute CTE-LDT on /oxf-fs1/gp1.

Note

Make sure that the free space in your file system exceeds the disk space requirement for CTE-LDT.

CTE-LDT Requirements for Backup

CTE offers the option to backup encrypted data from files through a security rule, which skips the Apply Key function when reading encrypted files by backup applications or processes. Such files can also be restored from backup streams, to the same or a different GuardPoint, without Apply Key. If you choose to restore to another GuardPoint, the target GuardPoint must be protected with the same key and security rules as the source GuardPoint.

If you backup encrypted data from files inside GuardPoints with CTE-LDT policies, CTE-LDT imposes a hard requirement on the backup application, or process, to backup or restore CTE-LDT metadata. The CTE-LDT metadata is stored as an extended attribute on Linux and as alternate data streams on files on Windows platforms. If the backup process cannot backup the metadata, then CTE-LDT protected GuardPoints must be backed up in clear key.

Customers are required to verify their backup application, or process, to ensure extended attributes (on Linux) or alternate data streams (on Windows) are backed up and restored through their backup/restore processes.

Note

Make sure that you suspend CTE-LDT operations before you start the backup process, and resume them after the backup process completes.

Learn Mode

Learn Mode provides a temporary method for disabling the blocking behavior of regular CTE or CTE-LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set.

Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption.

Note

Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.

Quality of Service (QoS)

By default, the QoS component of CTE-LDT does not monitor live transformation operations unless you enable QoS on your host by entering QoS parameters in the CipherTrust Manager profile associated with the client. To avoid overhead of CTE-LDT on your production system, you must select QoS parameters suitable to your production environment. For information on tuning QoS, see ["Quality of Service" on page 29](#). It is critical that you understand the impact of CTE-LDT on your system and how to manage this impact using QoS.

Upgrade to CTE 7.0.0

Since the first release of the CTE-LDT feature, Thales has made several improvements in the areas of error handling, interoperability with applications, and Quality of Service (QoS). Thales strongly recommends that new deployments use version 7.0.0 (or later) of CTE. Thales further recommends that customers who have already deployed the CTE-LDT feature upgrade to version 7.0.0.

Windows Recommendations and Considerations

File Handling

The CTE-LDT process is subjected to all of the File System policies and attributes set on the files. In some cases, this prevents CTE-LDT from encrypting a file. If users or applications are accessing files while CTE-LDT is in progress, CTE-LDT cannot change the attributes of the files and encrypt the file. It is critical that you understand how CTE-LDT handles various types of files:

- **NTFS Encryption and Compression**

If NTFS encryption or compression is enabled on a file or folder, the CTE-LDT process cannot encrypt these files. To maintain the data coherency, CTE-LDT skips the encryption of these files. These files display as "passthrough" files in the CTE-LDT statistics.

- **Read-Only Files**

As the CTE-LDT process performs a read-encrypt-write operation on a file, it cannot encrypt read-only files. The CTE-LDT process skips these files and changes to the INCOMPLETE state.

- **Executable Files**

If an executable is running or files are exclusively locked by the application, the CTE-LDT process cannot encrypt those files as it is unable to acquire the required locks on the files. CTE-LDT skips these files and changes to the INCOMPLETE state.

File Modification

The CTE-LDT process performs a read-encrypt-write operation on the files that need to be encrypted, (also known as rekeying). Previously, file modification and access dates were changed when CTE-LDT was processing. In order to maintain compatibility for applications, we addressed this issue by saving a copy of the original access and modification times, and restoring them after the encryption completed. Preserved timestamps are updated during the rekey process, if an application/user accesses the files during rekey.

Note

Thales strongly recommends that you upgrade to the newly released v6.1.0 so that the access time and modification time is restored correctly.

CTE-LDT Limitations

- CTE-LDT on CIFS is not supported.
- CTE-LDT on a ReFS file system runs slowly because of limited support from the Extended Attributes on the ReFS file system.

Note

Customers running older versions of ReFS.sys on Windows Server 2012 R2 should be aware of the memory growth issue encountered by the Thales engineering team. This issue seems to occur only when CTE-LDT is running on a large number of files. As the system memory consumption by REFS file system increases, it can eventually make the system unresponsive. This issue does not occur with the recent versions of ReFS file system drivers available on Windows Server 2016. After consulting with Microsoft, they suggest that all customers migrate to Windows Server 2016 if they are using ReFS file.

Logical Sector Size

CTE-LDT Windows transformation is supported if the **logical sector size** is more than 512 Bytes. (A logical sector size of 4K is supported.) To find the logical sector size of the file system, type:

```
> fsutil fsinfo ntfsInfo <volume pathname>
```

For example:

```
> fsutil fsinfo ntfsInfo C:
NTFS Volume Serial Number :      0x5092568a92567506
NTFS Version      :              3.1
LFS Version      :              2.0
Number Sectors :      0x000000001c004eeb
Total Clusters :      0x00000000038009dd
Free Clusters  :      0x00000000008bb274
Total Reserved :      0x0000000000001864
Bytes Per Sector :              512
.
.
.
```

CTE-LDT Limitations on Linux

- CTE-LDT on NFS share is not supported.
- CTE-LDT support is limited to `ext3`, `ext4`, `XFS`, and `VxFS` file systems when `user_xattr` mount option is enabled.

CipherTrust Transparent Encryption

CTE-Live Data Transformation with Data Security Manager

Release 7.0.0

Document Version 1

September 22, 2020

The bottom half of the page features a dark blue background with abstract geometric shapes. On the left, there is a large, bright blue triangle pointing upwards. Below it, a smaller, darker blue triangle points upwards. In the bottom left corner, there is a blue circular shape with a dotted pattern. The right side of the page has a vertical gradient bar and a dotted pattern at the bottom.

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2009-2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Contents

Preface	9
Intended Audience	9
Assumptions	9
The CTE Agent Documentation Set	9
Document Conventions	10
Typographical Conventions	10
Notes, tips, cautions, and warnings	10
Sales and Support	11
 Chapter 1: Introduction to CTE-LDT	 12
Overview of CTE-LDT	12
Use Cases	12
Keys in CTE-LDT (Versioned Keys)	13
Rekey Key Rotation	13
CTE-LDT Policies	14
CTE-LDT Runtime Flow	14
CTE-LDT Administrator Roles	16
Resiliency	17
 Chapter 2: Getting Started	 18
Using CTE-LDT	18
Backup/Restore	19
Restrictions	19
Windows Only Limitations	19
Linux Only Limitations	19
 Chapter 3: Setting Up CTE-LDT	 20
System Requirements	20
CipherTrust Software Requirements	20
CTE-LDT License Requirements	20
Host System Requirements	20
Backup Requirements	20
Linux-Specific Requirements	21
Supported Applications in Linux	21
Replication	21
SAP HANA Fibre Channel Systems	21
Installing the CTE-LDT License	21
Installing and Registering the CTE Agent Software	22

Setting the Linux Kernel Time Zone	25
Enabling CTE-LDT on a Protected Host	25
Chapter 4: Using CTE-LDT	27
Creating and Viewing Versioned Keys	27
Creating a New Versioned Key for CTE-LDT	27
Viewing Versioned Key Information	28
Creating CTE-LDT Policies	29
Quality of Service	30
Purpose of QoS	30
Manage CTE-LDT Impact	31
Monitor and Control CPU Usage	31
Monitor and Control Rekey/Scan I/O Rate	31
Monitor and Control I/O Wait Time (Linux only)	32
QoS Scheduling During Backup/Restore	32
How to Set QoS	33
Creating a Custom QoS Schedule	34
QoS Best Practices	34
General Best Practices for QoS	34
Determine and Set the I/O wait time	37
Select and Set Rekey I/O Rate	39
Create an CTE-LDT GuardPoint	41
Create an CTE-LDT GuardPoint for an Unguarded Directory	42
Converting a Non-CTE-LDT GuardPoint to an CTE-LDT GuardPoint	43
Rotating Encryption Keys (Rekey)	44
Manual Key Rotation	44
Checking the Rekey Status	44
Obtaining Information About Keys Applied to Files	45
Key Report Option	45
Key Map Option	46
Showing GuardPoints During Rekey (Linux)	46
Suspending and Resuming Rekey and/or Scan Phase	46
Considerations	47
Automatic Suspend and Resume of CTE-LDT Operations Due to Insufficient Disk Space (Linux) ...	47
Behavior of Automatic Suspend and Resume of CTE-LDT Operations on ext4 File Systems	47
Rotating Encryption Keys While a Rekey is in Progress (Relaunch)	47
File System Operations	48
Renaming Files and Folders	48
Deleting a File	48
File Handling (Windows Only)	48

Enabling GuardPoints in Read-Only mounted file systems (Linux)	49
Copying Files Into a GuardPoint	49
Behavior of Hard Links Inside and Outside of GuardPoints (Windows)	50
Excluding Files or Directories from Rekey	50
Examples of Exclusion Key Rules	50
Encrypt Files With Exclusion Property a Non-Versioned Key	50
Exempt Excluded Files from Encryption (Set to clear_key)	51
Requirements for Exclusion Key Rules	51
Usage Notes and Limitations for Configuring Exclusion Key Rules	51
Adding an Exclusion Key Rule to an Existing Policy with Versioned Keys (Linux)	51
Adding an Exclusion Key Rule That is Part of an Active GuardPoint (Linux)	52
Changing an Exclusion Key Rule That is Part of an Active GuardPoint (Windows)	52
Conflicting Keys as the Result of Rename Operations	52
Overlapping Exclusion Key Rules	52
Caution About Applications That Create Temporary Files (Windows)	53
Rename Operations Crossing Key Rules (Linux)	53
Using Linked Files with Exclusion Key Rules (Linux)	53
Changing a Folder or Files from Versioned to Non-Versioned Key (Windows)	53
About the Exclusion Attribute for Files Matching an Exclusion Key Rule	54
The Exclusion Attribute is Persistent	54
Determining if a File is Included in an Exclusion Key Rule	55
Removing the Exclusion Attribute From a File	55
Rename and Restore Operations (Linux)	55
Listing All Files Included in an Exclusion Key Rule (Linux)	57
Listing All Files Included in an Exclusion Key Rule (Windows)	57
Using CTE-LDT with SAP HANA Fibre Channel Systems (Linux Only)	58
Chapter 5: CTE-LDT Administration	59
CTE-LDT Metadata in Extended Attributes	59
Listing Extended Attributes	60
MDS File (Linux)	61
Planning for CTE-LDT Attribute Storage	62
Using voradmin To Estimate Disk Space Required for CTE-LDT (Linux)	62
Displaying Metadata	63
Verifying Metadata (Windows only)	63
DFSR and Replication (Windows)	63
Multi-Node Configuration and Operation	64
CTE-LDT Behavior on Failover	64
Veritas Cluster Server	64
Backing Up and Restoring CTE-LDT GuardPoints	64

Clear Text Backup and Restore	64
Encrypted Backup and Restore	64
CTE-LDT Policy for Encrypted Backup and Restore	65
Backup/Restore of Metadata Store File (MDS) in GuardPoints Undergoing Rekey	66
Restoring a GuardPoint from a Backup	67
Potential Warnings During Restore Operation	68
Restore an Encrypted Backup	68
Restore a File Fully Rekeyed to the Latest Key Version	68
Restore a Partially Rekeyed/encrypted File	69
Restore a File Not Rekeyed/encrypted with an Older Key Version	69
Restoring Non-CTE-LDT Backup Data to an CTE-LDT GuardPoint	70
Using fsfreeze (Linux only)	70
CTE-LDT Backups Using a File System or Storage-Level Snapshot Tool	71
Windows Backup and Snapshots	72
Restoring ESXi VM Snapshots of a Protected Host	72
CTE-LDT Backup and Restore Troubleshooting	73
Restored files to a GuardPoint protected with conflicting key rules	73
CTE-LDT Command-Line Administration: voradmin command	73
Upgrading or Downgrading Agent Software On an CTE-LDT Host	74
Upgrading	74
Downgrading	74
Moving a CTE-LDT GuardPoint from One CTE-LDT Policy to Another	75
Scenario	75
Removing CTE-LDT and Security Encryption	76
Migrating a GuardPoint Out of CTE-LDT	76
Converting a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy	76
Remove Protection from a GuardPoint	77
Deleting CTE-LDT Metadata (Linux)	79
Deleting CTE-LDT Metadata (Windows)	80
Removing CTE-LDT from a Host	80
Uninstalling the Agent while CTE-LDT is Rekeying GuardPoints	80
Chapter 6: Troubleshooting CTE-LDT	81
Monitoring and Statistics	81
Obtaining Statistics in the DSM with GuardPoint Status	81
Obtaining CTE-LDT Statistics at the Command Line	83
Obtaining a Rekey Report	83
About the rekey report	83
Manually generating a rekey report	84
Monitoring Ongoing CTE-LDT Operations at the Command Line (Windows only)	84

Protecting CTE-LDT GuardPoints against Failure in Underlying Filesystems (Linux)	84
CTE-LDT Recovery Challenges	84
CTE-LDT Recovery Enhancement	84
Recovery Alerts	85
Alerts Playbook	85
Failure to Suspend or Resume CTE-LDT Operation	86
Insufficient Resources	86
Failed to Update CTE-LDT Attribute	87
Rekey Stopped	87
Incomplete Key Rotation	88
Skipped Key Rotation	88
Failed to Update CTE-LDT Metadata During Scan Phase	89
File system inconsistencies after system crash	89
Error Messages	90
Failed to Transform File During Rekey	90
Failure to Suspend CTE-LDT	90
Failure to Start or Stop Transformation	90
Failure to Restart Transformation	91
Temporary Failure to Start Transformation on a File	91
Transient Condition while enabling GuardPoint	91
Failed to transform passthrough files for AD database files (Windows Only)	91
Warning and Info Messages	92
Stopping Transformation of a File on Volume Dismount (Windows only)	92
Issues with Policy or System Configuration	92
Failure to Enable GuardPoint During Cleanup	92
General CTE-LDT Operations	92
Missing CTE-LDT extended attribute	92
Locking Contention	93
Initiation and completion of CTE-LDT metadata cleanup	93
Upgrading CTE Agent	93
Recommendations and Considerations	93
All Platform Recommendations and Considerations	93
Binary Re-signing	93
Check for available disk space for CTE-LDT metadata	94
CTE-LDT Requirements for Backup	94
Learn Mode	94
Quality of Service (QoS)	95
Upgrade to CTE 7.0.0	95
Windows Recommendations and Considerations	95
File Handling	95

File Modification	95
CTE-LDT Limitations	96
Logical Sector Size	96
Upgrade Notes	96
VSS Volumes	96
CTE-LDT Limitations on Linux	97

Preface

CTE-Live Data Transformation with Data Security Manager describes how to configure and use CipherTrust Transparent Encryption - Live Data Transformation (CTE-LDT) when the host is registered to a Vormetric Data Security Manager (DSM). If you want to use CipherTrust Manager as your key manager, see the *CTE-Live Data Transformation with CipherTrust Manager* guide.

CTE-LDT is an optional, separately licensed feature of CipherTrust Transparent Encryption (CTE). With CTE-LDT, a DSM Administrator can change the encryption key and re-encrypt GuardPoint data without suspending user or application access to the data.

Intended Audience

CTE-Live Data Transformation with Data Security Manager is for security teams who want to rekey the existing GuardPoint data, or who need to perform an initial encryption of their GuardPoint data.

Assumptions

CipherTrust Transparent Encryption - Live Data Transformation is an enhancement to existing functionality. This documentation assumes the reader is familiar with the following CipherTrust products and processes:

- Vormetric Data Security Manager (DSM)
- CipherTrust Transparent Encryption (CTE)
- Key management
- Data encryption

The CTE Agent Documentation Set

The following guides are available for CTE Agent:

- *CTE Agent for Linux Quick Start Guide*
- *CTE Agent for Linux Advanced Configuration and Integration Guide*
- *CTE Agent for Windows Quick Start Guide*
- *CTE Agent for Windows Advanced Configuration and Integration Guide*
- *CTE Agent for AIX Installation and Configuration Guide*
- *CTE-Live Data Transformation with Data Security Manager*
- *CTE-Live Data Transformation with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with Data Security Manager*
- *Compatibility Matrix for CTE Agent for AIX with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent for AIX with Data Security Manager*
- *Release Notes for CTE for Linux Version 7.0.0.47*
- *Release Notes for CTE for Windows Version 7.0.0.47*
- *Release Notes for CTE for AIX Version 7.0.0.11*

Document Conventions

The document conventions describe common typographical conventions and important notice and warning formats used in Thales technical publications.

Typographical Conventions

This section lists the common typographical conventions for Thales technical publications.

Table 3-1: Typographical Conventions

Convention	Usage	Example
bold regular font	GUI labels and options.	Click the System tab and select General Preferences.
<i>bold italic monospaced font</i>	variables or text to be replaced	https://<Token Server name>/admin/ Enter password: <Password>
<code>regular monospaced font</code>	Command and code examples XML examples	Example: session start iptarget=192.168.253.102
<i>italic regular font</i>	GUI dialog box titles	The <i>General Preferences</i> window opens.
	File names, paths, and directories	/usr/bin/
	Emphasis	<i>Do not</i> resize the page.
	New terminology	<i>Key Management Interoperability Protocol (KMIP)</i>
	Document titles	See <i>CTE-Live Data Transformation with Data Security Manager</i> for information about CipherTrust Transparent Encryption.
quotes	File extensions Attribute values Terms used in special senses	"js", ".ext" "true" "false", "0" "1+1" hot standby failover

Notes, tips, cautions, and warnings

Notes, tips, cautions, and warning statements may be used in this document.

A Note provides guidance or a recommendation, emphasizes important information, or provides a reference to related information. For example:

Note

It is recommended to keep tokenization keys separate from the other encryption/decryption keys.

A tip is used to highlight information that helps you complete a task more efficiently, such as a best practice or an alternate method of performing the task.

Tip

You can also use Ctrl+C to copy and Ctrl+P to paste.

Caution statements are used to alert you to important information that may help prevent unexpected results or data loss. For example:



CAUTION

Make a note of this passphrase. If you lose it, the card will be unusable.

A warning statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data. For example:



WARNING

Do not delete keys without first backing them up. All data that has been encrypted with deleted keys cannot be restored or accessed once the keys are gone.

Sales and Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

For support and troubleshooting issues:

- <https://supportportal.thalesgroup.com>
- (800) 545-6608

For Thales Sales:

- <https://cpl.thalesgroup.com/>
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

Chapter 1: Introduction to CTE-LDT

This chapter contains the following sections:

Overview of CTE-LDT	12
Keys in CTE-LDT (Versioned Keys)	13
CTE-LDT Policies	14
CTE-LDT Runtime Flow	14
CTE-LDT Administrator Roles	16
Resiliency	17

Overview of CTE-LDT

CipherTrust Transparent Encryption - Live Data Transformation (CTE-LDT) is an optional, separately licensed feature of CipherTrust Transparent Encryption (CTE). With CTE-LDT, after enabling a GuardPoint, a DSM Administrator can encrypt, or rekey, GuardPoint data without blocking user or application access to the data. In CTE-LDT, *rekey* means decrypting data with the current cryptographic key and then encrypting it with a new cryptographic key. The concept of rekey, and how CTE-LDT rekeys data, is described in this document.

After enabling GuardPoints, CTE-LDT performs *initial* encryption or rekeying in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block application and user access to data during encryption or rekey operations, which can seriously inconvenience users and affect operational efficiency.

With CTE-LDT, the DSM Administrator can create a single CTE-LDT policy for both initial encryption and subsequent rekeying. The same policy applies to production access and security rules without restricting user or application access to data. Applications have continuity of access to GuardPoint data during CTE-LDT.



WARNING

To prevent data loss or corruption, you must stop all applications and users that are accessing files inside a GuardPoint before enabling a Live Data Transformation encryption policy for that GuardPoint. Terminating the applications closes all files that are currently being accessed inside the GuardPoint.

Unlike non-Live Data Transformation policies, however, you do *not* need to keep the GuardPoint offline while data transformation takes place. Instead, you can restart all applications as soon as the GuardPoint has been applied to the host, and CTE will perform the data encryption in the background. This is the only application service downtime required when using CTE-LDT.

Use Cases

This section provides a summary of typical uses for CTE-LDT. The concepts mentioned in this section are described in more detail throughout the rest of this guide.

1. Encrypt unprotected data.

When protecting files in a directory, you must encrypt them. This process is called *initial data encryption*.

2. Convert non-CTE-LDT GuardPoints to CTE-LDT GuardPoints

Use when you have existing GuardPoints that are protected with policies created before you started using CTE-LDT.

3. Rekey process.

Changing the key from one version to another version of the same key provides more security. Using CTE-LDT, you can change the encryption keys to more secure keys.

4. Transform the encrypted data to clear data.

Keys in CTE-LDT (Versioned Keys)

CTE-LDT uses *versioned* keys. Each version of a particular versioned key has the same key name and encryption algorithm, but its own unique cryptographic material. That means that data encrypted with version 3 of a key named `LDT-Key` *cannot* be decrypted by *any* other version of `LDT-Key`, even though the key name remains the same.

Versioning allows you to add one key to your CTE-LDT encryption policy and then use different versions of that same key to periodically re-encrypt your data over time. CTE-LDT uses the new key material to transform data to the new key version, as part of the same Live Data Transformation policy that also protects the data. The process of re-encrypting data with a new version of the existing key is called *Key Rotation*.

When you create a versioned key in the DSM, you set its *life span*. The life span is the duration (in days) of the versioned key. You also define an *initial expiration date*. When the key reaches its expiration date, it automatically rotates to a new version. After that it rotates every time its life span ends. For example, if you set an initial expiration date of October 10, 2021 and a life span of 10 days, the data will be automatically rekeyed first on October 10th and then on October 20th, October 30th, and so on.

Versioned keys all have the same properties as non-versioned keys, plus three additional required properties:

- **Automatic Key Rotation:** Always select this option to make the key automatically rotate. Selecting this option tells the DSM that the key is a versioned key.
- **Key Version Life Span (days):** Frequency of key rotation in days. Applies only if Automatic Key Rotation is selected.
- **Expiration Date:** CTE-LDT uses the initial version of the key until this date occurs. On the expiration date, CTE-LDT creates a new key version. Subsequently, it creates new versions based on the Key Version Life Span.



WARNING

You *must* specify the Expiration Date. Without an Expiration Date, a versioned key never rotates from the initial key version, and consequently, never triggers CTE-LDT.

Rekey | Key Rotation

In CTE-LDT, *rekeying* or *key rotation* means decrypting the data with a previous version of the key and re-encrypting it with a new version of the key. CTE-LDT allows users and applications to access data while CTE-LDT is rekeying the data. Rotating the key and re-encrypting the GuardPoint data with the new version of the key helps to maintain a high level of data security.

Most often, the rekey happens automatically, because each versioned key has a Key Version Life Span that specifies the lifespan of the key. In addition to this automatic key version rotation, you can manually generate a new version of the current key if a new version is required.

For more information, see:

- ["Creating and Viewing Versioned Keys" on page 27](#)
- ["Rotating Encryption Keys \(Rekey\)" on page 44](#)

CTE-LDT Policies

In CTE-LDT, you define a single policy for initial data encryption and subsequent rekeying. The policy specifies:

- **Current key**

Associated with data that you want to protect using CTE-LDT. This is either a non-versioned key from an earlier policy, or `clear_key`, which means that the data is not currently encrypted.

- **Transformation key**

The versioned key that CTE-LDT applies to transform the data from the key used for initial data transformation. When the transformation key rotates, it transforms the data from a previous version of the transformation key to a new version.

Note

Transformation key and versioned key are used interchangeably throughout this document.

As soon as CTE-LDT applies the policy to a GuardPoint and enables protection for it, CTE-LDT triggers an initial transformation from the current key to the transformation key.

Note

With DSM 6.1 or later, you may select current or transformation keys for CBC or CBC-CS1 encryption modes.

When the transformation key expires, it generates the next version of the versioned key with new cryptographic material. The DSM then pushes the policy to the hosts. The policy now contains the new version of the key. This initiates a rekey process on the GuardPoint to transform data to the new version of the transformation key specified in the policy.

Users and applications can continue accessing data without any interruption during initial encryption and subsequent key transformations.

Note

During CTE-LDT policy creation, you must use the Apply Key effect in your policy. If you do not, then end users can see the clear text data until the file is transformed.

CTE-LDT Runtime Flow

This section presents an overview of how CTE-LDT works and what to expect when CTE-LDT is enabled and running in your environment. All of the tasks mentioned here are described in more detail later in this chapter.

First, the administrator completes CTE-LDT setup:

1. Upload the CTE-LDT license on the DSM.
2. Register CTE-LDT hosts with the DSM and be sure that the hosts are licensed for CTE-LDT.
3. Create one or more versioned keys.
For each key, specify **Automatic Key Rotation**, the **Expiration Date**, and the **Key Version Life Span**.
4. Define Live Data Transformation policies which use the versioned key(s) and contain rules governing CTE-LDT operations.

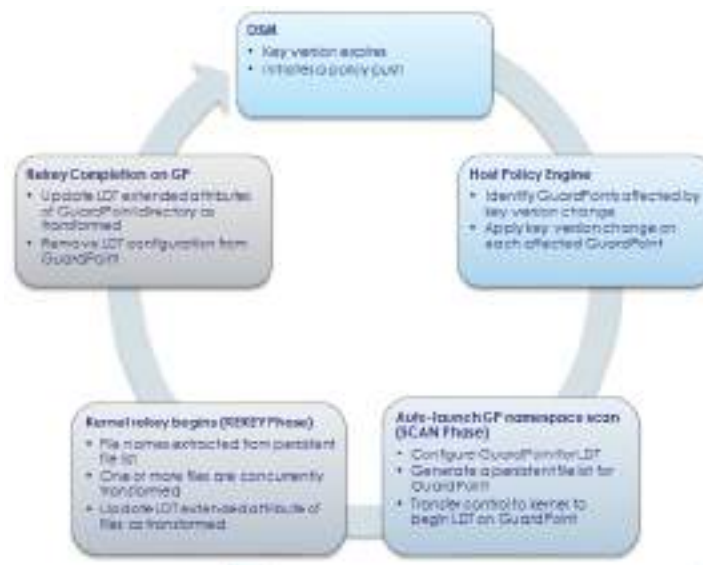
5. Optionally provide Quality of Service (QoS) settings for the CTE-LDT hosts. The QoS settings control the:
 - Window of time in which CTE-LDT operations are allowed to run.
 - Percentage of CPU resources that CTE-LDT can use, or the amount of data to transform according to the QoS setting per the DSM Administrator.

Note: Configuring the QoS settings is highly recommended as a best practice.

When these items are set up, CTE-LDT is ready to transform and encrypt data by applying policies to GuardPoints for live initial transformation and subsequent rekeys, as well as enforcement of security rules.

The following figure shows the sequence of events during ongoing usage of CTE-LDT.

Figure 1-1: Phases of CTE-LDT runtime operation after keys and policies are defined



1. Initial data transformation starts or key expires

CTE-LDT begins when an Live Data Transformation policy is first applied to a GuardPoint or when a current key version expires. The DSM pushes the new policy, or the notification of a key version change, to the hosts that are protected by the policy. (If the same versioned key is used in multiple policies, *all* of the hosts associated with the policies that contain the key are notified when the key changes.)

2. New key version triggers a rekey on the affected GuardPoints

On each host, CTE determines which GuardPoints are using the key that has just rotated to a new version. CTE starts an CTE-LDT rekey on each of those GuardPoints.

On Windows, you must wait for the current key rotation process to finish before you can launch another rekey request. On Linux, if another rekey is already underway on that GuardPoint, the new rekey is queued for later execution. For details, see ["Rotating Encryption Keys While a Rekey is in Progress \(Relaunch\)" on page 47](#).

3. Scan for files

On each GuardPoint where CTE has started a rekey, CTE-LDT determines which files to transform. CTE-LDT takes inventory of files encrypted with earlier versions of the rotated key and makes a persistent list of the files for transformation. During this phase, the Rekey Status in the GuardPoint Status window of the DSM Management Console displays Starting, then Scanning.

The scan phase might be interrupted, such as by a host reboot. In this case, when the host reboots and the GuardPoint is enabled again, the scan operation starts over from the beginning.

4. Rekey/Key Rotation

- a. Each file, from the persistent list of files, is decrypted using the old version of the key. The old key is applied to each file and then re-encrypted using the new version of the key. Note that new files created during the CTE-LDT process do not need to be rekeyed, as they inherit the new version of the key. Multiple files and multiple regions of files are rekeyed simultaneously.
- b. The CTE-LDT extended attribute of each file is updated. (For more about extended attributes, see ["CTE-LDT Metadata in Extended Attributes" on page 59.](#))
- c. You can suspend and resume the CTE-LDT rekey operation manually, or through the QoS schedule. This manages the impact CTE-LDT has on other applications and processes.

During this phase, the Rekey Status in the GuardPoint Status window of the DSM Management Console shows Rekeying or Suspended.

If system errors occur during rekeying, such as IO errors or crashes, CTE-LDT can manage and recover from them after the system error is fixed.

5. Finish

When all of the required files in the GuardPoint have been rekeyed, the system and storage resources used by CTE-LDT are released, except for the storage required for the extended attributes.

CTE-LDT creates a rekey report, listing all of the files that were rekeyed. For more information, see ["Obtaining a Rekey Report" on page 83.](#)

Upon completion of rekey, the Rekey Status in the GuardPoint Status window of the DSM Management Console shows Rekeyed.

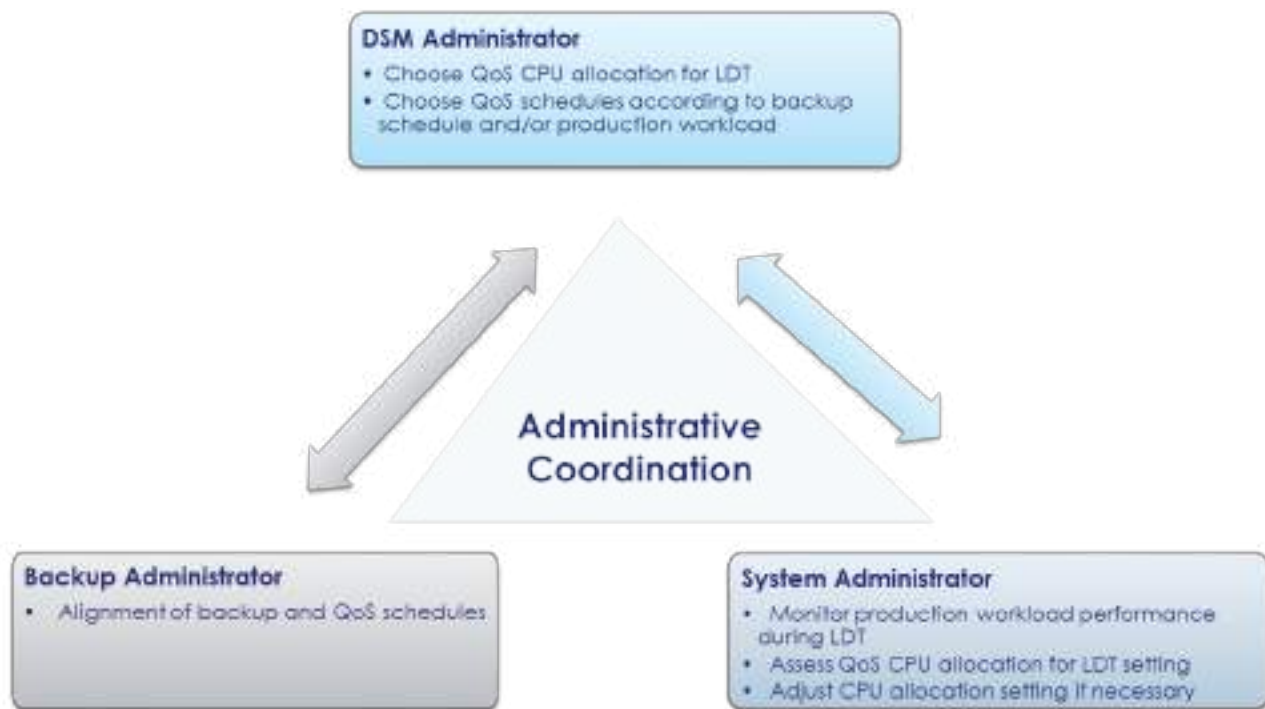
CTE-LDT Administrator Roles

Using CTE-LDT requires coordination and collaboration between several different administrators. Security, system, application performance and backup schedules are critical factors that affect planning. It is very important for the **DSM Security Administrator** to coordinate with the **system administrator** and the **backup administrators**. The following table describes the roles and responsibilities for these administrators.

CTE-LDT Administrators

Role	Responsibility	Actions
DSM Security Administrator	Administers Vormetric Data Security Manager (DSM)	Coordinates with system and backup administrators. Creates security policies and rules for CTE-LDT. Defines Quality of Service settings for CTE-LDT, applications, and backups.
System administrator	Administers servers on which CipherTrust Transparent Encryption (CTE) is deployed	Coordinates with the DSM Security Administrator to create Quality of Service schedule, taking into consideration the backup schedules.
Backup administrator	Manages data backups for data encrypted by CTE	Coordinates with the DSM Security Administrator to create Quality of Service schedule, taking into consideration the backup schedules.

The following process is recommended for coordination between the various administrators in order to achieve optimal QoS schedule settings and allocation of CPU resources when using CTE-LDT.



Resiliency

CipherTrust Transparent Encryption - Live Data Transformation is resilient to many user actions and system occurrences. Since it is designed to run periodically without intervention, it includes various features to provide this resilience.

Before CTE-LDT enables a GuardPoint, it checks for any inconsistencies in files that were undergoing rekey at the time when system operations were interrupted. If it finds any inconsistencies, CTE-LDT corrects them before it enables the GuardPoint. It should only take a few seconds to identify and correct any inconsistency. On Windows, this process is delayed until applications access the affected files.

During rekey, if an issue such as an I/O problem or system crash occurs, the resiliency features of CTE-LDT ensures the consistency of user data. Such issues can cause an interruption in the middle of a rekey operation. When system operations resume, CTE-LDT corrects the problems and then resumes rekeying.

Chapter 2: Getting Started

This chapter contains the following sections:

Using CTE-LDT	18
Backup/Restore	19
Restrictions	19

Using CTE-LDT

Notes

- If you are new to CTE and CTE-LDT, read the *DSM Administration Guide* first to familiarize yourself with the concepts of GuardPoints and Policies.
- Before installing CTE-LDT, see the *Compatibility Matrix for CTE Agent with Data Security Manager* to verify that your version of Linux is supported. Contact Thales Technical Support (<https://supportportal.thalesgroup.com>) for the matrix.

The following list contains the steps for successfully setting up and using CTE-LDT.

1. Install the CTE-LDT License on the DSM.
CipherTrust Transparent Encryption - Live Data Transformation is a separately-licensed feature of CTE. Before you can use it, you have to install the license to activate it. CTE-LDT is licensed for a specific number of hosts. For details about licensing, see the *DSM Administration Guide*.
2. Install the CTE Agent and select the CTE-LDT feature during the install. For more information, see ["Installing and Registering the CTE Agent Software" on page 22](#).
If the host is already registered, you can enable CTE-LDT through the DSM Management Console. For details, see ["Enabling CTE-LDT on a Protected Host" on page 25](#).
3. Create Versioned Keys.
CTE-LDT uses *versioned keys*. A versioned key rotates to the next version of the key generating new key material automatically without policy change. CTE-LDT encrypts data with keys that use encryption standards like AES-128 and AES-256. This allows data to be re-encrypted without users having to edit the policy.
For more information, see ["Keys in CTE-LDT \(Versioned Keys\)" on page 13](#) and ["Creating and Viewing Versioned Keys" on page 27](#).
4. Create CTE-LDT Policies.
CTE-LDT uses a single Live Data Transformation policy to address both initial encryption and subsequent rekeying. The same policy applies to production access and security rules without restricting user or application access to data. Applications have continuity of access to GuardPoint data during CTE-LDT.
For more information, see ["Creating CTE-LDT Policies" on page 29](#).
5. Set QoS Settings.
QoS enables administrators to manage and control CTE-LDT impact to application workloads by monitoring and controlling the use of host system resources, such as memory or I/O utilization, during CipherTrust Transparent Encryption - Live Data Transformation. Administrators can also choose schedules for data transformation, or manually pause or resume transformation operations.
For more information, see ["Quality of Service" on page 30](#).

6. Create GuardPoints and Apply CTE-LDT policies to the GuardPoints

A GuardPoint is a directory in the file system hierarchy, where its contents have a CipherTrust data protection policy applied to it. The CTE Agent intercepts any attempt to access anything in the GuardPoint and uses the policies obtained from the DSM to grant or deny the access attempt. Typically data copied into a GuardPoint is encrypted, and only authorized users can decrypt and use that GuardPoint data.

For more information, see ["Create an CTE-LDT GuardPoint" on page 41](#).

Backup/Restore

Before you enable GP with CTE-LDT policies, make sure that you back up your data.

For more information, see ["Backing Up and Restoring CTE-LDT GuardPoints" on page 64](#).

Restrictions

Remember the following restrictions when using CTE-LDT:

- CTE-LDT does not support nested GuardPoints, where a GuardPoint is contained inside another GuardPoint.
- For HA clusters, CTE-LDT only supports the Asymmetric (active/passive) configuration. CTE-LDT does not support Symmetric (active/active) configuration.

Windows Only Limitations

CTE-LDT does not support GuardPoints on CIFS network shared directories.

Linux Only Limitations

- CTE-LDT does not support Linux automounted file systems.
- CTE-LDT does not support system hibernation (`pm-hibernate`) on Linux hosts where CTE-LDT is in use.
- CTE-LDT does not support GuardPoints on NFS shares and `secvm` configured devices.
- Do not use CTE-LDT on GuardPoints over XFS and VxFS file systems at the same time.
- You cannot use CTE-LDT and Docker container on the same host.
- You cannot use CTE-LDT and OpenShift container on the same host.

Chapter 3: Setting Up CTE-LDT

This chapter contains the following sections:

System Requirements	20
Installing the CTE-LDT License	21
Installing and Registering the CTE Agent Software	22
Setting the Linux Kernel Time Zone	25
Enabling CTE-LDT on a Protected Host	25

System Requirements

CipherTrust Transparent Encryption - Live Data Transformation (CTE-LDT) requires the following environment.

Note

See the latest *Compatibility Matrix for CTE Agent with Data Security Manager*, in the online support portal, for a list of CTE versions and supported operating systems.

CipherTrust Software Requirements

Platform	CTE Agent Version	DSM Version
Linux	VTE Agent version 6.0.0 or higher or CTE Agent version 7.0 or higher installed on each protected host.	DSM version 6.0 or higher.
Windows	VTE Agent version 6.1.0 or higher or CTE Agent version 7.0 or higher installed on each protected host.	DSM version 6.1.x or higher.

CTE-LDT License Requirements

One CTE-LDT license is required for *each* protected host.

Host System Requirements

Memory requirements: Both Linux and Windows require a minimum of 8 GB memory on each protected host.

Disk space requirements: CTE-LDT requires a specific amount of disk space in the file system, over and above the space required for the guarded files themselves. CTE-LDT uses the additional space to store CTE-LDT metadata.

- For Linux, to estimate the amount of free file system disk space required by CTE-LDT on a Linux host, use the `voradmin ldt space` command.
- For Windows, the typical minimum space requirement for a GuardPoint is the number of files in the GuardPoint multiplied by 4K, plus 256MB. To estimate the amount of free space required for a GuardPoint, use the `voradmin ldt space <GuardPoint-name>` command.

Backup Requirements

The backup application must have the capability to back up user-extended attributes. For example, Thales tested CTE-LDT with NetBackup. You can also use other applications that can back up user-extended attributes.

Note

For Windows, the application must use Volume Shadow Copy service (VSS) for backup and restore.

Linux-Specific Requirements

To use CTE-LDT on an ext3 or ext4 file system, the block size **must** be 4K. Run `dumpe2fs` to determine the block size of the ext3 or ext4 file systems before using CTE-LDT. This limitation does not apply to XFS or VxFS file systems. You can use CTE-LDT on XFS with a block size of 1K or 2K.

For CTE-LDT to work properly, the underlying file system must support and enable user-extended attributes. All of the file systems supported by CTE-LDT support these attributes. If you are using CTE-LDT with ext3 or ext4 mount points, you must explicitly enable the extended attribute mount option by editing `/etc/fstab` and adding the `user_xattr` mount option. In the other file systems supported by CTE-LDT, user extended attributes are enabled by default, so you do not have to explicitly enable them.

Example `/etc/fstab` entry for ext3 on Red Hat 6 or SLES:

```
/dev/sdb1 /disk2 ext3 defaults,user_xattr 0 0
```

Example `/etc/fstab` entry for ext4 on Red Hat 6 or SLES 12 (ext4 is not supported on SLES 11):

```
/dev/sdc1 /disk3 ext4 auto,users,user_xattr,exec 0 0
```

For more information about extended attributes, see ["CTE-LDT Metadata in Extended Attributes" on page 59](#).

Supported Applications in Linux

For all of the supported operating systems for database applications, see the *Compatibility Matrix for CTE Agent with Data Security Manager*.

Replication

- `rsync`.
- Hardware/software based replication system.

SAP HANA Fibre Channel Systems

SAP HANA is compatible with CTE-LDT. See the *Compatibility Matrix for CTE Agent with Data Security Manager* and the *CTE Agent for Linux Advanced Configuration and Integration Guide*.

Installing the CTE-LDT License

CTE-LDT installs with the CTE Agent software, but it is a separately-licensed CTE feature. Before you can use it, you have to install the license on the DSM to activate CTE-LDT on the CTE host. CTE-LDT is licensed for a specific number of hosts.

1. Obtain an CTE-LDT license from Thales. You can purchase CTE-LDT along with the DSM software or you can add CTE-LDT later.
2. Install the license on the DSM.
If you purchase CTE-LDT with the DSM, it includes the CTE-LDT license in the same license file with the DSM license, so there is only a single file to install.
If you add the CTE-LDT license later, you need to install an additional license file. For details, see the *DSM Installation and Configuration Guide*

To confirm that the CTE-LDT license is in effect:

1. Ask the DSM Administrator to log on to the DSM Management Console and click **System > License**.
2. In the **Agent Type** column, find the row labeled **FS**. The number of host licenses displays in the **LDT License** column of this row.

Installing and Registering the CTE Agent Software

Install the CTE Agent software with the CTE-LDT feature on each host you want to protect. The following procedure describes how to use the interactive installer to install CTE and register CTE-LDT using the shared secret registration method. For additional registration options, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide*.

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

Note

If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -d /home/my-cte-dir/
```

Note: If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
# ./vee-fs-7.0.0-47-rh8-x86_64.bin -h
```

4. The Thales License Agreement displays. When prompted, type **y** and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.47
```

In order to register the CipherTrust Transparent Encryption File System Agent with a Vormetric Data Security Manager

- 1) you must know the host name of the machine running the DSM (the host name is displayed on the Dashboard window of the Management Console), and
- 2) unless you intend to use the 'shared secret' registration method, the agent's host machine must be pre-configured on the DSM as a host with the 'Reg. Allowed' checkbox enabled for this agent type on the Hosts window of the Management Console.

In order to register with a CipherTrust Manager you need a valid registration token from the CM.

Do you want to continue with agent registration? (Y/N) [Y]:

5. Enter **y** to continue with the registration process. The install script prompts you to enter the name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

Do you want to continue with agent registration? (Y/N) [Y]: **y**

Please enter the primary key manager host name: **dsm630-121079.i.vormetric.com**

You entered the host name dsm630-121079.i.vormetric.com

Is this host name correct? (Y/N) [Y]: **y**

6. Enter the host name when prompted. If the Shared Secret registration in your DSM is configured to require an existing host entry, his name must match the name used on the **Add Host** page of the DSM Management Console.

Please enter the host name of this machine, or select from the following list. If using the "fingerprint" registration method, the name you provide must precisely match the name used on the "Add Host" page of the Management Console.

```
[1] host14.i.example.com
[2] Host-RHEL-14.i.example.com
[3] 10.3.14.90
```

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: **3**
You selected "10.3.14.90".

7. When prompted for the registration method, enter **s** for shared secret registration and then enter the required information about the domain, optional host group, and optional host description. For example:

Would you like to register to the DSM using a
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: **S**

What is the registration shared secret?
Please enter the domain name for this host: **west-coast-domain**
Please enter the host group name for this host, if any:
Please enter a description for this host: **West Coast Data Center server 5**

```
Shared secret      : *****
Domain name       : west-coast-domain
Host Group        : (none)
Host description   : West Coast Data Center server 5
Are the above values correct? (Y/N) [Y]: Y
```

8. At the hardware association prompt, select whether you want to enable the hardware association feature that prevents a clone of this machine from accessing keys in the DSM. The default is **y** (enabled):

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]: **Y**

9. At this point, the install script asks you about some of the optional CTE features you may want to enable. Make sure you select **Y** for LDT.

For example:

Do you want this host to have docker support enabled on the server? (Y/N) [N]:

Do you want this host to have Efficient Storage support enabled on the server? (Y/N) [N]:

Do you want this host to have LDT support enabled on the server? (Y/N) [N]: **Y**

Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:

Make sure you enter **Y** for LDT support.

10. At this point the installation script completes the installation and indicates that it successfully registered the host with the DSM.

```
Generating certificate signing request for the kernel component...done.  
Signing certificate...done.  
Generating EC certificate signing request for the vmd...done.  
Signing certificate...done.  
Generating EC certificate signing request for the vmd...done.  
Signing certificate...done.  
Successfully registered the CipherTrust Transparent Encryption File System Agent with the  
Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.
```

11. Verify the installation by checking the CTE processes on the host:

- Run `vmd -v` to check the version of CTE.
- Run `vmsec status` to display the CTE processes.
- Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

Setting the Linux Kernel Time Zone

The Linux kernel contains an internal time structure that may or may not contain time zone information. On system configurations that do not contain time zone information, CTE-LDT stores and displays timestamps for rekey beginning and ending in UTC (Coordinated Universal Time) rather than the system's local time zone. If this occurs, the administrator can set the kernel's internal time zone to the local time zone if they desire timestamps in their local time zone.

To set the Linux Kernel time zone information, at boot time type:

```
# hwclock --systz
```

The command sets the kernel's time zone to the local time zone and resets the System Time based on the current time zone.

Note

On systems that do not set the time zone by default, existing timestamps for completed rekeys remain in UTC, even if you run `hwclock --systz`. Only timestamps for new rekeys display the local time zone.

Enabling CTE-LDT on a Protected Host

When you install CTE on a host, you can enable CTE-LDT during the registration process as described in ["Installing and Registering the CTE Agent Software" on page 22](#). If you have already registered the host with the DSM, you can enable CTE-LDT in the host entry in the DSM.

Note

The CTE-LDT license is valid for a certain number of hosts. Once you reach this limit, you can either purchase additional CTE-LDT licenses, or reclaim a license by removing a CTE-LDT host. For details, see ["Removing CTE-LDT and Security Encryption" on page 76](#).

You cannot disable CTE-LDT on a host once it has been enabled.

To enable CTE-LDT on an existing host:

1. In the DSM Management Console, click **Hosts > Hosts**.
2. In the Hosts table, click on the host name of the protected host.
3. On the Edit Host page, select the **Live Data Transformation** check box, then click **OK** or **Apply** to enable CTE-LDT on the protected host.

Note: After CTE-LDT has been enabled for the host, the check box is greyed out because you cannot change this option once it has been set.

Chapter 4: Using CTE-LDT

Creating and Viewing Versioned Keys	27
Creating CTE-LDT Policies	29
Quality of Service	30
Create an CTE-LDT GuardPoint	41
Rotating Encryption Keys (Rekey)	44
File System Operations	48
Excluding Files or Directories from Rekey	50
Using CTE-LDT with SAP HANA Fibre Channel Systems (Linux Only)	58

Setting up keys, policies, and GuardPoints with CTE-LDT is very similar to performing the same tasks in CTE without CTE-LDT. However, there are some differences.

This chapter contains the steps, in order, for successfully setting up and using CTE-LDT.

Creating and Viewing Versioned Keys

In CTE-LDT, you create a *versioned* key for a Live Data Transformation policy and define the *life span* of the key. The life span is the duration (in days) of the versioned key. You also define an *initial expiration date*. When the key reaches its expiration date, it automatically rotates to a new version.

Although an CTE-LDT policy specifies the same key name, when the key rotates, the rotation of the key automatically starts CTE-LDT on the data in the GuardPoints protected with the CTE-LDT policy. There is no need to change the policy. However, you can manually rotate the key if circumstances require it.

Use the **Add Agent Key** page in the DSM Management Console when creating versioned keys.



CAUTION

Make sure that you are working in the Symmetric tab. CTE-LDT does not support asymmetric keys.

Creating a New Versioned Key for CTE-LDT

1. Add a new key as described in the *DSM Administration Guide*. This procedure explains all of the steps and settings, including those related to versioned keys.
2. Set the following required fields:
 - **Expiration Date:** CTE-LDT uses the initial transformation key specified in the CTE-LDT policy until this date occurs. On the expiration date, CTE-LDT creates a new version of the transformation key. Thereafter, it creates new versions based on the **Key Version Life Span**.
 - **Expiration Date:** You must specify an expiration date. Without an Expiration Date, a versioned key is always viewed as the initial key version. This means that it does not trigger CipherTrust Transparent Encryption - Live Data Transformation during initial transformation or subsequent key rotations.
 - **Automatic Key Rotation:** When checked, this makes the key a versioned key. You can only use versioned keys for CTE-LDT.
 - **Key Version Life Span (Days):** Frequency of key rotation, in days, that determines how often the DSM automatically generates a new version of the key, after the initial expiration. This triggers CipherTrust Transparent Encryption - Live Data Transformation on all GuardPoints using the key. Applies only if **Automatic Key Rotation** is selected.

Note

It is important to understand the interaction between the Expiration Date and the Key Version Life Span. CTE-LDT uses the initial version of the key until the Expiration Date. The Life Span has no effect until after the Expiration Date passes. Unless an administrator forces a rekey manually, there is no key version rotation and no CipherTrust Transparent Encryption - Live Data Transformation until the Expiration Date arrives.

When creating or modifying a versioned key, set the key version life span with care. The rekey process uses system resources, and it may contend with host applications that also require these resources. The more often you rekey, the more often the CTE-LDT process requires system resources. Determining the life span is a balance between security, compliance, and convenience. If you have no contention problems between the CTE-LDT process and your host applications, you can rekey frequently. If you do encounter contention problems, then you may want to choose a longer interval between key versions.

The following figure shows an example of adding a versioned key. The key name is LDT_key_1, it expires on April 30, 2021, and it has a key version life span of 180 days. That means the DSM generates a new version of this key on April 30, 2021, which kicks off the CTE-LDT process for the first time. The DSM then generates a new key version every 180 days and automatically starts the CTE-LDT process over again.

The screenshot shows the 'Add Agent Key' dialog box with the following fields and values:

Field	Value
Name	LDT_key_1
Description	LDT versioned key
Template	Default SQL Symmetric Key Template
Expiration Date	4/30/2021
Algorithm	AES256
Encryption Mode - for VTE agents only	CBC_CS1
Key Type	Cached on Host
Unique to Host	☐
Key Creation Method	Generate
Key Refresh Period - for VAE keys only (minutes)	10080
Automatic Key Rotation	☒
Key Version Life Span (days)	180

For information about how versioned keys are rotated throughout the lifetime of the CTE-LDT policies that use them, see ["CTE-LDT Runtime Flow" on page 14](#). For information about how to manually rotate a versioned key at any time, see ["Rotating Encryption Keys \(Rekey\)" on page 44](#).

Viewing Versioned Key Information

To obtain information about keys, use the DSM Management Console. For example, you might use this procedure to:

- Find out which keys are versioned keys, and therefore available for use in CTE-LDT policies.
- Locate a past key version so you can use it to decrypt old data.

To view keys in the DSM Management Console:

1. In the DSM Management Console, click **Keys > Agent Keys > Keys**.
The currently defined keys display. You can filter the list by key name using the **Search** box.
2. To find your versioned keys, look for a checked box in the **Versioned** column.
If the **Current Version** for a key is 0, then this is the first version of the key and no key rotation has taken place. If the **Current Version** is greater than 0, the key has been rotated. Either the key version expired, which triggered an automatic rotation, or a DSM Administrator manually initiated a rekey as described in ["Manual Key Rotation" on page 44](#).
3. To find all versions of a key, click the name of the key in the **Name** column.
 - The **General** tab shows the most recent version of the key.
 - The **Versions** tab shows the key versions in reverse chronological order (most recent first). If the key has been rotated many times, the list takes up multiple pages. Click the arrow buttons to move from page to page.

Creating CTE-LDT Policies

CTE-LDT uses a single Live Data Transformation encryption policy to address both data transformation and ongoing protection. In contrast, if you do not use CTE-LDT, you need a separate policy for initial data transformation, or rekey, and another policy to protect the data while it is in production use. For more information about CTE-LDT policies, see ["CTE-LDT Policies" on page 14](#).

To create an Live Data Transformation encryption policy:

1. Select **Policies > Manage Policies > Manage Policies**.
2. Click **Add**.
3. In **Policy Type**, choose **Live Data Transformation**.

A default security access rule is automatically added in Security Rules. The action is `key_op`, and the effects are Permit and Apply Key. This rule permits key operations, for the policy, on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version. This rule is required by CTE-LDT, so you cannot edit it, move it, or delete it.

4. Fill in the other fields as appropriate for an CTE-LDT policy. Some of the fields have special considerations when you use CTE-LDT:

- **Policy Type:** Must be Live Data Transformation.
- **Learn Mode:** Learn Mode provides a temporary method for disabling the blocking behavior of CTE/CTE-LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set.

Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption.

Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.

- **Security Rules:** The Security Rules panel contains the policy rules for the production workload. One default rule is added automatically to every CTE-LDT policy, as described above. After this default rule, the other security rules are specified in the same way, whether or not CTE-LDT is in use.

If you set the **"When"** clause of `key_op` rules in CTE-LDT and a time period is set, it affects user I/O operations, not CTE-LDT I/O operations. CTE-LDT starts rekeying the GuardPoint regardless of the value in the `key_op` rule's When clause. CTE-LDT performs rekey operations according to the QoS schedule assigned to the host.

- **Key Selection Rules, Current Key:** Indicates the state of the data before the CTE-LDT policy is applied to the GuardPoint. The data might be clear text, or it might already have been encrypted using a non-versioned key.

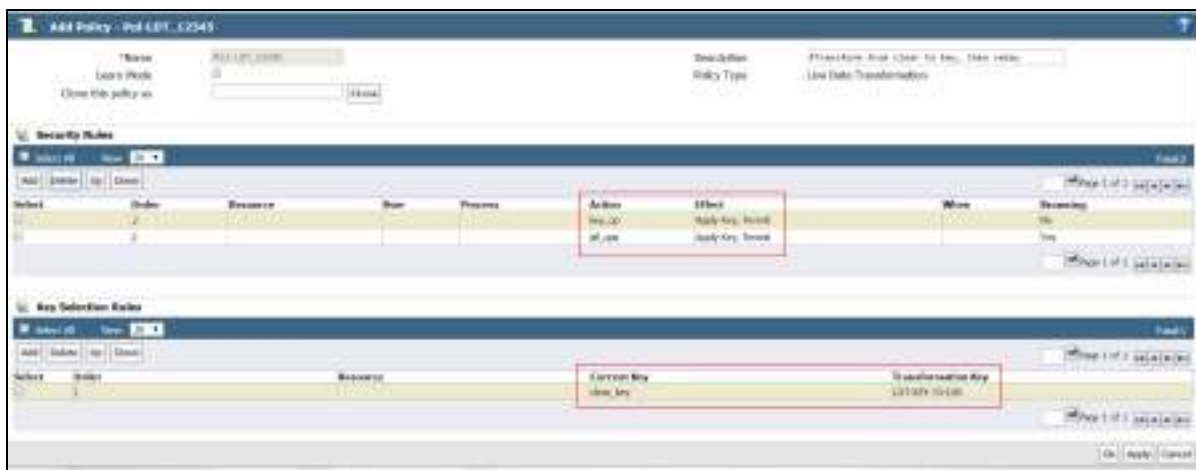
Specify *clear_key* in Current Key if the data has not yet been encrypted. Otherwise, specify the name of the non-versioned key that was used to encrypt the data into its current state.

- **Key Selection Rules, Transformation Key:** The **Transformation Key** is the versioned key that is applied to the data for its initial transformation. After the initial transformation, it rotates every time its life span ends. When the key rotates, all of its properties, including the key name and cryptographic algorithm, remain unchanged, except for the key material for encryption. Specify the versioned key name in the **Transformation Key** column. You can enter *clear_key* to transform your data to clear using CTE-LDT. *clear_key* is an exception to a non-versioned key in Transformation Key.
- **Key Selection Rules, Resource:** Allows you to add or edit a resource set. A resource set is a named collection of directories, files, or both, to which a user or process is permitted or denied access.

Note: Thales strongly recommends limiting the number of resource sets in CTE-LDT policies to 50 resources or less.

The following example shows a simple CTE-LDT policy that encrypts clear-text files using a versioned key named LDT-Key-33-100, as shown in the Key Selection Rules panel. The example *key_op* and *all_ops* actions in the Security Rules panel grant user and application access to files at all times, including during initial CTE-LDT and subsequent key rotations.

Figure 4-1: CTE-LDT Policy that encrypts clear-text files



Quality of Service

CTE-LDT runs in real time, while users actively interact with applications. This could impact performance. However, CTE-LDT is designed to not adversely affect application or system performance.

Purpose of QoS

Quality of Service (QoS) provides tools for an administrator to minimize the effect of CTE-LDT on system and application performance. It provides a set of parameters that administrators can set to control CTE-LDT use of system resources, primarily CPU and I/O bandwidth. When the QoS parameters are set appropriately, CTE-LDT stays within the defined boundaries to ensure that critical user applications are not adversely affected by CTE-LDT operations.

Manage CTE-LDT Impact

Administrators can pause or resume CTE-LDT operations to manage and control CTE-LDT impact to application workload. When data transformation occurs, either during initial or subsequent transformations, it requires substantial host CPU and I/O resources. This can cause contention for resources between the applications simultaneously running on the protected host. The administrator specifies QoS settings on each host, or at a host group level, that is using CTE-LDT. When CTE-LDT is running, QoS monitors CPU or rekey/scan rate on the host and enforces the QoS settings. QoS can also monitor and enforce an administrator imposed limit on the volume of data undergoing rekey per second. The QoS settings enable you to strike a balance between completing an CTE-LDT process and not interfering with host application performance.

Monitor and Control CPU Usage

QoS monitors and controls the use of host system resources during CTE-LDT, specifically, CPU usage and rekey/scan rate.

Note

You can control CPU usage or rekey/scan I/O rate, but not both. The CPU usage and rekey/scan I/O rate options are mutually exclusive.

Monitor and Control Rekey/Scan I/O Rate

Starting with VTE version 6.1.2 and onwards, you can choose Rekey I/O Rate as a threshold to control the CTE-LDT processing rate. When this threshold is entered, the Quality of Service continuously monitors CTE-LDT transformation and enforces the specified amount of data during:

- **Rekeying**—CTE-LDT is transforming the data on active GuardPoints based on the new key version.
- **Scanning**—CTE-LDT is analyzing files in GuardPoints. Scanning occurs:
 - Before initial transformation (Linux only)
 - Before a rekey (Linux only)
 - Following an interrupted rekey, such as a reboot on Linux or Windows, and also a directory rename or directory deletion on Windows

The Rekey I/O Rate is either 0, or greater than 0. By specifying 0, Quality of Service resets the previously specified Rekey I/O Rate, if any, and then stops monitoring the LDT rekey/scan processing rate.

When the Rekey I/O Rate is set, Quality of Service ignores the CPU and/or the iow (IOWAIT) thresholds previously set. After resetting the Rekey I/O Rate to 0, the Quality of Service will resume enforcing the CPU and/or the iow thresholds, provided one or both are set.

To rekey at full throttle, you can set the Rekey I/O Rate, the CPU, and IOWAIT thresholds to 0.

Note

IOWAIT has been deprecated on Linux, and it is not supported on Windows. Instead, use Rekey IO Rate to control the CTE-LDT I/O utilization on both Linux and Windows.

With the DSM version 6.2.0 and later, you can set the Rekey Rate or CPU threshold for all of the CTE-LDT GuardPoints on a host, or for all of the GuardPoints in a given host group, on the **GuardPoints** tab in the DSM.

You can override the DSM settings locally on a single host using the `voradmin ldt ior <iorate>` command on that host. When you do so, the `voradmin` setting overrides the Rekey I/O Rate or CPU Threshold set in the DSM.

A tolerance level is associated with the Rekey I/O Rate. Together, the tolerance and Rekey I/O Rate specify a range for the CTE-LDT processing rate. The Quality of Service selects a proper tolerance for a Rekey I/O Rate provided through the `voradmin` command, and maintains the CTE-LDT processing rate at the specified Rekey I/O Rate plus or minus the tolerance. The tolerance is selected as follows:

- When the Rekey I/O Rate is less than or equal to 10MB/sec, the tolerance is 3MB/sec.
- When the Rekey I/O Rate is greater than 10MB/sec. and less than 50MB/sec, the tolerance is 4MB/sec.
- When the Rekey I/O Rate is at 50MB/sec or higher, the tolerance is 10% of the specified Rekey I/O Rate.

To set or reset Rekey I/O Rate on a single host, use the `voradmin` command as follows:

- To set the threshold of 50 MB/sec., use the following command:

```
# voradmin ldt ior 50
```

- To reset the current threshold:

```
# voradmin ldt ior 0
```

For more information about setting the Rekey I/O Rate using `voradmin`, see ["Select and Set Rekey I/O Rate " on page 39.](#)

Monitor and Control I/O Wait Time (Linux only)



CAUTION

The Linux I/O wait option has been deprecated in favor of Rekey I/O Rate. Support for the I/O wait option will eventually be removed from CTE. If you are currently using I/O wait time option with QoS, please plan on switching from I/O Wait Time to Rekey I/O rate.

You can choose to add **I/O wait time** for monitoring and control. The I/O wait time threshold refers to the system's peak I/O wait time during its production workload. For a given threshold, you can specify a tolerance level that is the amount of I/O overhead allowed by CTE-LDT for rekeying data. By specifying the I/O wait time, and the tolerance level, QoS continuously monitors your system's average I/O wait time during CTE-LDT operations. It applies the tolerance factor to the average I/O wait time to adjust CTE-LDT I/O operations. This assures that the system's average I/O wait time remains within the desired range and does not exceed the threshold.

The desired range is the specified average I/O wait time (milliseconds) plus or minus the specified tolerance. **Tolerance** provides the range in which the average I/O wait time, which includes CTE-LDT I/O operations, is maintained.

For example, you may specify a desired I/O wait time during rekey. QoS maintains the desired I/O load for rekey according to the specified I/O wait time. If the total I/O wait time increases beyond the desired I/O wait time, QoS reduces the rekey I/O load by some percentage until the desired I/O wait time is achieved or the rekey I/O load reaches down to a preset N number of rekey operations.

QoS Scheduling During Backup/Restore

QoS scheduling plays an important role when backing up/restoring data without the *Apply Key* rule applied to the backup/restore process. During backup/restore, you **must** pause CTE-LDT operations before taking backups. QoS scheduling allows the administrator to enter the schedule for QoS aligned with the backup schedule, and pause the CTE-LDT processes for the duration of the backup. The schedule specifies which days of the week, and what times of day, CTE-LDT is permitted to run. CTE-LDT cannot run at any time that is not permitted by the QoS schedule. QoS suspends CTE-LDT operations at all times outside of the schedule.

When setting a QoS schedule, consider your system and application peak demand periods during the day and week. Also consider your schedule for data backups. Schedule CTE-LDT to pause when you need all available system resources for other tasks, such as meeting peak user demand or performing data backups.

Note

On Windows, if your backup applications are using VSS, then you do not need to pause CTE-LDT on Windows.

How to Set QoS

To set QoS for a host to enforce a threshold on CTE-LDT based on CPU percentage:

1. Click **Hosts > Hosts > *hostname* > GuardPoint**.

2. Set the **Schedule** parameter:

Choose one of the options from the drop-down list. By default, the list contains WEEKNIGHTS (rekey performed between 12 AM and 7:00 AM), WEEKENDS, or ANY_TIME. The default setting is ANY_TIME. By limiting CTE-LDT to periods of low application usage, you minimize the potential for resource contention between applications and CTE-LDT.

You can add to the choices in the Schedule drop-down by creating custom schedules. See ["Creating a Custom QoS Schedule" on the next page](#).

3. Enter the Rekey IO Rate threshold or percentage of CPU resources to allocate to CTE-LDT in the **Set % of available CPU usage for rekey** field:

Choose a Rekey IO Rate threshold or the percentage of total CPU resources that CTE-LDT processes can use. CTE-LDT applies a tolerance of +/- 2% on CPU threshold settings up to 7%. For threshold over 7%, CTE-LDT applies a tolerance of +/- 4%.

If CPU% is set to 0, QoS stops monitoring CPU usage and CTE-LDT operations run at maximum rekey rate within the available system resources. Setting CPU percentage to 0 does not affect CTE-LDT schedules, so CTE-LDT operations are suspended and resumed per QoS schedule.

If you do not enter CPU threshold percentage, CTE-LDT applies CPU threshold of 5% capped by default.

If CPU% is set to a very high value, such as 25%, the rekey process competes with other applications to use as many CPU cycles as it can. As a best practice, start with a setting of 10%, and increase or decrease it slowly by 5% until it reaches a reasonable level that does not adversely affect the performance of user applications. The higher the percentage, the more quickly CTE-LDT completes its processing. However, this speed causes increased competition for resources, which can significantly degrade the performance of other applications using this host.



CAUTION

Do not set CPU% to a very high value, or to 100%, in an attempt to force faster data transformation. This can potentially exhaust other system resources.

4. Set the **Cap CPU Allocation** for rekey.

Check this box to specify that the CPU allowance must never exceed the percentage set in CPU%. If Cap CPU Allocation is not checked, and additional CPU resources are available on the host, CTE-LDT consumes part of the available resources for rekey above the CPU threshold. Exceeding the threshold may impact your production workload as your production CPU resource consumption fluctuates over time.

For example, if CPU% is set to 10%, but Cap CPU Allocation is not set, the rekey process continues consuming available CPU cycles after reaching 10% CPU utilization, at which point the rekey process starts contending with applications for CPU cycles.

Note: If you choose Rekey IO Rate threshold to control the CTE-LDT processing rate, you do not need to also set the CPU threshold for CTE-LDT.

Creating a Custom QoS Schedule

CTE-LDT provides three predefined QoS schedules: ANY_TIME, WEEKENDS, and WEEKNIGHTS. You can define additional custom schedules that can be assigned to any host on the GuardPoints tab.

1. In the DSM, choose **Hosts > QoS Schedules**.
2. Click **Add**.
3. Enter a unique name for the new schedule.
This name displays in the **Schedule** dropdown list when you set QoS parameters.
4. Click **Add**.
5. Choose the start day/time and the end day/time for CTE-LDT operations.
6. Click **OK**.

QoS Best Practices

This section gives tips and examples to help you set QoS parameters for the best results.

General Best Practices for QoS

- Use Rekey I/O Rate threshold to limit CTE-LDT impact, if any, to your production workloads. Rekey I/O Rate approach is a simpler method for a DSM Administrator or system administrator to enforce a limit on the volume of data that CTE-LDT should rekey per second. You can choose a threshold, in units of MBs per second, which is a small percentage of peak IOPS from your production workload.
- You will see the effects of QoS settings only if the number and/or types of files in the GuardPoints stress the rekey or scan processes. On hosts with a relatively small number of files, the rekey or scan process may complete quickly without hitting a threshold and causing throttling to occur.
- Use QoS CPU parameters as an alternate method for controlling the effect CTE-LDT has on application performance.

Set limits on CTE-LDT CPU usage whenever runtime monitoring shows that user applications are affected by CTE-LDT. Start by setting the CPU parameter to 10%, then increase or decrease in 5% intervals, as needed, to tune the CPU allocation. When an acceptable level is reached, and CTE-LDT is not noticeably affecting user applications, leave the QoS CPU parameters at a constant setting.

- Use monitoring tools.

Monitor host CPU utilization with tools like `vmstat`, `top`, and `iotop` on Linux and `perfmon` on Windows.

You can also monitor and obtain statistics with the `voradmin ldt stats` command.

For more information about `voradmin ldt stats`, see ["Obtaining CTE-LDT Statistics at the Command Line" on page 83](#).

- Select CPU resource allocation for CTE-LDT from 1% to the available limit minus 5%.

If the monitoring tools indicate system CPU usage, without CTE-LDT, it is at N%, available CPU resource is M%, where $M = 100 - N$. Select a percentage within 1 - (M - 5) to allocate to CTE-LDT CPU usage. However, remember that QoS tolerates 2% - 4% leeway in the actual CPU usage, so adjust your selection by 2 - 4%.

- Do not set CPU resources to 0% or 100% in an attempt to minimize or stop CTE-LDT

A CPU% value of 0 or 100 is reserved for disabling the QoS CPU monitoring function. This does not stop CTE-LDT or minimize its resource usage; rather the opposite. It enables CTE-LDT to run with its maximum rekey rate. Note that when CPU % is not set, and it shows 100% setting on the DSM, CTE-LDT hosts enforce a 5% CPU threshold by default. We recommend that you change the 100% setting to 5% capped on the hosts installed with VTE versions lower than v6.1.

- Cap the CPU allocation.

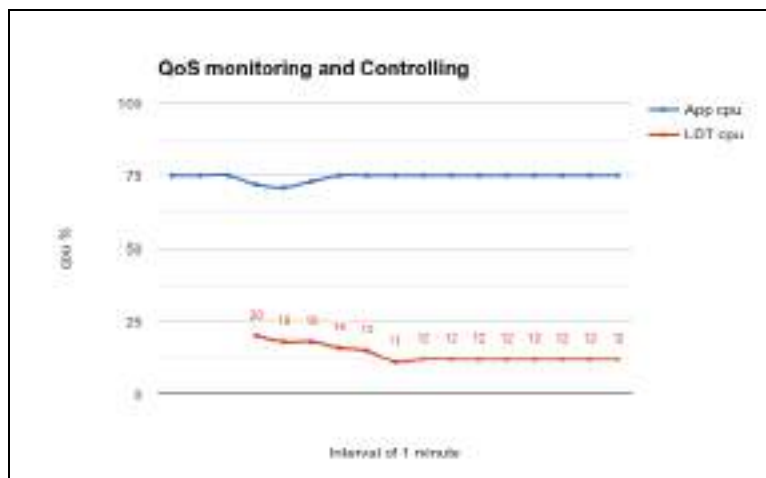
QoS provides a **CAP CPU Allocation** parameter. Set this parameter to **True**. This ensures that CTE-LDT resource usage never exceeds the allocated percentage.

- Apply **await** threshold very carefully to try controlling CTE-LDT I/O load.

Example: Setting QoS before starting CTE-LDT

You can be proactive and set up QoS parameters before enabling GuardPoints that are protected with CTE-LDT policies. This ensures QoS starts monitoring and controlling CTE-LDT resource usage from the start. The following graph shows an example where 10% of the CPU is assigned to CTE-LDT. QoS makes sure that CTE-LDT is restricted to use only 10% of the CPU. There is a tolerance level of +/- 4%, so actual CTE-LDT usage can range between 5% and 15% of CPU. In the following example, applications use 75% of the CPU resources. As the graph shows, when CTE-LDT starts, application CPU utilization drops for a moment, because CTE-LDT exceeds the CPU threshold. QoS immediately reduces CTE-LDT's CPU usage to 12%, which is within tolerance levels for a 10% setting, and the application CPU share returns to normal.

Figure 4-2: QoS makes visible improvement immediately when CTE-LDT starts



The graph above was obtained on a Linux system running sysbench.

- To find the amount of CPU resources currently in use by applications, type:

```
# top -n 1 -b | grep sysbench | awk 'BEGIN {cpu=0} {cpu += $9} END {print cpu}'
```
- To find the amount of CPU currently in use by the CTE-LDT-protected host, type:

```
# top | grep Cpu
```
- To find the amount of CPU currently in use by CTE-LDT, type:

```
# voradmin ldt stats | grep CPU
```

Example: Monitoring and controlling resource usage during CTE-LDT

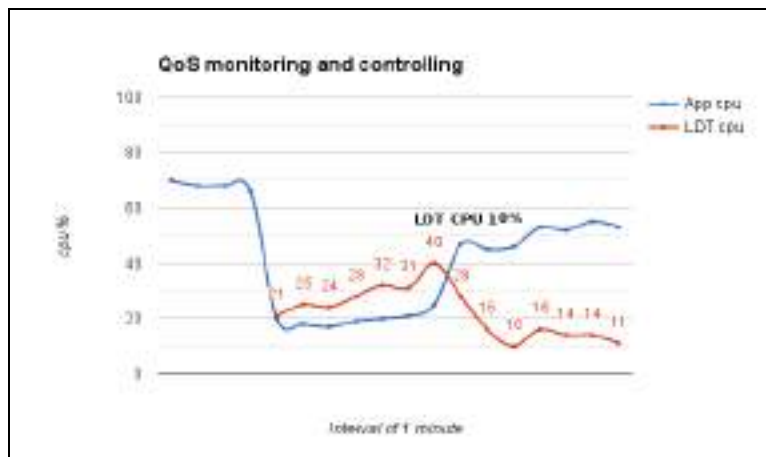
Suppose that CTE-LDT has started with CPU set to 25%, and users realize their applications are affected. For example, there might be a higher than expected level of CTE-LDT I/O operations. To return application performance to normal, reduce the CPU allocation for CTE-LDT.

1. Set the **CPU parameter** to a lower value, such as 10%.
2. Select the **Cap CPU Allocation** option.
3. Set the I/O wait parameter.

QoS restricts CTE-LDT CPU usage to 10%. The application user should monitor their application. If the application's performance is still affected, reduce the CPU parameter further, such as to 5%. Repeat this procedure until application performance returns to a satisfactory level.

The following graph shows an example where QoS is not enabled to monitor and control CTE-LDT CPU usage from the start. When CTE-LDT starts, application CPU usage drops from 65% to 20%. By setting the QoS CPU parameter to 10%, application usage is greatly improved.

Figure 4-3: CPU usage allocation before and after QoS CPU parameter is set



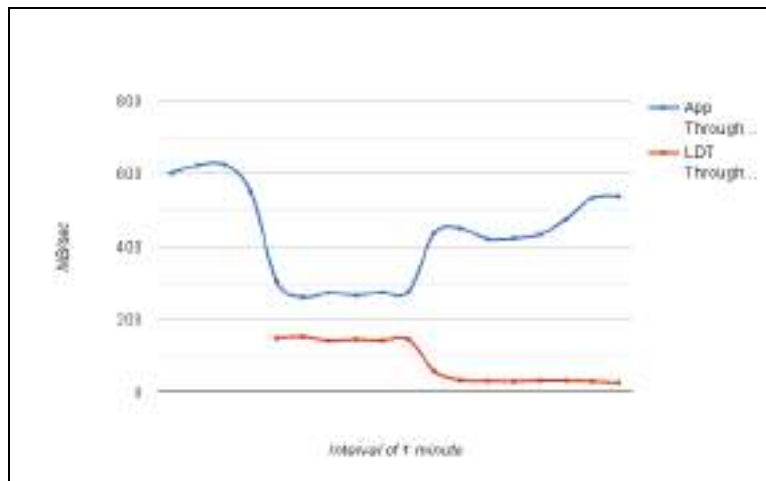
Example: How QoS CPU settings affect I/O bandwidth

Controlling CPU utilization indirectly controls I/O bandwidth. When CTE-LDT is consuming less CPU resources, it is usually performing fewer operations of all kinds, including input and output.

The following graph shows how an application's I/O throughput is affected by CTE-LDT, and how QoS can reduce this effect through monitoring and controlling the CTE-LDT CPU resource usage.

This graph is from the same system described in ["Example: Monitoring and controlling resource usage during CTE-LDT" on the previous page](#). No QoS parameters are set at first. When CTE-LDT starts, application I/O drops from more than 600 MB per second to below 30 MB per second. By setting the QoS CPU parameter to 10%, the CTE-LDT I/O operations drop to below the application's ability to perform so application I/O operations is greatly improved.

Figure 4-4: I/O operations before and after QoS CPU limit is set



To obtain the data for this graph:

- Use `iostat` and benchmarking tools on an RHEL system to obtain application I/O throughput.
- Use `voradmin ldt stats` to obtain the CTE-LDT I/O throughput and rekey rate.

Determine and Set the I/O wait time

Monitor the average I/O wait time using `iostat` on Linux, or `perfmon` on Windows, during the production workload. Thales recommends monitoring the average I/O wait time during the peak levels of the workload.

1. Run the `iostat` command and specify the number and duration of intervals to determine `iowait` time.

```
# iostat -txm 10 2
```

Note: For Windows, use `perfmon` to obtain: `\PhysicalDisk(_total)\Avg. Disk sec/Transfer`

- Get the total I/O wait time from the sampled data. It is the sum of the await field of disks.

Note: Do not include await values from volumes and device mappers.

Figure 4-5: Example of iostat data

```
Monday 04 September 2017 03:13:39 PDT
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.18    0.00    2.52   42.03    0.00   55.27
```

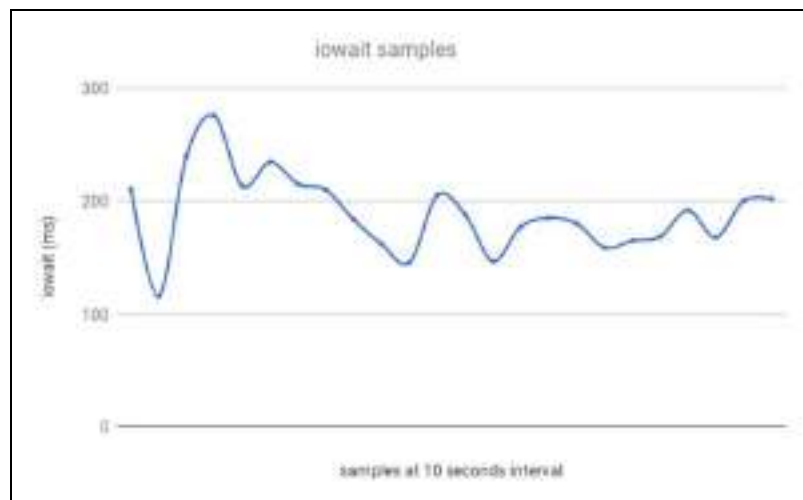
Device:	rrqm/s	wrqm/s	r/s	w/s	rmb/s	wmb/s	avgqu-sz	avgqu-sz	await	svctm	%util
fd0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
sda	0.00	0.00	0.03	2.17	0.00	0.03	28.77	0.00	0.61	0.16	0.04
sdb	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
sdc	0.00	0.33	0.00	0.47	0.00	0.00	14.06	0.00	0.00	0.00	0.00
sdd	0.07	17.20	0.53	12.53	0.01	0.18	29.31	1.14	88.90	76.30	99.70
sde	0.00	75.57	0.07	839.20	0.00	4.04	9.80	141.87	169.15	1.19	99.94
sdg	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
sdh	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
sdf	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
dm-0	0.00	0.00	0.11	2.17	0.00	0.01	0.19	0.02	7.49	0.28	0.00
dm-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.91	1.14	0.00
dm-2	0.00	0.00	0.15	4.97	0.01	0.02	10.73	0.05	8.80	0.04	0.02

For the above example:

Total I/O wait = .61+ 88.9 + 169.15 = 258.66

- Obtain multiple samples at 10 second intervals. Estimate the `iowait` time when it stabilizes.

In the following chart, the I/O wait time is nearly 200ms when in a stable state.



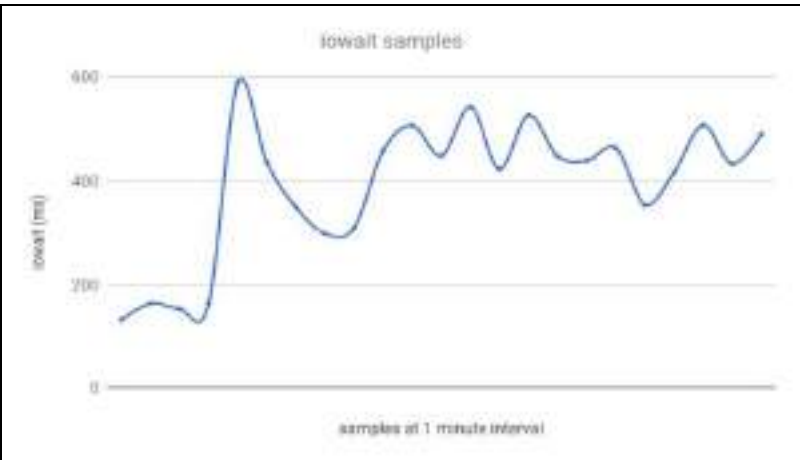
- Estimate the `iowait` threshold by running CTE-LDT and watching the degradation in I/O wait time. Set the `iowait` threshold and/or tolerance parameters in units of milliseconds using `voradmin` command, type:

```
# voradmin ldt iow iowait [tolerance]
```

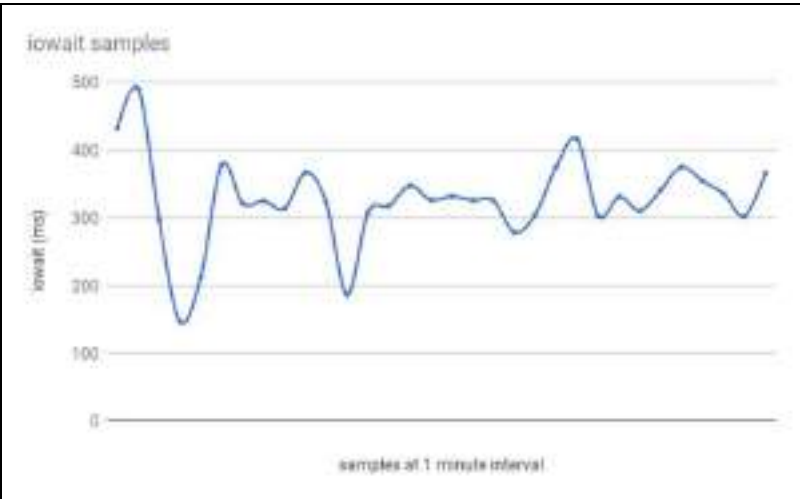
For example, to set the `iowait` to 350 milliseconds and the tolerance to 10 milliseconds, you would enter:

```
# voradmin ldt iow 350 10
```

In the following graph, observe that once CTE-LDT starts, the total I/O wait time jumps to 600 ms and oscillates between 400 to 500 ms. Without CTE-LDT, I/O wait time was 200 ms. If the application I/O wait time suffers because of CTE-LDT, reduce the CTE-LDT I/O usage by setting `iowait` threshold to a suitable level between 200 to 500 ms. In this example, we have chosen 350 ms as the desired/suitable level of total I/O while CTE-LDT and application workloads are running concurrently.



From the following graph, observe that QoS tried to control I/O wait time and now it oscillates near about 350 ms.



The following table explains what is monitored and controlled by QoS when CPU or I/O resource thresholds are set.

Resource Threshold Set	Monitored and Controlled by QoS
CPU (value must be greater than 0.)	CPU utilization to adjust CTE-LDT operations to maintain the set CPU threshold
I/O wait (value must be greater than 0.)	I/O average wait time to adjust CTE-LDT operations to maintain the set I/O wait threshold
CPU and I/O wait	CPU and I/O, both resources are controlled by their threshold limits
CPU and I/O wait set to 0	No resource is controlled or monitored

Select and Set Rekey I/O Rate

You can choose to set the Rekey I/O Rate to control I/O operations from CTE-LDT to minimize CTE-LDT impact to your production workload. It's assumed that you already know the maximum IOPS on your host system during your production workload. With this information, you can choose a threshold for Rekey I/O Rate and enforce the selected threshold during CipherTrust Transparent Encryption - Live Data Transformation. The work flow is as follows:

1. Set **Rekey I/O Rate** threshold using `voradmin` or in the DSM Management Console.
2. QoS retrieves the threshold and starts monitoring and controlling CTE-LDT according to the specified threshold and the tolerance factor corresponding to the threshold.
3. The selected threshold will be in effect within 2 to 4 minutes after entering the threshold.

When Rekey I/O Rate and CPU or IOWAIT thresholds are set, QoS will monitor and control the CTE-LDT processing rate based on the Rekey I/O Rate threshold. The CPU and/or IOWAIT thresholds will be ignored.

Set Rekey I/O Rate Threshold

1. Set **Rekey I/O Rate** threshold by using `voradmin`:

```
# voradmin ldt ior 10
```

You can also set the Rekey I/O Rate for one or more managed hosts on the QoS settings area of the **GuardPoint** tab under host configuration in the DSM (DSM version 6.2.0 or later). For more information about using the DSM method, see ["How to Set QoS" on page 33](#).

In the `voradmin` example above, QoS enforces the threshold of 10MB/sec with the tolerance of +/- 3MB/second. Effectively, CTE-LDT attempts to rekey the amount of data in the range of 7MBs/second to 13MB/second.

On Linux and Windows, you can use `voradmin ldt ior` to report the current threshold setting without specifying a value for threshold:

```
# voradmin ldt ior
QoS Rekey I/O rate threshold: 10 MB/sec
QoS Rekey I/O tolerance: 3 MB/sec
```

2. Be sure the threshold you enter is appropriate for your production workload. To verify this:

- a. Observe the Rekey I/O Rate for a few minutes using `voradmin`.

On Linux, you can do this using:

```
# voradmin ldt stats
Host level statistics:
File stats: rekeyed=202390, passed=0, created=0, removed=0
Data stats: rekeyed=6.2GB, truncated=0.0MB
QoS: IOR threshold=10MB/sec, tolerance=3MB/sec
current_rekey_rate=2MB/sec, current_iow=0ms
load_factor=50, delay_factor=0, delay_scan=0
```

On Windows, you can do this using:

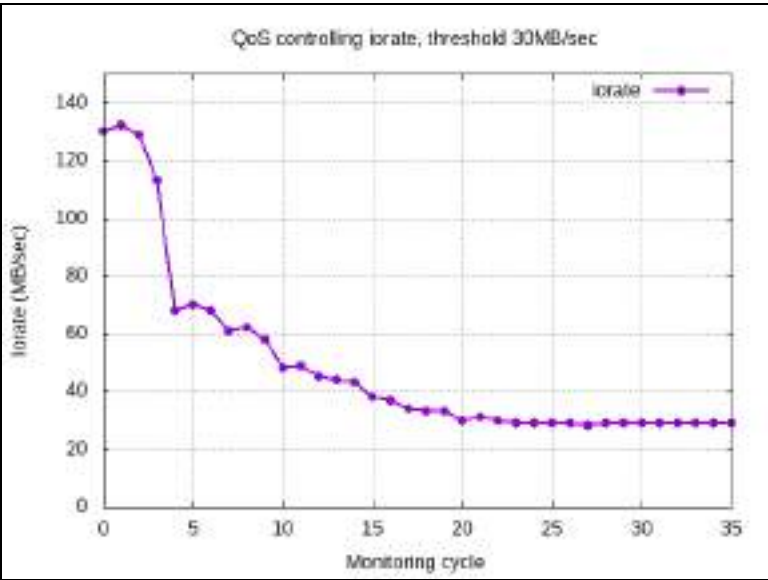
```
voradmin ldt monitor
Host Stats:
Total number of Guard Points    = 1
Rekey Status                    = Rekey done (Finished rekey on 1 out of 1 GP's)
Total files to be transformed   = 0
Total files transformed         = 0
Total files in progress         = 0
Total transformation threads    = 0

Current rekey rate              = 0 KB/s
Rekey IO rate threshold         = 1000 MB/s
Rekey IO rate tolerance         = 4 MB/s
```

- b. Set an appropriate threshold. Do not set the threshold value too high, as QoS might not be able to achieve it because of other resource bottlenecks.

3. Check the QoS controlling rekey rate.

QoS will monitor and control CTE-LDT utilization using the specified threshold. The following figure shows an example of how QoS monitors and controls CTE-LDT utilization. In this example, the threshold is 30 MB/sec. Throughput of CTE-LDT was nearly 130 MB/sec. QoS brings it down to within the range of 30 MB/second.



4. Disable QoS.

QoS will not monitor and control resources when all the thresholds, CPU, Rekey I/O rate, and IOWAIT are set to 0. When Rekey I/O Rate and IOWAIT are not explicitly set, it is considered to be set to 90 MB/second.

QoS continues to apply its schedules for suspending CTE-LDT operations at certain days and times regardless of what values are set for CPU, Rekey I/O Rate, and IOWAIT thresholds.

Summary of QoS Resources

The following table summarizes the available thresholds and the actions of QoS module to enforce the set thresholds:

Scenario	QoS Action
Only Rekey I/O Rate threshold is set	Monitor and control the CTE-LDT processing rate based on Rekey I/O Rate
Rekey I/O Rate and CPU threshold are set	Monitor and control the CTE-LDT processing rate based on Rekey I/O Rate. CPU threshold is ignored.
Rekey I/O Rate, CPU, and IOWAIT thresholds are set	Monitor and control the CTE-LDT processing rate based on Rekey I/O Rate. CPU and IOWAIT thresholds are ignored.

Create an CTE-LDT GuardPoint

After you have installed the license and registered the CTE-LDT host (see [Chapter 3: "Setting Up CTE-LDT" on page 20](#)), you can create an CTE-LDT GuardPoint on the host. When you create the CTE-LDT GuardPoint, you select a Live Data Transformation policy and apply that policy with its transformation keys to that GuardPoint. CTE automatically gets the Quality of Service settings from the **GuardPoint** tab of the Host entry in the DSM.

This section describes two scenarios:

- ["Create an CTE-LDT GuardPoint for an Unguarded Directory" below](#)
- ["Converting a Non-CTE-LDT GuardPoint to an CTE-LDT GuardPoint" on the facing page](#)

Create an CTE-LDT GuardPoint for an Unguarded Directory

To create an CTE-LDT GuardPoint on what was previously an unprotected/unguarded directory:

1. Create an Live Data Transformation policy that transforms data from clear text to a versioned key. In the policy, set Current Key to `clear_key` and Transformation Key to the versioned key. See ["Creating CTE-LDT Policies" on page 29](#).
2. Set, or modify, the Quality of Service (QoS) parameters to account for CTE-LDT on all GuardPoints. See ["Quality of Service" on page 30](#).
3. Click **Guard**.
4. The Guard File System window displays. Set the following values:
 - a. Select an CTE-LDT Policy.
 - b. Select **Directory (Auto Guard or Manual Guard)**.
 - c. Enter or browse for the directory to protect.
 - d. Do **not** check Automount. CTE-LDT is not supported on automounted file systems.
 - e. Check **Transform Sparse Regions** if you want those regions allocated with disk blocks.

A *sparse region* is a region within the file size that has not yet been written to. Therefore, it is not allocated with disk blocks. Any attempt to read a sparse region reads stream of zeros as data. A file may have one or more sparse regions, or an entire file may be sparse.

By selecting Transform Sparse Regions, CTE-LDT transforms a file without checking or skipping sparse regions, if they exist. Consequently, as CTE-LDT operations transform and fill sparse regions with encrypted stream of zeros, sparse regions are allocated with disk blocks. This increases the number of disk blocks utilized in the file system.

By not selecting Transform Sparse Regions, CTE-LDT detects and skips transforming sparse regions. Therefore, it does not change the number of blocks utilized in the file system.

5. Click **OK**.

The **GuardPoint** tab displays again. CipherTrust Transparent Encryption - Live Data Transformation starts immediately after you enable the GuardPoint on the host.
6. Wait a moment and check the status of the GuardPoint in the Rekey Status column of the GuardPoint tab.
7. In the Status column, click the status icon (the green circle) to get status details about this GuardPoint.

The GuardPoint Status window displays. For an explanation of all the items in the GuardPoint Status dialog, see ["Obtaining Statistics in the DSM with GuardPoint Status" on page 81](#).

Note: When you first apply a GuardPoint, the key version shown in GuardPoint Status is 0. This indicates the first version of the key.

8. Wait for CTE-LDT to complete the rekey process for the GuardPoint. When the Rekey Status column shows 100%, the GuardPoint has been rekeyed and the GuardPoint status changes to rekeyed. For information about the values in the Rekey Status column, see ["Checking the Rekey Status" on page 44](#).

Converting a Non-CTE-LDT GuardPoint to an CTE-LDT GuardPoint

If you have an earlier version of CipherTrust Transparent Encryption installed, you most likely have set up GuardPoints. These legacy GuardPoints are protected with policies that do not make use of CipherTrust Transparent Encryption - Live Data Transformation. This means that you must stop all users from accessing the files in these GuardPoints while the policy performs encryption.

After installing CTE 6.0.x or higher, and setting up CTE-LDT on the hosts, you can change legacy GuardPoints to CTE-LDT GuardPoints. CTE-LDT GuardPoints provide the advantage of allowing users to access all files in the GuardPoints while encryption is occurring. There is no downtime for the user except for the time needed to apply the GuardPoint.

1. Write a new CTE-LDT policy that transforms data from the non-CTE-LDT/non-versioned key used in the existing GuardPoint, to an CTE-LDT versioned key. See ["Creating CTE-LDT Policies" on page 29](#).

The following example shows an CTE-LDT production policy that transforms data encrypted by a non-versioned key (AES256) to data encrypted with a versioned key (LDT).

Add Policy - LDT_Policy

Policy Type: Live Data Transformation
Name: LDT_Policy
Description: Transform legacy GuardPoint to LDT
Learn Mode: ☐
Clone this policy as:

Security Rules

Select All View: 20 Total: 2

Select	Order	Resource	User	Process	Action	Effect	When	Browsing
☐	1				key_all	Permit, Apply Key		No
☐	2				all_ops	Permit, Apply Key		Yes

Page 1 of 1

Key Selection Rules

Select All View: 23 Total: 1

Select	Order	Resource	Current Key	Transformation Key
☐	1		AES256	LDT

Page 1 of 1

2. Make sure there is no application activity within the GuardPoint.



CAUTION

This step is critical. Do not skip it. Make sure there is no application activity within the GuardPoint.

3. Click **Unguard** to unguard the GuardPoint.
4. Guard the directory again using the new CTE-LDT policy. Use the steps in ["Create an CTE-LDT GuardPoint for an Unguarded Directory" on the previous page](#), but choose the policy that starts from the non-versioned/non-LDT key rather than a policy that starts from `clear_key`.

Rotating Encryption Keys (Rekey)

This following sections describe procedures related to encrypting an existing GuardPoint with a new key (also called rekeying).

Manual Key Rotation

If you need to rekey your GuardPoint prior to the expiration of the current key version, you can manually start a rekey process.

On Windows, you cannot rotate a key until all current data transformations that use the same key have completed, whether those transformations are an initial data transformation or a rekey. On Linux, you can rotate the key at any time. For details, see ["Rotating Encryption Keys While a Rekey is in Progress \(Relaunch\)" on page 47](#).

1. To manually generate a new version of a key, open the DSM Management Console and choose **Keys > Agent Keys > Keys**.
2. Click the name of the key you want to rotate.
Note the hex value shown next to **Key Hash** before and after you rotate the key. The hash value represents the current key version associated with the key. After rotating the key, CTE-LDT generates a new version of the key, and the hash value changes.
3. Click **Rotate**.
4. After clicking Rotate, a Rotate Key pop-up displays. Select the *Rotation Reason* and click **Rotate**. This initiates the rekey process on all GuardPoints using the key.
5. Check the status of the GuardPoint in the Rekey Status column of the GuardPoint tab. For example, just after clicking Rotate, the status might be "Rekeying 4%".
Once CTE-LDT transforms the data, you are finished.

Checking the Rekey Status

During a rekey, you can check the progress in the UI on the GuardPoint status page on the DSM. GuardPoint status is not relayed to the DSM in real time. A delay of several minutes before the DSM displays events on the host is likely. When the number of GuardPoints on the managed host is high, for example 100+, the delay in relaying GuardPoint status is due to delays in scheduling and the execution of CTE-LDT operations on the managed host for GuardPoints.

When the host and DSM are configured for one-way communication, the delay is longer because CTE-LDT statistics are sent to the DSM once per hour, or each time a GuardPoint enable or disable status changes.

To check when the DSM last received a status update from the host, look at the Last Status Update time stamp in the GuardPoint status dialog. For information about how to display this dialog, see ["Obtaining Statistics in the DSM with GuardPoint Status" on page 81](#). For the most up-to-date statistics, inspect the host itself. To find out whether your host is configured for one-way communication, open the DSM Management Console, choose **Hosts > Hosts**, click the name of the host, and look for the FS Agent One Way Communication check box.

To see the progress of a rekey and the estimated completion time:

1. Open the DSM Management Console.
2. Choose **Hosts > Hosts**.
3. Click the name of the host you want to check.
4. Click the **GuardPoint** tab.
5. The Rekey Status column shows the current status. The status is one of the following:

Rekey Status	Description
Error (Windows only)	Runtime error occurred. Check for CTE-LDT-ALERT messages. Typically occurs when Low disk space occurs or a volume got dismounted.
Exited (Windows only)	Exited an operation like renaming folder. CTE-LDT will be restarted in the next ~20 secs or as soon as the operation completes. On restart, it will go into scan phase if file/folder deleted/renamed.
Incomplete (Windows only)	CTE-LDT did not finish. The administrator must intervene to remove the obstacle so the rekey can finish. You can run the <code>voradmin ldt skip</code> command to obtain more information.
In-Progress	CTE-LDT is transforming each file one by one.
Not Started	CTE-LDT has not started. It will go into this state when a GuardPoint is added or a key is rotated or changed.
Paused	CTE-LDT is paused on the GuardPoint, because of the QoS schedule or a direct request from administrator.
Queued	When a key rotation is in progress and another rotation is initiated.
Rekeyed	GuardPoint has been transformed to the latest key version.
Rekeying	GuardPoint transformation is in process of transforming the data with the latest key.
Scanning	Linux: CTE-LDT started, it is scanning the GuardPoint and counting bytes, files to transform in the GP before starting transformation. Required for statistics and estimation. Windows: CTE-LDT is analyzing files in the GuardPoint before initial transformation, before a rekey, or following an interrupted rekey. The scan is required for statistics and estimation. CTE-LDT can scan multiple times on completing a traversal of the guarded directory. The scanning status does not include a percent complete estimate.
Starting	GuardPoint transformation is ready to begin, but has not yet begun.
Suspended	When CTE-LDT is suspended by user or due to QoS schedule.
Unknown	GuardPoint is not active on the host, so status could not be determined.

Obtaining Information About Keys Applied to Files

Key Report Option

In the following command, you can use the `report` option of the `voradmin` command to obtain information about all of the keys in use on the GuardPoint. The report lists all keys used in the GuardPoint. For each key, it gives the key name and key version number. It lists each unique key name and version combination only once, no matter how many files use the key.

The following example shows three keys used in the GuardPoint `/oxf-fs1/gp1`:

```
# voradmin ldt key report /oxf-fs1/gp1
LDT_KEY1,1
LDT_KEY2,2
LDT_KEY3,5
```

For an overview of `voradmin ldt`, see ["CTE-LDT Command-Line Administration: voradmin command" on page 73](#).

Key Map Option

In the `voradmin ldt key [report|map] <key_name> <guard_path>` command, you can use the `map` option to obtain information about which files in a GuardPoint were transformed with a specific key, where:

- `<key_name>` is the name of the key.
- `<guard_path>` is the path of the GuardPoint where the key was used.

For example, to view information about the key `LDT_KEY2` in the GuardPoint `/oxf-fs1/gp1`, you would enter:

```
# voradmin ldt key map LDT_KEY2 /oxf-fs1/gp1
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
/oxf-fs1/gp1/file12345.dat10
```

Keys without a version number are used by files in an exclusion key rule or files that have yet to undergo initial key rotation. Use `voradmin ldt key map` in conjunction with `voradmin ldt attr get` to determine if a file using a key without a version number is part of an exclusion key rule or awaiting initial key rotation.

Showing GuardPoints During Rekey (Linux)

Use the following command to display a list of known CTE-LDT metadata stores and any associated GuardPoints currently undergoing transformation.

```
# voradmin ldt list all
MDS_1: type=file, nguards=0, name=/disk2/::vorm:mds::
      Guard Table: version 1 nentries 0
MDS_2: type=file, nguards=0, name=/disk3/::vorm:mds::
      Guard Table: version 1 nentries 0
MDS_3: type=file, nguards=0, name=/disk4/::vorm:mds::
      Guard Table: version 1 nentries 0
```

For an overview of `voradmin ldt` commands, see ["CTE-LDT Command-Line Administration: voradmin command" on page 73](#).

Suspending and Resuming Rekey and/or Scan Phase

The QoS schedule specifies certain time windows when CTE-LDT operations must be stopped temporarily. However, you can also suspend or resume CTE-LDT at the host level at any time.

To suspend CTE-LDT through the DSM Management Console:

1. Go to **Hosts > Hosts**.
2. Click the name of the host where you want to suspend or resume rekey.
3. Click the **GuardPoint** tab.
4. Click **Suspend/Resume Rekey** to suspend/resume CTE-LDT operations on the host.

Considerations

- Disabling, or unguarding, an CTE-LDT GuardPoint where a rekey is in progress automatically suspends the CTE-LDT rekey operation.
- You can also use the `voradmin suspend/resume` command in Windows Powershell to suspend and resume the rekey. However, if you use the `voradmin ldt suspend` command to pause the rekey process, the CTE-LDT suspended state is not retained when the system reboots. If you want to retain the state after reboot, suspend the rekey from the DSM.
- On Linux, you can pause CTE-LDT during the scan phase of CTE-LDT. When paused during scan, CTE-LDT suspends operations that traverse through the namespace of GuardPoints in the scan phase of transformation. Suspending CTE-LDT during scan stops file lookup operations of CTE-LDT. This eliminates performance impact to I/O intensive production workloads, such as file serving type workloads, that access large number of files.

Automatic Suspend and Resume of CTE-LDT Operations Due to Insufficient Disk Space (Linux)

CTE-LDT requires adequate storage space headroom to perform CTE-LDT operations such as rekeying on GuardPoints. On Linux, if available storage space drops below the threshold required for CTE-LDT operations to continue, the CTE-LDT operations are automatically suspended. Once additional storage space is available in the file system, CTE-LDT operations automatically resume.

As available space approaches the threshold for automatic suspension, CTE-LDT sends an alert to the DSM to notify you that you should free up more storage space before CTE-LDT operations are suspended. The alert on the DSM is:

```
Low space on guard point [GuardPoint], increase free space or CTE-LDT will be suspended.
```

Behavior of Automatic Suspend and Resume of CTE-LDT Operations on ext4 File Systems

By default, ext4 file systems reserve a portion of the storage space for use only by privileged processes to prevent running out of storage space in file systems. In this situation, non-privileged processes are automatically blocked from writing to the file system until the free disk space level reaches the minimum threshold. As CTE-LDT operates in privileged mode, CTE-LDT operations continue without blockage even if the free disk space threshold is low. Because of this ext4 feature, CTE-LDT operations on ext4 file systems may not be suspended due to low available storage space, even when the `df` command reports storage is 100% allocated.

Rotating Encryption Keys While a Rekey is in Progress (Relaunch)

On Linux, if a key is rotated (either manually or automatically when a key version expires) while CTE-LDT is in progress on a GuardPoint, the key rotation is processed and queued, and the GuardPoint is marked for relaunch. Relaunch indicates the need to restart CTE-LDT after the current transformation completes. If the GuardPoint has been rekeyed and is flagged for relaunch, CTE-LDT launches as soon as the GuardPoint is enabled.

Files already undergoing transformation at the time of the new key rotation complete rekey to the key version already in progress. Files that start transformation after the new key rotation request are rekeyed to the new key version. Once the current CTE-LDT of the GuardPoint is complete, CTE-LDT automatically relaunches to transform any files that are not rekeyed to the latest key version.

For example:

```
# voradmin ldt attr get /oxf-fs1/gp1
LDT stats: version=2, rekey_status=rekeying,relaunch
           Number of times rekeyed:      1 time
           Rekey start time:              2020/03/18 16:54:00
```

```
Last rekey completion time:          2020/03/18 16:53:38
Estimated rekey completion time:    0 days 0 hours 6 minutes
Policy key version:                 344
Data stats:
    total=9.8GB, rekeyed=0.0MB
    truncated=0.0MB, sparse=0.0MB
File stats:
    total=1000, rekeyed=0, failed=0
    passed=0, skipped=0, created=0, removed=0, excluded=0
```

Note

Relaunch is supported on Linux only. It is not supported on Windows.

File System Operations

The following sections describe the file system operations that may require attention from the DSM Administrator.

Renaming Files and Folders

On both Linux and Windows hosts, you can rename files during initial transformation or rekey operations.

- On Linux, you cannot rename folders (directories) in a GuardPoint during a rekey operation. Any attempt to rename a directory is rejected with the error EAGAIN (try again) while CTE-LDT is in progress including the period during which transformation is suspended.
- On Windows with VTE version 6.1.0 or later, CTE-LDT stops if it is transforming the contents of a folder and a user attempts to rename/move that folder.

You can change the stopping behavior of CTE-LDT using the configuration parameter `oxf_stop_on_rename`.

Using the Registry Editor, or the Windows command line, add a registry entry in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Vmmgmt\Parameters` for `oxf_stop_on_rename`.

Registry Name	Values	Comments
<code>oxf_stop_on_rename</code>	0 - Disabled	CTE-LDT does not stop if there is contention.
	1 - Enabled	CTE-LDT stops if there is contention. Default: Enabled

For the target folder in rename operation, CTE-LDT is never stopped.

Deleting a File

When a file is removed before it is rekeyed, the file is not included in the total number of files transformed on the GuardPoint **Status** page. Any discrepancy between total number of files to transform and those transformed is due to the removal of files from GuardPoints during CTE-LDT.

The `voradmin` command provides more detailed file level statistics related to rekey operations on the host. You can run `voradmin` to get file level statistics:

```
# voradmin ldt stats <guard_path>
```

File Handling (Windows Only)

It is critical that you understand how the CTE-LDT process handles read-only, binary (executable), NTFS encrypted and NTFS compressed files.

The CTE-LDT process is subjected to all of the File System policies and attributes set on the files. In some cases, this prevents CTE-LDT from encrypting a file. If users or applications are accessing files while CTE-LDT is in progress, CTE-LDT cannot change the attributes of the files and encrypt the file. It is critical that you understand how CTE-LDT handles various types of files:

- **NTFS Encryption and Compression**

If NTFS encryption and compression is enabled on a file or folder, the CTE-LDT process cannot encrypt these files. To maintain the data coherency, CTE-LDT skips the encryption of these files. These files display as “passthrough” files in the CTE-LDT statistics.

- **Read-Only Files**

When CTE-LDT encounters read-only files, it rekeys the file by resetting the read-only attribute and then setting the attributes back again when the rekey completes. If a file is open, CTE-LDT skips this file.

1. If the file is not opened, CTE-LDT changes the attributes of the file and stores the original attributes in the file metadata.
2. CTE-LDT starts Rekey on this file.
3. If a user requests to open a file for writing while rekey is in progress, access is denied. User can only open files for reading.
4. CTE-LDT restores the attributes once rekey is done.

- **Executable Files**

If an executable is running, or files are exclusively locked by the application, the CTE-LDT process cannot encrypt those files as it is unable to acquire the required locks on the files. CTE-LDT skips these files and changes to the INCOMPLETE state.

Enabling GuardPoints in Read-Only mounted file systems (Linux)

Access to a GuardPoint enabled in a read-only mounted file system is restricted to read operations. You cannot modify data in such file systems, therefore, you cannot perform CTE-LDT operations on GuardPoints in read-only file systems. For this reason, CTE-LDT automatically suspends operations when GuardPoints are enabled on read-only file systems. CTE-LDT ignores all attempts to resume CTE-LDT operations until the underlying file system is remounted with read/write access.



WARNING

You must disable a GuardPoint before changing the read/write mount options of the underlying file system. After changing the mount options, you can re-enable the GuardPoint. CTE-LDT operations adapt to the read/write options of the underlying file system when you enable the GuardPoint. Changing the mount options while a GuardPoint is enabled is unsupported and may result in unexpected errors.

Copying Files Into a GuardPoint

If you copy a file into a GuardPoint without an Apply Key rule, make sure that the file was previously copied from the same GuardPoint, or a GuardPoint protected with the same policy/versioned key. A copy operation, without an Apply Key rule, is the same as a backup or restore of a file from/to an CTE-LDT protected GuardPoint.

CTE enforces key rules of an CTE-LDT policy while a GuardPoint is enabled. CTE cannot enforce the key rules while a GuardPoint is disabled. Modifying or adding data/files inside a disabled GuardPoint is not only unsupported, but it also results in unrecoverable data corruption.



WARNING

Do not add new files or modify existing files inside CTE-LDT protected GuardPoints while the GuardPoint is not enabled. This results in unrecoverable data corruption and/or files that cannot be accessed when the GuardPoint is enabled.

Behavior of Hard Links Inside and Outside of GuardPoints (Windows)

When using hard links on Windows, all the hard links to a file must be within the boundary of a GuardPoint and must use the same key. The following scenarios provide additional details:

- If hard links to the same file are inside a GuardPoint and outside a GuardPoint, the effect on the file depends on what process accesses which hard link first. If the hard link within the GuardPoint is opened first, the file is transformed. If the hard link outside the GuardPoint is opened first, the file won't be transformed.
- If hard links to the same file exist in different GuardPoints with different keys, the file will be corrupted.
- If hard links to the same file exist in the same GuardPoint but with different keys, such as if folder-based rules are used, there will be a conflict in the key.

Excluding Files or Directories from Rekey

You can exclude files or directories from the initial transformation and subsequent rekeys with exclusion key rules. For example, you can exclude a subset of non-secret files from a larger set of files that are encrypted with an Live Data Transformation policy.

You set up exclusion key rules on a DSM version 6.3.0 and higher. For details, see the *DSM Administration Guide*.

Examples of Exclusion Key Rules

This section describes some examples of how to use an exclusion key rule.

Encrypt Files With Exclusion Property a Non-Versioned Key

The following exclusion key rule applies the non-versioned key, `Key_TextFiles`, to any *new* files that are created with a `*.txt` extension.

Note

Existing `*.txt` files in the GuardPoint during the initial CTE-LDT data transformation process are assumed to be already encrypted with the same key that you specify in the exclusion key rule. These existing files are *not* transformed during the initial encryption or during any subsequent rekeys. The key you specify in the exclusion key rule is applied to new `*.txt` files only.

In the Policy, do the following:

1. Add a Key Rule.
2. In the **Resource** field, select a resource set that specifies `*.txt` in the **File** field.
3. Select the **Exclusion Rule** check box. The DSM changes to show only a single **Key** field.
4. In the **Key** field, select the key `Key_TextFiles`.

5. Add any other key rules or exclusion key rules to the policy that you want. You must add at least one non-exclusion key rule that specifies the current encryption key and the versioned encryption key that you want to use with this Live Data Transformation policy.

For example, you could add another exclusion key rule that specifies all **.doc** files should be encrypted with the key `Key_DocFiles`, or one that specifies all **.zip** files should be left unencrypted by specifying the key `clear_key`.

Exempt Excluded Files from Encryption (Set to `clear_key`)

The following exclusion key rule sets all files in the resource set `/oxf-fs1/gp1/Clear_Files_Folder` (Linux) or `\oxf-fs1\gp1\Clear_Files_Folder` (Windows) to `clear_key` (in other words, not encrypted). Files in other directories that match other key rules in the same policy may be encrypted. This could allow unrestricted access to the files in `/oxf-fs1/gp1/Clear_Files_Folder` (Linux) or `\oxf-fs1\gp1\Clear_Files_Folder` (Windows) while access may be restricted to files in parallel directories.

- Linux Exclusion Key Rule: The Resource Set **Directory** field should contain `/oxf-fs1/gp1/Clear_Files_Folder`, and the **Key** should be `clear_key`.
- Windows Exclusion Key Rule: The Resource Set **Directory** field should contain `\oxf-fs1\gp1\Clear_Files_Folder`, and the **Key** should be `clear_key`.

Requirements for Exclusion Key Rules

Keep in mind the following requirements when configuring exclusion key rules:

- Before adding an exclusion key rule to an existing policy, you must disable all GuardPoints protected with the policy. Log on to the DSM to disable the GuardPoint.
- You cannot choose a versioned key for the key in an exclusion key rule. Only non-versioned keys or `clear_key` (no encryption) are valid for exclusion key rules.
- Policies with exclusion key rules:
 - Can be added to Live Data Transformation policies created in the DSM 6.3 or higher.
 - Can be applied to GuardPoints on protected hosts running VTE version 6.2 or higher.Do *not* add an exclusion key rule to an existing Live Data Transformation policy if that policy is being used to protect hosts running VTE version 6.1.x or earlier.
- All exclusion key rules must be *above* all CTE-LDT transformation key rules in the **Key Selection Rules** area in the policy.

Usage Notes and Limitations for Configuring Exclusion Key Rules

Keep in mind the information in the following sections when configuring an exclusion key rule.

Adding an Exclusion Key Rule to an Existing Policy with Versioned Keys (Linux)

When adding an exclusion key rule to an existing policy, the exclusion rule only applies to newly created files. Existing files that match the exclusion key rule remain encrypted with the same versioned key(s) specified in the non-exclusion key rule in the policy and will be rekeyed to the key in the exclusion key rule when the versioned key(s) rotates.

To force an existing file that matches an exclusion key rule to be transformed to the key in the exclusion key rule (non-versioned in this example), use one of the following methods:

- Rotate the versioned key specified in the policy to initiate rekey operations on the GuardPoint.
- Copy the existing file within the GuardPoint. The new file will be associated with the resource set in the exclusion key rule and will be encrypted with the non-versioned key. You can then delete the original file.

To perform a similar conversion on Windows, see ["Changing a Folder or Files from Versioned to Non-Versioned Key \(Windows\)" on the facing page](#).

Adding an Exclusion Key Rule That is Part of an Active GuardPoint (Linux)

To edit and/or add an exclusion key rule to an CTE-LDT policy, all GuardPoints using the policy must first be disabled before the new key rule can be added. See “Add Key Selection Rules” in the “Policies” chapter of the *DSM Administration Guide*.

Changing an Exclusion Key Rule That is Part of an Active GuardPoint (Windows)

Changes that you make to an exclusion key rule that is part of an existing policy in an active GuardPoint do not take effect until the GuardPoint that the exclusion key rule is part of is disabled and enabled again.

Conflicting Keys as the Result of Rename Operations

Do not attempt to move or rename a file encrypted with a versioned key to a name associated with an exclusion key rule with `clear_key`. If you attempt such a move or rename, the original file is unaffected but following error is output on Linux systems and a log entry is created on the DSM:

```
<command name>: setting attribute 'user::secfs:xattr:' for 'user::secfs:xattr:': Invalid argument
<command name>: failed to close '<filename>': Invalid argument
```

No error is displayed on Windows systems. The target moved or renamed file is corrupted and should be deleted. The target file is also flagged with the `xattr_error` flag on Linux and `Rekey Status Excluded` on Windows. This flag prevents subsequent read/write access to the file. You can check the CTE-LDT attributes for the presence of this flag. See ["About the Exclusion Attribute for Files Matching an Exclusion Key Rule" on page 54](#).

Also, a log entry is sent to the DSM on Linux systems when this occurs. For example, if you moved the versioned file `/gp/foo.txt` into the GuardPoint `/gp/subdir/foo.txt` with an exclusion key rule that excludes matching files with the `clear_key`, the following log message would be created on the DSM:

```
[CGA] [WARN ] [29261] [CGS3268W] LDT-ALERT: encrypted data detected in filename [foo.txt] inode [35720037] in guard point [/gp] under clear exclusion key rule
```

Overlapping Exclusion Key Rules

Multiple exclusion key rules in the same policy may overlap each other. For example on Linux, if the non-versioned key `Key_A` is associated with resource `/oxf-fs1/gp1/Folder_Enc_With_KEY_A` and the non-versioned key `Key_B` is associated with resource `*.txt`, placement of the file `/oxf-fs1/gp/Folder_Enc_With_KEY_A/foo.txt` overlaps the two key rules. In such a case, the first rule in the policy is enforced on `/oxf-fs1/gp/Folder_Enc_With_KEY_A/foo.txt` when the file is created and in subsequent file access.

On Windows, if the non-versioned key `Key_A` is associated with resource `c:\oxf-fs1\gp1\Folder_Enc_With_KEY_A` and the non-versioned key `Key_B` is associated with resource `*.txt`, then they would overlap on the file `c:\oxf-fs1\gp\Folder_Enc_With_KEY_A\foo.txt`. In such a case, the first rule in the policy is enforced on `c:\oxf-fs1\gp\Folder_Enc_With_KEY_A\foo.txt` when the file is created and in subsequent file access.

Caution About Applications That Create Temporary Files (Windows)

Some applications on Windows create a temporary file version of the original file when you open and modify a file. This behavior can affect how you implement exclusion key rules.

If you have an exclusion key rule that uses a file extension to exclude files that may be opened and modified by such an application, exclude the temporary file name extension also. If you don't exclude the temporary file, the temporary file may be encrypted by another policy that matches the temporary file extension. Then the original file, which is copied from the temporary file, will be unreadable. Also keep in mind that other applications that may create temporary files with the same file extension and consider what policies should affect those temporary files.

This situation can happen with Microsoft Office files such as the `.docx` files used by Microsoft Word. When you open and modify a `.docx` file, Word creates a `.tmp` file version of that file. So for Microsoft Word you should add `*.tmp` to the exclusion key rule resource set if you add `*.docx`.

Rename Operations Crossing Key Rules (Linux)

On Linux, when a rename operation crosses key rules, the rename operation copies the source file to a new file using the new name and removes the original file. If the source file is flagged for exclusion key rule property, the target new file is disassociated with the exclusion key rule if the new name no longer matches the resource set associated with exclusion key rule. For more information, see ["About the Exclusion Attribute for Files Matching an Exclusion Key Rule" on the next page](#).

Using Linked Files with Exclusion Key Rules (Linux)

On Linux, do not create multiple hard links to the same target file such that the pathname of each hard link is associated with a resource set of an exclusion key and the key rules have different keys. Accessing the file through the pathname of each hard link results in a different key to be applied to the file resulting in data corruption in the target file due to application of multiple keys to the same data.

If you must create hard links, be sure the pathnames of hard links and the target file are within the same resource set.

Changing a Folder or Files from Versioned to Non-Versioned Key (Windows)

Exclusion key rules provide a way to convert a subset of guarded files or the contents of a folder from being encrypted by a versioned key to being encrypted by a non-versioned key. After this conversion, the excluded files or directory contents will be encrypted at the last version of the versioned key but the encryption keys for those items will not rotate to a new version when the keys for other non-excluded files are rotated. In other words, the excluded files or folder contents will be encrypted by a non-versioned key.

Follow these steps to change selected files or folder contents to a non-versioned key:

1. In the DSM, clone the versioned key that is used in the policy that you plan to edit. Cloning a key creates a non-versioned copy of the existing version of the versioned key.
2. In the DSM, disable the GuardPoint. Disabling the GuardPoint is required before modifying a policy applied in that GuardPoint.
3. Configure one or more resource sets to match the files that you want to exclude. For example, the resource set `star-dot-text` could contain `*.txt` and the resource set `sales-folder` could contain `\sales\*`.

4. Add one or more exclusion key rules to convert matching files to a non-versioned key. In the following example, files matching *.txt and files in the sales folder (as defined in resource sets) will be converted from the current version of the versioned key AES256_versioned to AES256_clone, assuming AES256_clone is a clone of AES256_versioned.

Order	Resource	Current Key	Transformation Key	Exclusion Rule
1	star-dot-txt	AES256_clone	AES256_clone	Y
2	sales-folder	AES256_clone	AES256_clone	Y
3		clear_key	AES256_versioned	N

Exclusion key rules must be ordered before other rules.

5. On the command line, run the following command to remove the CTE-LDT metadata from the files that you want to convert from versioned key to non-versioned key encryption:

```
voradmin ldt attr delete <path_to_files>
```

To recursively delete the CTE-LDT metadata from all files matching a pattern in all subfolders, use the following form, including * as a wildcard where needed:

```
voradmin ldt attr delete <path_to_files> -filter <filename>.<extension>
```

Note: Be careful when deleting the CTE-LDT metadata from files. If you delete the metadata from a file that does not match an exclusion key rule policy, the file will be unreadable after the next rekey.

Given the example exclusion key rule described in step 4, you would need to run this command on all files with the extension .txt (first example below) and on the files in \sales (second example below).

```
voradmin ldt attr delete c:\gp1 -filter *.txt  
voradmin ldt attr delete c:\gp1\sales
```

For more information about using voradmin on CTE-LDT metadata, run voradmin ldt attr /? on the command line.

6. In the DSM, re-enable the GuardPoint that includes the new exclusion key rule.
7. In the DSM, rotate the key for the policy that includes the new exclusion key rule.

Using the example exclusion key rule in step 4, after completing this procedure, files matching *.txt and files in the sales folder will have the exclusion attribute set and will be excluded from rekeying (see ["About the Exclusion Attribute for Files Matching an Exclusion Key Rule" below](#)). Files not matching the exclusion key rule will be rekeyed to the next version of the AES256_versioned key.

To perform a similar conversion on Linux, see ["Adding an Exclusion Key Rule to an Existing Policy with Versioned Keys \(Linux\)" on page 51](#).

About the Exclusion Attribute for Files Matching an Exclusion Key Rule

Files matching an exclusion key rule have the status rekey_excluded in the CTE-LDT attribute. For more information about CTE-LDT attributes, see ["CTE-LDT Metadata in Extended Attributes" on page 59](#). To check for the exclusion attribute on a file, see ["Determining if a File is Included in an Exclusion Key Rule" on the facing page](#).

The Exclusion Attribute is Persistent

Exclusion from rekey is a persistent property. A file excluded from rekey is not rekeyed regardless of changes that may seem to disassociate the file from the exclusion key rule. For example, if you rename a file to a new name within the same GuardPoint that no longer matches the exclusion key rule that the original name matched, the file with the new name retains the encryption type (non-versioned key or clear_key) of the exclusion key rule. To remove the exclusion attribute from a file you must copy the file rather than move or rename it (see ["Removing the Exclusion Attribute From a File" on the facing page](#)).

Determining if a File is Included in an Exclusion Key Rule

Use the `voradmin ldt attr get <path to file>` command to check whether a file is associated with an exclusion key rule.

- On Linux, an excluded file will include the status `rekey_excluded` in the `voradmin` output. For example:

```
# voradmin ldt attr get /oxf-fs1/gp1/foo.txt
CTE-LDT attributes: rekeyed_size=0, rekey_status=rekey_excluded
```

- On Windows, an excluded file will include the attribute `Rekey Status Excluded` in the `voradmin` output. For example:

```
C:\> voradmin ldt attr get c:\gp1\foo.txt
CTE-LDT attributes:
Rekey Status Excluded
Initial Rekeyed Size 9 Bytes
Data Transformed 0 Bytes
```

Key:

```
Current Key Name/Version (Clear_Key)
New Key Name/Version (Clear_Key)
```

Removing the Exclusion Attribute From a File

To disassociate a file from an exclusion key rule, you must copy the file to a new file not associated with the resource set of the same or another exclusion key rule as the source file. You can then remove the original file. The new file is created under the default key rule of whatever policy applies to the new file. Moving or renaming a file does not disassociate a file from an exclusion key rule (see ["The Exclusion Attribute is Persistent" on the previous page](#)).

For example, assume the following exclusion key rule where `Key_TextFiles` is a non-versioned key:

Exclusion Key Rule: Resource set = *.txt, Key = `Key_TextFiles`

If you copy the file `test1.txt` to `test1.foo`, `test1.foo` is created with whatever key is specified in the policy that matches the new file. The key for the new file could be a non-versioned key, versioned key, `clear_key`, or, no key at all if the new file is outside of a GuardPoint. The original file `test1.txt` remains unchanged and encrypted with the `Key_TextFiles` non-versioned key because the file remains in the exclusion key rule.

Rename and Restore Operations (Linux)

The effect of rename or backup/restore operations involving files associated or not associated with exclusion key rules is mixed and somewhat confusing. In some cases, the operations to restore or rename cause conflicts between the key associated with the source file and the key associated with the target file. For example, the result of a rename operation involving a source file not associated with an exclusion key rule and target file name associated with a resource set of an exclusion key rule is different from the result of the same operation when target file name is associated with the resource set of an exclusion key rule with `clear_key`.

Note

Be sure to review the effect of the operations below and avoid administrative operations that cross associations of files across multiple resource sets with conflicting key rules.

Backup/Restore

The table below illustrates the status and the key effect of restore operations involving mixed keys associated with source files from backup image and existing target files inside GuardPoint.

Key Applied to File in Backup	Key Applied to existing file in GuardPoint	Key Effect of Restore Operation on Existing file
Versioned	Versioned	Versioned
Versioned	Exclusion key	xattr_error (failed)
Versioned	Exclusion clear key	xattr_error (failed)
Exclusion key	Versioned	Exclusion key
Exclusion key	Exclusion key	Exclusion key
Exclusion key	Exclusion clear key	xattr_error (failed)
Exclusion clear key	Versioned	Exclusion clear key
Exclusion clear key	Exclusion key	xattr_error (failed)
Exclusion clear key	Exclusion clear key	Exclusion clear key

The table below illustrates the status and the key effect of restore operations involving mixed keys associated with source files from backup image and new target files not present inside GuardPoint.

Key Applied to File in Backup	Key Applied to existing file in GuardPoint	Key Effect of Restore Operation on Existing file
Versioned	Versioned	Versioned
Versioned	Exclusion key	xattr_error (failed)
Versioned	Exclusion clear key	xattr_error (failed)
Exclusion key	Versioned	Exclusion key
Exclusion key	Exclusion key	Exclusion key
Exclusion key	Exclusion clear key	xattr_error (failed)
Exclusion clear key	Versioned	Exclusion clear key
Exclusion clear key	Exclusion key	xattr_error (failed)
Exclusion clear key	Exclusion clear key	Exclusion clear key

Rename Operation

The table below illustrates the status and the key effect of rename operations for different combinations of versioned, exclusion key, and exclusion clear key.

Key Applied to File in Backup	Key Applied to existing file in GuardPoint	Key Effect of Restore Operation on Existing file
Versioned	Versioned	Versioned

Key Applied to File in Backup	Key Applied to existing file in GuardPoint	Key Effect of Restore Operation on Existing file
Versioned	Exclusion key	Exclusion key
Versioned	Exclusion clear key	xattr_error (failed)
Exclusion key	Versioned	Exclusion key
Exclusion key	Exclusion key	Exclusion key
Exclusion key	Exclusion clear key	Exclusion key
Exclusion clear key	Versioned	Exclusion clear key
Exclusion clear key	Exclusion key	Exclusion clear key
Exclusion clear key	Exclusion clear key	Exclusion clear key

Listing All Files Included in an Exclusion Key Rule (Linux)

Determining the files that match an exclusion key rule involves two steps. You list all the keys in a GuardPoint, choose the key that you're interested in, and then run a command to list the files that match that key. This process works for both standard key rules and exclusion key rules.

1. Decide on the GuardPoint that you want to check for excluded files. For example, for the GuardPoint `/oxf-fs1/gp1`, type the following on the command line:

```
# voradmin ldt key report /oxf-fs1/gp1
LDT_KEY1,1
LDT_KEY2,2
LDT_KEY3,5
NON_VERSIONED_KEY
```

The number after the comma is the key version number. See ["Key Report Option" on page 45](#) for more information about the `voradmin` key report.

2. From the key report output, choose the key rule for which you want to list matching files. For example, to see the files associated with the `NON_VERSIONED_KEY` in the previous step, you would type:

```
# voradmin ldt key map NON_VERSIONED_KEY /oxf-fs1/gp1
/oxf-fs1/gp1/file1.dat10
/oxf-fs1/gp1/file2.dat10
/oxf-fs1/gp1/file3.dat10
/oxf-fs1/gp1/file4.dat10
/oxf-fs1/gp1/file5.dat10
```

See ["Key Map Option" on page 46](#) for more information about the `voradmin` key map report.

Listing All Files Included in an Exclusion Key Rule (Windows)

Determining the files that match an exclusion key rule involves two steps. You list all the keys in a GuardPoint, choose the key that you're interested in, and then run a command to list the files that match that key. This process works for both standard key rules and exclusion key rules.

1. Decide on the GuardPoint that you want to check for excluded files. For example, for the GuardPoint `c:\gp1`, type the following on the command line:

```
C:\> voradmin ldt key report c:\gp1
Keys used for GP, c:\gp1 :
clear_key,0
CS1-CTE-LDT-AES256,11
```

The number after the comma is the key version number. The `clear_key` key is not versioned, so the version number is 0.

2. From the key report output, choose the key rule for which you want to list matching files. For example, to show the files associated with the `clear_key` listed above, you would type:

```
C:\> voradmin ldt key map c:\gp1 clear_key,0
Files rekey with key (clear_key,0)-
c:\gp1\file1.txt
c:\gp1\file2.txt
c:\gp1\file3.txt
c:\gp1\file4.txt
c:\gp1\file5.txt
```

Using CTE-LDT with SAP HANA Fibre Channel Systems (Linux Only)

You must add additional CTE commands to the HANA administrator entry. To do so, edit the `/etc/sudoers` with a text editor and add entries for `/usr/bin/voradmin` and `/usr/bin/vmsec`. For example:

```
# hanadm ALL=NOPASSWD:
/usr/bin/secfsd,/usr/bin/voradmin,/usr/bin/vmsec,/sbin/multipath,/sbin/multipathd,/etc/init.d/m
ultipathd,/usr/bin/sq_
persist,/bin/mount,/bin/umount,/bin/kill,/usr/bin/lsof,/sbin/vgchange,/sbin/vgscan
```

If you are using an ext3 file system, you must mount it with extended attributes. To do so, edit the storage section of the `global.ini` file using a text editor and add the following lines:

```
partition_*_data__mountOptions = -o user_xattr
partition_*_log__mountOptions = -o user_xattr
```

Note

See the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide* for more information about SAP HANA.

Chapter 5: CTE-LDT Administration

This chapter contains the following sections:

CTE-LDT Metadata in Extended Attributes	59
DFSR and Replication (Windows)	63
Multi-Node Configuration and Operation	64
Backing Up and Restoring CTE-LDT GuardPoints	64
CTE-LDT Command-Line Administration: voradmin command	73
Upgrading or Downgrading Agent Software On an CTE-LDT Host	74
Moving a CTE-LDT GuardPoint from One CTE-LDT Policy to Another	75
Removing CTE-LDT and Security Encryption	76
Uninstalling the Agent while CTE-LDT is Rekeying GuardPoints	80

CTE-LDT Metadata in Extended Attributes

An *extended attribute* is a name/value pair permanently associated with a file or directory stored in a file system. CipherTrust Transparent Encryption (CTE) creates and maintains its own user extended attributes on CTE-LDT GuardPoint directories and files. The extended attributes are used to store metadata related to each file or directory that is protected using an CTE-LDT policy.

On Linux, CTE-LDT sets extended attributes on GuardPoint directories. The CTE-LDT attribute of an CTE-LDT GuardPoint stores the following metadata:

- Current key version.
- Rekey status.
- Rekey start and end times.
- Estimated completion time.
- Total amount of data transformed.
- Total number of files transformed.
- Current key signature and applied key signature.

On both Linux and Windows, CTE-LDT sets extended attributes on files. The CTE-LDT attribute of a file stores the following metadata:

- Name of the current key.
- Name of the versioned key.
Also referred to in the DSM Management Console and product documentation as the new key or the transformation key.
- Version number of the versioned key.
- CTE-LDT rekey status of the file.

In most cases, the current and new key names are the same. The exception is during initial transformation from a legacy policy to an CTE-LDT policy, when the file has been encrypted with the current key and is being transformed to the current version of the transformation key.

Note

Before you set up a GuardPoint for CTE-LDT, ensure that there is sufficient disk space available in your file system for CTE-LDT metadata. The amount of disk space you need depends on the number of files in your GuardPoint. For more information about the disk space requirement, see ["Planning for CTE-LDT Attribute Storage" on page 62](#).

The state of a file changes during CTE-LDT operations. The extended attributes are continually updated to reflect the current file status, which falls into one of the following categories:

- Rekeyed to the current version of the key.
- Rekeyed to the previous version of the key, or the initial key state (before the first CTE-LDT rekey has been performed).
- Partially rekeyed, where some regions of the file are rekeyed to the new key version and other regions are still keyed to the previous key version or the initial key.

Listing Extended Attributes

You can list extended attributes by using native operating system commands, or system calls. As part of GuardPoint administration, CTE can modify or delete extended attributes.

In Linux, CTE-LDT attributes are set on GuardPoint directories and regular files in GuardPoint directories protected with CTE-LDT policies. The CTE extended attribute name is `::secfs:xattr:.`

The following example uses the native Linux operating system command `attr` to display the CTE-LDT attribute for the GuardPoint `/oxf-fs1/gp1` and the file `/oxf-fs1/gp1/File_1.txt`.

Example 1:

```
# attr -l /oxf-fs1/gp1/File_1.txt
Attribute "::secfs:xattr:" has a 1044 byte value for /oxf-fs1/gp1/File_1.txt
Attribute "selinux" has a 37 byte value for /oxf-fs1/gp1/File_1.txt
```

Example 2:

```
# attr -l /oxf-fs1/gp1
Attribute "::secfs:xattr:" has a 1044 byte value for /oxf-fs1/gp1
Attribute "selinux" has a 37 byte value for /oxf-fs1/gp1
```

Example 3:

In the following example, the file `/oxf-fs1/gp1/File_1.txt` has the same name for current and new keys at the same key version. In the following example, if the versioned key `LDT_KEY` is at version 755, the file is rekeyed to the latest key version under the CTE-LDT policy.

```
# voradmin ldt attr get /oxf-fs1/gp1/File_1.txt
CTE-LDT attributes: rekeyed_size=4096, rekey_status=none
Key:    name=LDT_KEY, version=755
```

Example 4: (Linux)

The following is example of an CTE-LDT attribute on a GuardPoint directory on Linux:

```
# voradmin ldt attr get /oxf-fs1/gp1
LDT stats: version=1, rekey_status=rekeying
  Number of times rekeyed:      3 times
  Rekey start time:             2018/08/04 16:24:45
  Last rekey completion time:   2018/07/04 16:24:04
  Estimated rekey completion time: N/A
  Policy key version:           2043
```

```
Data stats:
    total=3.3GB, rekeyed=1.5GB, truncated=0.0MB
File stats:
    total=4307, rekeyed=1181,
    passed=2, skipped=0, created=0, removed=0
```

Example 5: (Windows)

The attribute for the GuardPoint `c:\GP 1` contains the status (rekeyed) and statistics specific to the GuardPoint and CTE-LDT. Following is sample output of `voradmin` command on Windows for statistics on a file:

```
C:\> voradmin ldt attr get c:\GP\Test.txt
LDT attributes:
    Rekey Status          Rekeyed
    Initial Rekeyed Size  10 Bytes
Key:
    Key Name/Version      (LDT_KEY, 28)
```

The attribute for GuardPoint `C:\GP` contains the status (rekeyed) and statistics specific to the GuardPoint and CTE-LDT:

```
C:\> voradmin ldt attr get c:\gp\
LDT Stats
-----
    Rekey Status          LDT_ST_REKEYED
    Last rekey completion time    10/2/2017 4:26:50
    Rekey Start time            10/2/2017 4:26:17
    Estimated rekey completion time    000:00:00

File Stats:
    Total      444
    Rekeyed    444
    Skipped    0
    Errored    0
    Passed     0
    Removed    0

Data Stats:
    Total      11 GB (12649143417 Bytes)
    Rekeyed    11 GB (12649143417 Bytes)
    Truncated  0 Bytes
```

MDS File (Linux)

In addition to CTE-LDT attributes, the CTE-LDT process on Linux requires persistent storage for additional metadata related to encrypting, or rekeying, files in GuardPoints. CTE-LDT allocates the storage space as soon as the CTE-LDT process starts on a GuardPoint. It maintains this storage space during the entire transformation process, until the GuardPoint is completely transformed.

Storage for this metadata is allocated and managed in a special file, called the MDS (metadata store) file. The MDS file resides inside a GuardPoint directory so each GuardPoint has its own MDS file.

The MDS file is a CTE protected file with the name `::vorm:mds::`. For example:

```
# ls -l /oxf-fs1/gp1/::vorm:mds::
-rwxr-xr-x. 1 root  root 31754474496 Dec  8 09:09 /oxf-fs1/::vorm:mds::
# du -B 1024 /oxf-fs1/gp1/::vorm:mds::
25056    /oxf-fs1/::vorm:mds::
```

As shown above, the MDS file is sparse. In the example, the file size is approximately 30GB, however the file is allocated with approximately 25MB of disk storage. CTE-LDT automatically creates the MDS file the first time the CTE-LDT process starts on any GuardPoint in the file system namespace. It populates the MDS file with all of the metadata for the GuardPoint at the beginning of the CTE-LDT process. Disk space allocated to the MDS file is freed and the MDS file in the GuardPoint directory is removed when the CTE-LDT process completes on the GuardPoint.



WARNING

The MDS file is protected. You cannot remove it unless the administrator runs the `voradmin` command to manually remove the MDS file once it is no longer needed. See ["Deleting CTE-LDT Metadata \(Linux\)" on page 79](#) for more information.

CTE-LDT automatically allocates and deallocates disk space for the MDS file as part of the CTE-LDT process. Deallocation of disk space for a GuardPoint does not change the MDS file size, although it frees the disk blocks. MDS files are sparse and very large in size. With no GuardPoint undergoing CTE-LDT, the minimum allocation of an MDS file is approximately 25MB.

Planning for CTE-LDT Attribute Storage

Before a GuardPoint is enabled for CTE-LDT, make sure that there is sufficient free disk space in the file system to which the GuardPoint belongs. Free space is required for CTE-LDT attributes (CTE extended attributes) and (in Linux) metadata in the MDS file. CTE-LDT attributes are created during initial encryption and are never freed until the GuardPoint is permanently unguarded and removed from the protection of an CTE-LDT policy. In contrast, disk space for metadata in the MDS file is temporary, kept only during the live transformation process.

When planning how much free disk space to reserve for CTE-LDT on a GuardPoint, consider the following:

- Number of files in the GuardPoint
- (Linux) Average length of absolute pathnames of files in the GuardPoint

The CTE-LDT process pre-allocates disk space for the Linux MDS file based on a minimum of 200K files with an average pathname of 1024 bytes per GuardPoint. The minimum space amounts to 325MB of disk space for the MDS file for each GuardPoint, even if file count is very low. (In Windows, CTE-LDT reserves the space when the file is rekeyed.)

Using `voradmin` To Estimate Disk Space Required for CTE-LDT (Linux)

In Linux, you can use the `voradmin ldt space` command to estimate the amount of disk space required for CTE-LDT attributes and the MDS file. The result is rounded to the nearest MB. The syntax of the command is:

```
# voradmin ldt space <guard path>
```

The following example shows how to estimate the required disk space to perform CipherTrust Transparent Encryption - Live Data Transformation on 1501 files in the GuardPoint `/oxf-fs1/gp1`. Estimate the disk space before protecting `/oxf-fs1/gp1` using an CTE-LDT policy. For example:

```
# voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 1501 files without CTE-LDT extended attributes
CTE-LDT disk space requirements: total 169MB (CTE-LDT attributes=6MB, MDS=163MB)
```

The `voradmin` command reports that 1501 files in `/oxf-fs1/gp1` without CTE-LDT attributes. These files are new to CTE-LDT. 6MB of space is required for the CTE-LDT extended attributes and 163MB for metadata in the MDS file.

The following example shows the output of the same command after encryption completes. This estimates the additional disk space needed for the next CTE-LDT rekey operation. For example:

```
# voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 0 files without CTE-LDT extended attributes
CTE-LDT disk space requirements: total 163MB (CTE-LDT attributes=0MB, MDS=163MB)
```

The voradmin command still reports on the same 1501 files, but because encryption has occurred using CTE-LDT, the files all have their CTE-LDT attributes. No additional space is required for CTE-LDT extended attributes on the next run. However, since the MDS file is transient and deletes after it finishes encrypting the GuardPoint, it requires additional space for the next key rotation.

Note

Windows estimates space using the following equations:

- Permanent Space = Number of Files * 4K
- Temporary Space = 128K * (Number of CPU * 2)

Displaying Metadata

Use the following command to see CTE-LDT file attributes or GuardPoint attributes:

```
# voradmin ldt attr get [<file name path> | <guard path>]
```

For an overview of voradmin ldt, see ["CTE-LDT Command-Line Administration: voradmin command" on page 73](#).

Verifying Metadata (Windows only)

Use the following command to verify if the metadata is corrupt:

```
# voradmin ldt attr verify [<file name path> | <guard path>]
```

For an overview of voradmin ldt, see ["CTE-LDT Command-Line Administration: voradmin command" on page 73](#).

DFSR and Replication (Windows)

The Distributed File System Replication (DFSR) service is a multi-master replication engine used to maintain synchronized folders on multiple servers. Replicating data to multiple servers increases data availability and provides users in remote sites with fast, reliable access to files.

If you are creating GuardPoints in a DFSR environment, you must first add the DFSR private folder guard path to the exclusion list in the Windows Registry. CTE-LDT should not attempt data transformation on this read-only directory.

1. Using the Registry Editor, or the Windows command line, add a registry entry in: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Vmmgmt\Parameters` named "LDTEExclusionGPList" of type REG_MULTI_SZ.
2. Add the `DfsrPrivate` directory path to the `LDTEExclusionGPList`.
For example, if the DFSR private directory path is `D:\data\DfsrPrivate`, add this string in `LDTEExclusionGPList`.
3. Reboot the system to make the change take effect.

Note

CTE-LDT does not perform a rekey on the DFSR private directory. Its rekey status is always "N/A".

If an application, or user, is performing a rename or a delete folder operation inside a GuardPoint with an CTE-LDT policy, this may restart the rekey process. Files which are already rekeyed will not be rekeyed again.

- If a rename or a delete operation is already performed on rekeyed files/folder, then the rekey process does not restart.
- If a rename or delete operation is performed in a folder where a rekey is in progress, CTE-LDT needs to stop the rekey process and restart the rekey again.

Multi-Node Configuration and Operation

This section describes what to expect at runtime when CTE-LDT operates in a multi-node cluster environment.

CTE-LDT Behavior on Failover

In a multi-node cluster, CTE-LDT runs in active-passive mode. A GuardPoint is only enabled on the active node, and CTE-LDT only runs on the active node. On the DSM Management Console, you can only view statistics for the active host.

If the active host fails over, and the standby host takes control, CTE-LDT also fails over to the second host. On the DSM Management Console, CTE-LDT statistics now appear on the other host.

Veritas Cluster Server

In an HA environment with Veritas Cluster Server, manual failover of service to a stand-by host may require manual intervention. If any GuardPoint is in the scan phase at the time of the manual failover, the failover process fails with the error "UNABLE to OFFLINE". The reason for the failure may be the scan state of a GuardPoint that cannot be suspended. CTE-LDT suspends CTE-LDT operations during the rekey state of transformation. Because CTE-LDT scan operations cannot be suspended, the Veritas Cluster Server fails to suspend CTE-LDT on GuardPoints in the scan phase of CTE-LDT operation. This state of CTE-LDT operation prevents Veritas Cluster Server to manually offline the service for fail-over.

Backing Up and Restoring CTE-LDT GuardPoints

This section describes procedures and considerations related to backing up and restoring data in CTE-LDT GuardPoints.

In addition to the files in a GuardPoint, CTE-LDT stores metadata in extended file attributes. These CTE-LDT attributes contain information that is required for decrypting the files and for the proper operation of CTE-LDT. Therefore, it is critical that your backup application also backs up the extended attributes of the files along with file data.

Clear Text Backup and Restore

A policy that applies a Security Rule with the Apply Key effect on backup/restore operations does not require any special rules for data access by backup applications. Under such a policy, backup applications always read clear data and store clear data in backup media. The backup application is not required to back up the CTE-LDT extended attributes, and a QoS schedule is not required to suspend CTE-LDT during backups.

Encrypted Backup and Restore

When a policy does not enforce a Security Rule with the Apply Key effect on backup/restore operations, the policy does not decrypt data on I/O operations from that backup application. Under such a policy, the backup application stores encrypted data and the CTE-LDT extended attributes of the file on the backup media.

In Linux, CTE-LDT operations must be suspended during backup. Suspending CTE-LDT completes the ongoing rekey operations on regions of files before starting the backup. During live transformation, CTE-LDT first preserves those regions of a file to be rekeyed in the MDS file. Then it updates some of the metadata in order to update the status of the data preserved in the MDS file in preparation for the rekey. Then it starts rekeying and updating those regions in the underlying file.

Suspending CTE-LDT waits for ongoing rekey operations to complete, and saves the metadata in the CTE-LDT extended attribute section of the MDS file. Suspending CTE-LDT ensures that the rekey status stored in the CTE-LDT extended attribute accurately reflects the rekey status of the data in the entire file during backup.

Note

This requirement does not apply to CTE-LDT for Windows.

The following table summarizes the state of the data in files in backup media:

CTE-LDT State of File	Security Policy	Backup Metadata or Alternate Data Streams Along with File data	Effect
Not rekeyed	Permit	Yes	Data in backup may be in clear format or encrypted with older key version.
Rekey in progress	Permit	Yes	File in backup storage is partially rekeyed. Some parts are in clear format or encrypted with older key version, and other parts are encrypted with current key version.
Rekey complete	Permit	Yes	File in backup storage is in the encrypted format with new key version.

CTE-LDT Policy for Encrypted Backup and Restore

Suppose you have an CTE-LDT policy allowing a backup user, or a backup process, to perform an encrypted backup. The backup user, or the backup process, reads encrypted data from files and stores the same encrypted data in backup media.

For example, suppose you wanted to back up GuardPoint `/oxf-fs1/gp1` protected by `My_LDT_Policy_1`. The key version before the key rotation is 8. The following steps occur:

1. Key version 8 expires and is rotated to version 9.
2. Rotating the encryption key triggers CTE-LDT to start running on the data under the GuardPoint.
3. The QoS schedule suspends CTE-LDT because a backup process is running.
4. The backup process begins, runs and later ends.
5. The QoS schedule resumes CTE-LDT.
6. CTE-LDT on the GuardPoint completes.

Note

Although the backup/restore scenarios and examples described in the rest of this section are specific to CTE-LDT on Linux platform, the concepts also apply to CTE-LDT on the Windows platform.

Consider the state of the three files in the GuardPoint during the CTE-LDT process, right after CTE-LDT is suspended in preparation for the backup. You can obtain the state of each file through the `voradmin ldt attr get` command, which examines the CTE-LDT state of each file captured in the CTE-LDT extended attributes of those files. (For an overview of `voradmin CTE-LDT`, see ["CTE-LDT Command-Line Administration: voradmin command" on page 73](#)).

- **File_1.dat** is rekeyed/encrypted to completion. The applied and new key versions are at version 9 of the key.

```
# voradmin ldt attr get /oxf-fs1/gp1/data_files/file_1.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9
```

- **File_2.dat** is partially rekeyed/encrypted. The applied key version is at version 8 and the transformation key is at version 9.

```
# voradmin ldt attr get /oxf-fs1/gp1/data_files/file_2.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=rekeying,state_saved
Current Key:      name=LDT_AES256_KEY, version=8
New Key:          name=LDT_AES256_KEY, version=9
```

- **File_3.dat** has not been rekeyed/encrypted. The applied key and transformation key are both at version 8, which is the version before the current key rotation.

```
# voradmin ldt attr get /oxf-fs1/gp1/data_files/file_3.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=8
```

While CTE-LDT is suspended on the GuardPoint, the backup process starts and archives these three files, including extended attributes, in the backup media.

```
# my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_1.dat \
    /backup-media/oxf-fs1/gp1/data_files/file_1.dat
# my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_2.dat \
    /backup-media/oxf-fs1/gp1/data_files/file_2.dat
# my_backup --preserve=xattr /oxf-fs1/gp1/data_files/file_3.dat \
    /backup-media/oxf-fs1/gp1/data_files/file_3.dat
```

Notes

- On Linux platforms, you must perform backups on a GuardPoint during periods when CTE-LDT is not actively transforming data in the GuardPoint. You must schedule backups in conjunction with CTE-LDT schedules or during periods when CTE-LDT is paused. Make sure to coordinate with the backup administrator and schedule accordingly.
- If the preferred method of backup is to create device level snapshots of the file system on the managed host or in the storage array subsystem, you must ensure that the schedule for creating snapshots pauses CTE-LDT before a snapshot is created.

Backup/Restore of Metadata Store File (MDS) in GuardPoints Undergoing Rekey

Backing up an entire GuardPoint using commands such as `cp`, `tar`, or `rsync`, or even commercial backup products that sweep the file system namespace for backing up files is supported. This method of backup performed while live transformation is in progress over GuardPoint poses some challenges when files in GuardPoint are backed up in encrypted format. The challenge with this method of backup is existence of the CTE-LDT Metadata Store file (MDS) in GuardPoint during backup or restore process and strict protection enforced on MDS files preventing deletion or modification to MDS files. Second, your backup utility must backup and restore extended attributes of files, and because CTE-LDT extended attributes are also protected similar to MDS files, your backup must be enabled to restore extended attribute of files. To overcome both restrictions, your policy on GuardPoint must include a security rule without Apply Key Effect to enable your backup utility to replace MDS file and CTE-LDT extended attribute of files as

part of backup/restore operations. Additionally, your backup utility must be signed with a signature set from the DSM for added security, and be executed with the option to preserve extended attribute options available with the standard Linux utilities.

The following table lists the supported backup utilities, required options to preserve extended attributes, and supported versions of the utilities.

Command	Required options	Supported version
cp	--preserve=all	OS default
tar	--xattrs	OS default
rsync	-vapIXWP --inplace	OS default
netbackup	overwrite existing files	v7.6.1 and v7.7.3

You can also backup and restore GuardPoint data, including the MDS file, if the requirements listed above on the backup utility are satisfied. GuardPoints associated with an MDS file located outside of GuardPoint namespace cannot be backed up or restore using this method of backup.

Note

You must suspend CTE-LDT on GuardPoint before performing backup or restore.

You can check your GuardPoint to determine if you can use this method of backup. If the directory of your GuardPoint is a mount point, MDS files reside inside your GuardPoint and this method of backup can be used for backing up or restoring your GuardPoint. However, GuardPoint directories below file system mount points must be checked and verified to use this method of backup. To verify, you can run the `voradmin` command to determine the MDS file associated your GuardPoint.

For example:

```
# voradmin ldt list all
MDS_1:  type=file, nguards=1, name=/oxf-fs1/gp1/:vorm:mds::

Guard Table: version 1 nentries 1
Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/oxf-fs1/gp1
File List: count 4308
```

The report on `/oxf-fs1/gp1` GuardPoint indicates association of the MDS file `/oxf-fs1/gp1/:vorm:mds::` with the GuardPoint. As the MDS file resides inside the GuardPoint directory, you can use this method of backup to backup and restore this GuardPoint.

Before restoring the GuardPoint, you must suspend CTE-LDT operations on the GuardPoint if live transformation is in progress. Failure to do so will fail to restore the MDS file in the backup image. Failure to restore MDS file affects partially rekeyed files restored to the GuardPoint. In such a situation the restored data is invalid, and you must remove all the files restored to the GuardPoint and repeat the restore operation after suspending CTE-LDT.

Restoring a GuardPoint from a Backup

To properly restore GuardPoint along with the MDS file, the following steps must be done in order:

1. Verify if live transformation is in progress on the GuardPoint and suspend the CTE-LDT operations. (Skip this step if no live transformation is occurring.)
2. With the same tool that was used for backup, restore to the GuardPoint.

3. Once restore is complete, GuardPoint needs to be disabled and enabled again. Run the `voradmin` command as shown below to determine how the GuardPoint was suspended at the time of backup. For manual GuardPoint, run the `secfsd` command as shown below. For auto-guards, disable and enable GuardPoints on DSM.

```
# secfsd -unguard <GuardPoint>
# secfsd -guard <GuardPoint>
```

4. Since GuardPoint was in suspended state during the time of backup, it will be restored in suspended state. You must resume CTE-LDT to complete CTE-LDT on the restored GuardPoint. You must resume CTE-LDT on the DSM if CTE-LDT was suspended on the DSM at the time of backup, otherwise you will resume CTE-LDT using `voradmin` command.

Run the `voradmin` command below to determine if CTE-LDT must be resumed on DSM or through `voradmin`. If the tag string next to SUSPENDED state of GuardPoint is `vadm`, run `voradmin` command to resume CTE-LDT, otherwise the tag value is `qos` and CTE-LDT must be resumed on DSM. In the example below, GuardPoint `/oxf-fs1/gp1` was suspended using `voradmin`, and it must be resumed after restore using `voradmin` command.

```
# voradmin ldt list all
MDS_1:  type=file, nguards=1, name=/oxf-fs1/gp1::vorm:mds::
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/oxf-fs1/gp1
        File List: count 4308
# voradmin ldt resume /oxf-fs1/gp1
```

5. Wait for CTE-LDT completion on GuardPoint.
6. We strongly recommend that you disable and re-enable the GuardPoint once more.

The restore is now complete and files in your GuardPoint can be accessed.

The CTE Agent sends the following alert message to DSM if the restore operation is rejected:

```
LDT-ALERT: Restore of LDT protected file <GuardPoint> not allowed by policy
```

Potential Warnings During Restore Operation

When using `cp` for backup/restore, the `cp` command may report a failed attempt to preserve permissions on the Metadata Store File (MDS) during a restore. If you encounter the below message, continue to proceed with the restore steps since this will not affect the MDS file or dataset that is being restored.

```
cp: preserving permissions for '/oxf-fs1/gp1::vorm:mds::': Permission denied
```

When using `rsync` for backup/restore, the `rsync` command may report a failed attempt to set extended attribute when restoring the MDS file on system with selinux configured in enforced mode. If user encounters the below message, continue to proceed with the restore steps since this will not affect the MDS file or dataset that is being restored.

```
rsync: copy_xattrs: lsetxattr("/oxf-fs1/gp1::vorm:mds::","security.selinux") failed:
Permission denied (13)
rsync: rsync_xal_set: lsetxattr("/oxf-fs1/gp1::vorm:mds::","security.selinux") failed:
Permission denied (13)
```

Restore an Encrypted Backup

This section illustrates restoration of the three files from the backup media to the same GuardPoint, `/oxf-fs1/gp1`. The files are restored to a different directory under the GuardPoint.

Restore a File Fully Rekeyed to the Latest Key Version

Recall that `file_1.dat` was archived in the backup media when it was fully rekeyed to version 9 of the key. As the current version of the key is also 9, `file_1.dat` is restored from backup without any changes. After restoring the file, the state of the restored file and its applied and current key versions remain unchanged, as compared to the original file

that was backed up.

```
# my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files \ /file_1.dat /oxf-  
fs1/gp1/restored_files/file_1.dat  
  
# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_1.dat  
LDT attributes: rekeyed_size=1440743424, rekey_status=none  
Key:      name=LDT_AES256_KEY, version=9  
  
# voradmin ldt attr get /oxf-fs1/gp1/data_files/file_1.dat  
LDT attributes: rekeyed_size=1440743424, rekey_status=none  
Key:      name=LDT_AES256_KEY, version=9
```

Restore a Partially Rekeyed/encrypted File

Recall that *file_2.dat*, archived in the backup media, was partially rekeyed between versions 8 and 9. As the current version of the key was 9 at the time of backup, *file_2.dat* is restored to the GuardPoint with the same version of the key from the time of backup. The file is flagged for *lazy rekey*, meaning that a background rekey operation is scheduled to transform the file to the latest key version the next time an application tries to access the file.

At the completion of restoration, the file is fully transformed to the key version (v9). The key version is also the latest one in the policy. Although the file is flagged for lazy rekey (LAZY_RK), the file does not need to be transformed to the latest key version because it's already there. Had the file been partially rekeyed from version 7 to version 8 of the key at the time of backup, the restored file would have completed rekeying to version 8 at the end of the restoration. Therefore, the LAZY_RK flag would initiate a background transformation to update the key version to the latest key version when the file is accessed.

If this file is not accessed by any application, the file remains unchanged in the GuardPoint. It is not transformed to the latest key version. To trigger a rekey, either re-push the CTE-LDT policy from the DSM, or access the file with an application, such as a file explorer.

```
# my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files/\ file_1.dat /oxf-  
fs1/gp1/restored_files/file_2.dat  
  
# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_2.dat  
LDT attributes: rekeyed_size=1440743424, rekey_status=lazy_rekey  
Key:      name=LDT_AES256_KEY, version=9  
  
# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_2.dat  
LDT attributes: rekeyed_size=1440743424, rekey_status=none  
Key:      name=LDT_AES256_KEY, version=9
```

Restore a File Not Rekeyed/encrypted with an Older Key Version

Recall *file_3.dat* was archived in the backup media when it was keyed to version 8 of the key, one version below the latest version at the time of backup. At completion of the restoration, *file_3.dat* is restored from backup to the same version, version 8, that it was keyed to when it was backed up.

However, the file is flagged for lazy rekey. After restoring the file, it is keyed to version 8 and flagged for lazy rekey (LAZY_RK). The file is rekeyed to the latest key version, version 9, as soon as an application accesses the file. If this file is not accessed by any application, the file remains unchanged in the GuardPoint.

```
# my_backup --preserve=xattr /backup-media/oxf-fs1/gp1/data_files \ /file_3.dat /oxf-  
fs1/gp1/restored_files/file_3.dat  
  
# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_3.dat  
LDT attributes: rekeyed_size=1440743424, rekey_status=lazy_rekey  
Key:      name=LDT_AES256_KEY, version=8
```

```
# sum /oxf-fs1/gp1/restored_files/file_3.dat
39994 1406976

# voradmin ldt attr get /oxf-fs1/gp1/restored_files/file_3.dat
LDT attributes: rekeyed_size=1440743424, rekey_status=none
Key:      name=LDT_AES256_KEY, version=9
```

Restoring Non-CTE-LDT Backup Data to an CTE-LDT GuardPoint

This section describes how to restore data encrypted with a non-versioned key to an CTE-LDT GuardPoint.

If the backup was performed with the Apply Key effect, the backup files are in clear text. Simply restore the clear text files to the CTE-LDT GuardPoint with the Apply Key effect. All files will be encrypted with the versioned key.

If the backup of the non-CTE-LDT GuardPoint was performed without the Apply Key effect, the backup is encrypted, and you must do the following:

Note

The following example is for a manual guarding. The steps may differ slightly if your GuardPoint is configured for auto guard.

1. Create a temporary directory for restoring the files, type:

```
# mkdir -p /oxf-fs1/tmp_restore
```

2. Restore the encrypted backup files into the temporary directory, type:

```
# cp -pr /backup-media/oxf-fs1/gp1/data_files/* /oxf-fs1/tmp_restore
```

3. Create a Standard Policy with the Apply Key effect for all operations, using the same key as the policy applied on the GuardPoint at the time of backup.

4. Create and enable a new GuardPoint for the temporary directory using the Standard Policy just created.

```
# secfsd -guard /oxf-fs1/tmp_restore
```

5. Ensure that the temporary GuardPoint and CTE-LDT GuardPoint are both enabled.

```
# secfsd -status guard
```

GuardPoint	Policy	Type	ConfigState	Status	Reason
-----	-----	----	-----	-----	-----
/oxf-fs1/gp1	LDT_AES256	manual	guarded	guarded	N/A
/oxf-fs1/tmp_restore	AES256	manual	guarded	guarded	N/A

6. Move the restored files from the temporary folder to the GuardPoint enabled with the CTE-LDT policy. The CTE agent encrypts the files in the CTE-LDT GuardPoint using the current key version in effect for the CTE-LDT policy.

```
# mv /oxf-fs1/tmp_restore/* /oxf-fs1/gp1
```

7. Disable the temporary GuardPoint and remove the temporary restore directory.

```
# secfsd -unguard /oxf-fs1/tmp_restore
# rm -fr /oxf-fs1/tmp_restore
```

8. Delete the temporary GuardPoint on the DSM.

Using fsfreeze (Linux only)

If you use the `fsfreeze` command to quiesce access to the file system before creating a snapshot, refer to the `fsfreeze` section in CTE Admin Guide in the Linux Utilities chapter on how to run the `fsfreeze` command to quiesce access to both the file system and the GuardPoint(s).



WARNING

Do not use CTE-LDT schedules and do not pause CTE-LDT to align backup schedules with CTE-LDT. Instead, use the `fsfreeze` command.

- Running `fsfreeze -f` on the GuardPoint directory pauses CTE-LDT operations in-progress and freezes access to both the GuardPoint and the underlying file system.
- Running `freeze -u` reverses `freeze -f`, allowing access to underlying file system and resuming CTE-LDT operations.

CTE-LDT Backups Using a File System or Storage-Level Snapshot Tool

You can make a file system snapshot using a Logical Volume Manager service or mirroring/splitting storage level LUNs of a file system inside the storage subsystem. CTE-LDT does not have requirements for where and how you create a file system snapshot. However, it is required that you **suspend CTE-LDT processes before you take the file system snapshot**. Suspending CTE-LDT ensures data and metadata consistency between files and CTE-LDT extended attributes.

You may choose to suspend CTE-LDT manually on the managed host using `voradmin ldt suspend` command or `fsfreeze -f`, or suspend CTE-LDT on the DSM.

Note

Be aware that suspending CTE-LDT on the DSM suspends CTE-LDT on the entire host.

After creating a file system snapshot, you can resume CTE-LDT processes on the GuardPoint using `voradmin ldt resume`, or `fsfreeze -u`, or resuming CTE-LDT on the DSM. Do not mix the use of `fsfreeze` and `voradmin ldt suspend` to pause and resume CTE-LDT. CTE suspends or resumes CTE-LDT processes during live transformation when freezing or unfreezing GuardPoint access using `fsfreeze -f` or `-u` option. See the *CTE Agent for Linux Advanced Configuration and Integration Guide* on the use of the `fsfreeze` command on a GuardPoint.

Note

You can make sure CTE-LDT is suspended at backup time by setting the QoS schedule.

You can mount a file system snapshot for data recovery. Configuration for GuardPoints must be duplicated over the mount point of the snapshot file system. Make sure to use the same CTE-LDT policy. Enabling GuardPoints over or under the snapshot mount point provides access to the protected files for recovery. You can choose to manually resume key rotation on the GuardPoints of the snapshot file system, although this is not necessary.

Following is an example of the `fsfreeze` command used to freeze access to the file system `/oxf-fs1` in order to create a snapshot of the file system device. This examples illustrates three GuardPoints enabled inside the file system namespace, `/oxf-fs1/gp-1`, `/oxf-fs1/gp-2`, and `/oxf-fs1/gp-3`. Executing the command `fsfreeze -f` targets any of the GuardPoints in the `/oxf-fs1` mount point and suspends CTE-LDT processes on all of the GuardPoints. Then it freezes access to the file system.

```
# fsfreeze -f /oxf-fs1/gp-1
# voradmin ldt list all
MDS_1:  type=file, nguards=1, name=/oxf-fs1/gp-3::vorm:mds::
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED,
fs1/gp-3
                File List: count 4308

MDS_2:  type=file, nguards=1, name=/oxf-fs1/gp-2::vorm:mds::
        Guard Table: version 1 nentries 1
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-2
                File List: count 4308
```

```
MDS_3:  type=file, nguards=1, name=/oxf-fs1/gp-1/::vorm:mds::  
        Guard Table: version 1 nentries 1  
        Guard 0: type=GP, state=REKEYING SUSPENDED (vadm), flags=GP LOCKED, gp=/oxf-fs1/gp-1  
        File List: count 4308
```

After the file system snapshot is created, executing the `fsfreeze -u` command on any of the GuardPoints in the file system namespace unfreezes access to the file system and resumes CTE-LDT processes on all of the GuardPoints.

```
# fsfreeze -u /oxf-fs1/gp-1  
# voradmin ldt list all  
MDS_1:  type=file, nguards=1, name=/oxf-fs1/gp-3/::vorm:mds::  
        Guard Table: version 1 nentries 1  
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-3  
        File List: count 4308  
  
MDS_2:  type=file, nguards=1, name=/oxf-fs1/gp-2/::vorm:mds::  
        Guard Table: version 1 nentries 1  
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-2  
        File List: count 4308  
  
MDS_3:  type=file, nguards=1, name=/oxf-fs1/gp-1/::vorm:mds::  
        Guard Table: version 1 nentries 1  
        Guard 0: type=GP, state=REKEYING DIRTY, flags=GP LOCKED, gp=/oxf-fs1/gp-1  
        File List: count 4308
```

Windows Backup and Snapshots

On Windows, most backup applications use Volume Snapshot Service (VSS) for the backup. Using VSS is required for backing up files in CTE-LDT GuardPoints. VSS service provides a consistent view of the data to backup and restore applications by taking a snapshot of the volume. Windows Backup uses the snapshot volume, while other applications can continue using the original volume for normal I/O operations. VSS snapshot volume uses a “Copy on write” mechanism to provide a consistent view of the data. Some of the high-level steps of the Windows backup process are:

1. Backup application takes a snapshot of the volume using the VSS service.
2. Backup application mounts this VSS volume to read the data to be backed up.
3. The CTE Agent uses the same policy as that of the original volume to protect these snapshots.
4. The CTE Agent applies the policy and rules to all the I/O requests coming from the backup and restore applications.

Restoring ESXi VM Snapshots of a Protected Host

Some organizations may use ESXi virtual machines for protected hosts and create VM snapshots to back up sensitive data. If you are restoring an older ESXi VM snapshot of a protected host, that contains an previous encryption key, follow these steps:

1. Restore the VM to update to the latest version of the encryption key.
2. In the DSM Management Console, choose **Hosts > Hosts**, then click the name of the VM host.
3. Click the **GuardPoint** tab.
4. Click **Re-Push Policies**.

CTE-LDT Backup and Restore Troubleshooting

Restored files to a GuardPoint protected with conflicting key rules

When restoring an encrypted file from backup media to an CTE-LDT protected GuardPoint without the Apply Key effect, and the file in the backup media does not have an CTE-LDT extended attribute, the file restored to the GuardPoint is set with an CTE-LDT extended attribute that specifies the current key version of the key in the policy associated with the data in the restored file. As the key and key version in the policy do not match the key that was applied to the data at the time of backup, the file restored to the CTE-LDT protected GuardPoint is unreadable.

When restoring an encrypted file from backup media to an CTE-LDT protected GuardPoint without Apply Key effect, and the key specified in the CTE-LDT extended attribute of the file in backup media conflicts with the key rules of the policy on the GuardPoint, the restore operation fails and flags the restored file in error. You can only remove the file, or truncate it, to clear the error status on the file. Access to such files, except remove or truncate, fail with an EINVAL error.

CTE-LDT Command-Line Administration: voradmin command

Use the `voradmin` utility to gather statistics and administer CTE-LDT on a host. It has slightly different syntax and command capabilities depending on whether the host is running Linux or Windows.

Note

Refer to the `voradmin` man page for `voradmin` usage in Linux.

To use `voradmin`:

1. Log in to the host running the CTE Agent with CTE-LDT enabled.
2. At the command line, type `voradmin`.
3. Follow the usage outputs onscreen to find the available commands and their syntax. The general syntax is:

```
# voradmin ldt <command> [args]
```

Command	Description
<code>voradmin ldt attr get delete <guard path> <object path></code>	Get or delete attributes for a GuardPoint or Object path.
<code>voradmin ldt key <report map <key> > <guard path></code>	Creates a report, or map, containing statistics after each key rotation on a GuardPoint.
<code>voradmin ldt list all</code>	(Linux only) List all MDS files and GuardPoints undergoing CTE-LDT processing.
<code>voradmin ldt monitor [interval]</code>	(Windows only) Monitor CTE-LDT progress. If an interval is specified (in units of seconds), it continually updates the monitoring output at the specified interval.
<code>voradmin ldt rekey report <guard path> [output file]</code>	Generate a rekey report manually for a Guardpath.
<code>voradmin ldt resume <guard path> all</code>	Resume guarding the GuardPoint directory.
<code>voradmin ldt space <guard path></code>	Estimates disk space needed for metadata and mds store information.

Command	Description
<code>voradmin ldt stats [<guard path>] [<interval>]</code>	Obtains transformation CTE-LDT statistics such as: • Current rekey status • Start time • Estimated completion time • Percentage completed • Total data • Amount of data transformed • Total files • Number of files transformed • Number of files skipped • Number of files remaining for rekey

Upgrading or Downgrading Agent Software On an CTE-LDT Host

Consider the following when upgrading or downgrading software on protected hosts.

Upgrading

If a host contains an agent software version lower than 6.0, and you upgrade to version 6.0 or later, the CTE-LDT feature does not automatically enable on all upgraded hosts. You must:

1. Upgrade the DSM.
2. Install the CTE-LDT license.
3. Restart the 6.x agent, or reboot the host on which the CTE Agent is installed.
4. Select the CTE-LDT option to enable it, once the CTE-LDT option displays in the host's menu.

After upgrading the DSM, the keys and policies on the DSM remain unchanged. They are standard keys and policies not usable with CTE-LDT. To use CTE-LDT, create versioned keys and policies set to type: CipherTrust Transparent Encryption - Live Data Transformation.

On the DSM, select the Live Data Transformation option on the **Edit > Host** page to enable CTE-LDT on target host.

After upgrading a protected host to 6.x from an earlier version, existing policies, keys, and GuardPoints on the managed host remain unchanged and enforced.

Note

In v6.1, you can automatically register CTE-LDT with the DSM installation.

For more information, see [Chapter 3: "Setting Up CTE-LDT" on page 20](#).

Note

If you are using CTE-LDT with the Hadoop Distributed File System (HDFS), see the HDFS chapter in the *CTE Agent Installation and Configuration Guide* for more information.

Downgrading

To roll back from 6.0 (or greater) to a version before 6.0, it is not sufficient to uninstall the 6.0 software and reinstall the earlier version. You must migrate GuardPoints protected with CTE-LDT encryption policies to a non-CTE-LDT policy first, reverse the CTE-LDT host's registration with the DSM, then re register the host after installing the earlier software version. See ["Removing CTE-LDT and Security Encryption" on page 76](#).

Moving a CTE-LDT GuardPoint from One CTE-LDT Policy to Another

To change the CTE-LDT policy that an CTE-LDT GuardPoint uses, complete the following steps to ensure that the GuardPoint is migrated properly from one CTE-LDT policy to another CTE-LDT policy.

Scenario

The GuardPoint is currently attached to LDT-Policy-1, which rekeys from `clear_key` to `LDT-Key-1`. The objective is to migrate the data in the GuardPoint to another versioned key, `LDT-Key-2`. Migration to `LDT-Key-2` requires detaching the GuardPoint from `LDT-Policy-1`, and then attaching it to `LDT-Policy-2`, assuming `LDT-Key-2` is the versioned key specified in `LDT-Policy-2`. This is a two step migration:

1. Migrate a GuardPoint out of the CTE-LDT policy to protection under a standard policy.
The step requires cloning `LDT-Key-1` to a non-versioned key, and migrating the GuardPoint out of the CTE-LDT policy. Because the cloned key and the the current version of `LDT-Key-1` have the same key material, the data in the GuardPoint directory remains encrypted to the same key after migration of the GuardPoint out of CTE-LDT.
2. Migrate a GuardPoint protected under a standard policy to protection with an CTE-LDT policy.

Note that you may set the transformation key to `clear_key` instead of `LDT-Key-2` in the second policy (`LDT-Policy-2`). The effect of `clear_key` is transformation of the data in the GuardPoint directory to clear text. Although the transformation key in CTE-LDT policies must be a versioned key, `clear_key` is an exception. It allows CTE-LDT GuardPoints to be transformed to clear using the CTE-LDT process.

To properly move the GuardPoint from `LDT-Policy-1` to `LDT-Policy-2`:

Note

Ensure that no active processes or users are accessing files in the GuardPoint, or its subdirectories, until all steps have been completed.

1. Follow the instructions for, ["Converting a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy" on the next page](#).
2. Assuming the current version of the `LDT-Key-1` is version 5, then clone version 5 of the key to `Cloned-LDT-Key-1v5`.
 - a. In the DSM Management Console, select **Keys > Agent Keys > Keys**.
 - b. Click the name of the versioned key that you want to clone.
 - c. Click **Clone** to clone the key.
3. Follow the instructions for ["Using voradmin To Estimate Disk Space Required for CTE-LDT \(Linux\)" on page 62](#).
4. Follow instructions for ["Converting a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy" on the next page](#) using the cloned key (`Cloned-LDT-Key-1v5`) as the Initial Key and `LDT-Key-2` as the key for the new CTE-LDT policy. The files are now rekeyed from `Cloned-LDT-Key-1v5` to `LDT-Key-2`.

Removing CTE-LDT and Security Encryption

If you want to stop using CTE-LDT on a GuardPoint or on a whole host, follow the instructions in the following sections.

Migrating a GuardPoint Out of CTE-LDT

Migrating a GuardPoint from CTE-LDT removes the security encryption. It also provides a DSM Administrator with the flexibility to relax the compliance requirement, when strict compliance for frequent key rotation on specific data is no longer mandatory. The following sections describe how to migrate a GuardPoint from CTE-LDT to a non-CTE-LDT policy, or to remove encryption protection from it.

Converting a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy

If you want to do more than just change the policy on a GuardPoint from an CTE-LDT policy to a non-CTE-LDT policy, see ["Deleting CTE-LDT Metadata \(Linux\)" on page 79](#) or ["Deleting CTE-LDT Metadata \(Windows\)" on page 80](#).

1. Clone the versioned key associated with the CTE-LDT GuardPoint to a non-versioned key.

The clone function creates a new key with the same cryptographic encryption material as the current version of the cloned versioned key.

This allows CTE-LDT to use the cloned key in a non-CTE-LDT policy to convert the GuardPoint from an CTE-LDT to a non-CTE-LDT managed policy.

- a. In the DSM Management Console, select **Keys > Agent Keys > Keys**.
- b. Click the name of the versioned key that you want to clone.
- c. On the **General** tab, click **Clone** to clone the current version of the key.

By default, the DSM creates a name for the cloned key that combines the name of the key and the current version number. You can specify a different name if desired. For example, if you are cloning version 5 of a key named `LDT-Key-1`, the name of the cloned key would default to `LDT-Key-1__5`.

2. Click **Hosts > host_name > GuardPoint** tab.
3. Select the GuardPoint and then click **Disable**.
4. After CTE-LDT disables the GuardPoint, click **Unguard** to delete the GuardPoint.
5. (Linux only) Ensure that the GuardPoint is removed on the managed host:

```
# secfsd -status guard
No GuardPoints configured
```

6. CTE-LDT creates extended attributes for every file under the GuardPoint as well as the GuardPoint directory. Now that the CTE-LDT policy does not manage the GuardPoint, you must remove the extended attributes for every file in the GuardPoint, type:

```
# voradmin ldt attr delete /<GuardPoint>
```
7. The command may take some time depending on the number of files in the GuardPoint.

Note: For all of the file system mount points that contain an CTE-LDT protected GuardPoint, you must clean up the metadata first. See ["Deleting CTE-LDT Metadata \(Linux\)" on page 79](#).

8. Create a non-CTE-LDT policy using the cloned key you created earlier in this procedure.
 - a. Click **Policies > Manage Policies > Manage Policies**.
 - b. Click **Add**.
 - c. In Policy Type, choose **Standard**.
 - d. In Key Selection Rules, click **Add**.
 - e. In Key, choose the cloned key1.
 - f. Click **Select Key**.
 - g. Finish creating the policy as usual for a non-CTE-LDT policy.
9. Apply the non-CTE-LDT policy to the GuardPoint.



CAUTION

Make sure that you have removed all of the CTE-LDT metadata from the GuardPoint before applying the non-CTE-LDT policy.

- a. Click **Hosts > host_name > GuardPoint** tab.
- b. Click **Guard**.
- c. In the *Guard File System* window, select the Policy that you just created.
- d. Select *Type: Directory (Auto Guard) or (Manual Guard)*, and enter or browse to the directory to protect.

Remove Protection from a GuardPoint

When compliance may no longer require protecting data in a GuardPoint, you may choose to unprotect/decrypt it. Before removing protection from your GuardPoint, you must decrypt the data in your GuardPoint by setting it to clear. You have two options to decrypt your data:

- While a GuardPoint is protected and enabled under an CTE-LDT policy, you can use copy or backup/restore commands to save files in your GuardPoint to a location outside of your GuardPoint.
- Use the `dataxform` command to transform your GuardPoint to clear in an offline transformation process.

Copying Files to Decrypt Them

If you choose to copy your files, you must create a directory outside of the GuardPoint and then copy the files into the GuardPoint directory. After finishing copying, complete the following steps:

1. Click **Hosts > host_name > GuardPoint** tab.
2. Select the GuardPoint and then click **Disable**.
3. After CTE-LDT disables the GuardPoint, click **Unguard** to delete the GuardPoint.
4. (Linux only) Ensure that the GuardPoint is removed on the managed host:

```
# secfsd -status guard
No GuardPoints configured
```

This completes removal of the GuardPoint under an CTE-LDT policy. You can now remove the original files and data within the GuardPoint namespace.

Using Dataxform Command to Transform the Files

If you choose to use the dataxform command to transform data in your GuardPoint to clear, use the `voradmin` command to verify that earlier versions of the versioned key are not in use on your GuardPoint. Complete the following steps to clear all metadata in your GuardPoint. Then, transform your GuardPoint to clear.

1. Clone the key.
 - a. In the DSM Management Console, select **Keys > Agent Keys > Keys**.
 - b. Click the name of the versioned key that you want to clone.
 - c. Click **Clone** to clone the key.

By default, the DSM uses the name of the versioned key, and the current version number of the versioned key, for naming the cloned key. You can choose a different name, if desired.

2. Create an offline dataxform policy to transform your GuardPoint from the cloned key created in step 1 to `clear_key`. See the *DSM Administration Guide* for more information.

3. In the DSM Management Console, click **Hosts > Hosts > Hostname**.

4. Click the **GuardPoint** tab.

5. Click **Disable** to disable the GuardPoint.

6. After CTE-LDT disables the GuardPoint, click **Unguard** to delete the GuardPoint.

Before you apply the offline data transformation policy to your GuardPoint, you must clean up the CTE-LDT metadata from your GuardPoint. CTE-LDT creates extended attributes for every file under the GuardPoint, as well as the GuardPoint directory. Now that the CTE-LDT policy does not manage the GuardPoint, you can remove the extended attributes for every file in the GuardPoint.

7. Remove the extended attributes of files in a GuardPoint, type:

```
# voradmin ldt attr delete <GuardPoint>
```

The command may take some time depending on the number of files in the GuardPoint. After metadata deletion is complete, you can apply the offline transformation policy on the GuardPoint.

8. On the DSM, guard and enable the GuardPoint with the offline dataxform policy you created earlier.

9. After enabling your GuardPoint, run the dataxform command on the managed host to transform the GuardPoint to a `clear_key`, type:

```
# dataxform --rekey --gp /<GuardPoint>/ --preserve_modified_time --preserve_access_time --cleanup_on_success
```

10. After completion of dataxform, unguard the GuardPoint.

- a. Click the **Hosts > Hostname > GuardPoint** tab.
- b. Select the GuardPoint and click **Disable**.
- c. After CTE-LDT disables the GuardPoint, click **Unguard** to delete the GuardPoint.

11. Remove the GuardPoint from the dataxform policy on the DSM.

- a. Click **Policies > PolicyName**.
- b. Select the **GuardPoint**.
- c. Click **Delete**.
- d. Click **Apply**.

Deleting CTE-LDT Metadata (Linux)

To remove the metadata associated with the GuardPoint, you must run the `voradmin` command on the managed host to remove the CTE-LDT metadata associated with the GuardPoint.



WARNING

Before you attempt to remove an MDS file, make sure that no CTE-LDT-protected GuardPoints remain configured under the file system mount point.

In the following example:

- `/oxf-fs1` is the mount point
- `/oxf-fs1/gp1` is the CTE-LDT-protected GuardPoint

To delete the metadata associated with the GuardPoint:

1. Ensure that the GuardPoint is not enabled on the host. Run the command below and verify that the GuardPoint pathname does not appear in the output of the `secfsd` command, type:

```
# secfsd -status guard
```

2. Run the `voradmin` command to remove CTE-LDT attributes on the GuardPoint, type:

```
# voradmin ldt attr delete <GuardPoint path>
```

For example:

```
# voradmin ldt attr delete /oxf-fs1/gp1
LDT metadata has been removed from all files in GuardPoint /oxf-fs1/gp1
```

If the last transformation on your GuardPoint completed when the VTE Agent was running version 6.0.2, you may have to remove the MDS file that is located in the mount point directory of the file system in which GuardPoint resides. Before you remove the MDS file, make sure that the MDS file is not in use with other GuardPoints under the same file system mount point. For example, if you removed the metadata for GuardPoint `/oxf-fs1/gp-1` where `/oxf-fs1` is the mount point of the mounted file system, make sure that `/oxf-fs1` does not appear in the output of the `secfsd -status guard` command, and then proceed:

1. Remove the MDS file from the mount points or GuardPoints. As of the CTE 6.1 release, CTE-LDT always creates and manages the MDS file inside the GuardPoint directory. Earlier versions created and managed the MDS file inside mount point directory while sharing the MDS file with all the GuardPoints under the mount point. Type:

```
# voradmin ldt rmstore <mount_point>
```

For example:

```
# voradmin ldt rmstore /oxf-fs1
Enter YES if /oxf-fs1 does not include any GuardPoints associated with an CTE-LDT policy -
>YES
MDS file /oxf-fs1/::vorm:mds:: has been removed.
```

2. Verify that the metadata store has been removed from the secfs mount points, type:

```
# ls -altr <file_system_mount_point>
```

For example:

```
# ls -altr /oxf-fs1
```

You should not see `/oxf-fs1/::vorm:mds::` listed.

Deleting CTE-LDT Metadata (Windows)

Use the following command to delete the CTE extended attribute for a file or a GuardPoint. This is useful when removing a GuardPoint from under an CTE-LDT policy (see ["Migrating a GuardPoint Out of CTE-LDT" on page 76](#)).

```
# voradmin ldt attr delete [<file name path> | <guard path>]
```

For an overview of `voradmin ldt`, see ["CTE-LDT Command-Line Administration: voradmin command" on page 73](#).

Removing CTE-LDT from a Host

Once you have registered a host and enabled CTE-LDT, you cannot disable the CTE-LDT feature by unchecking the CTE-LDT box. You must unregister the host from the DSM, then register it again without CTE-LDT. When you remove the CTE-LDT feature from a host entirely, the host's CTE-LDT license becomes available for use on another host.

1. Stop all applications from accessing data in CTE-LDT GuardPoints on the host.
2. Migrate data in every CTE-LDT GuardPoint using the steps described in the section ["Remove Protection from a GuardPoint" on page 77](#).



WARNING

Potential data loss. Ensure that you have decrypted the data and, optionally, copied it out of the GuardPoint. Once the CTE Agent software is removed, access to data is no longer controlled by CTE. If the data was encrypted, it remains encrypted, and there is no way to read it.

3. Remove the GuardPoints on the host from the DSM.
 - a. Remove the CTE-LDT metadata from those GuardPoints.
 - b. Remove the MDS files associated with those GuardPoints, if necessary. See ["Deleting CTE-LDT Metadata \(Linux\)" on the previous page](#) for more information.
4. Remove the host from the DSM. For details, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* or the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
5. Re-install the agent on the host.
6. Register the host with the DSM. This time, do not select the CipherTrust Transparent Encryption - Live Data Transformation option. See ["Enabling CTE-LDT on a Protected Host" on page 25](#).

Uninstalling the Agent while CTE-LDT is Rekeying GuardPoints

You cannot uninstall the CTE Agent if CTE-LDT is rekeying any GuardPoints on that host.

If you want to uninstall the CTE Agent from a host that contains CTE-LDT GuardPoints, you must first unencrypt the files on each CTE-LDT GuardPoint using the steps noted in the previous sections.

Chapter 6: Troubleshooting CTE-LDT

Monitoring and Statistics	81
Protecting CTE-LDT GuardPoints against Failure in Underlying Filesystems (Linux)	84
Alerts Playbook	85
Error Messages	90
Warning and Info Messages	92
Upgrading CTE Agent	93
Recommendations and Considerations	93

The CTE-LDT administrator needs to monitor and respond to runtime statistics and alerts.

Monitoring and Statistics

This section describes how to find the runtime status of CTE-LDT and how to get statistics about its operation.

Note

When you check GuardPoint status on the DSM, be aware that the status is not relayed in real time. There can be a delay of several minutes before the DSM becomes aware of events on the host. When you configure the host and v for one-way communication, the delay is longer, up to an hour, because CTE-LDT sends statistics to the DSM only once per hour.

To find out when the DSM last received a status update from the host, check the Last Status Update timestamp in the GuardPoint Status dialog (for information about how to display this dialog, see ["Obtaining Statistics in the DSM with GuardPoint Status" below](#)). For the most up-to-date statistics, inspect the host. Run the `voradmin` command on the managed hosts to retrieve status and statistics pertaining to GuardPoints.

To find out whether your host is configured for one-way communication, open the DSM Management Console, choose **Hosts > Hosts**, click the name of the host, and look for the FS Agent One Way Communication checkbox.

Obtaining Statistics in the DSM with GuardPoint Status

During and after data transformation, you can view statistics about any GuardPoint on any host in your system. Either use the DSM Management Console, as described in this section, or use the `voradmin` command, as described in ["Obtaining CTE-LDT Statistics at the Command Line" on page 83](#).

To display the GuardPoint status in the DSM Management Console:

1. In the DSM Management Console, choose **Hosts > Hosts**.
2. Click the name of the host you want to inspect.
3. Click the **GuardPoint** tab.
4. In the Status column, click the icon.

The GuardPoint Status window opens. The window displays the following values:

GuardPoint Status Field	Description
Reason	If the key rotation was initiated manually on an CTE-LDT host, the requester selected a reason such as "normal maintenance" or "key compromised."

GuardPoint Status Field	Description
GuardPoint Status	Status of the GuardPoint.
GuardPoint State	State of the GuardPoint.
Usage	Displays the reference count for the GuardPoint.
Guarded on	Date when the policy went into effect on this GuardPoint.
Policy Name	Name of the policy.
Policy Version	The current policy version. If you make any changes to a policy after creating it, the policy version number increases by 1. The first version is number 0.
Last Status Update	Time stamp that displays when the DSM last received status information from the agent on the protected host. There can be a delay between status updates from agent to DSM. If it is imperative that you see the most recent data, go to the agent and use the voradmin command to inspect it. For an overview of voradmin CTE-LDT, see "CTE-LDT Command-Line Administration: voradmin command" on page 73 .
Policy Aggregate Key Version	Indicates the version of the key used to transform data.
Transformation Status	A one-word summary of the current (or most recent) CipherTrust Transparent Encryption - Live Data Transformation. The same value is shown in the Rekey Status column on the host's GuardPoint tab. For details about each status code, see "Checking the Rekey Status" on page 44 .
Last Transformation Completion Time	Timestamp from the last time that transformation completed successfully.
Last Transformation Start Time	Timestamp showing the last time transformation was started. If this time is later than the Last Transformation Completion Time, the transformation did not complete normally. The Transformation Status should reflect this, such as with Incomplete.
Estimated Rekey Completion Time	If transformation is underway, this field displays the rekey duration.
Total Number of Files Deleted	Number of files in the GuardPoint that were deleted by users while data transformation was underway.
Total Files to Be Transformed	Number of files found during the initial scan of the GuardPoint. For more information, see "CTE-LDT Runtime Flow" on page 14 .
Total Bytes to Be Transformed	Size of all of the files found during the initial scan of the GuardPoint.
Total Bytes Transformed	Number of bytes in the GuardPoint that were successfully transformed in the most recent CTE-LDT operation. If this does not match Total Bytes to Be Transformed, look for Total Files Skipped or Total Files Errored.
Total Files Transformed	Number of files in the GuardPoint that were successfully transformed in the most recent CTE-LDT operation. If this does not match Total Files to Be Transformed, look for Total Files Skipped or Total Files Errored.

GuardPoint Status Field	Description
Total Files Skipped	Total number of files that CTE-LDT did not transform in this pass. The files were intended for transformation, but were not transformed for some reason. For example, (on Windows) the file is read-only, or it is an executable file that is currently running. On a Windows host, transformation continues on the next available file in the GuardPoint, and CTE-LDT maintains a list of the files that it skipped.
Total Files Errored	Total number of files that triggered alerts. See "Alerts Playbook" on page 85 .

Obtaining CTE-LDT Statistics at the Command Line

You can obtain CTE-LDT statistics from the command line using the following command:

```
# voradmin ldt stats <guard path> [interval]
```

This command displays transformation statistics for a GuardPoint, or for all GuardPoints, if none are specified. If you specify an interval (in units of seconds), the command continually updates the statistics on the given interval. If no GuardPoint is specified, the command returns the aggregate statistics at the host level, including specific statistics related to QoS. If a GuardPoint is specified, statistics include:

- Current rekey status
- Rekey Start time
- Last rekey completion time
- Estimated Rekey completion time
- Data Statistics including the amount of data transformed
- File statistics including:
 - Number of files transformed
 - Number of files skipped
 - Number of files remaining for rekey

Obtaining a Rekey Report

CTE-LDT generates a report automatically after completion of a key rotation. The report lists the files in the GuardPoint and the key and version of the key applied to each file. This kind of report may be a common compliance requirement.

The administrator can also request a rekey report during rekey, if the need to see the partial transformation results so far.

About the rekey report

On Linux hosts, CTE-LDT writes rekey reports to a local file on the agent host in `/var/log/vormetric/`. The file name begins with `ldtaudit-log-`. It is followed by the file system directory name, GuardPoint directory name, and a timestamp. For example, for a GuardPoint at `/oxf-fs2/gp2` with rekey completed on November 19, 2016, just after 2:00 p.m. (hour 14), the rekey report file name would be `ldtaudit-log-_oxf-fs2_gp2-2016111914917`.

The report includes:

- Total number of files in the GuardPoint
- Number of files transformed
- Rekey start and end times
- List of all files transformed
- Applied key and key version for each file (for example, files in different resource sets might have used different keys)

Manually generating a rekey report

To generate a rekey report manually, use the following command:

```
# voradmin ldt rekey report <GuardPoint> [<logfile>]
```

In `<GuardPoint>`, type the GuardPoint path. In `<logfile>`, you can optionally direct the output to a file. If no logfile is specified, the report displays on `stdout`.

Monitoring Ongoing CTE-LDT Operations at the Command Line (Windows only)

Use the following syntax to monitor CTE-LDT progress. If an interval is specified (in units of seconds), it continually updates the monitoring output at the specified interval.

```
C:\> voradmin ldt monitor [interval]
```

For an overview of `voradmin ldt`, see ["CTE-LDT Command-Line Administration: voradmin command" on page 73](#).

Protecting CTE-LDT GuardPoints against Failure in Underlying Filesystems (Linux)

CTE-LDT Recovery Challenges

The main challenge with CTE-LDT recovery is a failure to access files or specific blocks in files inside a GuardPoint. Before CTE-LDT runs the recovery process on a GuardPoint, the underlying file system was recovered before file system was mounted. File system recovery may create orphan files in the `lost+found` directory inside the mount point. If an orphan file belongs to the GuardPoint, CTE-LDT cannot recover the file as the file is no longer in the same directory as it was prior to the crash while it was undergoing rekey.

CTE-LDT Recovery Enhancement

CTE-LDT has been improved for handling inconsistencies in the underlying file system during execution of CTE-LDT recovery. When enabling a GuardPoint after a system crash, CTE-LDT performs consistency checks on the files undergoing rekey at the time of crash before enabling GuardPoint. If the CTE-LDT recovery process is unable to recover any of the affected files, the GuardPoint will not be enabled and CTE-LDT will send the following alert to the DSM:

```
[CGS3266E] LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in  
underlying file system encountered during LDT recovery.
```

You can check the status of a GuardPoint and the reason for failing to enable a GuardPoint using the `secfsd -status guard` command. For example, the GuardPoint `/mnt/gp` failed to guard because Guard point needs LDT recovery as reported in the `Reason` column for the following example GuardPoint.

GuardPoint	Policy	Type	ConfigState	Status	Reason
/mnt/gp	LDT220	manual	guarded	not guarded	Guard point needs LDT recovery

Details on the specific issues encountered, including any files that could not be recovered, are reported to a log file in the `/var/log/vormetric` directory. The log file name is in the format:

```
ldt_recovery_log:<guardpoint_name>:<timestamp>.txt
```

The log file name starts with `ldt_recovery_log`, followed by the GuardPoint pathname and the date and time of the recovery attempt. The GuardPoint pathname and date and time are separated with “:”. For example:

```
/var/log/vormetric/ldt_recovery_log:_mnt_gp:2018-12-08-14:6:12.txt
```

Refer to the issues listed in the log file, and resolve those issues before enabling the GuardPoint again. A GuardPoint cannot be enabled in subsequent guard attempts until those issues are resolved. Each attempt generates a new log file. Check the CTE-LDT log file for missing files whose inode numbers match inode numbers of orphan files in `lost+found`. If there is a match, restore the file from `lost+found` to the pathname specified in the CTE-LDT recovery log file. Be sure to run the `mv` command to restore the file to the original location, do not run the `cp` command. After resolving all or some of the reported issues, you must run the command `voradmin ldt recover <GuardPoint>` to repeat the recovery process.

```
voradmin ldt recover <GuardPoint>
```

Running this command resolves the problems that can be corrected and clears the failed recovery status on the GuardPoint, allowing the GuardPoint to enable automatically within 30 seconds. If the GuardPoint does not enable, you can enable it using `secfsd -guard` command, if manual guard, or enable it on the DSM, if auto-guard. Note that if you are unable to resolve all of the reported issues, you accept the loss of some data or files, as reported in the latest recovery log file for the GuardPoint, when you run the command `voradmin ldt recover <GuardPoint>`.

Recovery Alerts

CTE-LDT sends two alerts to DSM if CTE-LDT fails to resolve the issues encountered during recovery.

The alert below is an error report sent to the DSM whenever CTE-LDT encounters failure during recovery prior to enabling GuardPoint. This alert also reports the GuardPoint specified in the message is not enabled:

```
[CGS3266E] LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in underlying file system encountered during LDT recovery.
```

The alert below is a warning report sent to the DSM only if `voradmin ldt recover` encounters errors and continues anyway. This alert reports the GuardPoint specified in the message has been enabled with some files in error status.

```
[CGS3267W] LDT-ALERT: LDT manual recovery on guard point [GuardPoint] completed with [#] errors.
```

The full message body does not currently appear in the logs on the DSM. At this time, the DSM shows the message ID without the message body.

Alerts Playbook

This section lists the CTE-LDT alerts and describes what to do in each case. CTE-LDT generates alerts when issues arise that require attention from the DSM Administrator. Without prompt attention, alerts can delay the rekey process or cause the process to remain incomplete.

Failure to Suspend or Resume CTE-LDT Operation

- **LDT-ALERT: Failed to suspend rekey on GuardPoint [GuardPoint]**

Solution: An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, you must fix the problem at the host OS or storage level.

The appropriate corrective action depends on when this problem occurs and the reason for the suspension. If the suspend request was at the host level as part of a QoS schedule, or it was initiated by a user on the DSM, the failure occurred at the host level rather than the specified GuardPoint.

Otherwise, the source is probably the initiation of a suspension on a specific GuardPoint before backup. If the backup operation is in progress when this alert message occurs, you must fix the cause of the suspension failure and then restart the backup. If the backup has already completed when the alert message occurs, the backup image on the GuardPoint may have inconsistent data and CTE-LDT metadata. Discard this backup image and do a fresh backup.

If you cannot find and fix the host OS or storage issue, contact Thales Support for troubleshooting and recovery.

- **LDT-ALERT: Failed to resume rekey on GuardPoint [GuardPoint]**

- **LDT-ALERT: Failed to resume rekey on all GuardPoints**

Solution: An I/O error is the most common cause of failure when updating persistent state of a GuardPoint. For I/O errors, you must fix the problem at the host OS or storage level.

The appropriate corrective action depends on when this problem occurs and the source of the problem. If the resume request was at the host level as part of a QoS schedule, or the resume request was initiated by a user on the DSM, the failure occurred at the host level rather than the specified GuardPoint.

Otherwise, the source is probably initiation of a resume operation on a specific GuardPoint after a backup is completed.

If you cannot find and fix the host OS or storage issue, contact Thales Support for troubleshooting and recovery.

Insufficient Resources

The following alerts trigger when there are not enough resources for CTE-LDT operations.

- **LDT-ALERT: Aborting rekey of file [FileName] due to insufficient disk space**

The key rotation process was stopped on a GuardPoint because there was not enough available disk space.

Solution: Resize or free up space in the file system where the PathName resides. Key rotation automatically starts again when sufficient free space becomes available.

- **LDT-ALERT: Failed to launch transformation on [GuardPoint]**

CTE-LDT failed to launch the data transformation process on the specified GuardPoint.

Solution: The most common causes of this failure are:

- Low amount of system resources, such as free disk space.
- Check the system logs for insufficient free space in underlying file systems. You can free up space by removing older files or resizing your underlying file system. You may resize the file system on-line or off-line.

For other issues, contact Customer Support.

- **LDT-ALERT: QoS failed to start**

The Quality of Service subsystem failed to launch QoS services due to lack of system resources.

Solution: A low amount of available memory is the most common cause of this failure.

Contact Customer Support.

- **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint] due to insufficient disk space**

- **LDT-ALERT: MDS file [PathName] exceeded disk space quota on gp [GuardPoint]**

There was not enough storage space in one or more file systems containing GuardPoints undergoing rekey.

Solution: Check the file systems where your GuardPoints reside to see how much space it is using. Add more storage space as needed. After the condition is corrected and disk space is available, CTE-LDT operations resume automatically.

- **LDT-ALERT: Low space on guard point [GuardPoint], increase free space or LDT will be suspended.**

Available storage space in the file system containing the GuardPoint is nearing the threshold below which CTE-LDT rekeying cannot continue. If available space does drop below that threshold, rekeying will be automatically suspended.

Solution: Check the file system where your GuardPoint resides to see how much space is available. Make more free space available if necessary. After the condition is corrected and storage space is available, rekeying resumes automatically.

Failed to Update CTE-LDT Attribute

The following alerts trigger when CTE-LDT extended attributes are not properly updated.

- **LDT-ALERT: Failed to update LDT attribute on GuardPoint [GuardPoint]. Error: [ErrorNumber]**

Solution: I/O error is the most common cause of failure when updating CTE-LDT extended attributes. For I/O errors, fix the problems at the host OS or storage level. In Linux, if you experience an I/O error, identify the file that had the error, and restore it from backup. See ["Backing Up and Restoring CTE-LDT GuardPoints" on page 64](#).

In Windows, you can recover a file that has corrupt metadata as follows:

- If the file is fully encrypted, remove the metadata. Type:

```
# voradmin ldt attr delete <file name path>
```

Then apply the same policy that was used to encrypt the data.

- If the file was only partially rekeyed, restore the file from a backup.

If you cannot find and fix the underlying host OS or storage issue that is causing corrupt metadata, contact Customer Support for troubleshooting and recovery.

- **LDT-ALERT: Failed to update LDT attribute**

CTE-LDT failed to create or update an CTE-LDT extended attribute of a file in a GuardPoint.

Solution: An I/O error is the most common cause of failure when updating an CTE-LDT extended attribute. For I/O errors, fix the problem at the host OS or storage level.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

Rekey Stopped

The following alert is specific to Windows and is triggered when rekey is stopped before it completes normally.

LDT-ALERT: Suspending rekey of binary file [PathName] during its execution

CTE-LDT operations encountered an executable file that is running.

CTE-LDT cannot rekey a running executable file until the execution of the binary file stops.

Solution (Windows)

1. Obtain the name of the executable file from the alert message.
2. Stop execution of the binary file.

Incomplete Key Rotation

- **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint]. Another rekey operation is already in progress** (Windows only)
- **LDT-ALERT: Key rotation failed on GuardPoint [GuardPoint]**

CTE-LDT failed to complete the key rotation process on the specified GuardPoint. On Windows, this may occur if a key rotation process is already in progress on the GuardPoint. This pre-existing rekey operation could be active, or it could be in a suspended state, either because of the QoS schedule or a manual pause initiated by the administrator. See ["Suspending and Resuming Rekey and/or Scan Phase" on page 46](#).

Solution

1. On Linux, you can run the following command to see whether key rotation is in progress on the GuardPoint.

```
# voradmin ldt list all
```
2. On Linux or Windows, check the rekey status of GuardPoints in the DSM Management Console.
3. If key rotation is already in progress on a Windows GuardPoint, wait for the key rotation to complete.
4. On the **GuardPoint** tab on the DSM, select **Re-push Policies** to manually re-push the policies to the host to initiate key rotation on GuardPoints ready for key rotation.

Contact Customer Support if this error occurs on Linux or if the cause of key rotation failure on Windows is not a key rotation in progress.

Skipped Key Rotation

The following alerts trigger when CTE-LDT skips key rotation.

- **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint]. It is on a read-only file system**
Key rotation is skipped on a specified GuardPoint because the mount point where the GuardPoint resides does not permit write operations.

Solution:

1. Remount the file system where the GuardPoint resides, and change the mount option to read/write.
 2. On the GuardPoint page on the DSM, press **Re-push Policies** to manually re-push the policies to the host to initiate key rotation on GuardPoints ready for key rotation.
- **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint] during pre-commit**
 - **LDT-ALERT: Failed to rotate key on GuardPoint [GuardPoint] during commit**
 - **LDT-ALERT: Skipped key rotation on GuardPoint [GuardPoint]. Error: [ErrorNumber]**

- **LDT-ALERT: Failed to update LDT attribute on GuardPoint [GuardPoint]. Error: [ErrorNumber]**

CTE-LDT failed to start a key rotation process on a GuardPoint during a guard operation or when processing a key rotation notification from the DSM. For [ErrorNumber], a Linux error number is substituted, such as `errorcode 17`.

Solution: The host returns error code 17 during CTE-LDT key rotation if it cannot perform the key rotation because there is already a rekey in progress. This pre-existing rekey operation could be active, or it could be in a suspended state, either because of the QoS schedule or a manual pause initiated by the administrator. See ["Suspending and Resuming Rekey and/or Scan Phase" on page 46](#).

An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, fix the problem at the host OS or storage level.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

Failed to Update CTE-LDT Metadata During Scan Phase

CTE-LDT triggers the following alerts when CTE-LDT cannot properly update metadata during the scan phase. (See ["CTE-LDT Runtime Flow" on page 14](#) for information about the scan phase.)

- **LDT-ALERT: Scan error on [GuardPoint] removing MDS guard for relaunching dataxform**

CTE-LDT failed to update metadata when restarting a scan on the specified GuardPoint.

Solution: An I/O error is the most common cause of failure when updating CTE-LDT metadata. For I/O errors, fix the problem at the host OS or storage level and then restart operations.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Thales Support for troubleshooting and recovery.

- **LDT-ALERT: Online Dataxform failed during post scan stage on [GuardPoint]**

CTE-LDT failed to update metadata when transitioning from scan to rekey phase on the specified GuardPoint.

Solution: An I/O error is the most common cause of failure when updating CTE-LDT metadata. For I/O errors, the problem must be fixed at the host OS or storage level and the operation restarted.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

File system inconsistencies after system crash

CTE-LDT sends two alerts to the DSM if CTE-LDT fails to resolve the issues encountered during recovery.

The alert below is an error report sent to the DSM whenever CTE-LDT encounters failure during recovery prior to enabling GuardPoint. This alert also reports the GuardPoint specified in the message is not enabled:

- **LDT-ALERT: Cannot enable guard point [GuardPoint] due to inconsistencies in underlying file system encountered during LDT recovery**

The alert below is a warning report sent to the DSM only if `voradmin ldt recover` encounters errors and continues anyway. This alert reports the GuardPoint specified in the message has been enabled with some files in error status.

- **LDT-ALERT: LDT manual recovery on guard point [GuardPoint] completed with [#] errors.**

Solution: See ["Protecting CTE-LDT GuardPoints against Failure in Underlying Filesystems \(Linux\)" on page 84](#).

Error Messages

This section describes runtime error messages. For information about other types of runtime messages, see ["Alerts Playbook" on page 85](#) and ["Warning and Info Messages" on page 92](#).

Failed to Transform File During Rekey

CTE-LDT could not complete transformation on a file.

Related Messages:

- **LDT: Rekey failed for file [PathName] on GuardPoint [GuardPoint]**
- **LDT: Extended attribute of inode [InodeNumber] is corrupted under GuardPoint [GuardPoint]**

Solution: An I/O error is the most common cause of failure when updating CTE-LDT metadata. For I/O errors, fix the problem at the host OS or storage level, and then restore the file from a backup.

If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

Failure to Suspend CTE-LDT

A request to stop CTE-LDT processing did not succeed. The suspend request was at the host level as part of a QoS schedule, or the suspend request was initiated by a user on the DSM.

Related Messages:

- **LDT: Failed to suspend rekey on all GuardPoints**
- **LDT operations could not be suspended on the host**

Solution: An I/O error is the most common cause of failure when updating the persistent state of a GuardPoint. For I/O errors, fix the problem at the host OS or storage level.

If a backup operation is in progress when this message occurs, you must fix the cause of the suspend failure and then restart the backup. If the backup has already completed when the alert message occurs, the backup image on the GuardPoint may have inconsistent data and CTE-LDT metadata. Discard this backup image and do a fresh backup.

If you cannot find and fix the host OS or storage issue, contact Customer Support for troubleshooting and recovery.

Failure to Start or Stop Transformation

The following general messages are recorded when there are errors attempting to start or stop CTE-LDT:

- **LDT: Failed to abort key rotation on GuardPoint [GuardPoint]**
- **LDT: Failed to start**
- **LDT: Failed to stop**
- **LDT: Failed to exit**

Solution: Examine system logs for additional information as to the cause. If you cannot find and fix the underlying host OS or storage issue that is causing the error, contact Customer Support for troubleshooting and recovery.

Failure to Restart Transformation

The following message is recorded when an attempt to restart transformation after a system reboot fails because the file system is mounted as read-only. Transformation on the specified GuardPoint cannot continue until the file system is mounted with write permission.

- **LDT: Skipped LDT recovery on read-only file system [GuardPoint]**

Solution: Re-mount the file system with write permissions.

Temporary Failure to Start Transformation on a File

The following messages are recorded when there are communication issues or lack of resources on the host. Once the condition is corrected, transformation of the file continues automatically:

- **LDT: Insufficient memory condition encountered during LDT on GuardPoint [GuardPoint]**
- **LDT: Encryption key for file [PathName] unavailable for LDT, possibly due to loss of communication to DSM**
- **LDT: Aborting rekey of file [PathName] due to lack of free memory. Try closing other application to resolve the issue**

Solution: Resolve the communication issues or increase the available resources, then verify that CTE-LDT has resumed processing.

Transient Condition while enabling GuardPoint

The following messages are recorded when a request is made to guard an CTE-LDT GuardPoint when GuardPoint initialization is already in progress. During the GuardPoint initialization, the system initializes MDS file associated with the GuardPoint in preparation for CTE-LDT. Initialization of the MDS file can take a few minutes. During this time, if the system retries the guard operation, one of the following messages displays.

Related Messages:

- **Not re-guarding path [path] (Reason: GuardPoint initialization already in progress)**
- **Not re-guarding path [path] from container [container] (Reason: GuardPoint initialization already in progress)**

Solution: Wait for the current GuardPoint initialization to complete and then resubmit the new GuardPoint initialization request if desired.

Failed to transform passthrough files for AD database files (Windows Only)

CTE-LDT skipped the transformation of passthrough files for all AD database files. The problem occurs when the AD database remains in the default folder location.

Related Messages:

- **Skipping transformation of passthrough file [filename]. The file resides in the boot directory. CTE cannot encrypt boot directory files.**
- **Skipping transformation of passthrough file [filename]. CTE cannot encrypt these files. They are already encrypted using NTFS encryption or compressed.**
- **Skipping transformation of passthrough file [filename]. File is not in a GuardPoint directory.**

Solution: To fix this issue, move the AD database to any folder other than `c:\windows` or `c:\program files`.

Warning and Info Messages

This section describes runtime error messages. For information about other types of runtime messages, see ["Alerts Playbook" on page 85](#) and ["Error Messages" on page 90](#).

Stopping Transformation of a File on Volume Dismount (Windows only)

The following warning message is recorded when transformation of a file is stopped because the containing volume is dismounted.

- **LDT: Volume dismounted. Aborting transformation at file [PathName]**

Issues with Policy or System Configuration

The following warning messages are recorded when CTE cannot perform CTE-LDT on the GuardPoint, because there are errors in the policy associated with the GuardPoint, or the file system containing the GuardPoint is not supported by CTE-LDT. Files in the GuardPoint can still be accessed, but no CTE-LDT encryption occurs.

- **LDT: The GuardPoint [GuardPoint] does not have a valid transformation policy, there is no new key rule**
- **LDT: The GuardPoint [GuardPoint] does not have a valid transformation policy, there is no key_op rule**
- **LDT: The GuardPoint [GuardPoint] does not support online rekey, only file operations from the offline data transform process will be allowed**

Failure to Enable GuardPoint During Cleanup

CTE-LDT records the following informational message when a user attempts to enable a newly added GuardPoint. This message displays if the GuardPoint directory was previously guarded with an CTE-LDT policy and the CTE-LDT metadata cleanup is in progress when user is guarding under the new policy.

- **LDT: Cannot enable GuardPoint [GuardPoint] during LDT clean-up process**
Solution: Retry the operation once the cleanup completes.

General CTE-LDT Operations

The following informational messages are recorded during various CTE-LDT operations. No action is required.

- **LDT: Successfully suspended rekey on GuardPoint [GuardPoint]**
- **LDT: Successfully suspended rekey on all GuardPoints**
- **LDT: Successfully resumed rekey on GuardPoint [GuardPoint]**
- **LDT: Successfully resumed rekey on all GuardPoints**
- **LDT: Rekey operation completed on GuardPoint [GuardPoint]**

Missing CTE-LDT extended attribute

The following warning message reports that the file with the specified inode number in the specified GuardPoint directory does not have an CTE-LDT extended attribute, therefore, access to the file is denied.

- **LDT: Extended attribute of inode [InodeNumber] is missing under GuardPoint [GuardPoint]**
Solution: CTE-LDT cannot determine the encryption key associated with the data in the file, therefore, you can only remove the file.

Locking Contention

The following messages are recorded during the rekey process on a file. When user access to the file is very high, it causes a high degree of locking contention between the rekey process and user access. The second message reports when the contention is no longer in effect and the rekey process has resumed accessing file to rekey.

- **LDT: Exclusive access for rekey delayed on inode [InodeNumber]**
- **LDT: Exclusive access for rekey granted after delay on inode [InodeNumber]**

Initiation and completion of CTE-LDT metadata cleanup

The following messages are recorded at the beginning and completion of CTE-LDT metadata cleanup through voradmin command.

- **LDT: Metadata will start getting removed from all files in GuardPoint [GuardPoint]**
- **LDT: Metadata has been removed from all files in GuardPoint [GuardPoint]**

Upgrading CTE Agent

On Windows, you cannot upgrade the CTE agent if there is an CTE-LDT GuardPoint with an active rekey in progress, that is at the mount point. On Linux, CTE-LDT is forced-suspended when upgrading CTE.

Reboot is required when upgrading earlier versions of CTE Agent to 6.0.1, if CTE-LDT is in-progress on a GuardPoint. Perform following steps to upgrade to version 7.0.0:

1. From the DSM Management Console, click **Host > Hosts > hostName > GuardPoint** tab.
2. Click **Suspend Rekey**.
3. Click **Refresh** and ensure that the GuardPoint(s) being rekeyed now show a status of Suspended.
4. Reboot the host.
5. Run the 7.0.0 CTE Agent install program and upgrade the agent.
Wait for the upgrade to complete.
6. From the DSM Management Console, click **Host > Hosts > hostName > GuardPoint** tab.
7. Click **Resume Rekey**.
8. Click **Refresh** and ensure that the GuardPoints being rekeyed now show a status of Rekeying.

Recommendations and Considerations

The following information provides guidance for a better user experience.

All Platform Recommendations and Considerations

Binary Re-signing

Any executable that is part of either a Signature set or a Host setting, and that resides in a GuardPoint that uses an CTE-LDT policy, will use different signatures for an CTE-LDT key rotation. The result is that the Host Settings binaries will no longer be authenticated, or that the Signature Set policy rules will no longer trigger for those binaries.

To prevent these issues, the Security Administrator must manually re-sign each affected binary after each key rotation.

Alternatively, CTE can generate unencrypted signatures of binaries inside GuardPoints to avoid these problems. For details, see the *DSM Administration Guide*.

Check for available disk space for CTE-LDT metadata

Before launching CTE-LDT on a GuardPoint:

1. Check the available free disk space in the file system where your GuardPoint resides.
2. Type the following command to check the disk space requirement of CTE-LDT on a target GuardPoint:

```
# voradmin ldt space /oxf-fs1/gp1
/oxf-fs1/gp1: found 1501 files without LDT extended attributes
LDT disk space requirements: total 169MB (LDT attributes=6MB, MDS=163MB)
```

In this example, the output shows that CTE-LDT requires 169MB of available disk space to launch and execute CTE-LDT on /oxf-fs1/gp1.

Note

Make sure that the free space in your file system exceeds the disk space requirement for CTE-LDT.

CTE-LDT Requirements for Backup

CTE offers the option to backup encrypted data from files through a security rule, which skips the Apply Key function when reading encrypted files by backup applications or processes. Such files can also be restored from backup streams, to the same or a different GuardPoint, without Apply Key. If you choose to restore to another GuardPoint, the target GuardPoint must be protected with the same key and security rules as the source GuardPoint.

If you backup encrypted data from files inside GuardPoints with CTE-LDT policies, CTE-LDT imposes a hard requirement on the backup application, or process, to backup or restore CTE-LDT metadata. The CTE-LDT metadata is stored as an extended attribute on Linux and as alternate data streams on files on Windows platforms. If the backup process cannot backup the metadata, then CTE-LDT protected GuardPoints must be backed up in clear key.

Customers are required to verify their backup application, or process, to ensure extended attributes (on Linux) or alternate data streams (on Windows) are backed up and restored through their backup/restore processes.

Note

Make sure that you suspend CTE-LDT operations before you start the backup process, and resume them after the backup process completes.

Learn Mode

Learn Mode provides a temporary method for disabling the blocking behavior of regular CTE or CTE-LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set.

Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption.

Note

Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.

Quality of Service (QoS)

By default, the QoS component of CTE-LDT does not monitor live transformation operations unless you enable QoS on your host by entering QoS parameters on the DSM. To avoid overhead of CTE-LDT on your production system, you must select QoS parameters suitable to your production environment. For information on tuning QoS, see ["Quality of Service" on page 30](#). It is critical that you understand the impact of CTE-LDT on your system and how to manage this impact using QoS.

Upgrade to CTE 7.0.0

Since the the first release of the CTE-LDT feature, Thales has made several improvements in the areas of error handling, interoperability with applications, and Quality of Service (QoS). Thales strongly recommends that new deployments use version 7.0.0 (or later) of CTE. Thales further recommends that customers who have already deployed the CTE-LDT feature upgrade to version 7.0.0.

Windows Recommendations and Considerations

File Handling

The CTE-LDT process is subjected to all of the File System policies and attributes set on the files. In some cases, this prevents CTE-LDT from encrypting a file. If users or applications are accessing files while CTE-LDT is in progress, CTE-LDT cannot change the attributes of the files and encrypt the file. It is critical that you understand how CTE-LDT handles various types of files:

- **NTFS Encryption and Compression**

If NTFS encryption or compression is enabled on a file or folder, the CTE-LDT process cannot encrypt these files. To maintain the data coherency, CTE-LDT skips the encryption of the these files. These files display as "passthrough" files in the CTE-LDT statistics.

- **Read-Only Files**

As the CTE-LDT process performs a read-encrypt-write operation on a file, it cannot encrypt read-only files. The CTE-LDT process skips these files and changes to the INCOMPLETE state.

- **Executable Files**

If a executable is running or files are exclusively locked by the application, the CTE-LDT process cannot encrypt those files as it is unable to acquire the required locks on the files. CTE-LDT skips these files and changes to the INCOMPLETE state.

File Modification

The CTE-LDT process performs a read-encrypt-write operation on the files that need to be encrypted, (also known as rekeying). Previously, file modification and access dates were changed when CTE-LDT was processing. In order to maintain compatibility for applications, we addressed this issue by saving a copy of the original access and modification times, and restoring them after the encryption completed. Preserved timestamps are updated during the rekey process, if an application/user accesses the files during rekey.

Note

Thales strongly recommends that you upgrade to the newly released v6.1.0 so that the access time and modification time is restored correctly.

CTE-LDT Limitations

- CTE-LDT on CIFS is not supported.
- CTE-LDT on a ReFS file system runs slowly because of limited support from the Extended Attributes on the ReFS file system.

Note

Customers running older versions of ReFS.sys on Windows Server 2012 R2 should be aware of the memory growth issue encountered by the Thales engineering team. This issue seems to occur only when CTE-LDT is running on a large number of files. As the system memory consumption by REFS file system increases, it can eventually make the system unresponsive. This issue does not occur with the recent versions of ReFS file system drivers available on Windows Server 2016. After consulting with Microsoft, they suggest that all customers migrate to Windows Server 2016 if they are using ReFS file.

Logical Sector Size

CTE-LDT Windows transformation is supported if the **logical sector size** is more than 512 Bytes. (A logical sector size of 4K is supported.) To find the logical sector size of the file system, type:

```
> fsutil fsinfo ntfsInfo <volume pathname>
```

For example:

```
> fsutil fsinfo ntfsInfo C:
NTFS Volume Serial Number :      0x5092568a92567506
NTFS Version      :              3.1
LFS Version      :              2.0
Number Sectors :      0x000000001c004eeb
Total Clusters :      0x00000000038009dd
Free Clusters :      0x00000000008bb274
Total Reserved :      0x0000000000001864
Bytes Per Sector :      512
.
.
.
```

Upgrade Notes



CAUTION

Do not upgrade the Windows agent without valid DSM connectivity.

During the upgrade, InstallShield cleans up the agent configuration on the host. If the agent does not have DSM connectivity, then it cannot pull the configuration from the DSM after it reboots. As the configuration is cleaned up, the Windows agent removes all of the GuardPoints from the host.

VSS Volumes

If a Shadow Copy volume is present on a volume before CTE-LDT starts, and this volume is accessed by the application or user, then CTE reads the CTE-LDT metadata from the shadow copy volume snapshot and incorrectly uses this metadata for the original file. Because the metadata on the snapshot is old, this may lead to double encryption of the files inside the GuardPoint.

Thales highly recommends that, if you are running a version of VTE earlier than 6.0.3.68, you must delete all of the old VSS volumes where CTE-LDT GuardPoints exist in order to avoid this issue.

CTE-LDT Limitations on Linux

- CTE-LDT on NFS share is not supported.
- CTE-LDT support is limited to `ext3`, `ext4`, `XFS`, and `VxFS` file systems when `user_xattr` mount option is enabled.



CTE OS Support Life Cycle

Version: v1.0.0 (latest)

30 January 2026

Contents

- CTE OS Lifecycle Taxonomy 3
 - CipherTrust Transparent Encryption Support 3
 - CipherTrust Transparent Encryption UserSpace Support 6
 - Extended Support Considerations 7
 - CipherTrust Transparent Encryption for Kubernetes Support. 8
 - CTE OS Support Guidelines. 9

CTE OS Lifecycle Taxonomy

- CTE OS Support Guidelines
- CipherTrust Transparent Encryption Support
- CipherTrust Transparent Encryption UserSpace Support
- CipherTrust Transparent Encryption for Kubernetes Support
- Extended Support Considerations

CipherTrust Transparent Encryption Support

CipherTrust Transparent Encryption is an agent that runs in the kernel of an operating system. Due to the nature of the product, CipherTrust Transparent Encryption has many updates per year. On average, there are two to three feature releases per year. These releases contain major and/or minor new features or enhancements, support for new third-party databases or applications, and support for new major or minor versions of operating systems. During the rest of the year, Thales may release an update to CipherTrust Transparent Encryption on an almost weekly basis, in order to roll in new operating system kernel patch support and hot fixes. Following are the details of the CipherTrust Transparent Encryption product lifecycle, as well as the OS support guidelines.

CipherTrust Transparent Encryption Release Types

The following table describes the CipherTrust Transparent Encryption release types:

CipherTrust Transparent Encryption Release	Major	Service Pack	Cumulative Patch	Hot Fix or New Kernel Support Build
Numbering	1.0.0	1.1.0	1.1.1	1.1.0.x
Cadence	3+ Years	6 Months	As needed	As needed
Contents	Major change in functionality	New features, fixes, major or minor OS support	New minor features, fixes, minor OS support	Hot fix or minor OS support, kernel updates if new CipherTrust Transparent Encryption build is needed

CipherTrust Transparent Encryption Support Phase Definitions

The following table contains the CipherTrust Transparent Encryption support phase definitions:

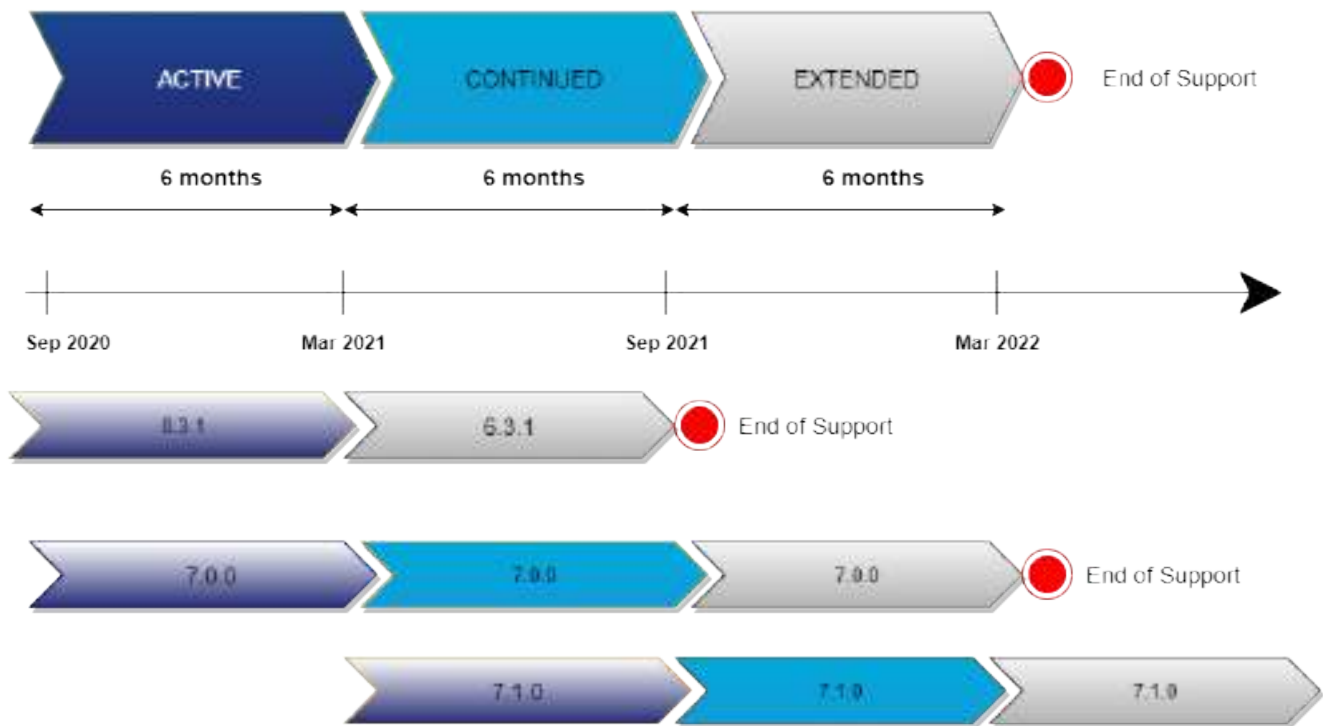
Support Phase	Definition	Timeframe
Active	Period during which Thales	From GA to the start of Continued

Support Phase	Definition	Timeframe
	customer support assists customers with issues. A maintenance agreement makes the customer eligible for patches, and service packs.	Support
Continued Support	Customer support can be engaged mainly for troubleshooting and workarounds. Thales engineering will fix bugs and provide validation for new OS kernels and new minor OS releases on an as-need basis. However, no additional investment will be made by development and engineering departments.	Begins with the release of the next Service Pack; Ends after 6 months.
Extended Support	Support provided on an as-needed basis. An extended maintenance agreement must be in place. Thales will provide bug fixes only. Thales will not add support for new operating systems or kernels.	Support time frame begins after Continued Support ends, and lasts for 6 months.

CipherTrust Transparent Encryption Life Cycle

Following is a diagram of the CipherTrust Transparent Encryption Life cycle. The version numbers are an example. They are not valid version numbers. The actual release time lines for these versions of CipherTrust Transparent Encryption may be different. In general, there will be two “live” CipherTrust Transparent Encryption versions at a time: one CipherTrust Transparent Encryption version that is in active phase, and one that is in the Continued Support phase. In some cases, a third CipherTrust Transparent Encryption version will also be in the extended support phase. This is to allow customers more time to move to the newer versions.

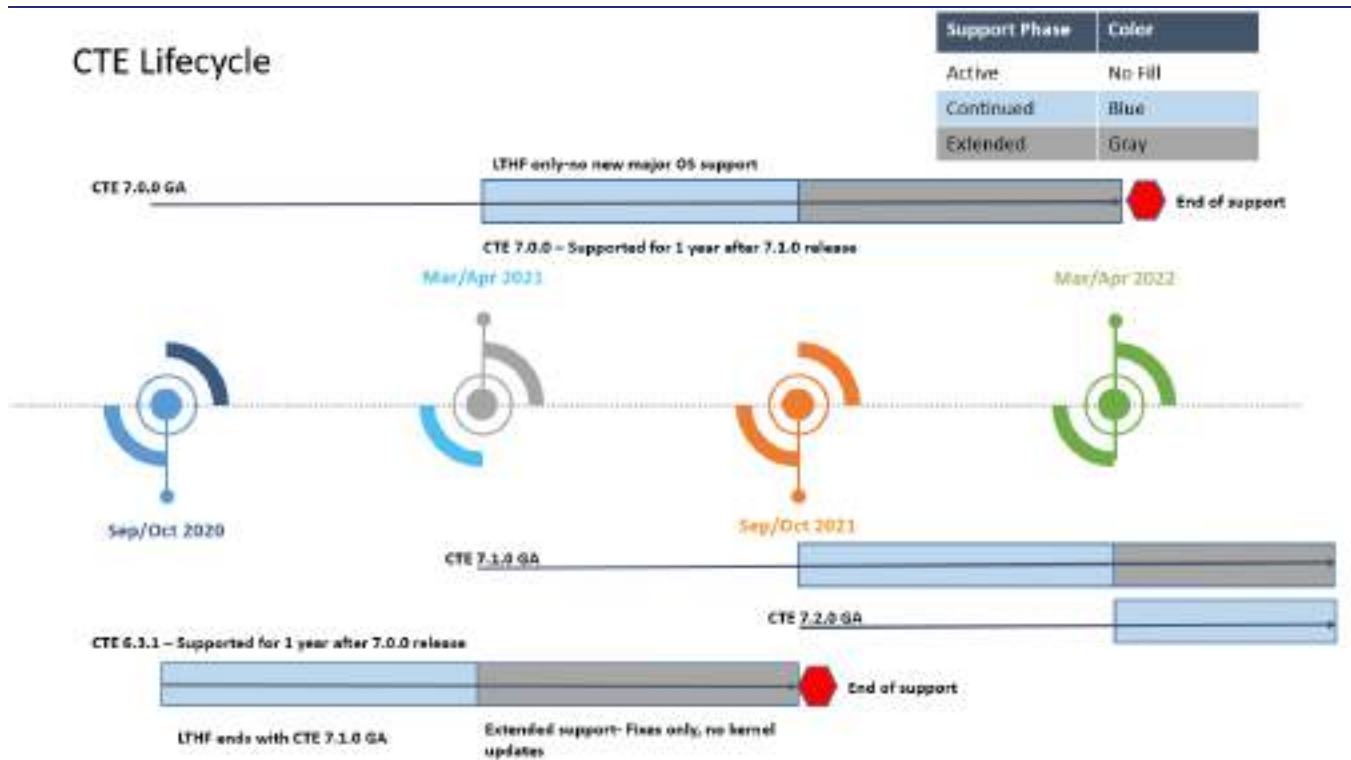
CTE Lifecycle



LTHF = Linux Taxonomy Hot Fix

Linux Taxonomy refers to the qualification of new Linux kernel releases with CTE.

When a cumulative patch is released for a CipherTrust Transparent Encryption version that will be considered as the **active** CipherTrust Transparent Encryption version, the current active service pack version, and the previous service pack release, continue to be supported for the continued support period. For instance, for the two active CipherTrust Transparent Encryption versions 7.0.0 and 7.1.0, if a cumulative patch for 7.1.1 is released, CipherTrust Transparent Encryption 7.1.1 and CipherTrust Transparent Encryption 7.1.0 would be the supported versions for hot fixes.



CipherTrust Transparent Encryption UserSpace Support

Overview

CipherTrust Transparent Encryption Userspace, (formerly SafeNet ProtectFile FUSE), is a file-system level transparent encryption solution that leverages the cryptographic and key management features of the platform to protect unstructured data. CipherTrust Transparent Encryption Userspace is based on Linux FUSE and hence, is not required to be updated when there is a Linux kernel update from the OS vendor. Following are the details of the CipherTrust Transparent Encryption Userspace product lifecycle.

CipherTrust Transparent Encryption Userspace Release Types

CTE Release	Major	Service Pack	Cumulative Patch
Numbering	1.0.0	1.1.0	1.1.1
Cadence	3+ Years	6 Months	As needed
Contents	Major change in functionality	New features, fixes, major or minor OS support	New minor features, fixes, minor OS support

CipherTrust Transparent Encryption Userspace Definitions

Support Phase	Definition	Timeframe
Active	Period during which Thales customer support will assist customers with issues. A	From GA to the start of Continued Support.

Support Phase	Definition	Timeframe
	maintenance agreement will make the customer eligible for patches, and service packs.	
Continued Support	Customer support can be engaged mainly for troubleshooting and workarounds. Thales engineering will provide bugs and security fixes on an as-needed basis. No additional investment will be made by development and engineering departments.	Begins with the release of the next Service Pack; Ends after 6 months.
Extended Support	Support provided on an as-needed basis. An extended maintenance agreement must be in place. Thales will provide bug fixes only.	Only applies to the last Service pack before a Major release. Support timeframe begins after Continued Support ends and lasts 6 months.

Extended Support Considerations

Support changes for Red Hat Enterprise Linux v7 with CipherTrust Transparent Encryption 7.8.0

In May, 2022, Red Hat released a new major version of its Enterprise Linux operating system: v9. Thales was able to begin supporting Red Hat Enterprise Linux (RHEL) 9 immediately with CipherTrust Transparent Encryption version 7.2.0 as a participant in the Early Adopter Program (EAP). This means that Thales is phasing out support for RHEL v7. Thales tries to maintain the operating system support policy of providing support with CipherTrust Transparent Encryption for the two latest major versions of an operating system as outlined in this guide. Accordingly, Thales has shifted to a One-Off manual qualification process on a need-only basis for RHEL 7.9 kernels. Thales understand that this is a highly adopted and widely used operating system, so Thales is willing to extend CipherTrust Transparent Encryption support for a grace period to allow customers to move their RHEL 7 systems to a newer version before removing support.

According to Red Hat support portal, End of “Maintenance Support 2 (Product Retirement)” from Red Hat for RHEL 7 will be June 30, 2024. Thales would like to align, as best as possible, to this date.

Thales will review the need for supporting RHEL 7 during the Extended Lifecycle Support (ELS) which ends, June 30, 2026, and it will only be available to customers with additional extended support contracts for CipherTrust Transparent Encryption agents.

Thales will provide priority bug fixes on an as-needed basis and technical support for customers with paid support contracts. Thales will not add any new features, enhancements, performance improvements, update third party databases or provide application interoperability support on the CipherTrust Transparent Encryption agents for RHEL 7.

Support changes for Red Hat Enterprise Linux v8 with CipherTrust Transparent Encryption 7.9.0

In May, 2025, Red Hat released a new major version of its Enterprise Linux operating system: v10. Thales was able to begin supporting Red Hat Enterprise Linux (RHEL) 10 kernels immediately with CipherTrust Transparent Encryption version 7.8.0 as a participant in the Early Adopter Program (EAP). This means that Thales is phasing

out support for RHEL v8. Thales tries to maintain the operating system support policy of providing support with CipherTrust Transparent Encryption for the two latest major versions of an operating system as outlined in this guide. Accordingly, Thales has shifted to a One-Off manual qualification process on a need-only basis for RHEL 8.10 kernels. Thales understands that this is a highly adopted and widely used operating system, so Thales is willing to extend CipherTrust Transparent Encryption support for a grace period to allow customers to move their RHEL 8 systems to a newer version before removing support.

CTE 7.9.0, would be the last release supporting RHEL 8.10 formally and CTE 8.0.0 would stop supporting RHEL 8.

According to Red Hat support portal, End of “Maintenance Support (Standard)” from Red Hat for RHEL 8 will be May 31, 2029. Thales would continue to support new kernels as they become available for RHEL 8.10 with CTE 7.9.0 latest patch release.

Thales will provide priority bug fixes on an as-needed basis and technical support for customers with valid support contracts. Thales will not add any new features, enhancements, performance improvements, or update third party application interoperability support on the CipherTrust Transparent Encryption 7.9.0 agents for RHEL 8.

With reference to CTE-UserSpace, considering it is not dependent on Linux kernel, we'll continue to maintain support for RHEL 8 in future CTE-UserSpace releases until End of “Maintenance Support (Standard)” from Red Hat for RHEL 8.

CipherTrust Transparent Encryption for Kubernetes Support

CTE for Kubernetes is an implementation of the CipherTrust Transparent Encryption with native support for Kubernetes through the implementation of a CSI (Container Storage Interface) driver. Unlike traditional CTE, product installation and GuardPoint management is done through Kubernetes. This means that as the cluster scales up with more nodes, CTE for Kubernetes scales with it. CTE for Kubernetes is designed to protect Kubernetes Persistent Storage Claims that are backed by storage with filesystem semantics.



Thales qualifies only [Active Kubernetes releases](#) when releasing a CTE-K8s feature release.

CTE for Kubernetes release types

CTE Release	Major	Service Pack	Cumulative Patch
Numbering	1.0.0	1.1.0	1.1.1
Cadence	3+ Years	4+ Months	As needed
Contents	Major change in functionality	New features, fixes	New minor features, fixes

Support Phase Definitions

Support Phase	Definition	Timeframe
Active	Period during which Thales customer support will assist customers with issues. A maintenance agreement will make the customer eligible for patches, and service packs.	From GA to the start of Continued Support
Continued Support	Customer support can be engaged mainly for troubleshooting and work-arounds. Thales engineering will provide bugs and security fixes on an as-needed basis. No additional investment will be made by development and engineering departments.	Begins with the release of the next Service Pack; Ends after six months.
Extended Support	Support provided on an as-needed basis. An extended maintenance agreement must be in place. Thales will provide bug fixes only.	Only applies to the last Service pack before a Major release. Support timeframe begins after Continued Support ends and lasts six months

CTE OS Support Guidelines

CipherTrust Transparent Encryption supports the latest **TWO** major versions of an OS, for example RedHat Enterprise Linux 7 & 8, at any given time. CipherTrust Transparent Encryption also supports the latest minor version (or Service Pack) of a major OS. Two examples are RedHat Enterprise Linux (RHEL) 7.9 and RHEL 8.4. Thales will qualify new kernel patches on the most recent minor or service pack version of an OS only. This mainly applies to Linux operating systems where kernel compatibility is critical. CipherTrust Transparent Encryption is generally compatible with new kernel patches for any OS, but Linux creates patches more frequently and there is a higher probability for incompatibility.

CipherTrust Transparent Encryption Compatibility Portal

The [CipherTrust Transparent Encryption compatibility portal](#) online compatibility portal lists all of the supported operating system kernels.

In addition, go to [CTE Packages Repository](#) to download a JSON file of all of the CTE supported kernels. Upload this file to your Key Manager to monitor agent compatibility. Request credentials to the packages repository from the [Thales Support team](#).

OS Kernel Validation Process

Operating system vendors (especially Linux) release new kernel patches very frequently. Thales will automatically pick up these kernel patches, and test them with the latest version of CipherTrust Transparent Encryption. In the majority of cases, CipherTrust Transparent Encryption will not need an update to support a new kernel patch. Once validation is completed, Thales will announce kernel support with the current CipherTrust Transparent Encryption version, or release a new build. Keep in mind that Thales will test kernel patches from the latest service pack (or minor version) of the two most recent major OS versions. The compatibility matrices will be updated (including the JSON file version) with the new kernel support, and if a new build is required, it will be posted for download from the Thales repositories.

Extended Update or Long-Term Support Kernels

Thales does not regularly validate kernel patches from OS versions that have entered Extended Update (EUS) or long-term support phases. This is in keeping with the policy of supporting the latest two major, and the latest minor version, of an OS. However, OS vendors are required to patch vulnerabilities in their software even if the OS has gone into an extended support or long-term support phase of the lifecycle. They are frequently releasing new kernel patches to their customers on these extended support branches. For this reason, Thales will validate EUS kernels for RHEL and LTSS kernels for SUSE, on a case-by-case basis using a “one-off” (or manual) validation process.

The following tables contain information on the validation processes for the OS distributions:

RedHat Enterprise Linux Support

RHEL Release	Thales Release	Time frame for support (by vendor, from GA date)	Example	Comment
Major	Next major or service pack CTE release	60 Business Days	RHEL 8	Major OS releases typically include significant kernel enhancements, new features and file systems.
Minor/Service Pack	Next major, service pack, or cumulative patch CTE release	20 Business Days	RHEL 8.4	OS Service pack or update releases do not include significant new features but on occasion break kernel binary compatibility.
Critical kernel security patch	Next CTE release, any type	4 Business Days		In exceptional cases, when more than 4 days are required, Thales will inform customers of the planned release date.
One-off EUS Kernel	Next CTE release, any type	30 Business Days		Must have Product Management

RHEL Release	Thales Release	Time frame for support (by vendor, from GA date)	Example	Comment
				approval; contact Thales support to request a one-off validation.

SUSE Linux Enterprise Server Support

Note

Thales does not generally support long-term service pack support kernels, (LTSS).

SUSE Linux Release	Thales Release	Time frame for support (by vendor, from GA date)	Example	Comment
Major	Next major or service pack CTE release	Up to 90 business days	SLES 15	Major OS releases typically include significant kernel enhancements, new features and file systems.
Minor/Service Pack	Next major, service pack, or cumulative patch CTE release	Up to 60 business days	SLES 15 SP1	OS Service pack or update releases do not include significant new features but on occasion break kernel binary compatibility.
Critical kernel security patch	Next CTE release, any type	Up to 4 business days		In exceptional cases, when more than 20 days are required, Thales will inform customers of the planned release date.
One-off LTSS kernel	Next CTE release, any type	Up to 30 business days		Must have Product Management approval; contact Thales support to request a one-off validation.

Ubuntu Server Linux Support

Thales Ubuntu support includes an exception. Thales will support two kernel series on the latest two major versions: e.g., the GA kernel and the HWE (hardware enablement) kernel series.

Ubuntu Linux security patches often break compatibility, and require a new build of CTE. Thales will release a new build according to the SLA noted below. The “one-off” kernel validation process does not apply to Ubuntu.

Ubuntu Linux Release	Thales Release	Time frame for support (by vendor, from GA date)	Example	Comment
Major	Next major or service pack CTE release	Up to 90 business days	Ubuntu 20.04	Major OS releases typically include significant kernel enhancements, new features and file systems.
Minor/Service Pack	Next major, service pack, or cumulative patch CTE release	Up to 60 business days	Ubuntu 20.04.1	OS Service pack do not include significant new features but on occasion break kernel binary compatibility.
Critical kernel security patch	Next CTE release, any type	Up to 15 business days		

Windows Support

Thales supports both Windows Server and Windows Client versions. Check the [CipherTrust Transparent Encryption compatibility portal](#) for the list of supported operating systems.

Windows Release	Thales Release	Time frame for support (from the time of GA by vendor)	Example	Comment
Major/Long-term servicing channel	Next major or service pack CTE release	Up to 90 business days	Windows 2019	Windows long-term servicing channel releases typically include significant enhancements, new features and file systems.
Semi-annual channel releases	Next major, service pack, or cumulative patch CTE release	Up to 60 business days		Semi-annual channel releases do not include significant new features, but on occasion break kernel compatibility.
Security,	N/A	N/A		Windows patches

Windows Release	Thales Release	Time frame for support (from the time of GA by vendor)	Example	Comment
Cumulative Patches				rarely break compatibility. No CTE update required.

Note

CipherTrust Transparent Encryption Windows will drop support for Operating systems when end of support is announced by Microsoft for an Operating system.

AIX

AIX Release	Thales Release	Time frame for support (from the time of GA by vendor)	Example	Comment
Major	Next major or service pack CTE release	Up to 180 business days	AIX 8.1	Major releases typically include significant kernel enhancements, new features and file systems.
Technology Level	Next major, service pack, or cumulative patch CTE release	Up to 90 business days	AIX 7.2 TL1	Technology Level releases do not include significant new features but on occasion break kernel binary compatibility.
Kernel & Security patches or service pack for Technology Level	Next major, service pack, or cumulative patch CTE release	Up to 30 business days	AIX 7.2 TL1 SP5	Kernel patches or TL SP typically do not break compatibility. When they do, Thales will release a new CTE patch.



CipherTrust Data Security Platform

CipherTrust Data Security Event and Log Messages Guide

Release 7.8.0

Document Version 1

June 17, 2025

CipherTrust Data Security CipherTrust Transparent Encryption
CipherTrust Data Security CipherTrust Data Security Event and Log Messages Guide
Release 7.8.0
June 17, 2025
Document Version 1

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2009 - 2025 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Table of Contents

<u>Logger CGA: Errors</u>	1
<u>Message ID : CGA2614E</u>	1
<u>Message ID : CGA2617E</u>	1
<u>Message ID : CGA2618E</u>	2
<u>Message ID : CGA2619E</u>	3
<u>Message ID : CGA2620E</u>	3
<u>Message ID : CGA2621E</u>	4
<u>Message ID : CGA2624E</u>	5
<u>Message ID : CGA2625E</u>	6
<u>Message ID : CGA2626E</u>	6
<u>Message ID : CGA2627E</u>	7
<u>Message ID : CGA2628E</u>	8
<u>Message ID : CGA2629E</u>	9
<u>Message ID : CGA2634E</u>	10
<u>Message ID : CGA2635E</u>	11
<u>Message ID : CGA2636E</u>	12
<u>Message ID : CGA2637E</u>	13
<u>Message ID : CGA2638E</u>	13
<u>Message ID : CGA2639E</u>	14
<u>Message ID : CGA2645E</u>	15
<u>Message ID : CGA2648E</u>	16
<u>Message ID : CGA2649E</u>	17
<u>Message ID : CGA2650E</u>	18
<u>Message ID : CGA2651E</u>	19
<u>Message ID : CGA2652E</u>	20
<u>Message ID : CGA2653E</u>	21
<u>Message ID : CGA2654E</u>	22

Table of Contents

Logger CGA: Errors

<u>Message ID : CGA2655E</u>	23
<u>Message ID : CGA2656E</u>	24
<u>Message ID : CGA2657E</u>	25
<u>Message ID : CGA2658E</u>	26
<u>Message ID : CGA2659E</u>	27
<u>Message ID : CGA2662E</u>	28
<u>Message ID : CGA3003E</u>	28
<u>Message ID : CGA3004E</u>	29
<u>Message ID : CGA3007E</u>	30
<u>Message ID : CGA3008E</u>	31
<u>Message ID : CGA3009E</u>	32
<u>Message ID : CGA3010E</u>	33
<u>Message ID : CGA3011E</u>	34
<u>Message ID : CGA3012E</u>	35
<u>Message ID : CGA3013E</u>	35
<u>Message ID : CGA3014E</u>	36
<u>Message ID : CGA3015E</u>	37
<u>Message ID : CGA3016E</u>	37
<u>Message ID : CGA3017E</u>	38
<u>Message ID : CGA3018E</u>	39
<u>Message ID : CGA3021E</u>	40
<u>Message ID : CGA3022E</u>	41
<u>Message ID : CGA3023E</u>	42
<u>Message ID : CGA3024E</u>	42
<u>Message ID : CGA3059E</u>	43
<u>Message ID : CGA3060E</u>	44

Table of Contents

Logger CGA: Errors

<u>Message ID : CGA3061E</u>	45
<u>Message ID : CGA3062E</u>	46
<u>Message ID : CGA3063E</u>	47
<u>Message ID : CGA3064E</u>	48
<u>Message ID : CGA3065E</u>	49
<u>Message ID : CGA3066E</u>	50
<u>Message ID : CGA3067E</u>	50
<u>Message ID : CGA3068E</u>	51
<u>Message ID : CGA3069E</u>	52
<u>Message ID : CGA3070E</u>	53
<u>Message ID : CGA3071E</u>	54
<u>Message ID : CGA3072E</u>	55
<u>Message ID : CGA3073E</u>	56
<u>Message ID : CGA3074E</u>	56
<u>Message ID : CGA3075E</u>	57
<u>Message ID : CGA3076E</u>	58
<u>Message ID : CGA3077E</u>	59
<u>Message ID : CGA3078E</u>	60
<u>Message ID : CGA3079E</u>	61
<u>Message ID : CGA3080E</u>	62
<u>Message ID : CGA3081E</u>	62
<u>Message ID : CGA3082E</u>	63
<u>Message ID : CGA3083E</u>	64
<u>Message ID : CGA3084E</u>	65
<u>Message ID : CGA3085E</u>	66
<u>Message ID : CGA3086E</u>	67

Table of Contents

Logger CGA: Errors

<u>Message ID : CGA3087E</u>	68
<u>Message ID : CGA3088E</u>	69
<u>Message ID : CGA3089E</u>	70
<u>Message ID : CGA3090E</u>	71
<u>Message ID : CGA3091E</u>	72
<u>Message ID : CGA3092E</u>	72
<u>Message ID : CGA3093E</u>	73
<u>Message ID : CGA3094E</u>	74
<u>Message ID : CGA3095E</u>	75
<u>Message ID : CGA3096E</u>	76
<u>Message ID : CGA3097E</u>	77
<u>Message ID : CGA3098E</u>	78
<u>Message ID : CGA3099E</u>	78
<u>Message ID : CGA3100E</u>	79
<u>Message ID : CGA3101E</u>	80
<u>Message ID : CGA3102E</u>	81
<u>Message ID : CGA3103E</u>	82
<u>Message ID : CGA3109E</u>	83
<u>Message ID : CGA3110E</u>	84
<u>Message ID : CGA3111E</u>	84
<u>Message ID : CGA3112E</u>	85
<u>Message ID : CGA3113E</u>	86
<u>Message ID : CGA3114E</u>	87
<u>Message ID : CGA3115E</u>	88
<u>Message ID : CGA3116E</u>	89
<u>Message ID : CGA3117E</u>	90

Table of Contents

Logger CGA: Errors

<u>Message ID : CGA3118E</u>	91
<u>Message ID : CGA3119E</u>	92
<u>Message ID : CGA3120E</u>	93
<u>Message ID : CGA3121E</u>	94
<u>Message ID : CGA3122E</u>	95
<u>Message ID : CGA3123E</u>	96
<u>Message ID : CGA3124E</u>	97
<u>Message ID : CGA3125E</u>	97
<u>Message ID : CGA3126E</u>	98
<u>Message ID : CGA3127E</u>	99
<u>Message ID : CGA3128E</u>	100
<u>Message ID : CGA3129E</u>	101
<u>Message ID : CGA3130E</u>	102
<u>Message ID : CGA3131E</u>	103
<u>Message ID : CGA3132E</u>	104
<u>Message ID : CGA3133E</u>	105
<u>Message ID : CGA3134E</u>	106
<u>Message ID : CGA3135E</u>	107
<u>Message ID : CGA3136E</u>	108
<u>Message ID : CGA3137E</u>	109
<u>Message ID : CGA3138E</u>	110
<u>Message ID : CGA3139E</u>	110
<u>Message ID : CGA3140E</u>	111
<u>Message ID : CGA3141E</u>	112
<u>Message ID : CGA3142E</u>	113
<u>Message ID : CGA3143E</u>	114

Table of Contents

Logger CGA: Errors

<u>Message ID : CGA3144E</u>	115
<u>Message ID : CGA3145E</u>	116
<u>Message ID : CGA3146E</u>	117
<u>Message ID : CGA3147E</u>	118
<u>Message ID : CGA3148E</u>	119
<u>Message ID : CGA3149E</u>	120
<u>Message ID : CGA3150E</u>	121
<u>Message ID : CGA3151E</u>	122
<u>Message ID : CGA3152E</u>	123
<u>Message ID : CGA3153E</u>	123
<u>Message ID : CGA3154E</u>	124
<u>Message ID : CGA3155E</u>	125
<u>Message ID : CGA3156E</u>	126
<u>Message ID : CGA3157E</u>	127
<u>Message ID : CGA3158E</u>	128
<u>Message ID : CGA3159E</u>	129
<u>Message ID : CGA3160E</u>	130
<u>Message ID : CGA3161E</u>	131
<u>Message ID : CGA3162E</u>	132
<u>Message ID : CGA3163E</u>	133
<u>Message ID : CGA3164E</u>	134
<u>Message ID : CGA3165E</u>	135
<u>Message ID : CGA3166E</u>	136
<u>Message ID : CGA3167E</u>	136
<u>Message ID : CGA3168E</u>	137
<u>Message ID : CGA3169E</u>	138

Table of Contents

Logger CGA: Errors

<u>Message ID : CGA3170E</u>	139
<u>Message ID : CGA3171E</u>	140
<u>Message ID : CGA3172E</u>	141
<u>Message ID : CGA3173E</u>	142
<u>Message ID : CGA3174E</u>	143
<u>Message ID : CGA3175E</u>	144
<u>Message ID : CGA3176E</u>	145
<u>Message ID : CGA3177E</u>	146
<u>Message ID : CGA3178E</u>	147
<u>Message ID : CGA3179E</u>	148
<u>Message ID : CGA3180E</u>	149
<u>Message ID : CGA3181E</u>	149
<u>Message ID : CGA3182E</u>	150
<u>Message ID : CGA3184E</u>	151
<u>Message ID : CGA3185E</u>	152
<u>Message ID : CGA3187E</u>	153
<u>Message ID : CGA3188E</u>	154
<u>Message ID : CGA3189E</u>	155
<u>Message ID : CGA3190E</u>	156
<u>Message ID : CGA3191E</u>	156
<u>Message ID : CGA3192E</u>	157
<u>Message ID : CGA3206E</u>	158
<u>Message ID : CGA3212E</u>	159
<u>Message ID : CGA3218E</u>	160
<u>Message ID : CGA3220E</u>	161
<u>Message ID : CGA3222E</u>	162

Table of Contents

Logger CGA: Errors

<u>Message ID : CGA3223E</u>	163
<u>Message ID : CGA3227E</u>	164
<u>Message ID : CGA3228E</u>	165
<u>Message ID : CGA3229E</u>	166
<u>Message ID : CGA3230E</u>	167
<u>Message ID : CGA3232E</u>	168
<u>Message ID : CGA3233E</u>	169
<u>Message ID : CGA3235E</u>	170
<u>Message ID : CGA3236E</u>	170
<u>Message ID : CGA3237E</u>	171
<u>Message ID : CGA3238E</u>	172
<u>Message ID : CGA3239E</u>	173
<u>Message ID : CGA3252E</u>	174
<u>Message ID : CGA3256E</u>	175
<u>Message ID : CGA3272E</u>	176
<u>Message ID : CGA3274E</u>	177
<u>Message ID : CGA3275E</u>	178
<u>Message ID : CGA3278E</u>	179
<u>Message ID : CGA3279E</u>	180
<u>Message ID : CGA3280E</u>	180
<u>Message ID : CGA3282E</u>	181
<u>Message ID : CGA3284E</u>	182
<u>Message ID : CGA3289E</u>	183
<u>Message ID : CGA3292E</u>	184
<u>Message ID : CGA3295E</u>	185
<u>Message ID : CGA3298E</u>	186

Table of Contents

Logger CGA: Errors

<u>Message ID : CGA3301E</u>	187
<u>Message ID : CGA3304E</u>	187
<u>Message ID : CGA3306E</u>	188
<u>Message ID : CGA3307E</u>	189
<u>Message ID : CGA3308E</u>	190
<u>Message ID : CGA3309E</u>	191
<u>Message ID : CGA3310E</u>	192
<u>Message ID : CGA3356E</u>	193
<u>Message ID : CGA3361E</u>	194

Logger CGA: Information.....196

<u>Message ID : CGA2622I</u>	196
<u>Message ID : CGA2630I</u>	196
<u>Message ID : CGA2631I</u>	197
<u>Message ID : CGA2632I</u>	198
<u>Message ID : CGA2633I</u>	198
<u>Message ID : CGA2640I</u>	199
<u>Message ID : CGA2641I</u>	200
<u>Message ID : CGA2642I</u>	200
<u>Message ID : CGA2643I</u>	201
<u>Message ID : CGA2644I</u>	202
<u>Message ID : CGA2646I</u>	202
<u>Message ID : CGA2647I</u>	203
<u>Message ID : CGA2660I</u>	204
<u>Message ID : CGA2661I</u>	205
<u>Message ID : CGA3001I</u>	206

Table of Contents

Logger CGA: Information

<u>Message ID : CGA3005I</u>	207
<u>Message ID : CGA3006I</u>	207
<u>Message ID : CGA3019I</u>	208
<u>Message ID : CGA3020I</u>	209
<u>Message ID : CGA3058I</u>	210
<u>Message ID : CGA3105I</u>	211
<u>Message ID : CGA3183I</u>	212
<u>Message ID : CGA3186I</u>	213
<u>Message ID : CGA3193I</u>	214
<u>Message ID : CGA3194I</u>	214
<u>Message ID : CGA3195I</u>	215
<u>Message ID : CGA3196I</u>	216
<u>Message ID : CGA3197I</u>	217
<u>Message ID : CGA3198I</u>	218
<u>Message ID : CGA3199I</u>	219
<u>Message ID : CGA3200I</u>	220
<u>Message ID : CGA3201I</u>	221
<u>Message ID : CGA3202I</u>	222
<u>Message ID : CGA3203I</u>	222
<u>Message ID : CGA3204I</u>	223
<u>Message ID : CGA3205I</u>	224
<u>Message ID : CGA3207I</u>	225
<u>Message ID : CGA3208I</u>	226
<u>Message ID : CGA3209I</u>	227
<u>Message ID : CGA3210I</u>	228
<u>Message ID : CGA3211I</u>	229

Table of Contents

Logger CGA: Information

<u>Message ID : CGA3213I</u>	229
<u>Message ID : CGA3214I</u>	230
<u>Message ID : CGA3215I</u>	231
<u>Message ID : CGA3216I</u>	232
<u>Message ID : CGA3217I</u>	233
<u>Message ID : CGA3219I</u>	234
<u>Message ID : CGA3221I</u>	234
<u>Message ID : CGA3224I</u>	236
<u>Message ID : CGA3225I</u>	237
<u>Message ID : CGA3226I</u>	237
<u>Message ID : CGA3240I</u>	238
<u>Message ID : CGA3241I</u>	239
<u>Message ID : CGA3242I</u>	240
<u>Message ID : CGA3244I</u>	241
<u>Message ID : CGA3245I</u>	242
<u>Message ID : CGA3246I</u>	243
<u>Message ID : CGA3247I</u>	244
<u>Message ID : CGA3248I</u>	244
<u>Message ID : CGA3257I</u>	245
<u>Message ID : CGA3258I</u>	246
<u>Message ID : CGA3269I</u>	247
<u>Message ID : CGA3270I</u>	248
<u>Message ID : CGA3271I</u>	249
<u>Message ID : CGA3273I</u>	250
<u>Message ID : CGA3281I</u>	251
<u>Message ID : CGA3283I</u>	252

Table of Contents

Logger CGA: Information

<u>Message ID : CGA3287I</u>	252
<u>Message ID : CGA3288I</u>	253
<u>Message ID : CGA3290I</u>	254
<u>Message ID : CGA3291I</u>	255
<u>Message ID : CGA3293I</u>	256
<u>Message ID : CGA3294I</u>	257
<u>Message ID : CGA3296I</u>	258
<u>Message ID : CGA3297I</u>	259
<u>Message ID : CGA3299I</u>	260
<u>Message ID : CGA3300I</u>	261
<u>Message ID : CGA3305I</u>	262
<u>Message ID : CGA3343I</u>	263

Logger CGA: Warnings.....264

<u>Message ID : CGA2615W</u>	264
<u>Message ID : CGA2616W</u>	264
<u>Message ID : CGA2623W</u>	265
<u>Message ID : CGA2901W</u>	266
<u>Message ID : CGA3002W</u>	267
<u>Message ID : CGA3104W</u>	268
<u>Message ID : CGA3106W</u>	269
<u>Message ID : CGA3107W</u>	270
<u>Message ID : CGA3108W</u>	270
<u>Message ID : CGA3231W</u>	271
<u>Message ID : CGA3243W</u>	272
<u>Message ID : CGA3265W</u>	273

Table of Contents

Logger CGA: Warnings

<u>Message ID : CGA3276W</u>	274
<u>Message ID : CGA3285W</u>	275
<u>Message ID : CGA3286W</u>	276
<u>Message ID : CGA3346W</u>	277
<u>Message ID : CGA3352W</u>	278
<u>Message ID : CGA3353W</u>	279

Logger CGP: Errors.....280

<u>Message ID : CGP2602E</u>	280
<u>Message ID : CGP2604E</u>	281
<u>Message ID : CGP2606E</u>	282
<u>Message ID : CGP2608E</u>	284
<u>Message ID : CGP2610E</u>	285

Logger CGP: Information.....287

<u>Message ID : CGP2601I</u>	287
<u>Message ID : CGP2603I</u>	288
<u>Message ID : CGP2605I</u>	289
<u>Message ID : CGP2607I</u>	291
<u>Message ID : CGP2609I</u>	292

Logger CGS: Errors.....294

<u>Message ID : CGS2613E</u>	294
<u>Message ID : CGS3025E</u>	294
<u>Message ID : CGS3026E</u>	295
<u>Message ID : CGS3027E</u>	296

Table of Contents

Logger CGS: Errors

<u>Message ID : CGS3028E</u>	297
<u>Message ID : CGS3031E</u>	298
<u>Message ID : CGS3032E</u>	299
<u>Message ID : CGS3033E</u>	300
<u>Message ID : CGS3034E</u>	301
<u>Message ID : CGS3035E</u>	302
<u>Message ID : CGS3038E</u>	303
<u>Message ID : CGS3039E</u>	303
<u>Message ID : CGS3042E</u>	304
<u>Message ID : CGS3043E</u>	305
<u>Message ID : CGS3044E</u>	306
<u>Message ID : CGS3045E</u>	307
<u>Message ID : CGS3047E</u>	308
<u>Message ID : CGS3048E</u>	309
<u>Message ID : CGS3049E</u>	310
<u>Message ID : CGS3050E</u>	310
<u>Message ID : CGS3051E</u>	311
<u>Message ID : CGS3052E</u>	312
<u>Message ID : CGS3053E</u>	313
<u>Message ID : CGS3054E</u>	314
<u>Message ID : CGS3055E</u>	315
<u>Message ID : CGS3057E</u>	316
<u>Message ID : CGS3234E</u>	317
<u>Message ID : CGS3253E</u>	318
<u>Message ID : CGS3259E</u>	319
<u>Message ID : CGS3260E</u>	320

Table of Contents

Logger CGS: Errors

<u>Message ID : CGS3261E</u>	320
<u>Message ID : CGS3262E</u>	321
<u>Message ID : CGS3263E</u>	322
<u>Message ID : CGS3264E</u>	323
<u>Message ID : CGS3266E</u>	324
<u>Message ID : CGS3304E</u>	325
<u>Message ID : CGS3305E</u>	326
<u>Message ID : CGS3306E</u>	327
<u>Message ID : CGS3307E</u>	328
<u>Message ID : CGS3308E</u>	329
<u>Message ID : CGS3309E</u>	330
<u>Message ID : CGS3311E</u>	330
<u>Message ID : CGS3312E</u>	331
<u>Message ID : CGS3313E</u>	332
<u>Message ID : CGS3314E</u>	333
<u>Message ID : CGS3315E</u>	334
<u>Message ID : CGS3316E</u>	335
<u>Message ID : CGS3317E</u>	336
<u>Message ID : CGS3319E</u>	337
<u>Message ID : CGS3327E</u>	338
<u>Message ID : CGS3328E</u>	338
<u>Message ID : CGS3329E</u>	340
<u>Message ID : CGS3331E</u>	341
<u>Message ID : CGS3335E</u>	342
<u>Message ID : CGS3336E</u>	343
<u>Message ID : CGS3337E</u>	343

Table of Contents

Logger CGS: Errors

<u>Message ID : CGS3338E</u>	344
<u>Message ID : CGS3339E</u>	345
<u>Message ID : CGS3340E</u>	346
<u>Message ID : CGS3341E</u>	347
<u>Message ID : CGS3342E</u>	348
<u>Message ID : CGS3344E</u>	349
<u>Message ID : CGS3349E</u>	350
<u>Message ID : CGS3354E</u>	351
<u>Message ID : CGS3358E</u>	352
<u>Message ID : CGS3360E</u>	353
<u>Message ID : CGS3362E</u>	353
<u>Message ID : CGS3364E</u>	355
<u>Message ID : CGS3365E</u>	356
<u>Message ID : CGS3370E</u>	357
<u>Message ID : CGS3371E</u>	357

Logger CGS: Information.....359

<u>Message ID : CGS3029I</u>	359
<u>Message ID : CGS3030I</u>	360
<u>Message ID : CGS3036I</u>	360
<u>Message ID : CGS3037I</u>	361
<u>Message ID : CGS3040I</u>	362
<u>Message ID : CGS3041I</u>	363
<u>Message ID : CGS3046I</u>	364
<u>Message ID : CGS3056I</u>	365
<u>Message ID : CGS3249I</u>	366

Table of Contents

Logger CGS: Information

<u>Message ID : CGS3250I</u>	366
<u>Message ID : CGS3251I</u>	367
<u>Message ID : CGS3254I</u>	368
<u>Message ID : CGS3255I</u>	369
<u>Message ID : CGS3277I</u>	370
<u>Message ID : CGS3318I</u>	371
<u>Message ID : CGS3320I</u>	372
<u>Message ID : CGS3322I</u>	373
<u>Message ID : CGS3324I</u>	373
<u>Message ID : CGS3325I</u>	374
<u>Message ID : CGS3347I</u>	375
<u>Message ID : CGS3348I</u>	376
<u>Message ID : CGS3350I</u>	377
<u>Message ID : CGS3355I</u>	378
<u>Message ID : CGS3357I</u>	379
<u>Message ID : CGS3359I</u>	379

Logger CGS: Warnings.....**381**

<u>Message ID : CGS3267W</u>	381
<u>Message ID : CGS3268W</u>	382
<u>Message ID : CGS3302W</u>	383
<u>Message ID : CGS3303W</u>	384
<u>Message ID : CGS3310W</u>	385
<u>Message ID : CGS3321W</u>	385
<u>Message ID : CGS3323W</u>	386
<u>Message ID : CGS3326W</u>	387

Table of Contents

Logger CGS: Warnings

<u>Message ID : CGS3330W</u>	388
<u>Message ID : CGS3332W</u>	389
<u>Message ID : CGS3333W</u>	390
<u>Message ID : CGS3334W</u>	391
<u>Message ID : CGS3345W</u>	392
<u>Message ID : CGS3351W</u>	393
<u>Message ID : CGS3363W</u>	394
<u>Message ID : CGS3369W</u>	394

Logger COM: Errors.....**396**

<u>Message ID : COM4547E</u>	396
<u>Message ID : COM4631E</u>	396
<u>Message ID : COM4638E</u>	397
<u>Message ID : COM4644E</u>	398

Logger COM: Fatal errors.....**400**

<u>Message ID : COM4503F</u>	400
<u>Message ID : COM4506F</u>	400
<u>Message ID : COM4511F</u>	401
<u>Message ID : COM4512F</u>	402
<u>Message ID : COM4513F</u>	403
<u>Message ID : COM4514F</u>	404
<u>Message ID : COM4515F</u>	405
<u>Message ID : COM4521F</u>	405
<u>Message ID : COM4523F</u>	406
<u>Message ID : COM4527F</u>	407

Table of Contents

Logger COM: Fatal errors

<u>Message ID : COM4529F</u>	408
<u>Message ID : COM4531F</u>	409
<u>Message ID : COM4533F</u>	410
<u>Message ID : COM4534F</u>	410
<u>Message ID : COM4538F</u>	411
<u>Message ID : COM4542F</u>	412
<u>Message ID : COM4548F</u>	413
<u>Message ID : COM4551F</u>	414
<u>Message ID : COM4552F</u>	415
<u>Message ID : COM4554F</u>	415
<u>Message ID : COM4558F</u>	416
<u>Message ID : COM4562F</u>	417
<u>Message ID : COM4563F</u>	418
<u>Message ID : COM4567F</u>	419
<u>Message ID : COM4569F</u>	420
<u>Message ID : COM4571F</u>	421
<u>Message ID : COM4577F</u>	422
<u>Message ID : COM4578F</u>	422
<u>Message ID : COM4579F</u>	423
<u>Message ID : COM4583F</u>	424
<u>Message ID : COM4584F</u>	425
<u>Message ID : COM4586F</u>	426
<u>Message ID : COM4587F</u>	426
<u>Message ID : COM4588F</u>	427
<u>Message ID : COM4592F</u>	428
<u>Message ID : COM4599F</u>	429

Table of Contents

<u>Logger COM: Fatal errors</u>	
<u>Message ID : COM4600F</u>	430
<u>Message ID : COM4603F</u>	431
<u>Message ID : COM4604F</u>	432
<u>Message ID : COM4628F</u>	433
<u>Message ID : COM4629F</u>	434
<u>Message ID : COM4630F</u>	434
<u>Message ID : COM4637F</u>	436
<u>Logger COM: Information</u>	437
<u>Message ID : COM4601I</u>	437
<u>Message ID : COM4602I</u>	438
<u>Message ID : COM4626I</u>	438
<u>Message ID : COM4627I</u>	439
<u>Logger COM: Warnings</u>	441
<u>Message ID : COM4596W</u>	441
<u>Message ID : COM4597W</u>	442
<u>Message ID : COM4605W</u>	442
<u>Message ID : COM4632W</u>	443
<u>Message ID : COM4633W</u>	444
<u>Message ID : COM4634W</u>	446
<u>Message ID : COM4635W</u>	447
<u>Logger DGV: Errors</u>	449
<u>Message ID : DGV6001E</u>	449
<u>Message ID : DGV6002E</u>	449

Table of Contents

Logger DGV: Errors

<u>Message ID : DGV6003E</u>	450
<u>Message ID : DGV6004E</u>	451
<u>Message ID : DGV6005E</u>	452
<u>Message ID : DGV6006E</u>	453
<u>Message ID : DGV6007E</u>	454
<u>Message ID : DGV6008E</u>	455
<u>Message ID : DGV6009E</u>	455
<u>Message ID : DGV6010E</u>	456
<u>Message ID : DGV6011E</u>	457
<u>Message ID : DGV6012E</u>	458
<u>Message ID : DGV6013E</u>	459
<u>Message ID : DGV6014E</u>	460
<u>Message ID : DGV6015E</u>	461
<u>Message ID : DGV6016E</u>	461
<u>Message ID : DGV6017E</u>	462
<u>Message ID : DGV6018E</u>	463
<u>Message ID : DGV7007E</u>	464
<u>Message ID : DGV7009E</u>	465
<u>Message ID : DGV7011E</u>	466
<u>Message ID : DGV7012E</u>	467
<u>Message ID : DGV7014E</u>	468
<u>Message ID : DGV7019E</u>	469
<u>Message ID : DGV7023E</u>	469
<u>Message ID : DGV7030E</u>	470
<u>Message ID : DGV7033E</u>	471
<u>Message ID : DGV7038E</u>	472

Table of Contents

Logger DGV: Errors

<u>Message ID : DGV7041E</u>	473
<u>Message ID : DGV7046E</u>	474
<u>Message ID : DGV7054E</u>	474

Logger DGV: Information.....476

<u>Message ID : DGV6019I</u>	476
<u>Message ID : DGV6020I</u>	476
<u>Message ID : DGV6022I</u>	477
<u>Message ID : DGV7001I</u>	478
<u>Message ID : DGV7002I</u>	479
<u>Message ID : DGV7004I</u>	480
<u>Message ID : DGV7005I</u>	481
<u>Message ID : DGV7006I</u>	482
<u>Message ID : DGV7008I</u>	482
<u>Message ID : DGV7010I</u>	483
<u>Message ID : DGV7013I</u>	484
<u>Message ID : DGV7016I</u>	485
<u>Message ID : DGV7017I</u>	486
<u>Message ID : DGV7018I</u>	487
<u>Message ID : DGV7020I</u>	487
<u>Message ID : DGV7021I</u>	488
<u>Message ID : DGV7022I</u>	489
<u>Message ID : DGV7024I</u>	490
<u>Message ID : DGV7025I</u>	491
<u>Message ID : DGV7026I</u>	492
<u>Message ID : DGV7027I</u>	492

Table of Contents

Logger DGV: Information

<u>Message ID : DGV7028I</u>	493
<u>Message ID : DGV7029I</u>	494
<u>Message ID : DGV7031I</u>	495
<u>Message ID : DGV7032I</u>	496
<u>Message ID : DGV7034I</u>	497
<u>Message ID : DGV7035I</u>	497
<u>Message ID : DGV7036I</u>	498
<u>Message ID : DGV7037I</u>	499
<u>Message ID : DGV7039I</u>	500
<u>Message ID : DGV7040I</u>	501
<u>Message ID : DGV7042I</u>	502
<u>Message ID : DGV7043I</u>	502
<u>Message ID : DGV7044I</u>	503
<u>Message ID : DGV7045I</u>	504
<u>Message ID : DGV7049I</u>	505
<u>Message ID : DGV7050I</u>	506
<u>Message ID : DGV7051I</u>	507
<u>Message ID : DGV7052I</u>	507
<u>Message ID : DGV7053I</u>	508

Logger DGV: Warnings.....510

<u>Message ID : DGV6021W</u>	510
<u>Message ID : DGV7003W</u>	510
<u>Message ID : DGV7015W</u>	511
<u>Message ID : DGV7047W</u>	512
<u>Message ID : DGV7048W</u>	513

Table of Contents

<u>Logger DXF: Debug messages</u>	515
<u>Message ID : DXF4308D</u>	515
<u>Message ID : DXF4310D</u>	515
<u>Message ID : DXF4311D</u>	516
<u>Message ID : DXF4473D</u>	517
<u>Message ID : DXF4475D</u>	517
<u>Logger DXF: Errors</u>	519
<u>Message ID : DXF3205E</u>	519
<u>Message ID : DXF3206E</u>	520
<u>Message ID : DXF3207E</u>	520
<u>Message ID : DXF3208E</u>	521
<u>Message ID : DXF3209E</u>	522
<u>Message ID : DXF3215E</u>	523
<u>Message ID : DXF3216E</u>	524
<u>Message ID : DXF3217E</u>	525
<u>Message ID : DXF3218E</u>	526
<u>Message ID : DXF3219E</u>	526
<u>Message ID : DXF3220E</u>	527
<u>Message ID : DXF3221E</u>	528
<u>Message ID : DXF3222E</u>	529
<u>Message ID : DXF3223E</u>	530
<u>Message ID : DXF3224E</u>	531
<u>Message ID : DXF3225E</u>	532
<u>Message ID : DXF3226E</u>	532
<u>Message ID : DXF3227E</u>	533
<u>Message ID : DXF3228E</u>	534

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF3229E.....</u>	535
<u>Message ID : DXF3230E.....</u>	536
<u>Message ID : DXF3231E.....</u>	537
<u>Message ID : DXF3232E.....</u>	538
<u>Message ID : DXF3233E.....</u>	538
<u>Message ID : DXF3238E.....</u>	539
<u>Message ID : DXF3239E.....</u>	540
<u>Message ID : DXF3240E.....</u>	541
<u>Message ID : DXF3241E.....</u>	542
<u>Message ID : DXF3242E.....</u>	543
<u>Message ID : DXF3243E.....</u>	544
<u>Message ID : DXF3244E.....</u>	544
<u>Message ID : DXF3245E.....</u>	545
<u>Message ID : DXF3246E.....</u>	546
<u>Message ID : DXF3247E.....</u>	547
<u>Message ID : DXF3248E.....</u>	548
<u>Message ID : DXF3249E.....</u>	549
<u>Message ID : DXF3250E.....</u>	550
<u>Message ID : DXF3251E.....</u>	550
<u>Message ID : DXF3252E.....</u>	551
<u>Message ID : DXF4100E.....</u>	552
<u>Message ID : DXF4101E.....</u>	553
<u>Message ID : DXF4102E.....</u>	554
<u>Message ID : DXF4105E.....</u>	554
<u>Message ID : DXF4106E.....</u>	555
<u>Message ID : DXF4107E.....</u>	556

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF4108E.....</u>	557
<u>Message ID : DXF4109E.....</u>	558
<u>Message ID : DXF4111E.....</u>	559
<u>Message ID : DXF4112E.....</u>	560
<u>Message ID : DXF4113E.....</u>	561
<u>Message ID : DXF4114E.....</u>	562
<u>Message ID : DXF4115E.....</u>	563
<u>Message ID : DXF4116E.....</u>	564
<u>Message ID : DXF4117E.....</u>	565
<u>Message ID : DXF4119E.....</u>	566
<u>Message ID : DXF4120E.....</u>	567
<u>Message ID : DXF4121E.....</u>	567
<u>Message ID : DXF4124E.....</u>	568
<u>Message ID : DXF4125E.....</u>	569
<u>Message ID : DXF4133E.....</u>	570
<u>Message ID : DXF4134E.....</u>	570
<u>Message ID : DXF4135E.....</u>	571
<u>Message ID : DXF4136E.....</u>	572
<u>Message ID : DXF4137E.....</u>	573
<u>Message ID : DXF4138E.....</u>	574
<u>Message ID : DXF4139E.....</u>	575
<u>Message ID : DXF4140E.....</u>	576
<u>Message ID : DXF4141E.....</u>	576
<u>Message ID : DXF4142E.....</u>	577
<u>Message ID : DXF4149E.....</u>	578
<u>Message ID : DXF4150E.....</u>	579

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF4151E</u>	580
<u>Message ID : DXF4152E</u>	580
<u>Message ID : DXF4153E</u>	581
<u>Message ID : DXF4155E</u>	582
<u>Message ID : DXF4156E</u>	582
<u>Message ID : DXF4157E</u>	583
<u>Message ID : DXF4158E</u>	584
<u>Message ID : DXF4159E</u>	585
<u>Message ID : DXF4160E</u>	585
<u>Message ID : DXF4162E</u>	586
<u>Message ID : DXF4163E</u>	587
<u>Message ID : DXF4164E</u>	588
<u>Message ID : DXF4165E</u>	589
<u>Message ID : DXF4166E</u>	589
<u>Message ID : DXF4167E</u>	590
<u>Message ID : DXF4168E</u>	591
<u>Message ID : DXF4169E</u>	592
<u>Message ID : DXF4170E</u>	592
<u>Message ID : DXF4171E</u>	593
<u>Message ID : DXF4172E</u>	594
<u>Message ID : DXF4173E</u>	594
<u>Message ID : DXF4174E</u>	595
<u>Message ID : DXF4215E</u>	596
<u>Message ID : DXF4227E</u>	597
<u>Message ID : DXF4228E</u>	597
<u>Message ID : DXF4229E</u>	598

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF4230E</u>	599
<u>Message ID : DXF4231E</u>	599
<u>Message ID : DXF4232E</u>	600
<u>Message ID : DXF4233E</u>	601
<u>Message ID : DXF4234E</u>	601
<u>Message ID : DXF4235E</u>	602
<u>Message ID : DXF4236E</u>	603
<u>Message ID : DXF4237E</u>	603
<u>Message ID : DXF4238E</u>	604
<u>Message ID : DXF4239E</u>	605
<u>Message ID : DXF4240E</u>	605
<u>Message ID : DXF4241E</u>	606
<u>Message ID : DXF4243E</u>	607
<u>Message ID : DXF4244E</u>	607
<u>Message ID : DXF4247E</u>	608
<u>Message ID : DXF4248E</u>	609
<u>Message ID : DXF4249E</u>	610
<u>Message ID : DXF4250E</u>	611
<u>Message ID : DXF4251E</u>	612
<u>Message ID : DXF4252E</u>	612
<u>Message ID : DXF4255E</u>	613
<u>Message ID : DXF4266E</u>	614
<u>Message ID : DXF4270E</u>	615
<u>Message ID : DXF4271E</u>	616
<u>Message ID : DXF4272E</u>	617
<u>Message ID : DXF4282E</u>	618

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF4286E.....</u>	619
<u>Message ID : DXF4287E.....</u>	620
<u>Message ID : DXF4288E.....</u>	621
<u>Message ID : DXF4289E.....</u>	622
<u>Message ID : DXF4290E.....</u>	623
<u>Message ID : DXF4291E.....</u>	624
<u>Message ID : DXF4292E.....</u>	625
<u>Message ID : DXF4294E.....</u>	625
<u>Message ID : DXF4295E.....</u>	626
<u>Message ID : DXF4296E.....</u>	627
<u>Message ID : DXF4297E.....</u>	627
<u>Message ID : DXF4298E.....</u>	628
<u>Message ID : DXF4299E.....</u>	629
<u>Message ID : DXF4300E.....</u>	630
<u>Message ID : DXF4301E.....</u>	631
<u>Message ID : DXF4302E.....</u>	632
<u>Message ID : DXF4303E.....</u>	633
<u>Message ID : DXF4304E.....</u>	633
<u>Message ID : DXF4306E.....</u>	634
<u>Message ID : DXF4312E.....</u>	635
<u>Message ID : DXF4313E.....</u>	636
<u>Message ID : DXF4314E.....</u>	636
<u>Message ID : DXF4315E.....</u>	637
<u>Message ID : DXF4325E.....</u>	638
<u>Message ID : DXF4326E.....</u>	639
<u>Message ID : DXF4328E.....</u>	640

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF4330E</u>	641
<u>Message ID : DXF4331E</u>	642
<u>Message ID : DXF4334E</u>	642
<u>Message ID : DXF4335E</u>	643
<u>Message ID : DXF4336E</u>	644
<u>Message ID : DXF4340E</u>	645
<u>Message ID : DXF4341E</u>	645
<u>Message ID : DXF4342E</u>	646
<u>Message ID : DXF4343E</u>	647
<u>Message ID : DXF4346E</u>	647
<u>Message ID : DXF4347E</u>	648
<u>Message ID : DXF4349E</u>	649
<u>Message ID : DXF4350E</u>	650
<u>Message ID : DXF4353E</u>	650
<u>Message ID : DXF4354E</u>	651
<u>Message ID : DXF4355E</u>	652
<u>Message ID : DXF4356E</u>	652
<u>Message ID : DXF4357E</u>	653
<u>Message ID : DXF4358E</u>	654
<u>Message ID : DXF4360E</u>	655
<u>Message ID : DXF4367E</u>	656
<u>Message ID : DXF4368E</u>	657
<u>Message ID : DXF4376E</u>	658
<u>Message ID : DXF4377E</u>	659
<u>Message ID : DXF4379E</u>	659
<u>Message ID : DXF4381E</u>	660

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF4382E</u>	661
<u>Message ID : DXF4391E</u>	662
<u>Message ID : DXF4392E</u>	663
<u>Message ID : DXF4393E</u>	664
<u>Message ID : DXF4394E</u>	665
<u>Message ID : DXF4395E</u>	665
<u>Message ID : DXF4396E</u>	666
<u>Message ID : DXF4400E</u>	667
<u>Message ID : DXF4401E</u>	667
<u>Message ID : DXF4403E</u>	668
<u>Message ID : DXF4404E</u>	669
<u>Message ID : DXF4405E</u>	670
<u>Message ID : DXF4407E</u>	671
<u>Message ID : DXF4408E</u>	671
<u>Message ID : DXF4409E</u>	672
<u>Message ID : DXF4427E</u>	673
<u>Message ID : DXF4430E</u>	674
<u>Message ID : DXF4432E</u>	675
<u>Message ID : DXF4433E</u>	676
<u>Message ID : DXF4434E</u>	676
<u>Message ID : DXF4435E</u>	677
<u>Message ID : DXF4436E</u>	678
<u>Message ID : DXF4437E</u>	678
<u>Message ID : DXF4438E</u>	679
<u>Message ID : DXF4439E</u>	680
<u>Message ID : DXF4440E</u>	680

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF4441E</u>	681
<u>Message ID : DXF4442E</u>	682
<u>Message ID : DXF4443E</u>	682
<u>Message ID : DXF4444E</u>	683
<u>Message ID : DXF4445E</u>	684
<u>Message ID : DXF4446E</u>	684
<u>Message ID : DXF4447E</u>	685
<u>Message ID : DXF4448E</u>	686
<u>Message ID : DXF4449E</u>	686
<u>Message ID : DXF4450E</u>	687
<u>Message ID : DXF4451E</u>	688
<u>Message ID : DXF4452E</u>	688
<u>Message ID : DXF4453E</u>	689
<u>Message ID : DXF4454E</u>	690
<u>Message ID : DXF4455E</u>	690
<u>Message ID : DXF4456E</u>	691
<u>Message ID : DXF4457E</u>	692
<u>Message ID : DXF4458E</u>	692
<u>Message ID : DXF4459E</u>	693
<u>Message ID : DXF4460E</u>	694
<u>Message ID : DXF4461E</u>	694
<u>Message ID : DXF4462E</u>	695
<u>Message ID : DXF4463E</u>	696
<u>Message ID : DXF4464E</u>	696
<u>Message ID : DXF4465E</u>	697
<u>Message ID : DXF4466E</u>	698

Table of Contents

Logger DXF: Errors

<u>Message ID : DXF4467E</u>	699
<u>Message ID : DXF4468E</u>	699
<u>Message ID : DXF4469E</u>	700
<u>Message ID : DXF4470E</u>	701
<u>Message ID : DXF4471E</u>	701
<u>Message ID : DXF4472E</u>	702
<u>Message ID : DXF4474E</u>	703
<u>Message ID : DXF4476E</u>	703
<u>Message ID : DXF4477E</u>	704
<u>Message ID : DXF4478E</u>	705
<u>Message ID : DXF4479E</u>	706
<u>Message ID : DXF4480E</u>	706
<u>Message ID : DXF4482E</u>	707
<u>Message ID : DXF4483E</u>	708
<u>Message ID : DXF4484E</u>	709
<u>Message ID : DXF4486E</u>	710
<u>Message ID : DXF4494E</u>	710
<u>Message ID : DXF4498E</u>	711
<u>Message ID : DXF4499E</u>	712

Logger DXF: Fatal errors.....714

<u>Message ID : DXF4431E</u>	714

Logger DXF: Information.....715

<u>Message ID : DXF3211I</u>	715
<u>Message ID : DXF3235I</u>	716

Table of Contents

Logger DXF: Information

<u>Message ID : DXF3236I</u>	717
<u>Message ID : DXF3237I</u>	718
<u>Message ID : DXF4122I</u>	719
<u>Message ID : DXF4123I</u>	719
<u>Message ID : DXF4126I</u>	720
<u>Message ID : DXF4127I</u>	721
<u>Message ID : DXF4128I</u>	721
<u>Message ID : DXF4129I</u>	722
<u>Message ID : DXF4130I</u>	723
<u>Message ID : DXF4131I</u>	724
<u>Message ID : DXF4132I</u>	724
<u>Message ID : DXF4143I</u>	725
<u>Message ID : DXF4144I</u>	726
<u>Message ID : DXF4145I</u>	727
<u>Message ID : DXF4146I</u>	728
<u>Message ID : DXF4147I</u>	729
<u>Message ID : DXF4148I</u>	730
<u>Message ID : DXF4154I</u>	730
<u>Message ID : DXF4161I</u>	732
<u>Message ID : DXF4200I</u>	732
<u>Message ID : DXF4201I</u>	733
<u>Message ID : DXF4202I</u>	734
<u>Message ID : DXF4203I</u>	735
<u>Message ID : DXF4204I</u>	736
<u>Message ID : DXF4205I</u>	737
<u>Message ID : DXF4206I</u>	737

Table of Contents

Logger DXF: Information

<u>Message ID : DXF4207I.....</u>	738
<u>Message ID : DXF4208I.....</u>	739
<u>Message ID : DXF4209I.....</u>	740
<u>Message ID : DXF4210I.....</u>	741
<u>Message ID : DXF4211I.....</u>	742
<u>Message ID : DXF4212I.....</u>	742
<u>Message ID : DXF4213I.....</u>	743
<u>Message ID : DXF4214I.....</u>	744
<u>Message ID : DXF4216I.....</u>	745
<u>Message ID : DXF4217I.....</u>	746
<u>Message ID : DXF4218I.....</u>	746
<u>Message ID : DXF4219I.....</u>	747
<u>Message ID : DXF4220I.....</u>	748
<u>Message ID : DXF4221I.....</u>	749
<u>Message ID : DXF4222I.....</u>	750
<u>Message ID : DXF4223I.....</u>	751
<u>Message ID : DXF4224I.....</u>	751
<u>Message ID : DXF4225I.....</u>	752
<u>Message ID : DXF4226I.....</u>	753
<u>Message ID : DXF4253I.....</u>	754
<u>Message ID : DXF4257I.....</u>	755
<u>Message ID : DXF4258I.....</u>	756
<u>Message ID : DXF4259I.....</u>	757
<u>Message ID : DXF4260I.....</u>	757
<u>Message ID : DXF4261I.....</u>	758
<u>Message ID : DXF4262I.....</u>	759

Table of Contents

Logger DXF: Information

<u>Message ID : DXF4263I</u>	760
<u>Message ID : DXF4264I</u>	761
<u>Message ID : DXF4265I</u>	761
<u>Message ID : DXF4267I</u>	762
<u>Message ID : DXF4268I</u>	763
<u>Message ID : DXF4269I</u>	764
<u>Message ID : DXF4273I</u>	765
<u>Message ID : DXF4274I</u>	766
<u>Message ID : DXF4275I</u>	767
<u>Message ID : DXF4276I</u>	767
<u>Message ID : DXF4277I</u>	768
<u>Message ID : DXF4278I</u>	769
<u>Message ID : DXF4279I</u>	770
<u>Message ID : DXF4280I</u>	771
<u>Message ID : DXF4281I</u>	771
<u>Message ID : DXF4283I</u>	772
<u>Message ID : DXF4284I</u>	773
<u>Message ID : DXF4285I</u>	774
<u>Message ID : DXF4293I</u>	775
<u>Message ID : DXF4309I</u>	776
<u>Message ID : DXF4316I</u>	777
<u>Message ID : DXF4317I</u>	777
<u>Message ID : DXF4318I</u>	778
<u>Message ID : DXF4319I</u>	779
<u>Message ID : DXF4320I</u>	780
<u>Message ID : DXF4321I</u>	781

Table of Contents

Logger DXF: Information

<u>Message ID : DXF4322I</u>	781
<u>Message ID : DXF4323I</u>	782
<u>Message ID : DXF4329I</u>	783
<u>Message ID : DXF4332I</u>	784
<u>Message ID : DXF4344I</u>	785
<u>Message ID : DXF4345I</u>	786
<u>Message ID : DXF4352I</u>	787
<u>Message ID : DXF4361I</u>	787
<u>Message ID : DXF4362I</u>	788
<u>Message ID : DXF4363I</u>	789
<u>Message ID : DXF4364I</u>	790
<u>Message ID : DXF4365I</u>	791
<u>Message ID : DXF4366I</u>	792
<u>Message ID : DXF4369I</u>	793
<u>Message ID : DXF4370I</u>	794
<u>Message ID : DXF4371I</u>	795
<u>Message ID : DXF4372I</u>	796
<u>Message ID : DXF4375I</u>	797
<u>Message ID : DXF4378I</u>	797
<u>Message ID : DXF4380I</u>	798
<u>Message ID : DXF4383I</u>	799
<u>Message ID : DXF4384I</u>	800
<u>Message ID : DXF4385I</u>	801
<u>Message ID : DXF4386I</u>	802
<u>Message ID : DXF4387I</u>	803
<u>Message ID : DXF4388I</u>	804

Table of Contents

Logger DXF: Information

<u>Message ID : DXF4389I</u>	805
<u>Message ID : DXF4390I</u>	806
<u>Message ID : DXF4397I</u>	806
<u>Message ID : DXF4399I</u>	807
<u>Message ID : DXF4414I</u>	808
<u>Message ID : DXF4415I</u>	809
<u>Message ID : DXF4416I</u>	810
<u>Message ID : DXF4417I</u>	810
<u>Message ID : DXF4418I</u>	811
<u>Message ID : DXF4419I</u>	812
<u>Message ID : DXF4420I</u>	813
<u>Message ID : DXF4421I</u>	814
<u>Message ID : DXF4422I</u>	815
<u>Message ID : DXF4423I</u>	815
<u>Message ID : DXF4424I</u>	816
<u>Message ID : DXF4425I</u>	818
<u>Message ID : DXF4429I</u>	819
<u>Message ID : DXF4481I</u>	819
<u>Message ID : DXF4485I</u>	820
<u>Message ID : DXF4487I</u>	821
<u>Message ID : DXF4488I</u>	822
<u>Message ID : DXF4489I</u>	823
<u>Message ID : DXF4490I</u>	823
<u>Message ID : DXF4491I</u>	824
<u>Message ID : DXF4492I</u>	825
<u>Message ID : DXF4493I</u>	826

Table of Contents

Logger DXF: Information

<u>Message ID : DXF4495I.....</u>	826
<u>Message ID : DXF4496I.....</u>	827
<u>Message ID : DXF4497I.....</u>	828

Logger DXF: Warnings.....830

<u>Message ID : DXF3210W.....</u>	830
<u>Message ID : DXF4103W.....</u>	831
<u>Message ID : DXF4104W.....</u>	831
<u>Message ID : DXF4118W.....</u>	832
<u>Message ID : DXF4242W.....</u>	833
<u>Message ID : DXF4254W.....</u>	834
<u>Message ID : DXF4307W.....</u>	835
<u>Message ID : DXF4324W.....</u>	836
<u>Message ID : DXF4327W.....</u>	836
<u>Message ID : DXF4333W.....</u>	837
<u>Message ID : DXF4337W.....</u>	838
<u>Message ID : DXF4338W.....</u>	839
<u>Message ID : DXF4339W.....</u>	840
<u>Message ID : DXF4351W.....</u>	840
<u>Message ID : DXF4359W.....</u>	841
<u>Message ID : DXF4373W.....</u>	842
<u>Message ID : DXF4398W.....</u>	843
<u>Message ID : DXF4406W.....</u>	844
<u>Message ID : DXF4410W.....</u>	845
<u>Message ID : DXF4413W.....</u>	846
<u>Message ID : DXF4428W.....</u>	846

Table of Contents

<u>Logger FAM: Information</u>	848
<u>Message ID : FAM7001I</u>	848
<u>Message ID : FAM7004I</u>	848
<u>Message ID : FAM7005I</u>	850
<u>Message ID : FAM7006I</u>	852
<u>Message ID : FAM7007I</u>	853
<u>Logger FAM: Warnings</u>	855
<u>Message ID : FAM7002W</u>	855
<u>Logger FUS: Errors</u>	856
<u>Message ID : FUS3368E</u>	856
<u>Logger FUS: Information</u>	857
<u>Message ID : FUS3366I</u>	857
<u>Logger FUS: Warnings</u>	858
<u>Message ID : FUS3367W</u>	858
<u>Logger POL: Errors</u>	859
<u>Message ID : POL4556E</u>	859
<u>Message ID : POL4580E</u>	860
<u>Message ID : POL4613E</u>	861
<u>Message ID : POL4701E</u>	862
<u>Message ID : POL4704E</u>	863

Table of Contents

<u>Logger POL: Fatal errors</u>	864
<u>Message ID : POL4510F</u>	864
<u>Message ID : POL4516F</u>	865
<u>Message ID : POL4528F</u>	866
<u>Message ID : POL4530F</u>	867
<u>Message ID : POL4545F</u>	868
<u>Message ID : POL4564F</u>	868
<u>Message ID : POL4581F</u>	869
<u>Message ID : POL4593F</u>	870
<u>Message ID : POL4614F</u>	871
<u>Logger POL: Information</u>	873
<u>Message ID : POL4537I</u>	873
<u>Message ID : POL4553I</u>	874
<u>Message ID : POL4573I</u>	875
<u>Message ID : POL4574I</u>	876
<u>Message ID : POL4575I</u>	877
<u>Message ID : POL4576I</u>	877
<u>Message ID : POL4582I</u>	878
<u>Message ID : POL4615I</u>	879
<u>Message ID : POL4702I</u>	880
<u>Logger POL: Warnings</u>	882
<u>Message ID : POL4703W</u>	882

Table of Contents

<u>Logger VAD: Errors</u>	883
<u>Message ID : VAD4642E</u>	883
<u>Logger VAD: Information</u>	885
<u>Message ID : VAD4641I</u>	885
<u>Logger VAD: Warnings</u>	887
<u>Message ID : VAD4643W</u>	887
<u>Logger VMD: Errors</u>	888
<u>Message ID : VMD3203E</u>	888
<u>Message ID : VMD3204E</u>	889
<u>Message ID : VMD3503E</u>	889
<u>Message ID : VMD3507E</u>	890
<u>Message ID : VMD3509E</u>	891
<u>Message ID : VMD3510E</u>	892
<u>Message ID : VMD3514E</u>	892
<u>Message ID : VMD3517E</u>	893
<u>Message ID : VMD3520E</u>	894
<u>Message ID : VMD3525E</u>	894
<u>Message ID : VMD3527E</u>	895
<u>Message ID : VMD3533E</u>	896
<u>Message ID : VMD3544E</u>	896
<u>Message ID : VMD3546E</u>	897
<u>Message ID : VMD3550E</u>	898
<u>Message ID : VMD3559E</u>	899
<u>Message ID : VMD3563E</u>	899

Table of Contents

Logger VMD: Errors

<u>Message ID : VMD3572E</u>	900
<u>Message ID : VMD3578E</u>	901
<u>Message ID : VMD3581E</u>	902
<u>Message ID : VMD3596E</u>	902
<u>Message ID : VMD3597E</u>	903
<u>Message ID : VMD3605E</u>	904
<u>Message ID : VMD3607E</u>	905
<u>Message ID : VMD3611E</u>	905
<u>Message ID : VMD3612E</u>	906
<u>Message ID : VMD3616E</u>	907
<u>Message ID : VMD3617E</u>	907
<u>Message ID : VMD3628E</u>	908
<u>Message ID : VMD3629E</u>	909
<u>Message ID : VMD3633E</u>	910
<u>Message ID : VMD3644E</u>	910
<u>Message ID : VMD3645E</u>	911
<u>Message ID : VMD3651E</u>	912
<u>Message ID : VMD3655E</u>	913
<u>Message ID : VMD3665E</u>	913
<u>Message ID : VMD3666E</u>	914
<u>Message ID : VMD3667E</u>	915
<u>Message ID : VMD3674E</u>	915
<u>Message ID : VMD3676E</u>	916
<u>Message ID : VMD3681E</u>	917
<u>Message ID : VMD3683E</u>	917
<u>Message ID : VMD3685E</u>	918

Table of Contents

Logger VMD: Errors

<u>Message ID : VMD3686E</u>	919
<u>Message ID : VMD3689E</u>	919
<u>Message ID : VMD3697E</u>	920
<u>Message ID : VMD3700E</u>	921
<u>Message ID : VMD3702E</u>	922
<u>Message ID : VMD3707E</u>	922
<u>Message ID : VMD3713E</u>	923
<u>Message ID : VMD3718E</u>	924
<u>Message ID : VMD3723E</u>	924
<u>Message ID : VMD3724E</u>	925
<u>Message ID : VMD3726E</u>	926
<u>Message ID : VMD3730E</u>	926
<u>Message ID : VMD3734E</u>	927
<u>Message ID : VMD3736E</u>	928
<u>Message ID : VMD3747E</u>	928
<u>Message ID : VMD3748E</u>	929
<u>Message ID : VMD3750E</u>	930
<u>Message ID : VMD3758E</u>	930
<u>Message ID : VMD3759E</u>	931
<u>Message ID : VMD3760E</u>	932
<u>Message ID : VMD3761E</u>	932
<u>Message ID : VMD3779E</u>	933
<u>Message ID : VMD3780E</u>	934
<u>Message ID : VMD3782E</u>	935
<u>Message ID : VMD3784E</u>	936
<u>Message ID : VMD3786E</u>	937

Table of Contents

Logger VMD: Errors

<u>Message ID : VMD3787E</u>	938
<u>Message ID : VMD3788E</u>	938
<u>Message ID : VMD3789E</u>	939
<u>Message ID : VMD3790E</u>	940
<u>Message ID : VMD3792E</u>	941
<u>Message ID : VMD3795E</u>	942
<u>Message ID : VMD3796E</u>	943
<u>Message ID : VMD3799E</u>	943
<u>Message ID : VMD3801E</u>	944
<u>Message ID : VMD3802E</u>	945
<u>Message ID : VMD3807E</u>	946
<u>Message ID : VMD3809E</u>	947
<u>Message ID : VMD3811E</u>	947
<u>Message ID : VMD3812E</u>	949
<u>Message ID : VMD3816E</u>	950
<u>Message ID : VMD3819E</u>	950
<u>Message ID : VMD3822E</u>	951
<u>Message ID : VMD3828E</u>	952
<u>Message ID : VMD3830E</u>	953
<u>Message ID : VMD3831E</u>	954
<u>Message ID : VMD3833E</u>	955
<u>Message ID : VMD3834E</u>	956
<u>Message ID : VMD3835E</u>	957
<u>Message ID : VMD3837E</u>	958
<u>Message ID : VMD3838E</u>	958
<u>Message ID : VMD3840E</u>	959

Table of Contents

Logger VMD: Errors

<u>Message ID : VMD3843E</u>	960
<u>Message ID : VMD3844E</u>	961
<u>Message ID : VMD3845E</u>	962
<u>Message ID : VMD3846E</u>	963
<u>Message ID : VMD3848E</u>	964
<u>Message ID : VMD3849E</u>	965
<u>Message ID : VMD3855E</u>	966
<u>Message ID : VMD3858E</u>	967
<u>Message ID : VMD3864E</u>	968
<u>Message ID : VMD3865E</u>	969
<u>Message ID : VMD3866E</u>	970
<u>Message ID : VMD3867E</u>	970
<u>Message ID : VMD3872E</u>	971
<u>Message ID : VMD3873E</u>	972
<u>Message ID : VMD3874E</u>	973
<u>Message ID : VMD3875E</u>	974
<u>Message ID : VMD3876E</u>	975
<u>Message ID : VMD3877E</u>	975
<u>Message ID : VMD3878E</u>	976
<u>Message ID : VMD3879E</u>	977
<u>Message ID : VMD3888E</u>	978
<u>Message ID : VMD3890E</u>	979
<u>Message ID : VMD3891E</u>	980
<u>Message ID : VMD3892E</u>	980
<u>Message ID : VMD3901E</u>	981
<u>Message ID : VMD3903E</u>	982

Table of Contents

Logger VMD: Errors

<u>Message ID : VMD3905E</u>	983
<u>Message ID : VMD3907E</u>	984
<u>Message ID : VMD3909E</u>	985
<u>Message ID : VMD3911E</u>	986
<u>Message ID : VMD3913E</u>	987
<u>Message ID : VMD3915E</u>	988
<u>Message ID : VMD3916E</u>	989
<u>Message ID : VMD3917E</u>	989
<u>Message ID : VMD3918E</u>	990
<u>Message ID : VMD3922E</u>	991
<u>Message ID : VMD3923E</u>	992
<u>Message ID : VMD3927E</u>	993
<u>Message ID : VMD3929E</u>	994
<u>Message ID : VMD3932E</u>	994
<u>Message ID : VMD4245E</u>	995
<u>Message ID : VMD4594E</u>	996
<u>Message ID : VMD4606E</u>	997
<u>Message ID : VMD4607E</u>	998
<u>Message ID : VMD4608E</u>	999
<u>Message ID : VMD4609E</u>	1000
<u>Message ID : VMD4610E</u>	1001
<u>Message ID : VMD4612E</u>	1002
<u>Message ID : VMD4617E</u>	1002

Table of Contents

<u>Logger VMD: Fatal errors.....</u>	1004
<u>Message ID : VMD3767F.....</u>	1004
<u>Message ID : VMD3768F.....</u>	1005
<u>Message ID : VMD3769F.....</u>	1006
<u>Message ID : VMD3770F.....</u>	1006
<u>Message ID : VMD3771F.....</u>	1008
<u>Message ID : VMD3772F.....</u>	1009
<u>Message ID : VMD3797F.....</u>	1009
<u>Message ID : VMD3894F.....</u>	1010
<u>Message ID : VMD4595F.....</u>	1011
<u>Message ID : VMD4616F.....</u>	1012
<u>Logger VMD: Information.....</u>	1014
<u>Message ID : VMD3201I.....</u>	1014
<u>Message ID : VMD3202I.....</u>	1015
<u>Message ID : VMD3548I.....</u>	1015
<u>Message ID : VMD3558I.....</u>	1016
<u>Message ID : VMD3626I.....</u>	1017
<u>Message ID : VMD3640I.....</u>	1018
<u>Message ID : VMD3663I.....</u>	1019
<u>Message ID : VMD3773I.....</u>	1020
<u>Message ID : VMD3778I.....</u>	1021
<u>Message ID : VMD3781I.....</u>	1021
<u>Message ID : VMD3785I.....</u>	1022
<u>Message ID : VMD3794I.....</u>	1023
<u>Message ID : VMD3798I.....</u>	1024
<u>Message ID : VMD3800I.....</u>	1025

Table of Contents

Logger VMD: Information

<u>Message ID : VMD3803I</u>	1026
<u>Message ID : VMD3804I</u>	1026
<u>Message ID : VMD3814I</u>	1027
<u>Message ID : VMD3815I</u>	1028
<u>Message ID : VMD3817I</u>	1029
<u>Message ID : VMD3818I</u>	1030
<u>Message ID : VMD3820I</u>	1031
<u>Message ID : VMD3821I</u>	1032
<u>Message ID : VMD3823I</u>	1033
<u>Message ID : VMD3825I</u>	1034
<u>Message ID : VMD3827I</u>	1035
<u>Message ID : VMD3829I</u>	1036
<u>Message ID : VMD3832I</u>	1036
<u>Message ID : VMD3836I</u>	1037
<u>Message ID : VMD3839I</u>	1038
<u>Message ID : VMD3841I</u>	1039
<u>Message ID : VMD3842I</u>	1040
<u>Message ID : VMD3847I</u>	1041
<u>Message ID : VMD3851I</u>	1042
<u>Message ID : VMD3852I</u>	1043
<u>Message ID : VMD3853I</u>	1044
<u>Message ID : VMD3854I</u>	1045
<u>Message ID : VMD3856I</u>	1046
<u>Message ID : VMD3857I</u>	1046
<u>Message ID : VMD3859I</u>	1047
<u>Message ID : VMD3861I</u>	1048

Table of Contents

Logger VMD: Information

<u>Message ID : VMD3862I</u>	1049
<u>Message ID : VMD3863I</u>	1050
<u>Message ID : VMD3868I</u>	1051
<u>Message ID : VMD3870I</u>	1052
<u>Message ID : VMD3880I</u>	1053
<u>Message ID : VMD3881I</u>	1054
<u>Message ID : VMD3883I</u>	1054
<u>Message ID : VMD3885I</u>	1055
<u>Message ID : VMD3886I</u>	1057
<u>Message ID : VMD3893I</u>	1058
<u>Message ID : VMD3895I</u>	1059
<u>Message ID : VMD3896I</u>	1059
<u>Message ID : VMD3897I</u>	1060
<u>Message ID : VMD3898I</u>	1061
<u>Message ID : VMD3900I</u>	1062
<u>Message ID : VMD3902I</u>	1063
<u>Message ID : VMD3904I</u>	1064
<u>Message ID : VMD3906I</u>	1065
<u>Message ID : VMD3908I</u>	1066
<u>Message ID : VMD3910I</u>	1067
<u>Message ID : VMD3912I</u>	1068
<u>Message ID : VMD3914I</u>	1069
<u>Message ID : VMD3919I</u>	1070
<u>Message ID : VMD3926I</u>	1071
<u>Message ID : VMD3930I</u>	1072
<u>Message ID : VMD3934I</u>	1072

Table of Contents

Logger VMD: Information

<u>Message ID : VMD3935I</u>	1073
<u>Message ID : VMD4246I</u>	1074
<u>Message ID : VMD4611I</u>	1075
<u>Message ID : VMD4619I</u>	1076
<u>Message ID : VMD4620I</u>	1077

Logger VMD: Warnings.....**1078**

<u>Message ID : VMD3714W</u>	1078
<u>Message ID : VMD3762W</u>	1078
<u>Message ID : VMD3805W</u>	1079
<u>Message ID : VMD3806W</u>	1080
<u>Message ID : VMD3813W</u>	1081
<u>Message ID : VMD3824W</u>	1082
<u>Message ID : VMD3826W</u>	1083
<u>Message ID : VMD3850W</u>	1084
<u>Message ID : VMD3860W</u>	1085
<u>Message ID : VMD3869W</u>	1085
<u>Message ID : VMD3871W</u>	1086
<u>Message ID : VMD3882W</u>	1087
<u>Message ID : VMD3887W</u>	1088
<u>Message ID : VMD3889W</u>	1089
<u>Message ID : VMD3899W</u>	1090
<u>Message ID : VMD3920W</u>	1091
<u>Message ID : VMD3921W</u>	1091
<u>Message ID : VMD3924W</u>	1092
<u>Message ID : VMD3925W</u>	1093

Table of Contents

Logger VMD: Warnings

<u>Message ID : VMD3928W</u>	1094
<u>Message ID : VMD3931W</u>	1095
<u>Message ID : VMD3933W</u>	1096
<u>Message ID : VMD4618W</u>	1097
<u>Message ID : VMD4621W</u>	1098
<u>Message ID : VMD4622W</u>	1099
<u>Message ID : VMD4623W</u>	1100
<u>Message ID : VMD4624W</u>	1101
<u>Message ID : VMD4625W</u>	1102
<u>Message ID : VMD4636W</u>	1103
<u>Message ID : VMD4639W</u>	1104
<u>Message ID : VMD4640W</u>	1105

Logger XFM: Errors.....1107

<u>Message ID : XFM4501E</u>	1107
<u>Message ID : XFM4502E</u>	1108
<u>Message ID : XFM4504E</u>	1108
<u>Message ID : XFM4535E</u>	1109
<u>Message ID : XFM4568E</u>	1110
<u>Message ID : XFM4589E</u>	1111
<u>Message ID : XFM4590E</u>	1112
<u>Message ID : XFM4591E</u>	1113

Logger XFM: Fatal errors.....1114

<u>Message ID : XFM4508E</u>	1114
<u>Message ID : XFM4509E</u>	1114

Table of Contents

Logger XFM: Fatal errors

<u>Message ID : XFM4518F</u>	1115
<u>Message ID : XFM4519F</u>	1116
<u>Message ID : XFM4525F</u>	1117
<u>Message ID : XFM4532F</u>	1118
<u>Message ID : XFM4536F</u>	1119
<u>Message ID : XFM4539F</u>	1120
<u>Message ID : XFM4540F</u>	1120
<u>Message ID : XFM4541F</u>	1121
<u>Message ID : XFM4544F</u>	1122
<u>Message ID : XFM4546F</u>	1123
<u>Message ID : XFM4561F</u>	1124
<u>Message ID : XFM4565F</u>	1125

Logger XFM: Information.....1126

<u>Message ID : XFM4507I</u>	1126
<u>Message ID : XFM4517I</u>	1126
<u>Message ID : XFM4522I</u>	1127
<u>Message ID : XFM4526I</u>	1128
<u>Message ID : XFM4549I</u>	1129
<u>Message ID : XFM4557I</u>	1130
<u>Message ID : XFM4559I</u>	1131

Logger XFM: Warnings.....1132

<u>Message ID : XFM4550W</u>	1132

Logger CGA: Errors

Message ID : CGA2614E

Severity

Error

Long Form

Syntax error: Domain name '*' is reserved

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2617E

Severity

Error

Long Form

[[{0}]] Set [{1}] used but not defined

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2618E

Severity

Error

Long Form

Failed to import password object

Short Form

No short form is provided for this message type

Message ID : CGA2617E

Description

None

Message ID : CGA2619E

Severity

Error

Long Form

Policy [{0}]: Invalid policy

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2620E

Severity

Error

Message ID : CGA2618E

Long Form

Policy [{0}]: Invalid policy length

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2621E

Severity

Error

Long Form

Policy [{0}]: Policy import failed

Short Form

No short form is provided for this message type

Message ID : CGA2620E

Description

None

Message ID : CGA2624E

Severity

Error

Long Form

Policy [{0}]: Failed to import Name Identifier

Short Form

Name import failed

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Description

None

Message ID : CGA2621E

Message ID : CGA2625E

Severity

Error

Long Form

Failed to import keys

Short Form

Keys import failed

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA2626E

Severity

Error

Message ID : CGA2625E

Long Form

Policy [{0}]: Invalid root path

Short Form

Invalid rootpath

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Description

None

Message ID : CGA2627E

Severity

Error

Long Form

Policy [{0}]: Failed to import root path

Message ID : CGA2626E

Short Form

Import rootpath fail

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Description

None

Message ID : CGA2628E

Severity

Error

Long Form

Policy [{0}]: [{1}] Set [{2}] not defined

Short Form

Undefined policy type/set

Message ID : CGA2627E

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
oType	vds_oType	Text	Object type in policy rule
oName	vds_oName	Text	Object name in policy rule

Description

None

Message ID : CGA2629E

Severity

Error

Long Form

Policy [{0}]: Key rule not yet built

Short Form

Invalid key rule

Message ID : CGA2628E

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Description

None

Message ID : CGA2634E

Severity

Error

Long Form

Policy [{0}]: Invalid Rule

Short Form

Invalid rules object

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Message ID : CGA2629E

Description

None

Message ID : CGA2635E

Severity

Error

Long Form

Policy [{0}]: Invalid syntax for key effect [{1}]

Short Form

Invalid key effect

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
act	act	Text	Action being requested or performed

Message ID : CGA2634E

Description

None

Message ID : CGA2636E

Severity

Error

Long Form

Policy [{0}]: Invalid name and/or access

Short Form

Invalid name/access

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Description

None

Message ID : CGA2635E

Message ID : CGA2637E

Severity

Error

Long Form

Policy [{0}]: Invalid rule syntax: Effect not defined

Short Form

Undefined effect

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Description

None

Message ID : CGA2638E

Severity

Error

Long Form

Policy [{0}]: Invalid rule syntax: Action [{1}] not defined

Short Form

Undefined action

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
act	act	Text	Action being requested or performed

Description

None

Message ID : CGA2639E

Message ID : CGA2638E

Severity

Error

Long Form

Policy [{0}]: Invalid rule syntax: GoTo label [{1}] not defined

Short Form

Undefined label

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
label	vds_label	Text	Label in rule sequence

Description

None

Message ID : CGA2645E

Message ID : CGA2639E

Severity

Error

Long Form

Policy [{0}]: Recursive GoTo detected at rule number [{1}]

Short Form

Recursive goto

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
ruleNo	vds_ruleNo	Numeric	Index into policy rule set

Description

None

Message ID : CGA2648E

Message ID : CGA2645E

Severity

Error

Long Form

Policy [{0}]: Invalid GoTo - Missing destination label

Short Form

Invalid goto

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Description

None

Message ID : CGA2649E

Severity

Error

Message ID : CGA2648E

Long Form

Policy [{0}]: Invalid effect syntax [{1}]

Short Form

Invalid syntax

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
act	act	Text	Action being requested or performed

Description

None

Message ID : CGA2650E

Severity

Error

Message ID : CGA2649E

Long Form

Policy [{0}]: Invalid action syntax [{1}]

Short Form

Invalid action

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
act	act	Text	Action being requested or performed

Description

None

Message ID : CGA2651E

Severity

Error

Message ID : CGA2650E

Long Form

No policy defined for [{0}] set [{1}]

Short Form

Undefined policy set

Parameters

Label	CEF Label	Type	Usage
oType	vds_oType	Text	Object type in policy rule
oName	vds_oName	Text	Object name in policy rule

Description

None

Message ID : CGA2652E

Severity

Error

Message ID : CGA2651E

Long Form

Policy [{0}]: old and new key rule numbers do not match [old {1}, new {2}]

Short Form

Mismatched rule numbers

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
ruleNo	vds_ruleNo	Numeric	Index into policy rule set
altRuleNo	vds_altRuleNo	Numeric	Alternate rule number

Description

None

Message ID : CGA2653E

Severity

Error

Message ID : CGA2652E

Long Form

Policy [{0}]: old and new key names do not match [key rule {1}, old {2}, new {3}]

Short Form

Mismatched key names

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
ruleNo	vds_ruleNo	Numeric	Index into policy rule set
key	cs3	Text	Name of key or key pair
altKey	vds_altKey	Text	Name of alternate key for multi-key operations

Description

None

Message ID : CGA2654E

Severity

Error

Message ID : CGA2653E

Long Form

Policy [{0}]: old and new key resources do not match [key rule {1}]

Short Form

Mismatched key resource

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
ruleNo	vds_ruleNo	Numeric	Index into policy rule set

Description

None

Message ID : CGA2655E

Severity

Error

Message ID : CGA2654E

Long Form

Failed to import key [{0}]

Short Form

Key import failed

Parameters

Label	CEF Label	Type	Usage
key	cs3	Text	Name of key or key pair

Description

None

Message ID : CGA2656E

Severity

Error

Long Form

Failed to find encryption key [%lld]

Message ID : CGA2655E

Short Form

Encryption key not found

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA2657E

Severity

Error

Long Form

Failed to validate policy on [{0}], rekey in progress

Short Form

Policy failure, rekey in progress

Message ID : CGA2656E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA2658E

Severity

Error

Long Form

Failed to validate policy on [{0}]

Short Form

Policy validation failure

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA2657E

Description

None

Message ID : CGA2659E

Severity

Error

Long Form

Unsupported key type in policy on [{0}]

Short Form

Unsupported key type in policy

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA2658E

Message ID : CGA2662E

Severity

Error

Long Form

Failed to validate key [{0}]

Short Form

Key validation failed

Parameters

Label	CEF Label	Type	Usage
key	cs3	Text	Name of key or key pair

Description

None

Message ID : CGA3003E

Message ID : CGA2662E

Severity

Error

Long Form

EVENT: {0}

Short Form

Event

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGA3004E

Severity

Error

Message ID : CGA3003E

Long Form

An invalid host password was entered

Short Form

Invalid host password

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3007E

Severity

Error

Long Form

NOTUSED

Message ID : CGA3004E

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA3008E

Severity

Error

Long Form

Pid [{0}] has not been initialized properly in [{1}]

Short Form

Bad caller

Parameters

Label	CEF Label	Type	Usage
pid	dvcpid	Numeric	Numeric process ID

Message ID : CGA3007E

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

Internal error; try start/stop of agent or reinstallation of agent.

Message ID : CGA3009E

Severity

Error

Long Form

NOTUSED

Short Form

No short form is provided for this message type

Description

An internal error occurred. Please contact Thales Support.

Message ID : CGA3010E

Severity

Error

Long Form

Failed to write to file [{0}] in [{1}]

Short Form

Write fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
func	vds_func	Text	A function name

Description

None

Message ID : CGA3011E

Severity

Error

Long Form

Failed to read file [{0}] in [{1}]

Short Form

Read fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
func	vds_func	Text	A function name

Description

None

Message ID : CGA3012E

Severity

Error

Long Form

NOTUSED

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA3013E

Severity

Error

Long Form

NOTUSED

Message ID : CGA3012E

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA3014E

Severity

Error

Long Form

NOTUSED

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA3013E

Message ID : CGA3015E

Severity

Error

Long Form

Bad version [{0}] in configuration

Short Form

Bad config version

Parameters

Label	CEF Label	Type	Usage
verno	vds_verno	Numeric	A version number

Description

None

Message ID : CGA3016E

Severity

Error

Long Form

NOTUSED

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA3017E

Severity

Error

Long Form

Failed to apply new security configuration

Message ID : CGA3016E

Short Form

Security config update failed

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3018E

Severity

Error

Long Form

Challenge/Response: An invalid challenge/response was entered

Short Form

Invalid challenge/response

Message ID : CGA3017E

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3021E

Severity

Error

Long Form

Challenge/Response: Error processing challenge/response

Short Form

Challenge/Response encryption error

Parameters

No parameters are provided for this message type

Message ID : CGA3018E

Description

None

Message ID : CGA3022E

Severity

Error

Long Form

Key Protection: Key integrity check failed in [{0}]

Short Form

Key integrity check failed

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3021E

Message ID : CGA3023E

Severity

Error

Long Form

NOTUSED

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA3024E

Severity

Error

Long Form

Key Protection: Extract rkey: Hardware signature has changed

Message ID : CGA3023E

Short Form

Hardware signature changed

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3059E

Severity

Error

Long Form

[AUDIT] Process[{0}] Pid[{1}] Uid[{2}] Operation[{3}] File[{4}] Failure[{5}] Effect[PERMIT]

Short Form

Sysfile modified error

Parameters

Label	CEF Label	Type	Usage
command	command	Text	Task struct comm field
pid	dvcpid	Numeric	Numeric process ID
uid	suid	Numeric	User id
op_name	op_name	Text	Operation name
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGA3060E

Severity

Error

Long Form

[ALARM] Process[{0}] Pid[{1}] Uid[{2}] Operation[{3}] File[{4}] Effect[DENIED]

Message ID : CGA3059E

Short Form

Sysfile protected

Parameters

Label	CEF Label	Type	Usage
command	command	Text	Task struct comm field
pid	dvcpid	Numeric	Numeric process ID
uid	suid	Numeric	User id
op_name	op_name	Text	Operation name
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3061E

Severity

Error

Message ID : CGA3060E

Long Form

Key Protection: Encryption/Decryption: Bad arguments in function [{0}]

Short Form

En/Decrypt BadArgs

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3062E

Severity

Error

Long Form

Key Protection: Private key write: Null key in function [{0}]

Message ID : CGA3061E

Short Form

PrivKeyWrite NullKey

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3063E

Severity

Error

Long Form

Key Protection: Private key write: Invalid key length in function [{0}]

Short Form

PrivKeyWrite InvalKeylen

Message ID : CGA3062E

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3064E

Severity

Error

Long Form

Key Protection: Verify sanity: Bad configuration directory and/or session key arguments in function [{0}]

Short Form

VrfySan BadArgs

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Message ID : CGA3063E

Description

None

Message ID : CGA3065E

Severity

Error

Long Form

Key Protection: Verify password: Bad configuration directory and/or password arguments in function [{0}]

Short Form

VrfyPwd BadArgs

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3064E

Message ID : CGA3066E

Severity

Error

Long Form

Key Protection: Get salt: Bad configuration directory argument in function [{0}]

Short Form

GetSalt BadArg

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3067E

Severity

Error

Long Form

Key Protection: Shared secret: Bad configuration directory argument in function [{0}]

Short Form

ShrdSecret BadArg

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3068E

Severity

Error

Message ID : CGA3067E

Long Form

Key Protection: Key integrity check: Bad arguments in function [{0}]

Short Form

KeyIntegChk BadArgs

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3069E

Severity

Error

Long Form

Key Protection: Key integrity check: Invalid key length in function [{0}]

Message ID : CGA3068E

Short Form

KeyIntegChk BadLen

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3070E

Severity

Error

Long Form

Key Protection: Extract rkey: Bad arguments in function [{0}]

Short Form

ExtrRkey BadArgs

Message ID : CGA3069E

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3071E

Severity

Error

Long Form

Key Protection: Extract rkey: Invalid extraction method in function [{0}]

Short Form

ExtrRkey BadMeth

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Message ID : CGA3070E

Description

None

Message ID : CGA3072E

Severity

Error

Long Form

Key Protection: Policy key update: Bad configuration directory argument in function [{0}]

Short Form

PolKeyUpd BadArg

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3071E

Message ID : CGA3073E

Severity

Error

Long Form

Key Protection: Signature update: Bad signature update argument in function [{0}]

Short Form

SigUpd BadArg

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3074E

Severity

Error

Long Form

Key Protection: Session key decryption: Bad arguments in function [{0}]

Short Form

SessKeyDcrpt BadArgs

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3075E

Severity

Error

Message ID : CGA3074E

Long Form

Key Protection: Host password: Invalid argument in function [{0}]

Short Form

HostPwd BadArg

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3076E

Severity

Error

Long Form

Key Protection: Challenge 256: Invalid argument in function [{0}]

Message ID : CGA3075E

Short Form

Chlng256 BadArg

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3077E

Severity

Error

Long Form

Key Protection: Challenge: Invalid argument in function [{0}]

Short Form

ChlngBadArg

Message ID : CGA3076E

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3078E

Severity

Error

Long Form

Key Protection: Failed to write private key in function [{0}]

Short Form

PrivKeyWr Fail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Message ID : CGA3077E

Description

None

Message ID : CGA3079E

Severity

Error

Long Form

Key Protection: Failed to read private key in function [{0}]

Short Form

PrivkeyRd Fail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3078E

Message ID : CGA3080E

Severity

Error

Long Form

Key Protection: Extract password: Private key unavailable in function [{0}]

Short Form

ExtrPwd PrivKeyUnavail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3081E

Severity

Error

Long Form

Key Protection: Verify configuration sanity: Private key unavailable in function [{0}]

Short Form

VrfyConfig: PrivKeyUnavail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3082E

Severity

Error

Message ID : CGA3081E

Long Form

Key Protection: Extract rkey: Private key unavailable in function [{0}]

Short Form

ExtrRkey PrivKeyUnavail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3083E

Severity

Error

Long Form

Key Protection: Extract password: Failed to decrypt using private key in function [{0}]

Message ID : CGA3082E

Short Form

ExtrPwd PrivKeyDcrpt Fail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3084E

Severity

Error

Long Form

Key Protection: Verify configuration sanity: Failed to decrypt using private key in function [{0}]

Short Form

VrfyCfg PrivKeyDcrpt Fail

Message ID : CGA3083E

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3085E

Severity

Error

Long Form

Key Protection: Extract rkey CR256: Failed to decrypt using private key in function [{0}]

Short Form

ExtrRkey256 PrivKeyDcrpt Fail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Message ID : CGA3084E

Description

None

Message ID : CGA3086E

Severity

Error

Long Form

Key Protection: Extract rkey: Failed to decrypt using private key in function [{0}]

Short Form

ExtrRkey PrivKeyDecrypt Fail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3085E

Message ID : CGA3087E

Severity

Error

Long Form

Key Protection: Verify configuration sanity: Bad session key in file [{0}], function [{1}] line [{2}]

Short Form

VrfyCfg BadSessKey

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
func	vds_func	Text	A function name

Description

None

Message ID : CGA3088E

Severity

Error

Long Form

Key Protection: Verify configuration sanity: Failed HMAX verification in file [{0}], function [{1}] line [{2}]

Short Form

VrfyCfg FailHMAXVrfy Fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
func	vds_func	Text	A function name

Description

None

Message ID : CGA3089E

Severity

Error

Long Form

Key Protection: Verify configuration sanity: Bad rkey in file [{0}], function [{1}] line [{2}]

Short Form

VrfyCfg BadRkey

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
func	vds_func	Text	A function name

Description

None

Message ID : CGA3090E

Severity

Error

Long Form

Key Protection: File session key decrypt: Failed description in file [{0}] in function [{1}]

Short Form

FileSessKeyDcrpt Fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
func	vds_func	Text	A function name

Description

None

Message ID : CGA3091E

Severity

Error

Long Form

Key Protection: Extract rkey: Bad password in function [{0}]

Short Form

ExtrRkey BadPwd

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3092E

Severity

Error

Long Form

Key Protection: Policy key update: Bad password in function [{0}]

Short Form

PolKeyUpd BadPwd

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3093E

Severity

Error

Message ID : CGA3092E

Long Form

Key Protection: Policy key update: Extract rkey failure in function [{0}]

Short Form

PolKeyUpd ExtrRkey Fail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3094E

Severity

Error

Long Form

Compare dir key: Failed to get dir

Message ID : CGA3093E

Short Form

CmpDirKey FailGetDir

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3095E

Severity

Error

Long Form

Compare dir key: Failed to add keyset

Short Form

CmpDirKey FailAddKeyset

Message ID : CGA3094E

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3096E

Severity

Error

Long Form

Get keyid: Invalid key object in [{0}] at [{1}]

Short Form

GetKeyid InvalKeyObj

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Message ID : CGA3095E

Description

None

Message ID : CGA3097E

Severity

Error

Long Form

Get keyid: Local key get failed in [{0}] at [{1}]

Short Form

GetKeyid LclKeyGet Fail

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3096E

Message ID : CGA3098E

Severity

Error

Long Form

Policy validation failed

Short Form

PolVald Fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3099E

Severity

Error

Message ID : CGA3098E

Long Form

LDT: Failed to start

Short Form

LDT: Fail to start

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3100E

Severity

Error

Long Form

LDT: Failed to stop

Message ID : CGA3099E

Short Form

LDT: Fail to stop

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3101E

Severity

Error

Long Form

LDT: Failed to exit

Short Form

LDT: Fail to exit

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3102E

Severity

Error

Long Form

LDT: Cross guard point key compare failed

Short Form

LDT: Cross guard point key compare failed

Parameters

No parameters are provided for this message type

Message ID : CGA3101E

Description

None

Message ID : CGA3103E

Severity

Error

Long Form

LDT: Not enough disk space for file [{0}], aborting transformation

Short Form

LDT: Out of disk space

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3102E

Message ID : CGA3109E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Simulation mode)

Short Form

IgnrCntnrGrd SimMode

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3110E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Simulation mode)

Short Form

IgnrGrd SimMode

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3111E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Contains symlinks or is malformed)

Short Form

IgnrCntnrGrd HasSymlnks

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3112E

Message ID : CGA3111E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Contains symlinks or is malformed)

Short Form

IgnrGrd HasSymlnks

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3113E

Severity

Error

Message ID : CGA3112E

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Can't guard root)

Short Form

IgnrCntnrGrd NoRoot

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3114E

Severity

Error

Message ID : CGA3113E

Long Form

Not guarding path [{0}] (Reason: Can't guard root)

Short Form

IgnrGrd NoRoot

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3115E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Path too long)

Message ID : CGA3114E

Short Form

IgnrCntnrGrd PathLong

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3116E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Path too long)

Message ID : CGA3115E

Short Form

IgnrGrd PathLong

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3117E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: AUTOFS, but type is not automount)

Short Form

IgnrCntnrGrd AUTOFS

Message ID : CGA3116E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3118E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: AUTOFS, but type is not automount)

Short Form

IgnrGrd AUTOFS

Message ID : CGA3117E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3119E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Not allowed)

Short Form

IgnrCntnrGrd IsInval

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3118E

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3120E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Not allowed)

Short Form

IgnrGrd IsInval

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3119E

Description

None

Message ID : CGA3121E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Raw device not supported)

Short Form

IgnrCntnrGrd RawDev

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Message ID : CGA3120E

Description

None

Message ID : CGA3122E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Raw device not supported)

Short Form

IgnrGrd RawDev

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3121E

Message ID : CGA3123E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Unknown)

Short Form

IgnrCntnrGrd BadFlag

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3123E

Message ID : CGA3124E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Unknown)

Short Form

IgnrCntnrGrd BadFlag

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3125E

Severity

Error

Long Form

Not unguarding path [{0}] from container [{1}] (Reason: Unknown)

Short Form

IgnrCntnrUngrd BadFlag

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3126E

Message ID : CGA3125E

Severity

Error

Long Form

Not unguarding path [{0}] (Reason: Unknown)

Short Form

IgnrUngrd BadFlag

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3127E

Severity

Error

Message ID : CGA3126E

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Nested paths not allowed)

Short Form

BadCntnrGrdPath IsNested

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3128E

Severity

Error

Message ID : CGA3127E

Long Form

Not guarding path [{0}] (Reason: Nested paths not allowed)

Short Form

BadGrdPath IsNested

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3129E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Busy, will continue to retry)

Message ID : CGA3128E

Short Form

BadCntnrGrdPath IsBusy

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3130E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Busy, will continue to retry)

Message ID : CGA3129E

Short Form

BadGrdPath IsBusy

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3131E

Severity

Error

Long Form

Not unguarding path [{0}] from container [{1}] (Reason: Busy, will continue to retry)

Short Form

BadCntnrUngrdPath IsBusy

Message ID : CGA3130E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3132E

Severity

Error

Long Form

Not unguarding path [{0}] (Reason: Busy, will continue to retry)

Short Form

BadUngrdPath IsBusy

Message ID : CGA3131E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3133E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Does not exist)

Short Form

BadCntnrGrdPath NotExist

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3132E

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3134E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Does not exist)

Short Form

BadGrdPath NotExist

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3133E

Description

None

Message ID : CGA3135E

Severity

Error

Long Form

Not unguarding path [{0}] from container [{1}] (Reason: Does not exist)

Short Form

BadCntnrUngrdPath NotExist

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Message ID : CGA3134E

Description

None

Message ID : CGA3136E

Severity

Error

Long Form

Not unguarding path [{0}] (Reason: Does not exist)

Short Form

BadUngrdPath NotExist

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3135E

Message ID : CGA3137E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Already mounted)

Short Form

BadCntnrGrdPath AlreadyMounted

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3138E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Already mounted)

Short Form

BadGrdPath AlreadyMounted

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3139E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Max guard point limit reached)

Short Form

BadCntnrGrd MaxGrds

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3140E

Message ID : CGA3139E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Max guard point limit reached)

Short Form

BadGrd MaxGrds

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3141E

Severity

Error

Message ID : CGA3140E

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Resource not available)

Short Form

BadCntnrGrd ResrcUnavail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3142E

Severity

Error

Message ID : CGA3141E

Long Form

Not guarding path [{0}] (Reason: Resource not available)

Short Form

BadGrd ResrcUnavail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3143E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Operation timed out, retrying)

Message ID : CGA3142E

Short Form

BadCntnrGrd TimedOut

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3144E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Operation timed out, retrying)

Message ID : CGA3143E

Short Form

BadGrd TimedOut

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3145E

Severity

Error

Long Form

Not unguarding path [{0}] from container [{1}] (Reason: Operation timed out, retrying)

Short Form

BadCntnrUngrd TimedOut

Message ID : CGA3144E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3146E

Severity

Error

Long Form

Not unguarding path [{0}] (Reason: Operation timed out, retrying)

Short Form

BadUngrd TimedOut

Message ID : CGA3145E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3147E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Invalid guard point)

Short Form

BadCntnrGrdPath InvalGrdPath

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3146E

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3148E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Invalid guard point)

Short Form

BadGrdPath InvalGrdPath

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3147E

Description

None

Message ID : CGA3149E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Invalid, AUTOFS but type is not automount)

Short Form

BadCntnrGrdPath AUTOFSNoAuto

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Message ID : CGA3148E

Description

None

Message ID : CGA3150E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Invalid, AUTOFS but type is not automount)

Short Form

BadGrdPath AUTOFSNoAuto

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3149E

Message ID : CGA3151E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Partially guarded)

Short Form

BadCntnrGrd PartialGrd

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3152E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Partially guarded)

Short Form

BadGrd PartialGrd

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3153E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Logical drive or path compressed)

Short Form

BadCntnrGrd IsCompressed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3154E

Message ID : CGA3153E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Logical drive or path compressed)

Short Form

BadGrd IsCompressed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3155E

Severity

Error

Message ID : CGA3154E

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Logical drive or path encrypted)

Short Form

BadCntnrGrd IsEncrypt

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3156E

Severity

Error

Message ID : CGA3155E

Long Form

Not guarding path [{0}] (Reason: Logical drive or path encrypted)

Short Form

BadGrd IsEncrypt

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3157E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: System Error/Module not present)

Message ID : CGA3156E

Short Form

BadCntnrGrd SysError

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3158E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: System Error/Module not present)

Message ID : CGA3157E

Short Form

BadGrd SysError

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3159E

Severity

Error

Long Form

Not unguarding path [{0}] from container [{1}] (Reason: System Error/Module not present)

Short Form

BadCntnrUngrd SysError

Message ID : CGA3158E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3160E

Severity

Error

Long Form

Not unguarding path [{0}] (Reason: System Error/Module not present)

Short Form

BadUngrd SysError

Message ID : CGA3159E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3161E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Protected file system is stale)

Short Form

BadCntnrGrdPath StaleFS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3160E

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3162E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Protected file system is stale)

Short Form

BadGrdPath StaleFS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3161E

Description

None

Message ID : CGA3163E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Unsupported filesystem type)

Short Form

BadCntnrGrdPath FSNotSupp

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Message ID : CGA3162E

Description

None

Message ID : CGA3164E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Unsupported filesystem type)

Short Form

BadGrdPath FSNotSupp

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3163E

Message ID : CGA3165E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Guard point has metadata, only Live Data Transform policy allowed)

Short Form

BadCntnrGrd BadPol

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3166E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Guard point has metadata, only Live Data Transform policy allowed)

Short Form

BadGrd BadPol

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3167E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Filesystem type is not supported with Live Data Transform policy)

Short Form

BadCntnrGrd BadFS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3168E

Message ID : CGA3167E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Filesystem type is not supported with Live Data Transform policy)

Short Form

BadGrd BadFS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3169E

Severity

Error

Message ID : CGA3168E

Long Form

Not guarding path [{0}] from container [{1}] (Reason: File system not mounted with Extended attribute support)

Short Form

BadCntnrGrd XattrDisabled

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3170E

Severity

Error

Message ID : CGA3169E

Long Form

Not guarding path [{0}] (Reason: File system not mounted with Extended attribute support)

Short Form

BadGrd XattrDisabled

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3171E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Nested mount path not allowed for LDT)

Message ID : CGA3170E

Short Form

BadCntnrGrd NestMount

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3172E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Nested mount path not allowed for LDT)

Message ID : CGA3171E

Short Form

BadGrd NestMount

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3173E

Severity

Error

Long Form

Not unguarding path [{0}] from container [{1}] (Reason: LDT metadata removal in progress)

Short Form

BadCntnrGrd LDTMetadata

Message ID : CGA3172E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3174E

Severity

Error

Long Form

Not unguarding path [{0}] (Reason: LDT metadata removal in progress)

Short Form

BadGrd LDTMetadata

Message ID : CGA3173E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3175E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Inactive)

Short Form

BadCntnrGrd Inactive

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3174E

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3176E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Inactive)

Short Form

BadGrd Inactive

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3175E

Description

None

Message ID : CGA3177E

Severity

Error

Long Form

Not unguarding path [{0}] from container [{1}] (Reason: Inactive)

Short Form

BadCntnrUngrd Inactive

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Message ID : CGA3176E

Description

None

Message ID : CGA3178E

Severity

Error

Long Form

Not unguarding path [{0}] (Reason: Inactive)

Short Form

BadUngrd Inactive

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3177E

Message ID : CGA3179E

Severity

Error

Long Form

Not guarding path [{0}] from container [{1}] (Reason: Unknown)

Short Form

BadCntnrGrd BadFlag

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3180E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Unknown)

Short Form

BadGrd BadFlag

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3181E

Severity

Error

Long Form

Not unguarding path [{0}] from container [{1}] (Reason: Unknown)

Short Form

BadCntnrUngrd BadFlag

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3182E

Message ID : CGA3181E

Severity

Error

Long Form

Not unguarding path [{0}] (Reason: Unknown)

Short Form

BadUngrd BadFlag

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3184E

Severity

Error

Message ID : CGA3182E

Long Form

Failed to guard path [{0}] (Reason: [{1}] file system not supported)

Short Form

FS NotSupp

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3185E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Can't guard root)

Message ID : CGA3184E

Short Form

GrdPath IsRoot

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3187E

Severity

Error

Long Form

An encryption policy was applied to a folder containing NTFS compressed files, [{0}]. NTFS compressed files are not encrypted

Short Form

Folder IsCompressed

Message ID : CGA3185E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3188E

Severity

Error

Long Form

An encryption policy was applied to a folder containing NTFS encrypted files, [{0}]. NTFS encrypted files are not encrypted

Short Form

Folder IsCrypt

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3187E

Description

None

Message ID : CGA3189E

Severity

Error

Long Form

Guard path [{0}]: Guard point has metadata, only Live Data Transform policy allowed

Short Form

Bad GrdPath Pol

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3188E

Message ID : CGA3190E

Severity

Error

Long Form

Guard path [{0}]: Wrong fs type for this guard point

Short Form

Bad GrdPath FS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3191E

Severity

Error

Long Form

Guard path [{0}]: Extended attribute not enabled for guard point

Short Form

GrdPath XattrDisabled

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3192E

Severity

Error

Message ID : CGA3191E

Long Form

Guard path [{0}]: Nested mount not allowed for Live Data Transform

Short Form

GrdPath NestMount

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3206E

Severity

Error

Long Form

LDT: failed to encrypt data

Message ID : CGA3192E

Short Form

LDT Crypt Fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3212E

Severity

Error

Long Form

LDT-ALERT: Error in scanning guardpoint [{0}].

Short Form

LDT-ALERT: Error in scanning guardpoint

Message ID : CGA3206E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3218E

Severity

Error

Long Form

LDT: Skipping transformation of file [{0}], due to pre-check error.

Short Form

LDT: Skipping transformation of file, due to pre-check error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3212E

Description

None

Message ID : CGA3220E

Severity

Error

Long Form

LDT: Error recovering ranges from previous transformation for file [{0}].

Short Form

LDT: Error recovering ranges from previous transformation for file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3218E

Message ID : CGA3222E

Severity

Error

Long Form

[AUDIT] Process[{0}] Pid[{1}] Uid[{2}] Operation[{3}] File[{4}] ContainerID[{5}] Failure[{6}] Effect[PERMIT]

Short Form

Sysfile modified error

Parameters

Label	CEF Label	Type	Usage
command	command	Text	Task struct comm field
pid	dvcpid	Numeric	Numeric process ID
uid	suid	Numeric	User id
op_name	op_name	Text	Operation name
filePath	filePath	Text	Full path to file
cid	cid	Text	Container ID
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGA3223E

Severity

Error

Long Form

[ALARM] Process[{0}] Pid[{1}] Uid[{2}] Operation[{3}] File[{4}] ContainerID[{5}] Effect[DENIED]

Short Form

Sysfile protected

Parameters

Label	CEF Label	Type	Usage
command	command	Text	Task struct comm field
pid	dvcpid	Numeric	Numeric process ID
uid	suid	Numeric	User id
op_name	op_name	Text	Operation name

Message ID : CGA3222E

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
cid	cid	Text	Container ID

Description

None

Message ID : CGA3227E

Severity

Error

Long Form

LDT: Error while rekeying guardpoint [{0}]

Short Form

LDT: Error while rekeying guardpoint

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3223E

Description

None

Message ID : CGA3228E

Severity

Error

Long Form

Ptrace denied on authenticator [{0}] pid [{1}]

Short Form

Ptrace authenticator denied

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
pid	dvcpid	Numeric	Numeric process ID

Message ID : CGA3227E

Description

None

Message ID : CGA3229E

Severity

Error

Long Form

Ptrace denied on protected process [{0}] pid [{1}]

Short Form

Ptrace protected denied

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
pid	dvcpid	Numeric	Numeric process ID

Message ID : CGA3228E

Description

None

Message ID : CGA3230E

Severity

Error

Long Form

LDT: Terminating rekey ON [{0}] due to data corruption

Short Form

LDT: terminated, corruption

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3229E

Message ID : CGA3232E

Severity

Error

Long Form

LDT: Data transformation is aborted on file [{0}]. Error : {1}

Short Form

LDT: Data transformation is aborted on file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGA3233E

Severity

Error

Long Form

LDT: Data transformation is aborted on file [{0}]. Error : {1}. Reason : {2}

Short Form

LDT: Data transformation is aborted on file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGA3235E

Severity

Error

Long Form

Key Protection: Failed to generate derived key in function [{0}]

Short Form

Generate derived key failed

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3236E

Severity

Error

Long Form

Key Protection: Encryption error in function [{0}]

Short Form

Encryption error

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3237E

Severity

Error

Message ID : CGA3236E

Long Form

Key Protection: Invalid access file in [{0}] at [{1}]

Short Form

Invalid access file

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name

Description

None

Message ID : CGA3238E

Severity

Error

Long Form

Not re-guarding path [{0}] from container [{1}] (Reason: Guard point initialization already in progress)

Message ID : CGA3237E

Short Form

BadCntnrGrd InProgress

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3239E

Severity

Error

Long Form

Not re-guarding path [{0}] (Reason: Guard point initialization already in progress)

Message ID : CGA3238E

Short Form

BadGrd InProgress

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3252E

Severity

Error

Long Form

LDT-ALERT: Cannot enable guard point [{0}], LDT initialization failed with error [{1}]

Short Form

LDT: enable failure

Message ID : CGA3239E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGA3256E

Severity

Error

Long Form

LDT-ALERT: Error initializing resources, LDT will not be operational.

Short Form

LDT init fail

Message ID : CGA3252E

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3272E

Severity

Error

Long Form

{0} does not have UUID

Short Form

UUID does not exist

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3256E

Description

None

Message ID : CGA3274E

Severity

Error

Long Form

Failed to write classification {0} to {1}

Short Form

Failed to write

Parameters

Label	CEF Label	Type	Usage
tag	tag	Text	Tag
filePath	filePath	Text	Full path to file

Message ID : CGA3272E

Description

None

Message ID : CGA3275E

Severity

Error

Long Form

Data classification transaction {0} failed for operation {1} with {2} : {3}

Short Form

Classification transaction failed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
filePath	filePath	Text	Full path to file

Message ID : CGA3274E

Description

None

Message ID : CGA3278E

Severity

Error

Long Form

Key Conflict for File [{0}]: key information in LDT metadata does not match with the key specified under policy

Short Form

Mismatch policy

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3275E

Message ID : CGA3279E

Severity

Error

Long Form

ESG/IDT-ALERT: IO error on header for ESG/IDT-Capable device [{0}]

Short Form

header IO error

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3280E

Severity

Error

Long Form

ESG/IDT-ALERT: Data transformation failure on ESG/IDT-Capable device [{0}]

Short Form

IDT fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3282E

Severity

Error

Message ID : CGA3280E

Long Form

ESG/IDT-ALERT: Failed to update new device size on ESG/IDT-Capable device [{0}]

Short Form

resize fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3284E

Severity

Error

Long Form

LDT: Failed to flag GuardPoint [{0}] for deferred key rotation, error [{1}]

Message ID : CGA3282E

Short Form

Defer rotate fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGA3289E

Severity

Error

Long Form

Failed to have permission to remediate {0}

Message ID : CGA3284E

Short Form

Failed to have permission to remediate

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3292E

Severity

Error

Long Form

Failed to prepare remediation for {0}

Short Form

Failed to prepare remediation

Message ID : CGA3289E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3295E

Severity

Error

Long Form

Failed to remediate {0} offline

Short Form

Failed to remediate offline

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3292E

Description

None

Message ID : CGA3298E

Severity

Error

Long Form

Failed to commit remediation for {0}

Short Form

Failed to commit remediation

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3295E

Message ID : CGA3301E

Severity

Error

Long Form

Failed to remediate {0} online

Short Form

Failed to remediate online

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3304E

Severity

Error

Long Form

ESG-ALERT: Process [{0}] disallowed on ESG device [{1}]

Short Form

Disallow ESG

Parameters

Label	CEF Label	Type	Usage
sproc	sproc	Text	Source process
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3306E

Message ID : CGA3304E

Severity

Error

Long Form

LDT: Skipping transformation of file [{0}], Unable to retrieve the File Information MD.

Short Form

LDT: Skipped invalid INF

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3307E

Severity

Error

Message ID : CGA3306E

Long Form

LDT: Skipping transformation of file [{0}], As failed to validate LDT file MetaData. Please contact support for more information.

Short Form

LDT: Skipped invalid metadata

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3308E

Severity

Error

Long Form

LDT: Skipping transformation of file [{0}], Key in the policy doesn't match with the key in the MD. Please contact support for more information.

Message ID : CGA3307E

Short Form

LDT: Skipped key mismatch

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3309E

Severity

Error

Long Form

LDT: Skipping transformation of file [{0}],file is being restored or exclusively accessed by the application. Please retrigger the rekey again after application finishes the processing on the file.

Short Form

LDT: Skipped restore

Message ID : CGA3308E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3310E

Severity

Error

Long Form

LDT: Skipping transformation of file [{0}],As failed to remove the read-only attribute of the file. Please retrigger the rekey again after checking the file permissions.

Short Form

LDT: Skipped read only

Parameters

Label	CEF Label	Type	Usage

Message ID : CGA3309E

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3356E

Severity

Error

Long Form

Not guarding path [{0}] (Reason: Can't guard directory inside a system folder)

Short Form

IgnrGrd InsideRoot

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3310E

Description

None

Message ID : CGA3361E

Severity

Error

Long Form

[ALARM] User[{0},uid={1},gid={2}] Process[{3}] Action[{4}] Res[{5}{6}] Effect[MFA {7}]

Short Form

MFA denied

Parameters

Label	CEF Label	Type	Usage
user	suser	Text	User name
uid	suid	Numeric	User id
gid	vds_gid	Numeric	Group id
command	command	Text	Task struct comm field

Message ID : CGA3356E

Label	CEF Label	Type	Usage
op_name	op_name	Text	Operation name
gp	fileId	Text	GuardPoint base directory
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Logger CGA: Information

Message ID : CGA2622I

Severity

Information

Long Form

Access Check Tracing: Invalid policy, use default policy object

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2630I

Severity

Information

Long Form

Policy [{0}]: Key match file is [{1}]

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2631I

Severity

Information

Long Form

Policy [{0}]: Key match resource domain is [{1}]

Short Form

No short form is provided for this message type

Message ID : CGA2630I

Description

None

Message ID : CGA2632I

Severity

Information

Long Form

Policy [{0}]: Using Key [{1}] of rule number [{2}]

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2633I

Severity

Information

Message ID : CGA2631I

Long Form

Policy [{0}]: No key rule matched: Using clear key

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2640I

Severity

Information

Long Form

Access check tracing: Policy [{0}]: Proc[{1}] Gen[{2}] User[{3} {4} {5}] Res[{6}]

Short Form

No short form is provided for this message type

Message ID : CGA2633I

Description

None

Message ID : CGA2641I

Severity

Information

Long Form

Access check tracing: Policy [{0}]: Empty rules table

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2642I

Severity

Information

Message ID : CGA2640I

Long Form

Access check tracing: Policy [{0}]: [{1}] Domain [{2}] matched

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2643I

Severity

Information

Long Form

Access check tracing: Policy [{0}]: Rule number [{1}] matched

Short Form

No short form is provided for this message type

Message ID : CGA2642I

Description

None

Message ID : CGA2644I

Severity

Information

Long Form

Access check tracing: Policy [{0}]: GoTo rule number [{1}]

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2646I

Severity

Information

Message ID : CGA2643I

Long Form

Access checkK tracing: Policy [{0}]: No rule matched - default action is [Deny]

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2647I

Severity

Information

Long Form

Access checkK tracing: Policy [{0}]: Using effect of rule number [{1}]: [{2} {3} {4}]

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2660I

Severity

Information

Long Form

Policy [{0}]: Set [{1}] empty with no [{2}]

Short Form

Empty policy set

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
oType	vds_oType	Text	Object type in policy rule
oName	vds_oName	Text	Object name in policy rule

Message ID : CGA2647I

Description

None

Message ID : CGA2661I

Severity

Information

Long Form

Policy: Set [{0}] empty with no [{1}]

Short Form

Empty policy set

Parameters

Label	CEF Label	Type	Usage
oType	vds_oType	Text	Object type in policy rule
oName	vds_oName	Text	Object name in policy rule

Description

None

Message ID : CGA3001I

Severity

Information

Long Form

EVENT: {0}

Short Form

Event

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGA2661I

Message ID : CGA3005I

Severity

Information

Long Form

Host password successfully supplied

Short Form

Host password accepted.

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3006I

Severity

Information

Message ID : CGA3005I

Long Form

A host password was entered, but was not required

Short Form

Host password not required

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3019I

Severity

Information

Long Form

Challenge/Response: Successfully unlocked keys

Short Form

Challenge/Response successful

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3020I

Severity

Information

Long Form

Challenge/Response: Challenge/response was entered, but was not required

Short Form

Challenge/Response not required

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3058I

Severity

Information

Long Form

[AUDIT] Process[{0}] Pid[{1}] Uid[{2}] Operation[{3}] File[{4}] Effect[PERMIT]

Short Form

Sysfile modified

Parameters

Label	CEF Label	Type	Usage
command	command	Text	Task struct comm field
pid	dvcpid	Numeric	Numeric process ID

Message ID : CGA3020I

Label	CEF Label	Type	Usage
uid	suid	Numeric	User id
op_name	op_name	Text	Operation name
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3105I

Severity

Information

Long Form

LDT: Error deleting stale metadata for [{0}]. Delete existing metadata before guarding with a production or data transform policy.

Short Form

LDT: Error deleting stale metadata

Parameters

Label	CEF Label	Type	Usage

Message ID : CGA3058I

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3183I

Severity

Information

Long Form

Successfully unguarded path [{0}]

Short Form

Ungrd Success

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3105I

Description

None

Message ID : CGA3186I

Severity

Information

Long Form

Successfully configured automount for path [{0}]

Short Form

Automnt Success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3183I

Message ID : CGA3193I

Severity

Information

Long Form

Successfully guarded [{0}]

Short Form

Grd Success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3194I

Severity

Information

Long Form

Successfully guarded [{0}] in simulation mode

Short Form

SimMode Grd Success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3195I

Severity

Information

Message ID : CGA3194I

Long Form

Successfully guarded [{0}] from container [{1}]

Short Form

Cntnr Grd Success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3196I

Severity

Information

Message ID : CGA3195I

Long Form

Successfully guarded [{0}] from container [{1}] in simulation mode

Short Form

SimMode Cntnr Grd Success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3197I

Severity

Information

Message ID : CGA3196I

Long Form

[{0}] System lock enabled

Short Form

System lock enabled

Parameters

Label	CEF Label	Type	Usage
stime	start	Text	A start time stamp

Description

None

Message ID : CGA3198I

Severity

Information

Long Form

[{0}] System lock disabled

Message ID : CGA3197I

Short Form

SysLock Disabled

Parameters

Label	CEF Label	Type	Usage
stime	start	Text	A start time stamp

Description

None

Message ID : CGA3199I

Severity

Information

Long Form

{{0}} FS agent lock enabled

Short Form

FSAgentLock Enabled

Message ID : CGA3198I

Parameters

Label	CEF Label	Type	Usage
stime	start	Text	A start time stamp

Description

None

Message ID : CGA3200I

Severity

Information

Long Form

[[{0}]] FS agent lock disabled

Short Form

FSAgentLock Disabled

Parameters

Label	CEF Label	Type	Usage
stime	start	Text	A start time stamp

Message ID : CGA3199I

Description

None

Message ID : CGA3201I

Severity

Information

Long Form

[[0]] Concise logging enabled

Short Form

ConsLog Enabled

Parameters

Label	CEF Label	Type	Usage
stime	start	Text	A start time stamp

Description

None

Message ID : CGA3200I

Message ID : CGA3202I

Severity

Information

Long Form

[{0}] Concise logging disabled

Short Form

ConsLog Disabled

Parameters

Label	CEF Label	Type	Usage
stime	start	Text	A start time stamp

Description

None

Message ID : CGA3203I

Severity

Information

Long Form

Policy [{0}] took effect or was modified

Short Form

Pol Modified

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name

Description

None

Message ID : CGA3204I

Severity

Information

Message ID : CGA3203I

Long Form

Successfully unguarded [{0}] from container [{1}]

Short Form

Cntnr Ungrd Success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
dockerid	dockerid	Text	Docker image or container id

Description

None

Message ID : CGA3205I

Severity

Information

Message ID : CGA3204I

Long Form

Successfully unguarded [{0}]

Short Form

Ungrd Success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3207I

Severity

Information

Long Form

FS Agent lock successful

Message ID : CGA3205I

Short Form

FSAgent Lock Success

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3208I

Severity

Information

Long Form

FS Agent unlock successful

Short Form

FSAgent Unlock Success

Message ID : CGA3207I

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3209I

Severity

Information

Long Form

System is now locked

Short Form

System Lock Success

Parameters

No parameters are provided for this message type

Message ID : CGA3208I

Description

None

Message ID : CGA3210I

Severity

Information

Long Form

System is now unlocked

Short Form

System Unlock Success

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3209I

Message ID : CGA3211I

Severity

Information

Long Form

McAfee Host Intrusion Prevention is disabled while the system is unlocked

Short Form

HIPS Disabled

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3213I

Severity

Information

Message ID : CGA3211I

Long Form

LDT: Completed scanning guardpoint [{0}].

Short Form

LDT: Completed scanning guardpoint

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3214I

Severity

Information

Long Form

LDT: Starting transformation for guardpoint [{0}].

Message ID : CGA3213I

Short Form

LDT: Starting transformation for guardpoint

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3215I

Severity

Information

Long Form

LDT: Completed transformation for guardpoint [{0}].

Short Form

LDT: Completed transformation for guardpoint

Message ID : CGA3214I

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3216I

Severity

Information

Long Form

LDT: Skipping transformation of passthrough file [{0}].

Short Form

LDT: Skipping transformation of passthrough file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3215I

Description

None

Message ID : CGA3217I

Severity

Information

Long Form

LDT: Skipping transformation of read-only file [{0}].

Short Form

LDT: Skipping transformation of read-only file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3216I

Message ID : CGA3219I

Severity

Information

Long Form

LDT: Starting transformation of file [{0}].

Short Form

LDT: Starting trasformation of file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3221I

Severity

Information

Long Form

[AUDIT] Process[{0}] Pid[{1}] Uid[{2}] Operation[{3}] File[{4}] ContainerID[{5}] Effect[PERMIT]

Short Form

Sysfile modified

Parameters

Label	CEF Label	Type	Usage
command	command	Text	Task struct comm field
pid	dvcpid	Numeric	Numeric process ID
uid	suid	Numeric	User id
op_name	op_name	Text	Operation name
filePath	filePath	Text	Full path to file
cid	cid	Text	Container ID

Description

None

Message ID : CGA3221I

Message ID : CGA3224I

Severity

Information

Long Form

LDT: Completed transformation of guardpoint [{0}] {1}

Short Form

LDT: Completed transformation of guardpoint

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ldt_stats	ldt_stats	Text	LDT statistics

Description

None

Message ID : CGA3225I

Severity

Information

Long Form

LDT: Skipping transformation of reparse point or link [{0}].

Short Form

LDT: Skipping transformation of reparse point

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3226I

Severity

Information

Long Form

LDT: Scan completed for guardpoint [{0}]. Data statistics for guard point: {1}.

Short Form

LDT: GP stats:

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ldt_stats	ldt_stats	Text	LDT statistics

Description

None

Message ID : CGA3240I

Severity

Information

Long Form

LDT: Skipping transformation of passthrough file [{0}]. The file resides in the boot directory. CTE cannot encrypt boot directory files.

Short Form

LDT: Skipping passthrough bootdir

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3241I

Severity

Information

Message ID : CGA3240I

Long Form

LDT: Skipping transformation of passthrough file [{0}]. CTE cannot encrypt these files. They are already encrypted using NTFS encryption or compressed.

Short Form

LDT: Skipping passthrough encrypted

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3242I

Severity

Information

Long Form

LDT: Skipping transformation of passthrough file [{0}]. File is not in a GuardPoint directory.

Message ID : CGA3241I

Short Form

LDT: Skipping passthrough notfiltered

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3244I

Severity

Information

Long Form

Volume [{0}] is being mounted. Guard points on this volume will be protected by Thales CTE

Short Form

Volume is being mounted

Message ID : CGA3242I

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3245I

Severity

Information

Long Form

CTE upgrade enabled

Short Form

VTE upgrade enabled

Parameters

No parameters are provided for this message type

Message ID : CGA3244I

Description

None

Message ID : CGA3246I

Severity

Information

Long Form

CTE upgrade disabled

Short Form

VTE upgrade disabled

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3245I

Message ID : CGA3247I

Severity

Information

Long Form

CTE upgrade canceled

Short Form

VTE upgrade canceled

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3248I

Severity

Information

Message ID : CGA3247I

Long Form

CTE upgraded on reboot

Short Form

VTE upgraded on reboot

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3257I

Severity

Information

Long Form

LDT: Exclusive access for rekey delayed on inode [%lld].

Message ID : CGA3248I

Short Form

LDT exclusive delayed

Parameters

Label	CEF Label	Type	Usage
node	vds_node	Numeric	A node identifier

Description

None

Message ID : CGA3258I

Severity

Information

Long Form

LDT: Exclusive access for rekey granted after delay on inode [%lld].

Short Form

LDT exclusive granted

Message ID : CGA3257I

Parameters

Label	CEF Label	Type	Usage
node	vds_node	Numeric	A node identifier

Description

None

Message ID : CGA3269I

Severity

Information

Long Form

Key change detected on {0} with Operation [{1}] and classification {2}

Short Form

Classification key change

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3258I

Label	CEF Label	Type	Usage
tag_op	tag_op	Text	Tag operation
tag	tag	Text	Tag

Description

None

Message ID : CGA3270I

Severity

Information

Long Form

Operation {0} failed because data classification is not enabled on {1}

Short Form

Classification not enabled

Parameters

Label	CEF Label	Type	Usage
tag_op	tag_op	Text	Tag operation

Message ID : CGA3269I

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3271I

Severity

Information

Long Form

Data classification initialization has not been finished for guard point {0}

Short Form

classification not initialized

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGA3270I

Description

None

Message ID : CGA3273I

Severity

Information

Long Form

Succeeded to write classification {0} to {1}

Short Form

Succeeded to write

Parameters

Label	CEF Label	Type	Usage
tag	tag	Text	Tag
filePath	filePath	Text	Full path to file

Message ID : CGA3271I

Description

None

Message ID : CGA3281I

Severity

Information

Long Form

ESG/IDT-INFO: Data transformation complete on ESG/IDT-Capable device [{0}]

Short Form

IDT ok

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3273I

Message ID : CGA3283I

Severity

Information

Long Form

LDT: Deferred key rotation on GuardPoint [{0}] until after completion of current transformation

Short Form

Defer rotate ok

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3287I

Severity

Information

Long Form

Acquiring permission to remediate {0}

Short Form

Acquiring permission to remediate

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3288I

Severity

Information

Message ID : CGA3287I

Long Form

Got permission to remediate {0}

Short Form

Got permission to remediate

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3290I

Severity

Information

Long Form

Preparing to remediate {0}

Message ID : CGA3288I

Short Form

Preparing to remediate

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3291I

Severity

Information

Long Form

Ready to remediate {0}

Short Form

Ready to remediate

Message ID : CGA3290I

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3293I

Severity

Information

Long Form

Remediating {0} from {1} to {2} offline

Short Form

Remediating offline

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3291I

Label	CEF Label	Type	Usage
key	cs3	Text	Name of key or key pair
key	cs3	Text	Name of key or key pair

Description

None

Message ID : CGA3294I

Severity

Information

Long Form

Remediated {0} from {1} to {2} offline

Short Form

Remediated offline

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3293I

Label	CEF Label	Type	Usage
key	cs3	Text	Name of key or key pair
key	cs3	Text	Name of key or key pair

Description

None

Message ID : CGA3296I

Severity

Information

Long Form

Committing remediation for {0}

Short Form

Committing remediation

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3294I

Description

None

Message ID : CGA3297I

Severity

Information

Long Form

Committed remediation for {0}

Short Form

Committed remediation

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3296I

Message ID : CGA3299I

Severity

Information

Long Form

Remediating {0} from {1} to {2} online

Short Form

Remediating online

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
key	cs3	Text	Name of key or key pair
key	cs3	Text	Name of key or key pair

Description

None

Message ID : CGA3300I

Severity

Information

Long Form

Remediated {0} from {1} to {2} online

Short Form

Remediated online

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
key	cs3	Text	Name of key or key pair
key	cs3	Text	Name of key or key pair

Description

None

Message ID : CGA3305I

Severity

Information

Long Form

ESG-INFO: Process [{0}] allowed on ESG device [{1}]

Short Form

Allow ESG

Parameters

Label	CEF Label	Type	Usage
sproc	sproc	Text	Source process
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3343I

Severity

Information

Long Form

Remediation is being done on other cte client for {0}

Short Form

Remediation on nfs

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Logger CGA: Warnings

Message ID : CGA2615W

Severity

Warning

Long Form

[[{0} {1}]: Sub-domain [{2}] not found

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2616W

Severity

Warning

Long Form

[{0} {1}]: Undefined sub-domain [{2}]

Short Form

No short form is provided for this message type

Description

None

Message ID : CGA2623W

Severity

Warning

Long Form

Policy [{0}]: Rename problem: source [{1}] is encrypted by key [{2}] but destination [{3}] by key [{4}]

Short Form

Policy rename failed

Message ID : CGA2616W

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
oldFilePath	oldFilePath	Text	Previous path to file (for rename and link)
key	cs3	Text	Name of key or key pair
filePath	filePath	Text	Full path to file
altKey	vds_altKey	Text	Name of alternate key for multi-key operations

Description

None

Message ID : CGA2901W

Severity

Warning

Long Form

Challenge/Response: Challenge/response requested to decrypt keys

Short Form

Challenge/Response requested to decrypt keys

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGA3002W

Severity

Warning

Long Form

EVENT: {0}

Short Form

Event

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGA3104W

Severity

Warning

Long Form

LDT: Volume dismounted. Aborting transformation at file [{0}]

Short Form

LDT: Stopping on dismount

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3002W

Description

None

Message ID : CGA3106W

Severity

Warning

Long Form

LDT: The guard point [{0}] does not have a valid transformation policy, there is no new key rule

Short Form

LDT: no new key rule

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3104W

Message ID : CGA3107W

Severity

Warning

Long Form

LDT: The guard point [{0}] does not have a valid transformation policy, there is no key_op rule

Short Form

LDT: no key_op rule

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3108W

Severity

Warning

Long Form

LDT: The guard point [{0}] does not support Live Data Transform, only file operations from the Offline Data Transform process will be allowed

Short Form

LDT: online rekey not supported

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3231W

Severity

Warning

Message ID : CGA3108W

Long Form

Failed to get a HDFS file name for {0}. Check the secfsd.log and the vor-hdfs-stderr.log for more details, and make sure the NameNode is running

Short Form

Failed to get HDFS file name

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3243W

Severity

Warning

Long Form

Volume [{0}] is getting dismounted. Guard Points on this volume will not be protected by Thales CTE

Message ID : CGA3231W

Short Form

Volume is getting dismounted

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3265W

Severity

Warning

Long Form

FSADM-ALERT: ESG/IDT required Signature Set for system utilities may have to be resigned {0}

Short Form

FSADM-ALERT: Resigning of file system binaries is required

Message ID : CGA3243W

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3276W

Severity

Warning

Long Form

Denied access to {0}{1} during classification initialization

Short Form

File access denied during initialization

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGA3265W

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3285W

Severity

Warning

Long Form

Denied access to data classification internal file {0}{1}

Short Form

Internal file access denied

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
filePath	filePath	Text	Full path to file

Message ID : CGA3276W

Description

None

Message ID : CGA3286W

Severity

Warning

Long Form

Denied access to {0}{1} during data remediation

Short Form

File access denied during remediation

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGA3346W

Severity

Warning

Long Form

Ptrace allowed on process [{0}] pid [{1}]

Short Form

Ptrace Attach Allowed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
pid	dvcpid	Numeric	Numeric process ID

Message ID : CGA3286W

Description

None

Message ID : CGA3352W

Severity

Warning

Long Form

LDT-NFS-ACCESSONLY-ALERT: Policy/key version validation failed for GuardPoint [{0}].Policy/Key version information doesn't match with primary node.

Short Form

LDT-NFS-ACCESSONLY-ALERT: Policy/key version mismatched

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGA3346W

Message ID : CGA3353W

Severity

Warning

Long Form

LDT-NFS-ACCESSIONLY-ALERT: Unable to perform the Policy/key validation for GuardPoint [{0}] , Disable->Enable the GuardPoints.

Short Form

LDT-NFS-ACCESSIONLY-ALERT: Policy/key validation failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Logger CGP: Errors

Message ID : CGP2602E

Severity

Error

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] Key[{7}] Effect[{8} {9}]

Short Form

Reject access

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
filePath	filePath	Text	Full path to file
key	cs3	Text	Name of key or key pair
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

A GuardPoint policy has blocked access to encrypted data. The reason for blocking the attempt is provided in the message fields.

Message ID : CGP2604E

Severity

Error

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] {7} Effect[{8} {9}]

Short Form

Reject access

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
gp	fileId	Text	GuardPoint base directory
filePath	filePath	Text	Full path to file
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

A GuardPoint policy has blocked access to encrypted data. The reason for blocking the attempt is provided in the message fields.

Message ID : CGP2606E

Severity

Error

Message ID : CGP2604E

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] Effect[{7} {8}]

Short Form

Reject node

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
gp	fileId	Text	GuardPoint base directory
filePath	filePath	Text	Full path to file
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

A GuardPoint policy has blocked access to encrypted data. The reason for blocking the attempt is provided in the message fields.

Message ID : CGP2608E

Severity

Error

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] [{7}{8}] Effect[{9} {10}]

Short Form

Reject link

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process

Label	CEF Label	Type	Usage
act	act	Text	Action being requested or performed
gp	fileId	Text	GuardPoint base directory
oldFilePath	oldFilePath	Text	Previous path to file (for rename and link)
filePath	filePath	Text	Full path to file
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGP2610E

Severity

Error

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] [{7}{8}] Effect[{9} {10}]

Short Form

Reject rename

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
gp	fileId	Text	GuardPoint base directory
oldFilePath	oldFilePath	Text	Previous path to file (for rename and link)
filePath	filePath	Text	Full path to file
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Logger CGP: Information

Message ID : CGP2601I

Severity

Information

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] Key[{7}] Effect[{8} {9}]

Short Form

Audit access

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
filePath	filePath	Text	Full path to file
key	cs3	Text	Name of key or key pair
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGP2603I

Severity

Information

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] {7} Effect[{8} {9}]

Short Form

Audit access

Message ID : CGP2601I

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
gp	fileId	Text	GuardPoint base directory
filePath	filePath	Text	Full path to file
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGP2605I

Severity

Information

Message ID : CGP2603I

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] Effect[{7} {8}]

Short Form

Audit node

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
gp	fileId	Text	GuardPoint base directory
filePath	filePath	Text	Full path to file
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGP2607I

Severity

Information

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] [{7}{8}] Effect[{9} {10}]

Short Form

Audit link

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process

Message ID : CGP2605I

Label	CEF Label	Type	Usage
act	act	Text	Action being requested or performed
gp	fileId	Text	GuardPoint base directory
oldFilePath	oldFilePath	Text	Previous path to file (for rename and link)
filePath	filePath	Text	Full path to file
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGP2609I

Severity

Information

Long Form

{0} Policy[{1}] User[{2}] Process[{3}] Action[{4}] Res[{5}{6}] [{7}{8}] Effect[{9} {10}]

Message ID : CGP2607I

Short Form

Audit rename

Parameters

Label	CEF Label	Type	Usage
cat	cat	Text	Event Category (e.g. AUDIT, TRACE)
pol	cs1	Text	Policy name
user	suser	Text	User name
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
gp	fileId	Text	GuardPoint base directory
oldFilePath	oldFilePath	Text	Previous path to file (for rename and link)
filePath	filePath	Text	Full path to file
denyStr	msg	Text	Code specifying reason for denying access, if any
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Logger CGS: Errors

Message ID : CGS2613E

Severity

Error

Long Form

Memory allocation failed in [{0}] at line [{1}]

Short Form

Out of memory

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3025E

Severity

Error

Long Form

LDT: Unable to remove LDT extended attribute on [{0}]. Error: [{1}]

Short Form

Extended attr delete

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGS3026E

Severity

Error

Long Form

LDT-ALERT: QoS failed to start

Short Form

QoS failed to start

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3027E

Severity

Error

Message ID : CGS3026E

Long Form

LDT-ALERT: Failed to launch transformation on [{0}]

Short Form

LDT: launch failure

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3028E

Severity

Error

Long Form

LDT: Encryption key for file [{0}] unavailable for LDT, possibly due to loss of communication to DSM

Message ID : CGS3027E

Short Form

LDT: Key unavailable

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGS3031E

Severity

Error

Long Form

LDT: Rekey failed for file [{0}] on guard point [{1}], Error {2}

Short Form

LDT: failed

Message ID : CGS3028E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3032E

Severity

Error

Long Form

LDT-ALERT: Key rotation failed on guard point [{0}]

Short Form

LDT: Key rotation failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3033E

Severity

Error

Long Form

LDT-ALERT: Failed to update LDT attribute on guard point [{0}]. Error: [{1}]

Short Form

LDT: Key rotation failure, EA

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGS3032E

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3034E

Severity

Error

Long Form

LDT-ALERT: Failed to suspend rekey on guard point [{0}]

Short Form

LDT: suspend failure

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3033E

Description

None

Message ID : CGS3035E

Severity

Error

Long Form

LDT: Failed to suspend rekey on all guard points

Short Form

LDT: suspend failure: all

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3034E

Message ID : CGS3038E

Severity

Error

Long Form

LDT-ALERT: Failed to resume rekey on guard point [{0}]

Short Form

LDT: resume failure

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3039E

Severity

Error

Long Form

LDT-ALERT: Failed to resume rekey on all guard points

Short Form

LDT: resume failure: all

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3042E

Severity

Error

Message ID : CGS3039E

Long Form

LDT: Skipped LDT recovery on read-only file system [{0}]

Short Form

Skipped LDT recovery: ROFS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3043E

Severity

Error

Long Form

LDT-ALERT: MDS file [{0}] exceeded diskpace quota on gp [{1}]

Message ID : CGS3042E

Short Form

MDS ENOSPC

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3044E

Severity

Error

Long Form

LDT: Insufficient memory condition encountered during LDT on guard point [{0}]

Message ID : CGS3043E

Short Form

MDS ENOMEM

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3045E

Severity

Error

Long Form

LDT-ALERT: Failed to update LDT attribute

Short Form

LDT: xattr failure

Message ID : CGS3044E

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3047E

Severity

Error

Long Form

LDT-ALERT: Aborting rekey of file [{0}] due to insufficient disk space

Short Form

LDT:SFS ENOSPC

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGS3045E

Description

None

Message ID : CGS3048E

Severity

Error

Long Form

LDT: Aborting rekey of file [{0}] due to lack of free memory. Try closing other applications to resolve the issue

Short Form

LDT:SFS ENOMEM

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGS3047E

Message ID : CGS3049E

Severity

Error

Long Form

LDT-ALERT: Skipped key rotation on guard point [{0}]. It is on a read-only file system

Short Form

LDT: Skipped ROFS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3050E

Severity

Error

Long Form

LDT-ALERT: Skipped key rotation on guard point [{0}] due to insufficient disk space

Short Form

LDT: Skipped ENOSPC

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3051E

Severity

Error

Message ID : CGS3050E

Long Form

LDT-ALERT: Failed to rotate key on guard point [{0}]. Another rekey operation is already in progress

Short Form

LDT: Skipped EBUSY

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3052E

Severity

Error

Long Form

LDT-ALERT: Skipped key rotation on guard point [{0}]. Error: [{1}]

Message ID : CGS3051E

Short Form

LDT: Skipped, error

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3053E

Severity

Error

Long Form

LDT-ALERT: Failed to rotate key on guard point [{0}] during pre-commit

Message ID : CGS3052E

Short Form

LDT: pre-commit failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3054E

Severity

Error

Long Form

LDT-ALERT: Failed to rotate key on guard point [{0}] during commit

Short Form

LDT: commit failed

Message ID : CGS3053E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3055E

Severity

Error

Long Form

LDT: Failed to abort key rotation on guard point [{0}]

Short Form

LDT: abort failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3054E

Description

None

Message ID : CGS3057E

Severity

Error

Long Form

LDT: Extended attribute of inode [%lld] is corrupted under guard point [{0}]

Short Form

LDT: xattr corrupted

Parameters

Label	CEF Label	Type	Usage
node	vds_node	Numeric	A node identifier
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3055E

Description

None

Message ID : CGS3234E

Severity

Error

Long Form

LDT: Rekey failed for file [{0}] on guard point [{1}]. Error {2}. Reason :{3}

Short Form

LDT: failed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : CGS3057E

Description

None

Message ID : CGS3253E

Severity

Error

Long Form

LDT: Extended attribute of inode [%lld] is missing under guard point [{0}]

Short Form

LDT: xattr missing

Parameters

Label	CEF Label	Type	Usage
node	vds_node	Numeric	A node identifier
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3234E

Description

None

Message ID : CGS3259E

Severity

Error

Long Form

IV of file [{0}] is corrupted

Short Form

file IV corrupted

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGS3253E

Message ID : CGS3260E

Severity

Error

Long Form

IV of file [{0}] is mismatched(file may be restored to wrong fs)

Short Form

file IV mismatched

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGS3261E

Severity

Error

Long Form

LDT-ALERT: failed to rekey segment [{0}] of [{1}]. Error: [{2}]

Short Form

LDT: failure to rekey segment

Parameters

Label	CEF Label	Type	Usage
segID	vds_segID	Numeric	Segment ID
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3262E

Message ID : CGS3261E

Severity

Error

Long Form

LDT-ALERT: Skipped rekeying [{0}] on guard point [{1}]. Error: [{2}]

Short Form

LDT: skipped rekey on file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3263E

Message ID : CGS3262E

Severity

Error

Long Form

LDT-ALERT: LDT recovery failure on guard point [{0}]. Error: [{1}]

Short Form

LDT-ALERT: LDT recovery failure

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3264E

Message ID : CGS3263E

Severity

Error

Long Form

LDT-ALERT: Restore of LDT protected file [{0}] not allowed by policy.

Short Form

LDT-ALERT: LDT restore denied

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGS3266E

Severity

Error

Message ID : CGS3264E

Long Form

LDT-ALERT: Cannot enable guard point [{0}] due to inconsistencies in underlying file system encountered during LDT recovery.
Status [{1}]

Short Form

LDT-ALERT: LDT recovery failure

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
count	vds_count	Numeric	A generic count value

Description

None

Message ID : CGS3304E

Severity

Error

Message ID : CGS3266E

Long Form

IDT-TD-ALERT: Node {0} did not respond to pcl command

Short Form

IDT-TD-ALERT: Remote node did not respond to pcl

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Description

None

Message ID : CGS3305E

Severity

Error

Long Form

IDT-TD-ALERT: Node {0} failed to perform voradmin task

Message ID : CGS3304E

Short Form

IDT-TD-ALERT: voradmin failed on remote node

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Description

None

Message ID : CGS3306E

Severity

Error

Long Form

IDT-TD-ALERT: Failed to find clique for disk {0}

Short Form

IDT-TD-ALERT: Failed to find clique

Message ID : CGS3305E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3307E

Severity

Error

Long Form

IDT-TD-ALERT: Failed to distribute IDT-Capable metadata file to remote nodes

Short Form

IDT-TD-ALERT: Failed to distribute IDT-Capable metadata

Parameters

No parameters are provided for this message type

Message ID : CGS3306E

Description

None

Message ID : CGS3308E

Severity

Error

Long Form

IDT-TD-ALERT: Failed to move or rename IDT-Capable metadata file on remote nodes

Short Form

IDT-TD-ALERT: Failed to move or rename IDT-Capable metadata

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3307E

Message ID : CGS3309E

Severity

Error

Long Form

IDT-TD-ALERT: Failed to get GuardPoint status on remote nodes

Short Form

IDT-TD-ALERT: Failed to get GuardPoint status

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3311E

Severity

Error

Long Form

IDT-TD-ALERT: Failed to complete rekey on remote nodes

Short Form

IDT-TD-ALERT: Failed to complete rekey

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3312E

Severity

Error

Long Form

LDT-NFS-ALERT: Host waiting to take over NFS GuardPoint {0} for LDT

Short Form

Waiting to take over

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3313E

Severity

Error

Long Form

LDT-ALERT: Cannot enable GuardPoint due to wrong policy applied to [{0}]

Short Form

Incorrect policy

Message ID : CGS3312E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3314E

Severity

Error

Long Form

LDT: Cannot enable [{0}] due to stale policy

Short Form

LDT: stale policy

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3313E

Description

None

Message ID : CGS3315E

Severity

Error

Long Form

LDT-NFS-ALERT: Cannot enable GuardPoint [{0}] on a read-only file system

Short Form

LDT-NFS: Guarding ROFS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3314E

Message ID : CGS3316E

Severity

Error

Long Form

LDT-ALERT: Failed to process directory rename for {0}, error {1}

Short Form

LDT: dir rename failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3317E

Severity

Error

Long Form

LDT-ALERT: Failed to rekey {0} file(s) in directory {1}

Short Form

LDT: dir rekey errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3319E

Severity

Error

Long Form

LDT-NFS-ALERT: Failed to start or stop rekey on GuardPoint [{0}] over NAS, error [{1}]

Short Form

LDT-NFS-ALERT: start or stop failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3327E

Severity

Error

Long Form

LDT-ALERT: Election of this host for LDT Group Primary role has failed for GuardPoint [{0}]

Short Form

LDT-NFS-ALERT: primary election failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3328E

Severity

Error

Long Form

LDT-NFS-ALERT: File operation recovery failed on new primary host after primary election, GuardPoint [{0}] objID [%llu] error [{1}] source [{2}]

Short Form

LDT-NFS-ALERT: fop recovery failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
node	vds_node	Numeric	A node identifier
ecode	cn1	Numeric	An error code
count	vds_count	Numeric	A generic count value

Description

None

Message ID : CGS3329E

Severity

Error

Long Form

LDT-NFS-ALERT: LDT recovery failed on new primary host after primary election, GuardPoint [{0}] objID [%llu] error [{1}]

Short Form

LDT-NFS-ALERT: LDT recovery failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
node	vds_node	Numeric	A node identifier
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3331E

Severity

Error

Long Form

LDT-NFS-ALERT: File operation failed on secondary host, GuardPoint [{0}] objID [%llu] error [{1}] source [{2}]

Short Form

LDT-NFS-ALERT: fop failed on secondary

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
node	vds_node	Numeric	A node identifier
ecode	cn1	Numeric	An error code
count	vds_count	Numeric	A generic count value

Description

None

Message ID : CGS3335E

Severity

Error

Long Form

LDT-ALERT: Failed to check rekey status on file {0}, error {1}

Short Form

LDT: monitor failed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3336E

Severity

Error

Long Form

LDT-ALERT: Failed to enable/apply GuardPoint [{0}]

Short Form

Guard failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3337E

Severity

Error

Long Form

LDT-ALERT: Failed to disable/delete GuardPoint [{0}]

Short Form

Unguard failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3338E

Severity

Error

Message ID : CGS3337E

Long Form

LDT-ALERT: Failed to join GuardPoint group [{0}]

Short Form

LGS join failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3339E

Severity

Error

Long Form

LDT-ALERT: Failed to leave GuardPoint group [{0}]

Message ID : CGS3338E

Short Form

LGS leave failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3340E

Severity

Error

Long Form

LDT-ALERT: Failed to enumerate GuardPoint [{0}], please verify the provided CIFS credentials. CIFS credentials may be expired or may not have permission to access.

Short Form

Invalid creds

Message ID : CGS3339E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3341E

Severity

Error

Long Form

LDT-ALERT: Failed to authenticate a user.

Short Form

CIFS Login error

Parameters

No parameters are provided for this message type

Message ID : CGS3340E

Description

None

Message ID : CGS3342E

Severity

Error

Long Form

LDT-NFS-ALERT: Error processing LDTC message for GuardPoint [{0}], error [{1}], source [{2}]

Short Form

LDT-NFS-ALERT: bad msg

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code
count	vds_count	Numeric	A generic count value

Message ID : CGS3341E

Description

None

Message ID : CGS3344E

Severity

Error

Long Form

LDT-NFS-ALERT: Not guarding path [{0}] (Reason: LDT version installed on host is incompatible with version on primary host)

Short Form

LDT-NFS-ALERT: msg ver mismatch

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3342E

Message ID : CGS3349E

Severity

Error

Long Form

LDT-NFS-ALERT: Demotion of Primary host of GuardPoint [{0}] failed, error [{1}]

Short Form

LDT-NFS-ALERT: Primary host demotion failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3354E

Severity

Error

Long Form

LDT-NFS-ALERT: Manual recovery of DEMOTED GuardPoint failed, GuardPoint [{0}] objID [%llu] error [{1}]

Short Form

LDT-NFS-ALERT: Primary DEMOTION recovery failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
node	vds_node	Numeric	A node identifier
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3358E

Severity

Error

Long Form

LDT-NFS-ALERT: DEMOTED GuardPoint [{0}] being recovered while the old demoted primary host is still alive, objID [%llu]

Short Form

LDT-NFS-ALERT: Primary DEMOTION admin recovery, old primary still alive

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
node	vds_node	Numeric	A node identifier

Description

None

Message ID : CGS3360E

Severity

Error

Long Form

LDT-RAW: Write operation to relocation zone on [/dev/secvm{0}] blocked

Short Form

LDT-RAW: write blocked

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3362E

Severity

Error

Long Form

RWP-RW-ALERT: Potential Ransomware activity[{0}] detected in process ID [{1}], Process name: [{2}]. Num original files written to disk: [{3}]. Sensitivity: [{4}] Mode: [{5}] Reboot or remount on separate VM to access clear files on disk. Prev Code Path: [0x{6}] Latest Code Path: [0x{7}]. Last file checked is [{8}], AlgoSuspect:1 proc flags: [{9}]

Short Form

RWP: Ransomware detected

Parameters

Label	CEF Label	Type	Usage
rwtype	rwtype	Text	string type of RW proocess flags
pid	dvcpid	Numeric	Numeric process ID
pname	pname	Text	Process name
nfiles	vds_nfiles	Numeric	The total number of files in an operation
rwsensvty	rwsensvty	Numeric	Numeric value of RWP sensitivity
rwmode	rwmode	Text	string mode of RW : alert/block
rwcodepath	rwcodepath	Numeric	hex code for tracing RW detection
rwcodepath	rwcodepath	Numeric	hex code for tracing RW detection

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
rwflags	rwflags	Numeric	bitmap for RW

Description

None

Message ID : CGS3364E

Severity

Error

Long Form

LDT-ALERT: Couldn't elect the primary during failover for [{0}], check DPS config.

Short Form

LDT-ALERT: Couldn't elect primary during failover, please check DPS config

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3362E

Description

None

Message ID : CGS3365E

Severity

Error

Long Form

LDT-ALERT: No primary exists to join GuardPoint group [{0}]

Short Form

LGS join failed no primary

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3364E

Message ID : CGS3370E

Severity

Error

Long Form

LDT-NFS-ALERT: Rekey started on LDT GuardPoint Group [{0}] containing different CTE versions

Short Form

LDT-NFS-ALERT: mixed mode rekey

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3371E

Severity

Error

Long Form

LDT-NFS-ALERT: GuardPoint Group Service recovery failed for [{0}] error [{1}]

Short Form

LDT-NFS-ALERT: Group Service recovery failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Logger CGS: Information

Message ID : CGS3029I

Severity

Information

Long Form

LDT: Cannot enable guard point [{0}] during LDT clean-up process

Short Form

LDT: EA removing

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3030I

Severity

Information

Long Form

LDT: Successfully rekeyed file [{0}]

Short Form

Successfully rekeyed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGS3036I

Severity

Information

Long Form

LDT: Successfully suspended rekey on guard point [{0}]

Short Form

LDT: suspend success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3037I

Severity

Information

Message ID : CGS3036I

Long Form

LDT: Rekey will be suspended on all applicable guard points

Short Form

LDT: suspend success: all

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3040I

Severity

Information

Long Form

LDT: Successfully resumed rekey on guard point [{0}]

Short Form

LDT: resume success

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3041I

Severity

Information

Long Form

LDT: Rekey will be resumed on all applicable guard points

Short Form

LDT: resume success: all

Message ID : CGS3040I

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3046I

Severity

Information

Long Form

LDT-ALERT: Suspending rekey of binary file [{0}] during its execution

Short Form

LDT:SFS EXTBUSY

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : CGS3041I

Description

None

Message ID : CGS3056I

Severity

Information

Long Form

LDT: Rekey operation completed on guard point [{0}]

Short Form

LDT: completed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3046I

Message ID : CGS3249I

Severity

Information

Long Form

LDT-ALERT: Skipped key rotation on guard point [{0}] on a read-only file system

Short Form

LDT: Skipped ROFS

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3250I

Severity

Information

Long Form

LDT-ALERT: Skipped key rotation on guard point [{0}] due to insufficient disk space

Short Form

LDT: Skipped ENOSPC

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3251I

Severity

Information

Message ID : CGS3250I

Long Form

LDT-ALERT: Skipped key rotation on guard point [{0}] while another rekey operation is in progress

Short Form

LDT: Skipped EBUSY

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3254I

Severity

Information

Long Form

LDT: Metadata will start getting removed from all files in guard point [{0}]

Message ID : CGS3251I

Short Form

Extended attr will be deleted from gp

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3255I

Severity

Information

Long Form

LDT: Metadata has been removed from all files in guard point [{0}]

Short Form

Extended attr deleted from gp

Message ID : CGS3254I

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3277I

Severity

Information

Long Form

LDT-ALERT: Low space on guard point [{0}], increase free space or LDT will be suspended.

Short Form

low disk

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3255I

Description

None

Message ID : CGS3318I

Severity

Information

Long Form

LDT-NFS-ALERT: Failed to preserve time stamps: GuardPoint [{0}] objID [{1}] error [{2}]

Short Form

LDT-NFS-ALERT: PTS Access

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
node	vds_node	Numeric	A node identifier
ecode	cn1	Numeric	An error code

Message ID : CGS3277I

Description

None

Message ID : CGS3320I

Severity

Information

Long Form

LDT: Skipping transformation of NOVIEW file [{0}]. File was opened with NOVIEW access.

Short Form

LDT: Skipping NOVIEW

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : CGS3318I

Message ID : CGS3322I

Severity

Information

Long Form

LDT-NFS-ALERT: LDT Communication Master is up

Short Form

LDT-NFS-ALERT: comm group master up

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3324I

Severity

Information

Message ID : CGS3322I

Long Form

LDT-NFS-ALERT: LDT Group Primary host has been elected for GuardPoint [{0}]

Short Form

LDT-NFS-ALERT: group primary elected

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3325I

Severity

Information

Long Form

LDT-NFS-ALERT: This host has been promoted to LDT Group Primary role for GuardPoint [{0}]

Message ID : CGS3324I

Short Form

LDT-NFS-ALERT: group primary promoted

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3347I

Severity

Information

Long Form

LDT-NFS-ALERT: Primary host of GuardPoint [{0}] demoting

Short Form

LDT-NFS-ALERT: Primary host demoting

Message ID : CGS3325I

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3348I

Severity

Information

Long Form

LDT-NFS-ALERT: Primary host of GuardPoint [{0}] demoted

Short Form

LDT-NFS-ALERT: Primary host demoted

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3347I

Description

None

Message ID : CGS3350I

Severity

Information

Long Form

LDT-NFS-ALERT: LDT Communication Master is going down gracefully

Short Form

LDT-NFS-ALERT: Comm group master down gracefully

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3348I

Message ID : CGS3355I

Severity

Information

Long Form

LDT-NFS-ALERT: File marked as INCOMPLETE after DEMOTION. Admin intervention is required for recovery, GuardPoint
[{}0}] objID [%llu] error [{1}]

Short Form

LDT-NFS-ALERT: Primary DEMOTION partial recovery

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
node	vds_node	Numeric	A node identifier
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3357I

Severity

Information

Long Form

LDT-NFS-ALERT: Manual recovery invoked on the DEMOTED GuardPoint [{0}]

Short Form

LDT-NFS-ALERT: Primary DEMOTION full ADMIN recovery

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3359I

Severity

Information

Long Form

LDT-NFS-ALERT: Secondary host DEMOTED due to loss of NAS connection, GuardPoint [{0}]

Short Form

LDT-NFS-ALERT: Secondary host demoted

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Logger CGS: Warnings

Message ID : CGS3267W

Severity

Warning

Long Form

LDT-ALERT: LDT manual recovery on guard point [{0}] completed with [{1}] errors.

Short Form

LDT-ALERT: LDT manual recovery forced

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
count	vds_count	Numeric	A generic count value

Description

None

Message ID : CGS3268W

Severity

Warning

Long Form

LDT-ALERT: encrypted data detected in filename [{0}] inode [%lld] in guard point [{1}] under clear exclusion key rule

Short Form

LDT-ALERT: encrypted data in clear file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
node	vds_node	Numeric	A node identifier
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3302W

Severity

Warning

Long Form

LDT-ALERT: Rekey is restarting due to previous transient error on guard point [{0}]. Error: [{1}]

Short Form

Res acc issue

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3303W

Severity

Warning

Long Form

LDT-ALERT: Rekey is restarting due to previous transient error on guard point [{0}]. Error: [{1}] Reason: [{2}]

Short Form

Res acc issue desc

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : CGS3310W

Severity

Warning

Long Form

IDT-TD-WARNING: Failed to delete IDT-Capable metadata file on remote nodes

Short Form

IDT-TD-WARNING: Failed to delete IDT-Capable metadata

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3321W

Severity

Warning

Long Form

LDT-NFS-ALERT: LDT Communication Master is down

Short Form

LDT-NFS-ALERT: Comm group master down

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3323W

Severity

Warning

Long Form

LDT-NFS-ALERT: LDT Group Primary host left the group for GuardPoint [{0}]

Short Form

LDT-NFS-ALERT: group primary left

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3326W

Severity

Warning

Long Form

LDT-NFS-ALERT: This host cannot be promoted to LDT Group Primary role for GuardPoint [{0}]

Short Form

LDT-NFS-ALERT: refused primary role

Message ID : CGS3323W

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3330W

Severity

Warning

Long Form

LDT-NFS-ALERT: Promotion process taking too long causing delay in file operation, GuardPoint [{0}] objID [%llu]

Short Form

LDT-NFS-ALERT: Promotion taking too long

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3326W

Label	CEF Label	Type	Usage
node	vds_node	Numeric	A node identifier

Description

None

Message ID : CGS3332W

Severity

Warning

Long Form

LDT-NFS-ALERT: Some members of LDT GuardPoint Group for [{0}] have not received latest key version

Short Form

LDT-NFS-ALERT: group doesn't have the same key

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3330W

Description

None

Message ID : CGS3333W

Severity

Warning

Long Form

LDT-NFS-ALERT: Lazy rekey operation failed to rekey file [{0}], error [{1}]

Short Form

LDT-NFS-ALERT: lazy rekey failed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : CGS3334W

Severity

Warning

Long Form

LDT-NFS-ALERT: LDT remote operation failed across LDT GuardPoint Group for GuardPoint [{0}], ino [%lld], filename [{1}], error [{2}], remote op [{3}]

Short Form

LDT-NFS-ALERT: remote op failed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
node	vds_node	Numeric	A node identifier
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Message ID : CGS3333W

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : CGS3345W

Severity

Warning

Long Form

LDT-ALERT: LDT rekey status on files in GuardPoint [{0}] have been manually edited.

Short Form

LDT: rkea_status edited

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : CGS3334W

Description

None

Message ID : CGS3351W

Severity

Warning

Long Form

LDT-NFS-ALERT: LDT Communication Cluster is down

Short Form

LDT-NFS-ALERT: Comm group cluster is down

Parameters

No parameters are provided for this message type

Description

None

Message ID : CGS3345W

Message ID : CGS3363W

Severity

Warning

Long Form

LDT-NFS-ALERT: Dynamically added resource-set is not supported on NFS Guardpoint [{0}].

Short Form

LDT-NFS-ALERT: Dyn resourceset not supp

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : CGS3369W

Severity

Warning

Long Form

LDT-NFS-ALERT: GuardPoint Group for [{0}] is in mixed mode; cannot start rekey

Short Form

LDT-NFS-ALERT: key rotation mixed mode

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Logger COM: Errors

Message ID : COM4547E

Severity

Error

Long Form

Internal error: Invalid configuration type given to communications subsystem. Contact support.

Short Form

No short form is provided for this message type

Description

None

Message ID : COM4631E

Severity

Error

Long Form

OPENSSL ERROR: {0}

Short Form

OpenSSL error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : COM4638E

Severity

Error

Long Form

We have detected a change in the system hardware. Communication to the Key Manager has been disabled. This condition can be fixed by re-registering this agent with the Key Manager.

Message ID : COM4631E

Short Form

Hardware Change

Parameters

No parameters are provided for this message type

Description

None

Message ID : COM4644E

Severity

Error

Long Form

An invalid REST object has been received - {0}

Short Form

Bad REST object

Message ID : COM4638E

Parameters

Label	CEF Label	Type	Usage
detail	vds_detail	Text	Fault detail

Description

None

Logger COM: Fatal errors

Message ID : COM4503F

Severity

Fatal error

Long Form

Communications module initialization failure. Contact support.

Short Form

Comms init fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : COM4506F

Severity

Fatal error

Long Form

Failed to set up logger "{0}". Contact support.

Short Form

Logger setup error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : COM4511F

Severity

Fatal error

Message ID : COM4506F

Long Form

The communication request to the Key Manager was garbled or otherwise incorrect: error {0}. Contact support.

Short Form

Bad policy request

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : COM4512F

Severity

Fatal error

Long Form

Policy response garbled: unable to find attribute "{0}".

Message ID : COM4511F

Short Form

Resp attr missing

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : COM4513F

Severity

Fatal error

Long Form

Unable to configure secure communication channel. Contact support.

Short Form

No short form is provided for this message type

Message ID : COM4512F

Description

None

Message ID : COM4514F

Severity

Fatal error

Long Form

The communication request to the Key Manager was garbled or otherwise incorrect: error {0}. Contact support.

Short Form

Server init req error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : COM4513F

Message ID : COM4515F

Severity

Fatal error

Long Form

There was a communication failure with the Key Manager. The server returned a fault: {0}{1}; "{2}"; Subcode: "{3}"; Reason: "{4}"; Detail: "{5}".

Short Form

No short form is provided for this message type

Description

None

Message ID : COM4521F

Severity

Fatal error

Long Form

Internal version not supported, version required: {0}.

Short Form

Bad SDK version

Parameters

Label	CEF Label	Type	Usage
version	vds_version	Text	Software version string

Description

None

Message ID : COM4523F

Severity

Fatal error

Long Form

Unable to establish a connection to a Key Manager for the purpose of policy evaluation. Verify that the configuration file has the correct URL(s) to the server.

Message ID : COM4521F

Short Form

Policy info missing

Parameters

No parameters are provided for this message type

Description

None

Message ID : COM4527F

Severity

Fatal error

Long Form

The Agent could not obtain configuration information. The Agent failed to initialize. Verify connectivity to the Key Manager and retry the operation.

Short Form

Agent config missing

Message ID : COM4523F

Parameters

No parameters are provided for this message type

Description

None

Message ID : COM4529F

Severity

Fatal error

Long Form

Unable to establish an initial connection to any Key Manager. Verify that the configuration file has the correct URL(s) to the server.

Short Form

No config from server

Parameters

No parameters are provided for this message type

Message ID : COM4527F

Description

None

Message ID : COM4531F

Severity

Fatal error

Long Form

Unable to configure secure communication channel. Contact support.

Short Form

SSL setup fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : COM4529F

Message ID : COM4533F

Severity

Fatal error

Long Form

{0} from file does not match that from backup. File: "{1}". Backup: "{2}".

Short Form

Backup opaque data mismatch

Parameters

No parameters are provided for this message type

Description

None

Message ID : COM4534F

Severity

Fatal error

Message ID : COM4533F

Long Form

File type mismatch: {0} must be a directory.

Short Form

Not a dir

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : COM4538F

Severity

Fatal error

Long Form

The Key Manager URL ({0}) must start with "https:".

Message ID : COM4534F

Short Form

Invalid URL

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

None

Message ID : COM4542F

Severity

Fatal error

Long Form

The agent could not allocate enough memory. Contact support.

Short Form

Out of memory

Message ID : COM4538F

Parameters

No parameters are provided for this message type

Description

None

Message ID : COM4548F

Severity

Fatal error

Long Form

Policy request garbled: unable to find attribute "{0}".

Short Form

Req attr missing

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : COM4542F

Description

None

Message ID : COM4551F

Severity

Fatal error

Long Form

The Agent failed to initialize, reporting "{0}". Verify the logging configuration on the Key Manager and retry the operation. If the problem persists, contact support.

Short Form

Agent init error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : COM4548F

Message ID : COM4552F

Severity

Fatal error

Long Form

Communication with the Key Manager was established, but an invalid response (error {0}) was received. The requested operation cannot continue. Contact support.

Short Form

Bad policy response

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : COM4554F

Severity

Fatal error

Long Form

Communication with the Key Manager was established, but an invalid response (error {0}) was received. The requested operation cannot continue. Contact support.

Short Form

Comms response error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : COM4558F

Severity

Fatal error

Message ID : COM4554F

Long Form

Key Manager communications failure. URL: {0}. Check the URL in the agent.conf file. Verify that the server url is correct and retry the operation.

Short Form

Bad config from server

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

None

Message ID : COM4562F

Severity

Fatal error

Long Form

The communication request to the Key Manager was garbled or otherwise incorrect: error {0}. Contact support.

Message ID : COM4558F

Short Form

Comms init error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : COM4563F

Severity

Fatal error

Long Form

Key Manager connection failure. Check the URL in the agent.conf file. Verify that the server url is correct and retry the operation.

Short Form

No short form is provided for this message type

Message ID : COM4562F

Description

None

Message ID : COM4567F

Severity

Fatal error

Long Form

Communication with the Key Manager was established, but an invalid response (error {0}) was received. The requested operation cannot continue. Contact support.

Short Form

SDK response error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : COM4563F

Message ID : COM4569F

Severity

Fatal error

Long Form

The Key Manager URL is too long. It is {0} characters, while the maximum size is {1} characters. The URL is {2}.

Short Form

URL too long

Parameters

Label	CEF Label	Type	Usage
slen	in	Numeric	Input byte count or length
dlen	out	Numeric	Output byte count or length
url	request	Text	A uniform resource location

Description

None

Message ID : COM4571F

Severity

Fatal error

Long Form

File access failure: Unable to open {0}: {1}.

Short Form

Open error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : COM4577F

Severity

Fatal error

Long Form

Error adding host {0} information to server.

Short Form

No short form is provided for this message type

Description

None

Message ID : COM4578F

Severity

Fatal error

Long Form

Request from {0} to add host is invalid.

Message ID : COM4577F

Short Form

No short form is provided for this message type

Description

None

Message ID : COM4579F

Severity

Fatal error

Long Form

Response to add host request from {0} is invalid: {1}.

Short Form

No short form is provided for this message type

Description

None

Message ID : COM4578F

Message ID : COM4583F

Severity

Fatal error

Long Form

Error initializing agent.

Short Form

Agent init fail

Parameters

No parameters are provided for this message type

Description

The agent is unable to reach the key manager. You may see any of the following error messages: COM4583F, COM4633W, VMD3770F, VMD3885I or VMD3886I. You may experience any of the following:

1. Connection to the key manager is down.
2. The VMD Host has been deleted from the key manager.
3. The host does not have "Communication Enabled" in the key manager UI.
4. The VMD's host may be deleted from the key manager. Run the register_host utility to re-register the VMD with the key manager.

Message ID : COM4584F

Severity

Fatal error

Long Form

Initialize Agent request invalid, {0} ({1}).

Short Form

Invalid config

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : COM4586F

Severity

Fatal error

Long Form

Error evaluating policy.

Short Form

Policy eval fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : COM4587F

Severity

Fatal error

Message ID : COM4586F

Long Form

Error evaluating policy request, {0}.

Short Form

Policy eval error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : COM4588F

Severity

Fatal error

Long Form

Error evaluating policy response, {0}.

Message ID : COM4587F

Short Form

Policy response error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : COM4592F

Severity

Fatal error

Long Form

Error running VMSDK server, {0} (port: {1}).

Short Form

VMSDK server error

Message ID : COM4588F

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
port	spt	Numeric	A socket port number

Description

None

Message ID : COM4599F

Severity

Fatal error

Long Form

An error was encountered when trying to listen to requests from the server. The listening interface is "{0}" and the port is {1}.
Error: {2}.

Short Form

No short form is provided for this message type

Message ID : COM4592F

Description

None

Message ID : COM4600F

Severity

Fatal error

Long Form

There was a communication failure with the Key Manager ({0}). The server returned a fault: {1}{2}; "{3}"; Subcode: "{4}"; Reason: "{5}"; Detail: "{6}".

Short Form

SOAP client error

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
showStr	reason	Text	Code specifying reason for allowing access, if any
ecode	cn1	Numeric	An error code
context	vds_context	Text	Fault context

Message ID : COM4599F

Label	CEF Label	Type	Usage
subcode	vds_subcode	Text	Fault subcode
showStr	reason	Text	Code specifying reason for allowing access, if any
detail	vds_detail	Text	Fault detail

Description

None

Message ID : COM4603F

Severity

Fatal error

Long Form

Unable to parse the URL {0}. This attribute is located in the config file at {1}. Please fix the URL or re-install this product.

Short Form

Bad URL

Parameters

Label	CEF Label	Type	Usage

Message ID : COM4600F

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
filePath	filePath	Text	Full path to file

Description

None

Message ID : COM4604F

Severity

Fatal error

Long Form

Internal error: unable to set attribute {0}.

Short Form

Cannot set attr

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : COM4603F

Description

None

Message ID : COM4628F

Severity

Fatal error

Long Form

Unable to connect to a Key Manager. URL: {0}. Please verify that the agent host is registered with a Key Manager.

Short Form

Server connect fail

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

None

Message ID : COM4604F

Message ID : COM4629F

Severity

Fatal error

Long Form

The server at {0} attempted to contact this machine, but it was denied access due to an invalid certificate.

Short Form

Bad cert from server

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

None

Message ID : COM4630F

Severity

Fatal error

Long Form

A machine identifying itself as {0} tried to contact the VMD, but there was an error: {1}{2}; "{3}"; Subcode: "{4}"; Reason: "{5}"; Detail: "{6}".

Short Form

SOAP server error

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
showStr	reason	Text	Code specifying reason for allowing access, if any
ecode	cn1	Numeric	An error code
context	vds_context	Text	Fault context
subcode	vds_subcode	Text	Fault subcode
showStr	reason	Text	Code specifying reason for allowing access, if any
detail	vds_detail	Text	Fault detail

Description

None

Message ID : COM4637F

Severity

Fatal error

Long Form

Failed to bind to port {0}. Please ensure that this port is not in use by another program.

Short Form

SDK bind error

Parameters

Label	CEF Label	Type	Usage
port	spt	Numeric	A socket port number

Description

None

Message ID : COM4630F

Logger COM: Information

Message ID : COM4601I

Severity

Information

Long Form

Successful Agent init with Key Manager ({0}).

Short Form

Comms init OK

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

None

Message ID : COM4602I

Severity

Information

Long Form

Failed Agent init with Key Manager ({0}).

Short Form

Comms init fail

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

None

Message ID : COM4626I

Severity

Information

Long Form

The agent failed to initialize with the Key Manager. This may indicate that the connection to the server is down, the agent's host has been deleted from the Key Manager, or "Communication Enabled" for the host has not been enabled in the Key Manager UI.

Short Form

No short form is provided for this message type

Description

None

Message ID : COM4627I

Severity

Information

Long Form

The agent's host may no longer be registered with a Key Manager. The agent's host may have been deleted from the Key Manager. You may want to run the register_host utility to re-register the agent with a Key Manager.

Message ID : COM4626I

Short Form

Agent not registered

Parameters

No parameters are provided for this message type

Description

None

Logger COM: Warnings

Message ID : COM4596W

Severity

Warning

Long Form

{0} Logging discarded due to backlog of {1} MB

Short Form

Backlog high

Parameters

Label	CEF Label	Type	Usage
logger	cs4	Text	Name of originating logger
count	vds_count	Numeric	A generic count value

Description

None

Message ID : COM4597W

Severity

Warning

Long Form

{0} Logging resumed due to reduced backlog

Short Form

Backlog OK

Parameters

Label	CEF Label	Type	Usage
logger	cs4	Text	Name of originating logger

Description

None

Message ID : COM4605W

Severity

Warning

Long Form

Logging destination changed from {0} to {1}

Short Form

Upload dest change

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name
url	request	Text	A uniform resource location

Description

None

Message ID : COM4632W

Message ID : COM4605W

Severity

Warning

Long Form

There was a communication failure with the Key Manager. The server returned a fault: {0}{1}; "{2}"; Subcode: "{3}"; Reason: "{4}"; Detail: "{5}".

Short Form

No short form is provided for this message type

Description

None

Message ID : COM4633W

Severity

Warning

Long Form

There was a communication failure with the Key Manager ({0}). The server returned a fault: {1}{2}; "{3}"; Subcode: "{4}"; Reason: "{5}"; Detail: "{6}".

Message ID : COM4632W

Short Form

SOAP client error

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
showStr	reason	Text	Code specifying reason for allowing access, if any
ecode	cn1	Numeric	An error code
context	vds_context	Text	Fault context
subcode	vds_subcode	Text	Fault subcode
showStr	reason	Text	Code specifying reason for allowing access, if any
detail	vds_detail	Text	Fault detail

Description

The agent is unable to reach the key manager. You may see any of the following error messages: COM4583F, COM4633W, VMD3770F, VMD3885I or VMD3886I. You may experience any of the following:

1. Connection to the key manager is down.
2. The VMD Host has been deleted from the key manager.
3. The host does not have "Communication Enabled" in the key manager UI.
4. The VMD's host may be deleted from the key manager. Run the register_host utility to re-register the VMD with the key manager.

Message ID : COM4634W

Severity

Warning

Long Form

The server at {0} attempted to contact this machine, but it was denied access due to an invalid certificate.

Short Form

Bad cert from server

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

An attempt to contact the agent was rejected. This may be due to attempting to register an agent with a new key manager after that agent was registered with a different key manager. A COM4635W log message may give more details.

Message ID : COM4635W

Severity

Warning

Long Form

A machine identifying itself as {0} tried to contact the VMD, but there was an error: {1}{2}; "{3}"; Subcode: "{4}"; Reason: "{5}"; Detail: "{6}".

Short Form

SOAP server error

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
showStr	reason	Text	Code specifying reason for allowing access, if any
ecode	cn1	Numeric	An error code
context	vds_context	Text	Fault context
subcode	vds_subcode	Text	Fault subcode
showStr	reason	Text	Code specifying reason for allowing access, if any
detail	vds_detail	Text	Fault detail

Description

The key manager tried to contact the agent but did not succeed. The "reason" field tells you why the certificate was rejected, and the "detail" field tells you what action was attempted at the time.

Logger DGV: Errors

Message ID : DGV6001E

Severity

Error

Long Form

Memory allocation failed in [{0}] at line [{1}]

Short Form

Out of memory

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6002E

Severity

Error

Long Form

Data governance exception with error [{0}] in [{1}] at line [{2}]

Short Form

Exception

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6003E

Severity

Error

Message ID : DGV6002E

Long Form

Invalid data governance connector type {0}

Short Form

Invalid connector

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6004E

Severity

Error

Long Form

Invalid data governance data source type {0}

Message ID : DGV6003E

Short Form

Invalid data source type

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6005E

Severity

Error

Long Form

HTTP request {0} failed with the status code {1} and message {2}

Short Form

HTTP request failed

Message ID : DGV6004E

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6006E

Severity

Error

Long Form

UUID creation failed with error {0}

Short Form

UUID creation failed

Parameters

No parameters are provided for this message type

Message ID : DGV6005E

Description

None

Message ID : DGV6007E

Severity

Error

Long Form

Type {0} is not found

Short Form

Type not found

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6006E

Message ID : DGV6008E

Severity

Error

Long Form

Attribute {0} value is not found

Short Form

Attribute value not found

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6009E

Severity

Error

Message ID : DGV6008E

Long Form

Failed to get attributes for {0} with error {1}

Short Form

Failed to get file attributes

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6010E

Severity

Error

Long Form

Failed to create the tag directory {0} with error {1}

Message ID : DGV6009E

Short Form

Failed to create tag directory

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6011E

Severity

Error

Long Form

User {0} in domain {1} failed to connect to network path {2}. Error code {3}

Short Form

Net connect error

Parameters

Label	CEF Label	Type	Usage
user	suser	Text	User name
domain	dntdom	Text	A domain name (policy, network, users, etc)
url	request	Text	A uniform resource location
ecode	cn1	Numeric	An error code

Description

None

Message ID : DGV6012E

Severity

Error

Long Form

AWS request exception {0}. Error message {1}

Short Form

AWS request error

Message ID : DGV6011E

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6013E

Severity

Error

Long Form

Failed to add tag {0} to {1}. Error message {2}

Short Form

Failed to add tag

Parameters

No parameters are provided for this message type

Message ID : DGV6012E

Description

None

Message ID : DGV6014E

Severity

Error

Long Form

Failed to delete tag {0} from {1}. Error message {2}

Short Form

Failed to delete tag

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6013E

Message ID : DGV6015E

Severity

Error

Long Form

Failed to initialize tag for {0}

Short Form

Failed to initialize tag

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6016E

Severity

Error

Message ID : DGV6015E

Long Form

Failed to process tagging event. Error message {0}

Short Form

Failed to process tagging event

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6017E

Severity

Error

Long Form

Atlas REST failed with SSL. Error message {0}

Message ID : DGV6016E

Short Form

Atlas REST failed with SSL

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6018E

Severity

Error

Long Form

Failed to get uuid for {0}

Short Form

Failed to get uuid

Message ID : DGV6017E

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7007E

Severity

Error

Long Form

DDC machine learning exception with error [{0}] in [{1}] at line [{2}]

Short Form

Machine learning exception

Parameters

No parameters are provided for this message type

Message ID : DGV6018E

Description

None

Message ID : DGV7009E

Severity

Error

Long Form

Failed to open {0} with errno {1} for the machine learning request {2}

Short Form

Machine learning open error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Message ID : DGV7007E

Description

None

Message ID : DGV7011E

Severity

Error

Long Form

Failed to write {0} with errno {1} for the machine learning request {2}

Short Form

Machine learning write error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : DGV7012E

Severity

Error

Long Form

Failed to read {0} with errno {1} for the machine learning request {2}

Short Form

Machine learning read error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Message ID : DGV7011E

Description

None

Message ID : DGV7014E

Severity

Error

Long Form

DDC machine learning REST failed with SSL. Error message {0}

Short Form

Machine learning REST failed with SSL

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7012E

Message ID : DGV7019E

Severity

Error

Long Form

Failed to download the machine learning model {0} for the request {1}

Short Form

Failed to download machine learning model

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7023E

Severity

Error

Message ID : DGV7019E

Long Form

Invalid scan filter {0}

Short Form

Machine learning invalid scan filter

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7030E

Severity

Error

Long Form

Failed to create the machine learning model {0} for the request {1}

Short Form

Failed to create machine learning model

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7033E

Severity

Error

Long Form

Failed to extract text from {0} for the machine learning request {1}

Short Form

Machine learning failed to extract text

Message ID : DGV7030E

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7038E

Severity

Error

Long Form

Failed the method {0} of the machine learning model {1} for the request {2}: batch size {3}, data size {4} bytes, source {5}

Short Form

Failed the machine learning model method

Parameters

No parameters are provided for this message type

Message ID : DGV7033E

Description

None

Message ID : DGV7041E

Severity

Error

Long Form

Skipped the folder {0}({1}) for the data store {2}({3}) for the machine learning request {4}

Short Form

Machine learning skipped the folder

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7038E

Message ID : DGV7046E

Severity

Error

Long Form

The checksum does not match for {0} of {1} for the machine learning request {2}

Short Form

Machine learning checksum verification failed

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7054E

Severity

Error

Message ID : DGV7046E

Long Form

Failed to send the event: {0}

Short Form

Failed to send the event

Parameters

No parameters are provided for this message type

Description

None

Logger DGV: Information

Message ID : DGV6019I

Severity

Information

Long Form

Starting scan of {0}

Short Form

Starting scan

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6020I

Severity

Information

Long Form

Finished scan of {0} in {1} seconds

Short Form

Finished scan

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV6022I

Severity

Information

Message ID : DGV6020I

Long Form

LDT rekey requested for path [{0}]

Short Form

LDT rekey request

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7001I

Severity

Information

Long Form

Starting the machine learning request {0}

Message ID : DGV6022I

Short Form

Starting machine learning

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7002I

Severity

Information

Long Form

Canceled the machine learning request {0}

Short Form

Canceled machine learning

Message ID : DGV7001I

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7004I

Severity

Information

Long Form

Finished the machine learning request {0}

Short Form

Finished machine learning

Parameters

No parameters are provided for this message type

Message ID : DGV7002I

Description

None

Message ID : DGV7005I

Severity

Information

Long Form

Initializing the machine learning model for the request {0}

Short Form

Initializing machine learning model

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7004I

Message ID : DGV7006I

Severity

Information

Long Form

Initialized the machine learning model for the request {0}

Short Form

Initialized machine learning model

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7008I

Severity

Information

Message ID : DGV7006I

Long Form

Processed {0} files for the machine learning request {1}

Short Form

Machine learning processed

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7010I

Severity

Information

Long Form

Paused the machine learning request {0}

Message ID : DGV7008I

Short Form

Paused machine learning

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7013I

Severity

Information

Long Form

Write {0} files to scan list for the machine learning request {1}

Short Form

Machine learning scanned

Message ID : DGV7010I

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7016I

Severity

Information

Long Form

Stopped the machine learning request {0}

Short Form

Stopped machine learning

Parameters

No parameters are provided for this message type

Message ID : DGV7013I

Description

None

Message ID : DGV7017I

Severity

Information

Long Form

Downloading the machine learning model {0} for the request {1}

Short Form

Downloading machine learning model

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7016I

Message ID : DGV7018I

Severity

Information

Long Form

Downloaded the machine learning model {0} for the request {1}

Short Form

Downloaded machine learning model

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7020I

Severity

Information

Message ID : DGV7018I

Long Form

The machine learning library is started on host {0}

Short Form

Machine learning library started

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7021I

Severity

Information

Long Form

The machine learning library is stopped on host {0}

Message ID : DGV7020I

Short Form

Machine learning library stopped

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7022I

Severity

Information

Long Form

The machine learning library is idle on host {0}

Short Form

Machine learning library idle

Message ID : DGV7021I

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7024I

Severity

Information

Long Form

The language {0} of {1} does not match the model {2} for the machine learning request {3}

Short Form

Machine learning model language mismatch

Parameters

No parameters are provided for this message type

Message ID : DGV7022I

Description

None

Message ID : DGV7025I

Severity

Information

Long Form

The file type {0} of {1} does not match the model {2} for the machine learning request {3}

Short Form

Machine learning model file type mismatch

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7024I

Message ID : DGV7026I

Severity

Information

Long Form

Downloading {0} of {1} for the machine learning request {2}

Short Form

Downloading machine learning file

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7027I

Severity

Information

Message ID : DGV7026I

Long Form

Downloaded {0} of {1} for the machine learning request {2}

Short Form

Downloaded machine learning file

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7028I

Severity

Information

Long Form

Creating the machine learning model {0} for the request {1}

Message ID : DGV7027I

Short Form

Creating machine learning model

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7029I

Severity

Information

Long Form

Created the machine learning model {0} for the request {1}

Short Form

Created machine learning model

Message ID : DGV7028I

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7031I

Severity

Information

Long Form

Extracting text from {0} for the machine learning request {1}

Short Form

Machine learning extracting text

Parameters

No parameters are provided for this message type

Message ID : DGV7029I

Description

None

Message ID : DGV7032I

Severity

Information

Long Form

Extracted text from {0} for the machine learning request {1} in {2} milliseconds

Short Form

Machine learning extracted text

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7031I

Message ID : DGV7034I

Severity

Information

Long Form

Generating file list under the folder {0} for the machine learning request {1}

Short Form

Machine learning generating file list

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7035I

Severity

Information

Message ID : DGV7034I

Long Form

Generated file list under the folder {0} for the machine learning request {1}

Short Form

Machine learning generated file list

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7036I

Severity

Information

Long Form

Calling the method {0} of the machine learning model {1} for the request {2}: batch size {3}, data size {4} bytes, source {5}

Message ID : DGV7035I

Short Form

Calling the machine learning model method

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7037I

Severity

Information

Long Form

Finished the method {0} of the machine learning model {1} for the request {2} in {3} milliseconds: batch size {4}, data size {5} bytes, source {6}

Short Form

Called the machine learning model method

Message ID : DGV7036I

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7039I

Severity

Information

Long Form

Extracted {0} from {1} for the machine learning request {2}

Short Form

Machine learning extracted archive

Parameters

No parameters are provided for this message type

Message ID : DGV7037I

Description

None

Message ID : DGV7040I

Severity

Information

Long Form

The machine learning agent has processed {0} predictions. Suggest to restart the agent.

Short Form

Machine learning processed predictions

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7039I

Message ID : DGV7042I

Severity

Information

Long Form

Resumed the machine learning request {0}

Short Form

Resumed machine learning

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7043I

Severity

Information

Message ID : DGV7042I

Long Form

Automatically paused the machine learning request {0}

Short Form

Automatically paused machine learning

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7044I

Severity

Information

Long Form

Automatically resumed the machine learning request {0}

Short Form

Automatically resumed machine learning

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7045I

Severity

Information

Long Form

The text of {0} is empty for the machine learning request {1}

Short Form

Empty machine learning text

Message ID : DGV7044I

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7049I

Severity

Information

Long Form

The machine learning agent certificate has been changed.

Short Form

Machine learning agent certificate changed

Parameters

No parameters are provided for this message type

Message ID : DGV7045I

Description

None

Message ID : DGV7050I

Severity

Information

Long Form

The agent is slowing down because the machine has {0} percent memory available.

Short Form

Available memory

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7049I

Message ID : DGV7051I

Severity

Information

Long Form

Skipped {0} for the machine learning request {1} because of the file type {2}.

Short Form

Skipped scan due to the file type

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7052I

Severity

Information

Message ID : DGV7051I

Long Form

Generating the embeddings with the machine learning model {0} for the request {1}: entity number {2}, remaining entity number {3}, source {4}

Short Form

Generating entity embeddings

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7053I

Severity

Information

Long Form

Generated the embeddings with the machine learning model {0} for the request {1} in {2} milliseconds: entity number {3}, remaining entity number {4}, source {5}

Message ID : DGV7052I

Short Form

Generated entity embeddings

Parameters

No parameters are provided for this message type

Description

None

Logger DGV: Warnings

Message ID : DGV6021W

Severity

Warning

Long Form

Skipping tags [{0}] for file [{1}]

Short Form

Skipping tags

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7003W

Severity

Warning

Long Form

Finished the machine learning request {0} with error

Short Form

Finished machine learning with error

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7015W

Severity

Warning

Message ID : DGV7003W

Long Form

DDC machine learning does not have value for the configuration {0}

Short Form

Machine learning configuration missing

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7047W

Severity

Warning

Long Form

{0} is an embedding model specified in the prediction request {1} without similarity search enabled.

Short Form

Embedding model without similarity search

Parameters

No parameters are provided for this message type

Description

None

Message ID : DGV7048W

Severity

Warning

Long Form

Skipped {0} for the machine learning request {1} because the file has the character set {2}.

Short Form

Skipped scan due to the character set

Message ID : DGV7047W

Parameters

No parameters are provided for this message type

Description

None

Logger DXF: Debug messages

Message ID : DXF4308D

Severity

Debug

Long Form

No files found in directory {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4310D

Severity

Debug

Long Form

Starting data transform of {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4311D

Severity

Debug

Long Form

Finished data transform of {0}

Short Form

No short form is provided for this message type

Message ID : DXF4310D

Description

None

Message ID : DXF4473D

Severity

Debug

Long Form

Process {0}: error {1} opening lock file at {2}. This may be due to an already running data transform instance

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4475D

Severity

Debug

Message ID : DXF4311D

Long Form

Starting scan of {0}

Short Form

No short form is provided for this message type

Description

None

Logger DXF: Errors

Message ID : DXF3205E

Severity

Error

Long Form

The secfs component doesn't support online data transform on "{0}". Please run the data transform utility without --oxf option to transform the data offline.

Short Form

No online Xform support.

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF3206E

Severity

Error

Long Form

Deep Scan operation is not supported with online data transformation. Please run deep scan without --oxf option.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF3207E

Severity

Error

Long Form

Cannot open or create current status file {0} : {1}

Short Form

No current status file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF3208E

Severity

Error

Long Form

Cannot write current status file {0} : {1}

Message ID : DXF3207E

Short Form

current status file write error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF3209E

Severity

Error

Long Form

Invalid data in current status file {0}

Message ID : DXF3208E

Short Form

Bad current status file content

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3215E

Severity

Error

Long Form

File "{0}" Invalid xf mode.

Short Form

Invalid xf mode.

Message ID : DXF3209E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3216E

Severity

Error

Long Form

File "{0}" vmfs get file system failed.

Short Form

vmfs get file system failed.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF3215E

Description

None

Message ID : DXF3217E

Severity

Error

Long Form

File "{0}" start self access failed.

Short Form

start self access failed.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3216E

Message ID : DXF3218E

Severity

Error

Long Form

File "{0}" File handle is invalid.

Short Form

File handle is invalid.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3219E

Severity

Error

Long Form

File "{0}" failed to get the inode.

Short Form

inode failure

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3220E

Severity

Error

Message ID : DXF3219E

Long Form

File "{0}" failed to get the GuardPoint MD.

Short Form

failed to get the GuardPoint MD.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3221E

Severity

Error

Long Form

File "{0}" failed to get the inode INF information.

Message ID : DXF3220E

Short Form

inode INF failure

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3222E

Severity

Error

Long Form

File "{0}" Inode is null.

Short Form

Inode is null.

Message ID : DXF3221E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3223E

Severity

Error

Long Form

File "{0}" failed to get the file name.

Short Form

inode name failure.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF3222E

Description

None

Message ID : DXF3224E

Severity

Error

Long Form

File "{0}" validation of MD failed.

Short Form

validation of MD failed.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3223E

Message ID : DXF3225E

Severity

Error

Long Form

File "{0}" file MD is null.

Short Form

file MD is null.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3226E

Severity

Error

Long Form

File "{0}" File MD is in the error state.

Short Form

File MD is in the error state.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3227E

Severity

Error

Message ID : DXF3226E

Long Form

File "{0}" Access check failed. Please check your policy.

Short Form

Access check failed. Please check your policy.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3228E

Severity

Error

Long Form

File "{0}" failed while quering the MD from the stream file.

Message ID : DXF3227E

Short Form

failed while quering the MD from the stream file.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3229E

Severity

Error

Long Form

File "{0}" Invalid GP meta data.

Short Form

Invalid GP meta data.

Message ID : DXF3228E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3230E

Severity

Error

Long Form

File "{0}" failed to get the GuardPoint file system.

Short Form

failed to get the GuardPoint file system.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF3229E

Description

None

Message ID : DXF3231E

Severity

Error

Long Form

File "{0}" GuardPoint MD is null.

Short Form

GuardPoint MD is null.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3230E

Message ID : DXF3232E

Severity

Error

Long Form

File "{0}" Rekey failed.

Short Form

Rekey failed.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3233E

Severity

Error

Long Form

File "{0}" Opening the file handle failed.

Short Form

Opening the file handle failed.

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3238E

Severity

Error

Message ID : DXF3233E

Long Form

LDT-ALERT: Scan error on [{0}] removing MDS guard for relaunching dataxform.

Short Form

LDT scan error

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF3239E

Severity

Error

Long Form

LDT-ALERT: Online Dataxfrom failed during post scan stage on [{0}]

Message ID : DXF3238E

Short Form

LDT postscan failure

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF3240E

Severity

Error

Long Form

Failed to initialize the context for container {0}.

Short Form

failed to initialize container

Message ID : DXF3239E

Parameters

Label	Type	Usage
dockerid	Text	Docker image or container id

Description

None

Message ID : DXF3241E

Severity

Error

Long Form

The container {0} is not running.

Short Form

container not running

Parameters

Label	Type	Usage
dockerid	Text	Docker image or container id

Message ID : DXF3240E

Description

None

Message ID : DXF3242E

Severity

Error

Long Form

Verify this is a guard point with valid data transformation policy, and check the system log files for any other problems. It may be due to one or more of following reasons; 1.policy has no valid key rule(s), and/or 2. policy has no key_op rule, and/or 3. policy has valid permit rule(s), and/or 4. policy rule that contains key_op in the action field also specifies other actions, and/or 5. verify that user has not enabled Header Style guardpoint as Offline transformation does not support header based guardpoints 6. Verify if guarding CIFS share with standard policy (new CBC-CS1 Key) for vmfiltr.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF3241E

Message ID : DXF3243E

Severity

Error

Long Form

The file {0} has an invalid header; skipping

Short Form

Skipping invalid header

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3244E

Severity

Error

Long Form

The file {0} was skipped. It has an invalid header

Short Form

Skipped - invalid header

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3245E

Severity

Error

Message ID : DXF3244E

Long Form

The file {0} was previously skipped. It has an invalid header

Short Form

Prev skipped - invalid header

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3246E

Severity

Error

Long Form

Number of files skipped due to an invalid header: {0}

Message ID : DXF3245E

Short Form

Files with invalid header

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF3247E

Severity

Error

Long Form

Number of files previously skipped due to an invalid header: {0}

Short Form

Prev files with invalid header

Message ID : DXF3246E

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF3248E

Severity

Error

Long Form

The file {0} is encrypted with a wrong key; skipping

Short Form

Skipping wrong key

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF3247E

Description

None

Message ID : DXF3249E

Severity

Error

Long Form

The file {0} was skipped. It is encrypted with a wrong key

Short Form

Skipped - wrong key

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3248E

Message ID : DXF3250E

Severity

Error

Long Form

The file {0} was previously skipped. It is encrypted with a wrong key

Short Form

Prev skipped - wrong key

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3251E

Severity

Error

Long Form

Number of files skipped due to a wrong key: {0}

Short Form

Files with wrong key

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF3252E

Severity

Error

Message ID : DXF3251E

Long Form

Number of files previously skipped due to a wrong key: {0}

Short Form

Prev files with wrong key

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4100E

Severity

Error

Long Form

. --deep_scan Perform scan as above with additional file

Message ID : DXF3252E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4101E

Severity

Error

Long Form

. access checks, and estimate time required to

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4100E

Message ID : DXF4102E

Severity

Error

Long Form

. complete data transformation of guard point

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4105E

Severity

Error

Long Form

Number of files previously in error for an unknown reason: {0}

Short Form

Prev unknown file errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4106E

Severity

Error

Long Form

Number of files in error for an unknown reason: {0}

Short Form

Unknown file errors

Message ID : DXF4105E

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4107E

Severity

Error

Long Form

The file {0} was previously in error for an unknown reason

Short Form

Prev error - unknown

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF4106E

Description

None

Message ID : DXF4108E

Severity

Error

Long Form

The file {0} was in error for an unknown reason

Short Form

Prev xform file in error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4107E

Message ID : DXF4109E

Severity

Error

Long Form

Error "{0}" opening lock file in {1}

Short Form

Lock file error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4111E

Severity

Error

Long Form

Process {0}: error "{1}" opening lock file at {2}. This may be due to an already running data transform instance

Short Form

Lock file open error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4112E

Severity

Error

Long Form

Error "{0}" creating lock file in {1}

Short Form

Lock file create fail

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4113E

Severity

Error

Long Form

Cannot create the data transform recovery/status file {0}, {1}

Short Form

Status file create error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4114E

Severity

Error

Long Form

Error "{0}" getting file info for {1}

Short Form

Stat fail

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4115E

Severity

Error

Long Form

Error "{0}" getting file attributes for {1}

Short Form

Attr fail

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4116E

Severity

Error

Long Form

Error "{0}" setting file attributes for {1}

Short Form

Attr set error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4117E

Severity

Error

Long Form

Cannot find files in {0}, {1}

Short Form

File first error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4119E

Severity

Error

Long Form

Error "{0}" setting file time for {1}

Short Form

Time set error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4120E

Severity

Error

Long Form

Cannot recover previous session as file list is missing

Short Form

Missing file list

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4121E

Severity

Error

Message ID : DXF4120E

Long Form

Cannot perform data transform for {0}, not a directory

Short Form

Not a dir

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4124E

Severity

Error

Long Form

The file {0} was skipped. There was insufficient memory to process it

Message ID : DXF4121E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4125E

Severity

Error

Long Form

The file {0} was previously skipped. There was insufficient memory to process it

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4124E

Message ID : DXF4133E

Severity

Error

Long Form

The file {0} was in error. dataxform had insufficient permission

Short Form

Bad perms

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4134E

Severity

Error

Long Form

The file {0} was previously in error. dataxform had insufficient permission

Short Form

Prev error bad perms

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4135E

Severity

Error

Message ID : DXF4134E

Long Form

Number of files in error due to insufficient permission: {0}

Short Form

Perm errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4136E

Severity

Error

Long Form

Number of files previously in error due to insufficient permission: {0}

Message ID : DXF4135E

Short Form

Prev perm errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4137E

Severity

Error

Long Form

The file {0} was in error. There was insufficient memory to process it

Short Form

Out of memory

Message ID : DXF4136E

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4138E

Severity

Error

Long Form

The file {0} was previously in error. There was insufficient memory to process it

Short Form

Prev error - no memory

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF4137E

Description

None

Message ID : DXF4139E

Severity

Error

Long Form

Number of files in error due to insufficient memory: {0}

Short Form

No-memory files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4138E

Message ID : DXF4140E

Severity

Error

Long Form

Number of files previously in error due to insufficient memory: {0}

Short Form

Prev no-memory files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4141E

Severity

Error

Long Form

Directory path too long: {0}

Short Form

Dir too long

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4142E

Severity

Error

Message ID : DXF4141E

Long Form

Unable to process directory {0}

Short Form

Dir in error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4149E

Severity

Error

Long Form

. --preserve_sparse_files Don't encrypt file holes. Not the default

Message ID : DXF4142E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4150E

Severity

Error

Long Form

Removal of data transformation status files completed

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4149E

Message ID : DXF4151E

Severity

Error

Long Form

Removal of data transformation status files abandoned

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4152E

Severity

Error

Long Form

Cleanup-on-success option is only valid with rekey operations

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4153E

Severity

Error

Long Form

. --cleanup_on_success Remove status files upon success

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4152E

Message ID : DXF4155E

Severity

Error

Long Form

The rekey list file provided contains an invalid entry "{0}". Please remove or correct the entry then try again.

Short Form

Invalid rekey file list entry

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4156E

Severity

Error

Long Form

. --unrecoverable Perform rekey without recording recovery data,

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4157E

Severity

Error

Long Form

. which may run considerably faster than a normal

Message ID : DXF4156E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4158E

Severity

Error

Long Form

. rekey, but if it fails restoration of the guarded

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4157E

Message ID : DXF4159E

Severity

Error

Long Form

. data from backup will be required.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4160E

Severity

Error

Long Form

Cannot continue a previous recoverable run with the "--unrecoverable" option set

Short Form

Prev op was recoverable rekey

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4162E

Severity

Error

Long Form

Cannot perform data transform for {0}, failed to get HDFS file name

Short Form

Failed to get HDFS file name

Message ID : DXF4160E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4163E

Severity

Error

Long Form

The file {0} was previously in error. Failed to get HDFS file name

Short Form

Prev error - failed to get HDFS file name

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF4162E

Description

None

Message ID : DXF4164E

Severity

Error

Long Form

Number of files in error due to failure getting HDFS file name: {0}

Short Form

HDFS file name errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4163E

Message ID : DXF4165E

Severity

Error

Long Form

Number of files previously in error due to failure getting HDFS file name: {0}

Short Form

Prev HDFS file name errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4166E

Severity

Error

Long Form

The file {0} was in error. There was insufficient disk space to process it

Short Form

Out of disk space

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4167E

Severity

Error

Message ID : DXF4166E

Long Form

. --cid Specify Docker container id.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4168E

Severity

Error

Long Form

. --migrate Migrate Data from Protect File Encryption.

Short Form

No short form is provided for this message type

Message ID : DXF4167E

Description

None

Message ID : DXF4169E

Severity

Error

Long Form

. --embed Convert all the files to CTE-U embedded header.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4170E

Severity

Error

Message ID : DXF4168E

Long Form

. --update_keyid Update to new keyid after a key migration.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4171E

Severity

Error

Long Form

. --console_level Change the logging level to the console.

Short Form

No short form is provided for this message type

Message ID : DXF4170E

Description

None

Message ID : DXF4172E

Severity

Error

Long Form

. Range: [ALL, TRACE, DEBUG, INFO, WARN, ERROR, OFF] Default: ERROR

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4173E

Severity

Error

Message ID : DXF4171E

Long Form

. --applog_level Override the logging level for the dataxform logs.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4174E

Severity

Error

Long Form

. Range: [ALL, TRACE, DEBUG, INFO, WARN, ERROR, OFF] Default: VMD setting

Short Form

No short form is provided for this message type

Message ID : DXF4173E

Description

None

Message ID : DXF4215E

Severity

Error

Long Form

The file {0} was in error. It was open and could not be modified safely

Short Form

Error open file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4174E

Message ID : DXF4227E

Severity

Error

Long Form

The options --preserve_sparse_files and --encrypt_sparse_file_holes are mutually exclusive

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4228E

Severity

Error

Long Form

. --preserve_sparse_files Don't encrypt file holes. Default behavior

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4229E

Severity

Error

Long Form

. --encrypt_sparse_file_holes The opposite of --preserve_sparse_files

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4228E

Message ID : DXF4230E

Severity

Error

Long Form

. This option has the potential to increase

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4231E

Severity

Error

Long Form

. the amount of space files take up on disk

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4232E

Severity

Error

Long Form

. --buf_size Performance tuning: The size, in KB, of the

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4231E

Message ID : DXF4233E

Severity

Error

Long Form

. buffer used for transforming data

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4234E

Severity

Error

Long Form

. Range: [4..128]. Default: 128

Message ID : DXF4233E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4235E

Severity

Error

Long Form

. --mt Performance tuning: The max. number of

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4234E

Message ID : DXF4236E

Severity

Error

Long Form

. threads that the secfs can use per file

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4237E

Severity

Error

Long Form

. Range: [1..16], Default: 16

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4238E

Severity

Error

Long Form

. --thd Performance tuning: The max. number of

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4237E

Message ID : DXF4239E

Severity

Error

Long Form

. files to transform at once

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4240E

Severity

Error

Long Form

. Range: [1..32]. Defaults: unix:28 win:8

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4241E

Severity

Error

Long Form

More than {0} files were encountered in the directory {1}. This will consume excessive system resources. Aborting. No files have been transformed. To disable this check, rerun with the "--disable_memory_checking" flag

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4243E

Severity

Error

Long Form

. --status_interval The frequency, in seconds, of how often to

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4244E

Severity

Error

Long Form

. report status to the logs. Default: 300

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4247E

Severity

Error

Long Form

Cannot open or create directory listing file {0} : {1}

Short Form

No dir file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : DXF4244E

Description

None

Message ID : DXF4248E

Severity

Error

Long Form

Cannot re-use invalid directory listing file {0}

Short Form

Bad dir file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4247E

Message ID : DXF4249E

Severity

Error

Long Form

Failed to cleanly close directory listing file {0} : {1}

Short Form

Close dir file error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4250E

Severity

Error

Long Form

Cannot rename directory listing file from {0} to {1} :{2}

Short Form

Rename dir file error

Parameters

Label	CEF Label	Type	Usage
oldFilePath	oldFilePath	Text	Previous path to file (for rename and link)
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4251E

Severity

Error

Long Form

Invalid data in listing file {0}

Short Form

Bad dir file content

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4252E

Severity

Error

Long Form

Cannot write directory listing file {0} : {1}

Short Form

Dir file write error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4255E

Severity

Error

Long Form

Inconsistent data in recovery files {0} and {1}.

Short Form

Inconsistent recovery files

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4266E

Message ID : DXF4255E

Severity

Error

Long Form

Error "{0}" updating status file {1}

Short Form

File update error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4270E

Severity

Error

Long Form

Number of files in error due to secfs component stopping data transform: {0}

Short Form

Secfs stop files errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4271E

Severity

Error

Message ID : DXF4270E

Long Form

Number of files in error due to a signal stopping the dataxform: {0}

Short Form

Signal stop files errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4272E

Severity

Error

Long Form

Number of files in error due to being open and could not be modified safely: {0}

Message ID : DXF4271E

Short Form

Unsafe file errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4282E

Severity

Error

Long Form

Error "{0}" reading directory entry {1}

Short Form

Read dir error

Message ID : DXF4272E

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4286E

Severity

Error

Long Form

Number of files previously in error due to secfs component stopping data transform: {0}

Short Form

Prev secfs stop files errors

Message ID : DXF4282E

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4287E

Severity

Error

Long Form

Number of files previously in error due to a signal stopping the dataxform: {0}

Short Form

Prev signal stop files errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Message ID : DXF4286E

Description

None

Message ID : DXF4288E

Severity

Error

Long Form

Number of files previously in error due to being open and could not be modified safely: {0}

Short Form

Prev unsafe file errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4287E

Message ID : DXF4289E

Severity

Error

Long Form

Unable to read {0}: {1}

Short Form

Read info error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4290E

Severity

Error

Long Form

Unable to create simulation file {0}: {1}

Short Form

Create sim file error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4291E

Severity

Error

Long Form

Error creating directory {0}: {1}

Short Form

Create sim dir error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4292E

Severity

Error

Long Form

Error removing directory {0}: {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4294E

Severity

Error

Long Form

About to perform a deep scan

Message ID : DXF4292E

Short Form

Deep scan start

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4295E

Severity

Error

Long Form

-- To enable consistent results, do not access the directory during the scan

Short Form

No short form is provided for this message type

Message ID : DXF4294E

Description

None

Message ID : DXF4296E

Severity

Error

Long Form

-- Transformation simulations will be performed, which may take some time

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4297E

Severity

Error

Message ID : DXF4295E

Long Form

Filesystem containing {0} is too full to perform simulations

Short Form

FS too full for sim

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4298E

Severity

Error

Long Form

Filesystem containing {0} is too full to create file lists

Message ID : DXF4297E

Short Form

FS too full

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4299E

Severity

Error

Long Form

Verify this is a guard point with valid data transformation policy, and check the system log files for any other problems. It may be due to one or more of following reasons; 1.policy has no valid key rule(s), and/or 2. policy has no key_op rule, and/or 3. policy has valid permit rule(s), and/or 4. policy rule that contains key_op in the action field also specifies other actions.

Message ID : DXF4298E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4300E

Severity

Error

Long Form

Out of Memory

Short Form

Out of memory

Parameters

No parameters are provided for this message type

Message ID : DXF4299E

Description

None

Message ID : DXF4301E

Severity

Error

Long Form

The secfs component doesn't support data transform on {0}

Short Form

No xform support

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4300E

Message ID : DXF4302E

Severity

Error

Long Form

Error {0} opening configuration file in {1}

Short Form

Config file error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4303E

Severity

Error

Long Form

Error {0} opening lock file in {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4304E

Severity

Error

Long Form

Error {0} creating lock file in {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4306E

Severity

Error

Long Form

Error invalid version {0} for configuration file in {1}

Short Form

Bad config version

Parameters

Label	CEF Label	Type	Usage
verno	vds_verno	Numeric	A version number
filePath	filePath	Text	Full path to file

Message ID : DXF4304E

Description

None

Message ID : DXF4312E

Severity

Error

Long Form

A file or directory in {0} may be corrupt or unreachable

Short Form

File inaccessible

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4306E

Message ID : DXF4313E

Severity

Error

Long Form

There was an invalid parameter while processing directory {0}

Short Form

Invalid dir param

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4314E

Severity

Error

Long Form

Out of memory while processing directory {0}

Short Form

Out of memory processing dir

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4315E

Severity

Error

Message ID : DXF4314E

Long Form

Error code {0} while processing directory {1}

Short Form

Dir processing error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4325E

Severity

Error

Message ID : DXF4315E

Long Form

Cannot perform data transform for {0}, does not exist

Short Form

Does not exist

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4326E

Severity

Error

Long Form

Cannot perform data transform for {0}, access denied

Message ID : DXF4325E

Short Form

Access denied

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4328E

Severity

Error

Long Form

Secfs component gave unexpected status {0}

Short Form

Unexpected Secfs error

Message ID : DXF4326E

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : DXF4330E

Severity

Error

Long Form

No file name provided to hold recovery file list

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4328E

Message ID : DXF4331E

Severity

Error

Long Form

Cannot open {0} to get recovery file list

Short Form

List access fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4334E

Severity

Error

Long Form

No value provided for command line parameter {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4335E

Severity

Error

Long Form

Unknown command line option {0}

Message ID : DXF4334E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4336E

Severity

Error

Long Form

Command line must specify an operation

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4335E

Message ID : DXF4340E

Severity

Error

Long Form

Command line must specify a guard point

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4341E

Severity

Error

Long Form

Directory specified on command line does not exist, {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4342E

Severity

Error

Long Form

Only one command line operation is allowed if scan is selected

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4341E

Message ID : DXF4343E

Severity

Error

Long Form

Attempt to normalize directory {0} got error code {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4346E

Severity

Error

Long Form

The command line is not valid

Message ID : DXF4343E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4347E

Severity

Error

Long Form

Unable to create the progress-reporting thread

Short Form

Thread create fail

Parameters

No parameters are provided for this message type

Message ID : DXF4346E

Description

None

Message ID : DXF4349E

Severity

Error

Long Form

Cannot set up data transform recovery/status files

Short Form

Status file setup fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4347E

Message ID : DXF4350E

Severity

Error

Long Form

Cannot delete data transform status and lock files

Short Form

Status/lock file delete fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4353E

Severity

Error

Long Form

Check the recovery files for errors, or run "--cleanup" option to remove them.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4354E

Severity

Error

Long Form

Make sure any files already transformed are restored before a cleanup is done.

Short Form

No short form is provided for this message type

Message ID : DXF4353E

Description

None

Message ID : DXF4355E

Severity

Error

Long Form

As the previous dataxform run used the "--unrecoverable" option, you need to restore the GuardPoint from a backup, then use the "--cleanup" option before running the rekey operation again.

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4356E

Severity

Error

Long Form

Could not notify secfs component about data transform on {0}

Short Form

Secfs notify fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4357E

Severity

Error

Message ID : DXF4356E

Long Form

Could not restrict access to {0}

Short Form

Access restrict fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4358E

Severity

Error

Long Form

Could not allow access to {0}

Message ID : DXF4357E

Short Form

Access allow fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4360E

Severity

Error

Long Form

Could not complete data transform, the policy for guard point {0} changed

Short Form

Policy changed

Message ID : DXF4358E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4367E

Severity

Error

Long Form

Data transform got errors on some files

Short Form

Prev xform fail

Parameters

No parameters are provided for this message type

Message ID : DXF4360E

Description

None

Message ID : DXF4368E

Severity

Error

Long Form

The file {0} could not be transformed in the previous data transform, it will not be transformed

Short Form

Prev file xform fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4367E

Message ID : DXF4376E

Severity

Error

Long Form

Data transform in guard point {0} failed for {1} files

Short Form

Prev xform failures

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
nfile	vds_nfile	Numeric	The number of files processed

Description

None

Message ID : DXF4377E

Severity

Error

Long Form

Error while scanning for hard links in directory {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4379E

Severity

Error

Long Form

Error scanning guard point {0} while processing directory {1}

Message ID : DXF4377E

Short Form

Scan error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4381E

Severity

Error

Long Form

Error scanning guard point {0}

Message ID : DXF4379E

Short Form

Scan fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4382E

Severity

Error

Long Form

Automatic data transform cannot be performed on {0}

Short Form

No xform support

Message ID : DXF4381E

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4391E

Severity

Error

Long Form

Data transform of files listed in {0} for guard point {1} failed

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4382E

Message ID : DXF4392E

Severity

Error

Long Form

Error {0} opening configuration file in {1}: does not exist

Short Form

Cfg file error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4393E

Severity

Error

Long Form

Error {0} opening lock file in {1}: does not exist

Short Form

Lock file error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4394E

Severity

Error

Long Form

Error {0} creating lock file in {1}: does not exist

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4395E

Severity

Error

Long Form

Error {0} getting file info for {1}

Message ID : DXF4394E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4396E

Severity

Error

Long Form

Error {0} getting file attributes for {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4395E

Message ID : DXF4400E

Severity

Error

Long Form

Error trying to create a worker thread

Short Form

Threadcreate fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4401E

Severity

Error

Message ID : DXF4400E

Long Form

Error {0} ({1}) trying to delete file {2}

Short Form

Delete file error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4403E

Severity

Error

Message ID : DXF4401E

Long Form

No path provided for recovery information file

Short Form

Missing recovery info

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4404E

Severity

Error

Long Form

Error {0} setting file attributes for {1}

Message ID : DXF4403E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4405E

Severity

Error

Long Form

Error {0} setting file time for {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4404E

Message ID : DXF4407E

Severity

Error

Long Form

Could not determine the Windows installation directory

Short Form

Cannot determine install dir

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4408E

Severity

Error

Message ID : DXF4407E

Long Form

Internal error: thread index {0} is not valid

Short Form

Bad thread id

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4409E

Severity

Error

Long Form

Cannot find files in {0}, error {1}

Message ID : DXF4408E

Short Form

Find first error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : DXF4427E

Severity

Error

Long Form

Failed to authorize this program with the secfs

Message ID : DXF4409E

Short Form

Cannot protect PID

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4430E

Severity

Error

Long Form

The data transformation process was denied permission to access the directory {0}

Short Form

Dir access denied

Message ID : DXF4427E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4432E

Severity

Error

Long Form

Build version: {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4430E

Message ID : DXF4433E

Severity

Error

Long Form

Build ID: {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4434E

Severity

Error

Long Form

Build Date: {0}

Message ID : DXF4433E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4435E

Severity

Error

Long Form

About to perform the requested data transform operation

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4434E

Message ID : DXF4436E

Severity

Error

Long Form

-- Be sure to back up your data

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4437E

Severity

Error

Long Form

-- Please do not access files in the guard point during the transform process

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4438E

Severity

Error

Long Form

-- Please do not attempt to terminate the application

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4437E

Message ID : DXF4439E

Severity

Error

Long Form

Do you wish to continue (y/n)?

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4440E

Severity

Error

Long Form

.Usage:

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4441E

Severity

Error

Long Form

. dataxform {operation} {operation options}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4440E

Message ID : DXF4442E

Severity

Error

Long Form

. where {operation} is the desired operation

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4443E

Severity

Error

Long Form

. --rekey Rekey the files in guard point

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4444E

Severity

Error

Long Form

. --rekey_supported Report if rekey is supported on guard point

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4443E

Message ID : DXF4445E

Severity

Error

Long Form

. --scan Display number of files and directories in

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4446E

Severity

Error

Long Form

. the guard point

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4447E

Severity

Error

Long Form

. --check_links Scan guard point and report any hard links

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4446E

Message ID : DXF4448E

Severity

Error

Long Form

. --cleanup Remove existing status files from a previous

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4449E

Severity

Error

Long Form

. rekey session

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4450E

Severity

Error

Long Form

. --recovery Generate a list of files already rekeyed in

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4449E

Message ID : DXF4451E

Severity

Error

Long Form

. guard point

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4452E

Severity

Error

Long Form

. --rekey_list Only rekey files listed in directive file

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4453E

Severity

Error

Long Form

. --version Display the version number

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4452E

Message ID : DXF4454E

Severity

Error

Long Form

. where {operation options} are parameters for the operation

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4455E

Severity

Error

Long Form

. --gp Specify name of guard point

Message ID : DXF4454E

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4456E

Severity

Error

Long Form

. Required for all operations except --version

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4455E

Message ID : DXF4457E

Severity

Error

Long Form

. --file_list Specify fully qualified name of directive

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4458E

Severity

Error

Long Form

. file for --rekey_list and --recovery

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4459E

Severity

Error

Long Form

. Defaults to dataxform_files in the guard

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4458E

Message ID : DXF4460E

Severity

Error

Long Form

. point directory

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4461E

Severity

Error

Long Form

. --dir_recovery Specify location for status file

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4462E

Severity

Error

Long Form

. Defaults to use log file location if there

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4461E

Message ID : DXF4463E

Severity

Error

Long Form

. is no --status_gp option

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4464E

Severity

Error

Long Form

About to remove the data transformation status files

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4465E

Severity

Error

Long Form

Shutting down data transform: received fatal signal {0}

Short Form

Xform killed by sigal

Parameters

Label	CEF Label	Type	Usage
sig	vds_sig	Numeric	A signal value

Message ID : DXF4464E

Description

None

Message ID : DXF4466E

Severity

Error

Long Form

Could not complete data transform for guard point {0}, data transform was interrupted by a signal

Short Form

Xform interrupted by signal

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4465E

Message ID : DXF4467E

Severity

Error

Long Form

. --preserve_access_time Preserve file access time after rekey

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4468E

Severity

Error

Long Form

. --preserve_modified_time Preserve file modified time after rekey

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4469E

Severity

Error

Long Form

. --nq Suppress prompts

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4468E

Message ID : DXF4470E

Severity

Error

Long Form

. --print_stat Display data transform statistics

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4471E

Severity

Error

Long Form

. --status_gp Write status file to the guard point

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4472E

Severity

Error

Long Form

. directory

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4471E

Message ID : DXF4474E

Severity

Error

Long Form

Process {0}: error {1} opening lock file at {2}. This may be due to an already running data transform instance

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4476E

Severity

Error

Long Form

The file {0} could not be transformed

Message ID : DXF4474E

Short Form

Prev xform file fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4477E

Severity

Error

Long Form

The file {0} could not be transformed, it had error in the previous data transform

Short Form

No short form is provided for this message type

Message ID : DXF4476E

Description

None

Message ID : DXF4478E

Severity

Error

Long Form

The file {0} could not be transformed, it was in progress in the previous data transform

Short Form

Prev xform file in progress

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4477E

Message ID : DXF4479E

Severity

Error

Long Form

The file {0} could not be transformed, the secfs component stopped the data transform

Short Form

Prev xform file stopped by Secfs

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4480E

Severity

Error

Long Form

The file {0} could not be transformed, a signal stopped the data transform

Short Form

Prev xform file stopped by signal

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4482E

Severity

Error

Message ID : DXF4480E

Long Form

Cannot create the data transform recovery/status file {0}, errno {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4483E

Severity

Error

Long Form

Cannot create the data transform recovery/status file {0}, the file name is too long

Short Form

File too long

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4484E

Severity

Error

Long Form

Verify this is a guard point with a data transformation rule, and check the system log files for any other problems

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4483E

Message ID : DXF4486E

Severity

Error

Long Form

Invalid format in recovery file {0}

Short Form

Bad recovery file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4494E

Severity

Error

Long Form

The file {0} was previously in error. The secfs component stopped the data transform

Short Form

Prev error - secfs stop

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4498E

Severity

Error

Message ID : DXF4494E

Long Form

The file {0} was previously in error. A signal stopped the dataxform

Short Form

Prev skipped - signal stop

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4499E

Severity

Error

Long Form

The file {0} was previously in error. It was open and could not be modified safely

Message ID : DXF4498E

Short Form

Prev error file open

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Logger DXF: Fatal errors

Message ID : DXF4431F

Severity

Fatal error

Long Form

Unable to determine the fully qualified host name of this machine: {0}. Please examine your machine's configuration.

Short Form

No short form is provided for this message type

Description

None

Logger DXF: Information

Message ID : DXF3211I

Severity

Information

Long Form

File {0} is being mapped or no-viewed, so it is skipped temporarily and moving on to next file

Short Form

File is being mapped or no-viewed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF3235I

Severity

Information

Long Form

LDT: Live data transform scan phase ran from {0} until {1}

Short Form

OXF run

Parameters

Label	CEF Label	Type	Usage
stime	start	Text	A start time stamp
etime	end	Text	An end time stamp

Description

None

Message ID : DXF3236I

Severity

Information

Long Form

LDT: Live data transform scan operation took {0} hours, {1} minutes and {2} seconds

Short Form

OXF duration

Parameters

Label	CEF Label	Type	Usage
hours	vds_hours	Numeric	Elapsed hours
mins	vds_mins	Numeric	Elaped minutes
secs	vds_secs	Numeric	Elapsed seconds

Description

None

Message ID : DXF3237I

Severity

Information

Long Form

LDT: Live data transformation scan operation took {0} hours, {1} minutes and {2} seconds

Short Form

OXF op duration

Parameters

Label	CEF Label	Type	Usage
hours	vds_hours	Numeric	Elapsed hours
mins	vds_mins	Numeric	Elaped minutes
secs	vds_secs	Numeric	Elapsed seconds

Description

None

Message ID : DXF3237I

Message ID : DXF4122I

Severity

Information

Long Form

Number of files skipped due to insufficient memory: {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4123I

Severity

Information

Long Form

Number of files previously skipped due to insufficient memory: {0}

Message ID : DXF4122I

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4126I

Severity

Information

Long Form

-- This is an estimated time using actual data transformations on test files

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4123I

Message ID : DXF4127I

Severity

Information

Long Form

-- This is an estimated time using simulated data transformations on test files

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4128I

Severity

Information

Long Form

-- The actual transformation time may be more or less than this estimate

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4129I

Severity

Information

Long Form

The file {0} was skipped. It was excluded by policy

Short Form

Skipped file by policy

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF4128I

Description

None

Message ID : DXF4130I

Severity

Information

Long Form

The file {0} was previously skipped. It was excluded by policy

Short Form

Prev skipped file by policy

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4129I

Message ID : DXF4131I

Severity

Information

Long Form

Number of files skipped due to policy exclusion: {0}

Short Form

Skipped files by policy

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4132I

Severity

Information

Long Form

Number of files previously skipped due to policy exclusion: {0}

Short Form

Prev skipped files by policy

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4143I

Severity

Information

Message ID : DXF4132I

Long Form

{0} is not a guard point with a rekey policy applied

Short Form

Xform not supported

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4144I

Severity

Information

Long Form

The deep scan will emulate transformation to derive timing estimates

Message ID : DXF4143I

Short Form

Emulating xforms

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4145I

Severity

Information

Long Form

The file {0} was skipped. It does not exist

Short Form

File missing

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4146I

Severity

Information

Long Form

Number of files skipped due to not existing: {0}

Short Form

Files missing

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Message ID : DXF4145I

Description

None

Message ID : DXF4147I

Severity

Information

Long Form

Number of files previously skipped due to not existing: {0}

Short Form

Prev files missing

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4146I

Message ID : DXF4148I

Severity

Information

Long Form

The file {0} was previously skipped. It does not exist

Short Form

Prev error - file missing

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4154I

Severity

Information

Long Form

The data transform program ran from {0} until {1}

Short Form

Xform run

Parameters

Label	CEF Label	Type	Usage
stime	start	Text	A start time stamp
etime	end	Text	An end time stamp

Description

None

Message ID : DXF4161I

Severity

Information

Long Form

Skipping junction point {0}

Short Form

Junction point

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4200I

Severity

Information

Long Form

The file {0} was skipped. It was an additional hard link

Short Form

Skipped dup hard link

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4201I

Severity

Information

Message ID : DXF4200I

Long Form

The file {0} was skipped. It was a soft link

Short Form

Skipped soft link

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4202I

Severity

Information

Long Form

The file {0} was skipped. It was a dataxform internal file

Message ID : DXF4201I

Short Form

Skipped internal file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4203I

Severity

Information

Long Form

The file {0} was skipped. dataxform had insufficient permission

Short Form

No short form is provided for this message type

Message ID : DXF4202I

Description

None

Message ID : DXF4204I

Severity

Information

Long Form

The file {0} was skipped. It had an ambiguous name

Short Form

Skipped bad name

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4203I

Message ID : DXF4205I

Severity

Information

Long Form

The file {0} was skipped. It was a special file

Short Form

Skipped special file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4206I

Severity

Information

Long Form

The file {0} was skipped. It was exempt from data transform

Short Form

Skipped except file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4207I

Severity

Information

Message ID : DXF4206I

Long Form

The file {0} was skipped. It was a compressed file

Short Form

Skipped compressed file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4208I

Severity

Information

Long Form

The file {0} was skipped. It was an encrypted file

Message ID : DXF4207I

Short Form

Skipped encrypted file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4209I

Severity

Information

Long Form

The file {0} was skipped. It was not a regular file

Short Form

Skipped non-file

Message ID : DXF4208I

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4210I

Severity

Information

Long Form

The file {0} was skipped. There was insufficient memory to process it

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4209I

Message ID : DXF4211I

Severity

Information

Long Form

The file {0} was skipped. It could not be classified

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4212I

Severity

Information

Long Form

The file {0} was skipped. It was no longer present when a transform was attempted

Short Form

File gone away

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4213I

Severity

Information

Long Form

The file {0} was skipped. A transform would have used the same key

Short Form

Skipped - same key

Message ID : DXF4212I

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4214I

Severity

Information

Long Form

The file {0} was skipped. Rekey was not supported for this file

Short Form

Skipped unsupported file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF4213I

Description

None

Message ID : DXF4216I

Severity

Information

Long Form

The file {0} was previously skipped. It was an additional hard link

Short Form

Prev skipped dup link

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4214I

Message ID : DXF4217I

Severity

Information

Long Form

The file {0} was previously skipped. It was a soft link

Short Form

Prev skipped soft link

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4218I

Severity

Information

Long Form

The file {0} was previously skipped. It was a dataxform internal file

Short Form

Prev skipped internal file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4219I

Severity

Information

Message ID : DXF4218I

Long Form

The file {0} was previously skipped. dataxform had insufficient permission

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4220I

Severity

Information

Long Form

The file {0} was previously skipped. It had an ambiguous name

Short Form

Prev skipped bad name

Message ID : DXF4219I

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4221I

Severity

Information

Long Form

The file {0} was previously skipped. It was a special file

Short Form

Prev skipped special file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF4220I

Description

None

Message ID : DXF4222I

Severity

Information

Long Form

The file {0} was previously skipped. It was exempt from data transform

Short Form

Prev skipped exempt file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4221I

Message ID : DXF4223I

Severity

Information

Long Form

The file {0} was previously skipped. It was a compressed file

Short Form

Prev skipped compressed file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4224I

Severity

Information

Long Form

The file {0} was previously skipped. It was an encrypted file

Short Form

Prev skipped encrypted file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4225I

Severity

Information

Message ID : DXF4224I

Long Form

Automatic data transform for guard point {0} deferred, no configuration file

Short Form

No config file

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4226I

Severity

Information

Long Form

The file {0} has the same "to" and "from" keys; skipping

Message ID : DXF4225I

Short Form

Skipping same keys

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4253I

Severity

Information

Long Form

There is no partial data transform for {0} to recover

Short Form

Nothing to recover

Message ID : DXF4226I

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4257I

Severity

Information

Long Form

Number of additional hard links skipped: {0}

Short Form

Hardlinks skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Message ID : DXF4253I

Description

None

Message ID : DXF4258I

Severity

Information

Long Form

Number of soft links skipped: {0}

Short Form

Softlinks skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4257I

Message ID : DXF4259I

Severity

Information

Long Form

Number of files skipped due to insufficient permission: {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4260I

Severity

Information

Long Form

Number of files skipped due to an ambiguous name: {0}

Message ID : DXF4259I

Short Form

Bad name errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4261I

Severity

Information

Long Form

Number of special files skipped: {0}

Short Form

Special files skipped

Message ID : DXF4260I

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4262I

Severity

Information

Long Form

Number of files exempt from data transform skipped: {0}

Short Form

Exempt files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Message ID : DXF4261I

Description

None

Message ID : DXF4263I

Severity

Information

Long Form

Number of compressed files skipped: {0}

Short Form

Compressed files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4262I

Message ID : DXF4264I

Severity

Information

Long Form

Number of encrypted files skipped: {0}

Short Form

Encrypted files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4265I

Severity

Information

Long Form

Number of non-regular files skipped: {0}

Short Form

Non-reg files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4267I

Severity

Information

Message ID : DXF4265I

Long Form

Number of files skipped due to being no longer present when transform attempted: {0}

Short Form

Files gone away

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4268I

Severity

Information

Long Form

Number of files skipped due to a duplicate key: {0}

Message ID : DXF4267I

Short Form

Files with dup key

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4269I

Severity

Information

Long Form

Number of files skipped due to rekey not supported for this file: {0}

Short Form

Unsupported files skipped

Message ID : DXF4268I

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4273I

Severity

Information

Long Form

Number of additional hard links previously skipped: {0}

Short Form

Prev hardlinks skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Message ID : DXF4269I

Description

None

Message ID : DXF4274I

Severity

Information

Long Form

Number of soft links previously skipped: {0}

Short Form

Prev softlinks skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4273I

Message ID : DXF4275I

Severity

Information

Long Form

Number of files previously skipped due to insufficient permission: {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4276I

Severity

Information

Long Form

Number of files previously skipped due to an ambiguous name: {0}

Message ID : DXF4275I

Short Form

Prev bad name errors

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4277I

Severity

Information

Long Form

Number of special files previously skipped: {0}

Short Form

Prev special files skipped

Message ID : DXF4276I

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4278I

Severity

Information

Long Form

Number of files exempt from data transform previously skipped: {0}

Short Form

Prev exempt files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Message ID : DXF4277I

Description

None

Message ID : DXF4279I

Severity

Information

Long Form

Number of compressed files previously skipped: {0}

Short Form

Prev compressed files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4278I

Message ID : DXF4280I

Severity

Information

Long Form

Number of encrypted files previously skipped: {0}

Short Form

Prev encrypted files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4281I

Severity

Information

Long Form

Number of non-regular files previously skipped: {0}

Short Form

Prev non-reg files skipped

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4283I

Severity

Information

Message ID : DXF4281I

Long Form

Number of files previously skipped due to being no longer present when transform attempted: {0}

Short Form

Prev files gone away

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4284I

Severity

Information

Long Form

Number of files previously skipped due to a duplicate key: {0}

Message ID : DXF4283I

Short Form

Prev files with dup key

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4285I

Severity

Information

Long Form

Number of files previously skipped due to rekey not supported for this file: {0}

Short Form

Prev unsupported files skipped

Message ID : DXF4284I

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4293I

Severity

Information

Long Form

Estimated data transformation time for {0} is {1}

Short Form

Estimate duration

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : DXF4285I

Label	CEF Label	Type	Usage
rt	rt	Text	Time of event

Description

None

Message ID : DXF4309I

Severity

Information

Long Form

Building the list of previously transformed files in {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4316I

Severity

Information

Long Form

Status information for directories in guard point

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4317I

Severity

Information

Long Form

Finished processing directory {0}

Short Form

Completed dir

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4318I

Severity

Information

Long Form

Partially processed directory {0}

Short Form

Partially processed dir

Message ID : DXF4317I

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4319I

Severity

Information

Long Form

Skipping directory {0}

Short Form

Skipped dir

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF4318I

Description

None

Message ID : DXF4320I

Severity

Information

Long Form

Skipping empty directory {0}

Short Form

Empty dir

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4319I

Message ID : DXF4321I

Severity

Information

Long Form

Skipping exempt directory {0}

Short Form

Exempt dir

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4322I

Severity

Information

Long Form

Unknown status for directory {0}

Short Form

Dir bad status

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4323I

Severity

Information

Message ID : DXF4322I

Long Form

Directory {0} contains {1} files ({2})

Short Form

Xform to do

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
nfile	vds_nfile	Numeric	The number of files processed

Description

None

Message ID : DXF4329I

Severity

Information

Message ID : DXF4323I

Long Form

Finished check for hard links in {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4332I

Severity

Information

Long Form

Setting recovery-file-list to {0}

Short Form

No short form is provided for this message type

Message ID : DXF4329I

Description

None

Message ID : DXF4344I

Severity

Information

Long Form

Data transform version {0}

Short Form

Datatform

Parameters

Label	CEF Label	Type	Usage
version	vds_version	Text	Software version string

Description

None

Message ID : DXF4332I

Message ID : DXF4345I

Severity

Information

Long Form

Data transform version {0}, using policy {1} on guard point {2}

Short Form

Auto dataxform

Parameters

Label	CEF Label	Type	Usage
version	vds_version	Text	Software version string
pol	cs1	Text	Policy name
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4352I

Severity

Information

Long Form

Data transform for {0} was previously completed

Short Form

Xform prev complete

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4361I

Severity

Information

Long Form

Data transform for guard point {0} finished

Short Form

Xform done

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4362I

Severity

Information

Message ID : DXF4361I

Long Form

Data transform for guard point {0} finished but {1} files were not processed due to errors

Short Form

Xform done with errors

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4363I

Severity

Information

Message ID : DXF4362I

Long Form

Data transform for guard point {0} finished but {1} files were skipped

Short Form

Xform done with skips

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4364I

Severity

Information

Message ID : DXF4363I

Long Form

Data transform for guard point {0} finished but {1} files were not processed due to errors and {2} files were skipped

Short Form

Xform done with errors and skips

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
count	vds_count	Numeric	A generic count value
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4365I

Severity

Information

Message ID : DXF4364I

Long Form

The data transform operation took {0} hours, {1} minutes and {2} seconds

Short Form

Xform duration

Parameters

Label	CEF Label	Type	Usage
hours	vds_hours	Numeric	Elapsed hours
mins	vds_mins	Numeric	Elapsed minutes
secs	vds_secs	Numeric	Elapsed seconds

Description

None

Message ID : DXF4366I

Severity

Information

Message ID : DXF4365I

Long Form

The current operation took {0} hours, {1} minutes and {2} seconds

Short Form

Xform op duration

Parameters

Label	CEF Label	Type	Usage
hours	vds_hours	Numeric	Elapsed hours
mins	vds_mins	Numeric	Elapsed minutes
secs	vds_secs	Numeric	Elapsed seconds

Description

None

Message ID : DXF4369I

Severity

Information

Message ID : DXF4366I

Long Form

Data transform had some files in progress

Short Form

Prev xform incomplete

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4370I

Severity

Information

Long Form

The file {0} was in progress in the previous data transform, it will not be transformed

Message ID : DXF4369I

Short Form

Prev xform file inprogress

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4371I

Severity

Information

Long Form

Data transform skipped some files

Short Form

No short form is provided for this message type

Message ID : DXF4370I

Description

None

Message ID : DXF4372I

Severity

Information

Long Form

The file {0} was skipped in the previous data transform, it will be skipped

Short Form

Prev xform file skipped

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4371I

Message ID : DXF4375I

Severity

Information

Long Form

Data transform last successfully transformed the file {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4378I

Severity

Information

Long Form

Scan found {0} files ({1}) in {2} directories for guard point {3}

Message ID : DXF4375I

Short Form

Scan result

Parameters

Label	CEF Label	Type	Usage
nfile	vds_nfile	Numeric	The number of files processed
ndir	vds_ndir	Numeric	The number of directories processed
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4380I

Severity

Information

Long Form

Transformed {0} files ({1}) of {2} files ({3}) for guard point {4}

Message ID : DXF4378I

Short Form

Scan stats

Parameters

Label	CEF Label	Type	Usage
nfile	vds_nfile	Numeric	The number of files processed
space	vds_space	Text	A string representation of file or disk space
nfiles	vds_nfiles	Numeric	The total number of files in an operation
space	vds_space	Text	A string representation of file or disk space
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4383I

Severity

Information

Message ID : DXF4380I

Long Form

Generating list of files previously transformed on {0}

Short Form

Recovery gen

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4384I

Severity

Information

Long Form

Automatic data transform status for {0}: previous attempt completed

Message ID : DXF4383I

Short Form

Prev auto xform done

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4385I

Severity

Information

Long Form

Automatic data transform status for {0}: previous attempt did not complete

Short Form

Prev auto xform fail

Message ID : DXF4384I

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4386I

Severity

Information

Long Form

Automatic data transform from host {0} for {1}: previous attempt completed

Short Form

Prev auto xform done

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Message ID : DXF4385I

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4387I

Severity

Information

Long Form

Automatic data transform from host {0} for {1}: previous attempt did not complete

Short Form

Prev auto xform fail

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name
gp	fileId	Text	GuardPoint base directory

Message ID : DXF4386I

Description

None

Message ID : DXF4388I

Severity

Information

Long Form

Automatic data transform for {0}: could not get status

Short Form

Auto xform stat fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4387I

Message ID : DXF4389I

Severity

Information

Long Form

Starting data transform of {0} for files listed in {1}

Short Form

Rekey file start

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4390I

Severity

Information

Long Form

Data transform of {0} of {1} files listed in {2} for guard point {3}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4397I

Severity

Information

Long Form

Found {0} references to hard link

Short Form

Hardlink count

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4399I

Severity

Information

Long Form

Hardlink reference {0} {1}

Short Form

Hardlink refs

Message ID : DXF4397I

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4414I

Severity

Information

Long Form

Executing script {0}

Short Form

Exec fail

Message ID : DXF4399I

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4415I

Severity

Information

Long Form

Generating list of files transformed during previous session for guard point {0}

Short Form

List create

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : DXF4414I

Description

None

Message ID : DXF4416I

Severity

Information

Long Form

Writing list of files transformed during previous session for guard point {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4417I

Severity

Information

Message ID : DXF4415I

Long Form

Checking if {0} is a guard point with a rekey policy applied

Short Form

Checking supported

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4418I

Severity

Information

Long Form

Preparing data transform

Message ID : DXF4417I

Short Form

Prepare xform

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4419I

Severity

Information

Long Form

Preparing data transform for next phase of execution

Short Form

xform thread idle

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4420I

Severity

Information

Long Form

Generating list of files to transform in directory {0}

Short Form

Generating list

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : DXF4419I

Description

None

Message ID : DXF4421I

Severity

Information

Long Form

Scanning for hard links in directory {0}

Short Form

Check links

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4420I

Message ID : DXF4422I

Severity

Information

Long Form

Processing the list of files specified in {0}

Short Form

Processing list

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4423I

Severity

Information

Long Form

Processed {0} files ({1}) of {2} files ({3}) in {4}

Short Form

Processed files

Parameters

Label	CEF Label	Type	Usage
nfile	vds_nfile	Numeric	The number of files processed
nfiles	vds_nfiles	Numeric	The total number of files in an operation
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4424I

Message ID : DXF4423I

Severity

Information

Long Form

Processed {0} files ({1}) of {2} files ({3}) in {4}, in progress {5}, completed {6}

Short Form

Processing files

Parameters

Label	CEF Label	Type	Usage
nfile	vds_nfile	Numeric	The number of files processed
nfiles	vds_nfiles	Numeric	The total number of files in an operation
filePath	filePath	Text	Full path to file
scount	vds_scount	Text	A generic count as a string
scount	vds_scount	Text	A generic count as a string

Description

None

Message ID : DXF4425I

Severity

Information

Long Form

Processed {0} files of {1} files specified by {2} in guard point {3}

Short Form

Processed list

Parameters

Label	CEF Label	Type	Usage
nfile	vds_nfile	Numeric	The number of files processed
nfiles	vds_nfiles	Numeric	The total number of files in an operation
filePath	filePath	Text	Full path to file
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4429I

Severity

Information

Long Form

{0} is a guard point with a rekey policy applied

Short Form

Xform supported

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4481I

Severity

Information

Long Form

The file {0} was skipped

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4485I

Severity

Information

Long Form

Data transform last processing was on the file {0}

Message ID : DXF4481I

Short Form

Last file xformed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4487I

Severity

Information

Long Form

The file {0} could not be transformed, it was skipped in a previous data transform

Short Form

No short form is provided for this message type

Message ID : DXF4485I

Description

None

Message ID : DXF4488I

Severity

Information

Long Form

Previous status information relates to a --rekey_file operation.

Short Form

Prev op was rekey

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4487I

Message ID : DXF4489I

Severity

Information

Long Form

Previous status information does not relate to a --rekey_file operation.

Short Form

Prev op was rekey_file

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4490I

Severity

Information

Message ID : DXF4489I

Long Form

Previous status information will be ignored

Short Form

Prev status ignored

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4491I

Severity

Information

Long Form

The file {0} was previously skipped. It was not a regular file

Short Form

Prev skipped non-file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4492I

Severity

Information

Long Form

The file {0} was previously skipped. There was insufficient memory to process it

Short Form

No short form is provided for this message type

Message ID : DXF4491I

Description

None

Message ID : DXF4493I

Severity

Information

Long Form

The file {0} was previously skipped. It could not be classified

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4495I

Severity

Information

Message ID : DXF4492I

Long Form

The file {0} was previously skipped. It was no longer present when a transform was attempted

Short Form

Prev error - file gone

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4496I

Severity

Information

Long Form

The file {0} was previously skipped. A transform would have used the same key

Message ID : DXF4495I

Short Form

Prev skipped - same key

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4497I

Severity

Information

Long Form

The file {0} was previously skipped. Rekey was not supported for this file

Short Form

Prev skipped unsupported file

Message ID : DXF4496I

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Logger DXF: Warnings

Message ID : DXF3210W

Severity

Warning

Long Form

If Shadow Copy was used on your system, you must back up your data before attempting to run dataxform. Once DataXform has been completed, you may restart Shadow Copy. Note, however, that all Shadow Copy backups made prior to running dataxform will be unusable and should be discarded. Attempting to restore your cleartext Shadow Copy backups made prior to running dataxform into your encrypted data will result in data corruption.

Short Form

Shadow copy

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4103W

Severity

Warning

Long Form

Transformation time estimation will be simulated as guard point does not support rekeying

Short Form

No rekey support

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4104W

Severity

Warning

Message ID : DXF4103W

Long Form

Missing {0} references to hard link {1}

Short Form

Missing hardlink refs

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4118W

Severity

Warning

Message ID : DXF4104W

Long Form

Could not return file time for {0} to its original value, got error {1}

Short Form

Time restore error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : DXF4242W

Severity

Warning

Message ID : DXF4118W

Long Form

More than {0} files were encountered in the directory {1}. Dataxform may consume excessive system resources while operating upon this directory. Proceeding

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4254W

Severity

Warning

Long Form

Note: data from a previous dataxform run is being used

Short Form

Prev run data in use

Message ID : DXF4242W

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4307W

Severity

Warning

Long Form

Skipping previously transformed directory {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4254W

Message ID : DXF4324W

Severity

Warning

Long Form

Cannot perform data transform for {0} with identical key

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4327W

Severity

Warning

Long Form

Secfs component returned stop-data-transform status

Message ID : DXF4324W

Short Form

Stopped by Secfs

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4333W

Severity

Warning

Long Form

Unknown version for recovery file list

Short Form

Bad version

Message ID : DXF4327W

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4337W

Severity

Warning

Long Form

Resetting read buffer size to {0}KB

Short Form

Setting buf size

Parameters

Label	CEF Label	Type	Usage
slen	in	Numeric	Input byte count or length

Message ID : DXF4333W

Description

None

Message ID : DXF4338W

Severity

Warning

Long Form

Resetting the maximum number of secfs threads to {0}

Short Form

Number kthreads

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4337W

Message ID : DXF4339W

Severity

Warning

Long Form

Resetting the maximum number of utility threads to {0}

Short Form

Max uthreads

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4351W

Severity

Warning

Long Form

Could not load previous data transform information

Short Form

Recovery file load fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : DXF4359W

Severity

Warning

Message ID : DXF4351W

Long Form

Could not notify secfs component that data transform completed on {0}

Short Form

Secfs notify complete fail

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4373W

Severity

Warning

Long Form

Data transform was previously run on guard point {0}

Message ID : DXF4359W

Short Form

Xform prev completed

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : DXF4398W

Severity

Warning

Long Form

Found {0} references to hard link but expected {1}

Short Form

Hardlink count error

Message ID : DXF4373W

Parameters

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value
count	vds_count	Numeric	A generic count value

Description

None

Message ID : DXF4406W

Severity

Warning

Long Form

Could not return file time for {0} to its original value, got error code {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4410W

Severity

Warning

Long Form

Could not read the Windows registry, section {0}

Short Form

Read read fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : DXF4406W

Message ID : DXF4413W

Severity

Warning

Long Form

Attempted to restrict access to unknown object ID {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : DXF4428W

Severity

Warning

Long Form

Unable to contact Key Manager; will perform all logging to the local log file

Short Form

No short form is provided for this message type

Description

None

Logger FAM: Information

Message ID : FAM7001I

Severity

Information

Long Form

Compact logging enabled

Short Form

CompLog Enabled

Parameters

No parameters are provided for this message type

Description

None

Message ID : FAM7004I

Severity

Information

Long Form

process {0}, action {1}, filePath {2}, oldfilePath {3}, access_code {4}, access_state {5}, action_status {6}, fam_policyname {7}, fam_rule_code {8}, uinfo {9}

Short Form

FAM Audit

Parameters

Label	CEF Label	Type	Usage
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
filePath	filePath	Text	Full path to file
oldFilePath	oldFilePath	Text	Previous path to file (for rename and link)
access_code	access_code	Numeric	Error code returned by the action
access_state	access_state	Text	The action state like CTE PERMIT/DENIED or OS PERMIT/DENIED
action_status	action_status	Text	Identifier if an action was success or failed
fam_policy	fam_policy	Text	FAM Policy name

Label	CEF Label	Type	Usage
fam_rule_code	fam_rule_code	Text	FAM Rule trace
user	suser	Text	User name

Description

None

Message ID : FAM7005I

Severity

Information

Long Form

process {0}, action {1}, filePath {2}, oldfilePath {3}, was_decrypted {4}, is_encrypted {5}, access_code {6}, access_state {7}, action_status {8}, fam_policyname {9}, fam_rule_code {10}, cte_policyname {11}, cte_rule_code {12}, uinfo {13}

Short Form

FAM Audit

Parameters

Label	CEF Label	Type	Usage

Message ID : FAM7004I

850

Label	CEF Label	Type	Usage
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
filePath	filePath	Text	Full path to file
oldFilePath	oldFilePath	Text	Previous path to file (for rename and link)
was_decrypted	was_decrypted	Text	Flag to specify whether file was decrypted or not
is_encrypted	is_encrypted	Text	Flag to specify whether file is encrypted by operation
access_code	access_code	Numeric	Error code returned by the action
access_state	access_state	Text	The action state like CTE PERMIT/DENIED or OS PERMIT/DENIED
action_status	action_status	Text	Identifier if an action was success or failed
fam_policy	fam_policy	Text	FAM Policy name
fam_rule_code	fam_rule_code	Text	FAM Rule trace
cte_policy	cte_policy	Text	CTE Policy name
cte_rule_code	cte_rule_code	Text	CTE Rule trace
user	suser	Text	User name

Description

None

Message ID : FAM7006I

Severity

Information

Long Form

process {0}, action {1}, filePath {2}, access_code {3}, access_state {4}, action_status {5}, fam_policyname {6}, fam_rule_code {7}, uinfo {8}

Short Form

FAM Audit

Parameters

Label	CEF Label	Type	Usage
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
filePath	filePath	Text	Full path to file
access_code	access_code	Numeric	Error code returned by the action
access_state	access_state	Text	The action state like CTE PERMIT/DENIED or OS PERMIT/DENIED
action_status	action_status	Text	Identifier if an action was success or failed

Label	CEF Label	Type	Usage
fam_policy	fam_policy	Text	FAM Policy name
fam_rule_code	fam_rule_code	Text	FAM Rule trace
user	suser	Text	User name

Description

None

Message ID : FAM7007I

Severity

Information

Long Form

process {0}, action {1}, filePath {2}, was_decrypted {3}, is_encrypted {4}, access_code {5}, access_state {6}, action_status {7}, fam_policyname {8}, fam_rule_code {9}, cte_policyname {10}, cte_rule_code {11}, uinfo {12}

Short Form

FAM Audit

Message ID : FAM7006I

853

Parameters

Label	CEF Label	Type	Usage
sproc	sproc	Text	Source process
act	act	Text	Action being requested or performed
filePath	filePath	Text	Full path to file
was_decrypted	was_decrypted	Text	Flag to specify whether file was decrypted or not
is_encrypted	is_encrypted	Text	Flag to specify whether file is encrypted by operation
access_code	access_code	Numeric	Error code returned by the action
access_state	access_state	Text	The action state like CTE PERMIT/DENIED or OS PERMIT/DENIED
action_status	action_status	Text	Identifier if an action was success or failed
fam_policy	fam_policy	Text	FAM Policy name
fam_rule_code	fam_rule_code	Text	FAM Rule trace
cte_policy	cte_policy	Text	CTE Policy name
cte_rule_code	cte_rule_code	Text	CTE Rule trace
user	suser	Text	User name

Description

None

Logger FAM: Warnings

Message ID : FAM7002W

Severity

Warning

Long Form

Compact logging disabled

Short Form

CompLog Disabled

Parameters

No parameters are provided for this message type

Description

None

Logger FUS: Errors

Message ID : FUS3368E

Severity

Error

Long Form

secfs_fuse: {0}

Short Form

secfs_fuse:

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Logger FUS: Information

Message ID : FUS3366I

Severity

Information

Long Form

secfs_fuse: {0}

Short Form

secfs_fuse:

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Logger FUS: Warnings

Message ID : FUS3367W

Severity

Warning

Long Form

secfs_fuse: {0}

Short Form

secfs_fuse:

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Logger POL: Errors

Message ID : POL4556E

Severity

Error

Long Form

ACCESS DENIED on request to {0} database {1}, on hostname {2}. Instance name is {3}, partition {4}, catnode {5}. The timestamp is {6}, and the DB2 version is {7}. The request protocol version is {8}.

Short Form

Access denied by policy

Parameters

Label	CEF Label	Type	Usage
act	act	Text	Action being requested or performed
dbname	vds_dbname	Text	Database name
shost	shost	Text	Source host name
dbinstance	vds_dbinstance	Text	Database instance
dbpart	vds_dbpart	Numeric	Database partition

Label	CEF Label	Type	Usage
node	vds_node	Numeric	A node identifier
rt	rt	Text	Time of event
dbver	vds_dbver	Numeric	Database version
version	vds_version	Text	Software version string

Description

None

Message ID : POL4580E

Severity

Error

Long Form

ACCESS DENIED on request to perform {0} for hostname {1}. Server name is {2}, server number {3}, object id {4}. The timestamp is {5}. The request protocol version is {6}.

Short Form

No short form is provided for this message type

Description

None

Message ID : POL4613E

Severity

Error

Long Form

ACCESS DENIED on request to perform {0} for hostname {1}. Server name is {2}, server number {3}. The timestamp is {4}. The request protocol version is {5}.

Short Form

Access denied

Parameters

Label	CEF Label	Type	Usage
act	act	Text	Action being requested or performed
shost	shost	Text	Source host name
dbinstance	vds_dbinstance	Text	Database instance
dbpart	vds_dbpart	Numeric	Database partition

Message ID : POL4580E

Label	CEF Label	Type	Usage
rt	rt	Text	Time of event
version	vds_version	Text	Software version string

Description

An online policy blocked access. Details of the attempted access are provided in the message fields.

Message ID : POL4701E

Severity

Error

Long Form

Memory allocation failed in [{0}] at line [{1}]

Short Form

Out of memory

Parameters

No parameters are provided for this message type

Description

None

Message ID : POL4704E

Severity

Error

Long Form

EVENT: {0}

Short Form

Event

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : POL4701E

Logger POL: Fatal errors

Message ID : POL4510F

Severity

Fatal error

Long Form

Fatal error while evaluating policy to {0} database {1}, on hostname {2}. Instance name is {3}, partition {4}, catnode {5}. The timestamp is {6}, and the DB2 version is {7}. The request protocol version is {8}.

Short Form

Policy eval error

Parameters

Label	CEF Label	Type	Usage
act	act	Text	Action being requested or performed
dbname	vds_dbname	Text	Database name
shost	shost	Text	Source host name
dbinstance	vds_dbinstance	Text	Database instance
dbpart	vds_dbpart	Numeric	Database partition

Label	CEF Label	Type	Usage
node	vds_node	Numeric	A node identifier
rt	rt	Text	Time of event
dbver	vds_dbver	Numeric	Database version
version	vds_version	Text	Software version string

Description

None

Message ID : POL4516F

Severity

Fatal error

Long Form

Attribute "{0}" parsing error in policy evaluation request.

Short Form

Req parse error

Message ID : POL4510F

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : POL4528F

Severity

Fatal error

Long Form

Attribute "{0}" parsing error in policy evaluation response.

Short Form

Resp parse error

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : POL4516F

Description

None

Message ID : POL4530F

Severity

Fatal error

Long Form

Global restore header invalid. Data corruption has possibly occurred. The restore operation will fail.

Short Form

Global restore header invalid

Parameters

No parameters are provided for this message type

Description

None

Message ID : POL4528F

Message ID : POL4545F

Severity

Fatal error

Long Form

Restore failed: Backup image created with future version.

Short Form

Restore fail - future image

Parameters

No parameters are provided for this message type

Description

None

Message ID : POL4564F

Severity

Fatal error

Long Form

The agent could not allocate enough memory. Contact support.

Short Form

Out of memory

Parameters

No parameters are provided for this message type

Description

None

Message ID : POL4581F

Severity

Fatal error

Long Form

Fatal error while evaluating policy to perform {0} for hostname {1}. Server name is {2}, server number {3}, object id {4}. The timestamp is {5}. The request protocol version is {6}.

Message ID : POL4564F

Short Form

No short form is provided for this message type

Description

None

Message ID : POL4593F

Severity

Fatal error

Long Form

The agent could not evaluate policy. Contact support.

Short Form

Cannot eval policy

Parameters

No parameters are provided for this message type

Message ID : POL4581F

Description

None

Message ID : POL4614F

Severity

Fatal error

Long Form

Fatal error while evaluating policy to perform {0} for hostname {1}. Server name is {2}, server number {3}. The timestamp is {4}. The request protocol version is {5}.

Short Form

Policy eval error

Parameters

Label	CEF Label	Type	Usage
act	act	Text	Action being requested or performed
shost	shost	Text	Source host name
dbinstance	vds_dbinstance	Text	Database instance
dbpart	vds_dbpart	Numeric	Database partition

Message ID : POL4593F

Label	CEF Label	Type	Usage
rt	rt	Text	Time of event
version	vds_version	Text	Software version string

Description

None

Logger POL: Information

Message ID : POL4537I

Severity

Information

Long Form

ACCESS GRANTED on request to {0} database {1}, on hostname {2}. Instance name is {3}, partition {4}, catnode {5}. The timestamp is {6}, and the DB2 version is {7}. The request protocol version is {8}.

Short Form

Access granted

Parameters

Label	CEF Label	Type	Usage
act	act	Text	Action being requested or performed
dbname	vds_dbname	Text	Database name
shost	shost	Text	Source host name
dbinstance	vds_dbinstance	Text	Database instance
dbpart	vds_dbpart	Numeric	Database partition

Label	CEF Label	Type	Usage
node	vds_node	Numeric	A node identifier
rt	rt	Text	Time of event
dbver	vds_dbver	Numeric	Database version
version	vds_version	Text	Software version string

Description

None

Message ID : POL4553I

Severity

Information

Long Form

Internal initialization successful.

Short Form

SDK Init OK

Message ID : POL4537I

Parameters

No parameters are provided for this message type

Description

None

Message ID : POL4573I

Severity

Information

Long Form

Backup failed.

Short Form

Backup fail

Parameters

No parameters are provided for this message type

Message ID : POL4553I

Description

None

Message ID : POL4574I

Severity

Information

Long Form

Restore failed.

Short Form

Restore fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : POL4573I

Message ID : POL4575I

Severity

Information

Long Form

Backup completed successfully.

Short Form

Backup complete OK

Parameters

No parameters are provided for this message type

Description

None

Message ID : POL4576I

Severity

Information

Message ID : POL4575I

Long Form

Restore completed successfully.

Short Form

Restore complete OK

Parameters

No parameters are provided for this message type

Description

None

Message ID : POL4582I

Severity

Information

Long Form

ACCESS GRANTED on request to perform {0} for hostname {1}. Server name is {2}, server number {3}, object id {4}. The timestamp is {5}. The request protocol version is {6}.

Message ID : POL4576I

Short Form

No short form is provided for this message type

Description

None

Message ID : POL4615I

Severity

Information

Long Form

ACCESS GRANTED on request to perform {0} for hostname {1}. Server name is {2}, server number {3}. The timestamp is {4}. The request protocol version is {5}.

Short Form

Access granted

Parameters

Label	CEF Label	Type	Usage
act	act	Text	Action being requested or performed

Message ID : POL4582I

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name
dbinstance	vds_dbinstance	Text	Database instance
dbpart	vds_dbpart	Numeric	Database partition
rt	rt	Text	Time of event
version	vds_version	Text	Software version string

Description

None

Message ID : POL4702I

Severity

Information

Long Form

EVENT: {0}

Short Form

Event

Message ID : POL4615I

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Logger POL: Warnings

Message ID : POL4703W

Severity

Warning

Long Form

EVENT: {0}

Short Form

Event

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Logger VAD: Errors

Message ID : VAD4642E

Severity

Error

Long Form

{0}: {1} Failed to establish communication to Key Manager; return code={2}.

Short Form

Failed to establish communication to key manager

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name
act	act	Text	Action being requested or performed
ecode	cn1	Numeric	An error code

Description

None

Logger VAD: Information

Message ID : VAD4641I

Severity

Information

Long Form

{0}: {1} Successful communication to Key Manager; time= {2}.

Short Form

Successful communication to key manager

Parameters

Label	CEF Label	Type	Usage
func	vds_func	Text	A function name
act	act	Text	Action being requested or performed
etime	end	Text	An end time stamp

Description

None

Logger VAD: Warnings

Message ID : VAD4643W

Severity

Warning

Long Form

{0}: {1}.

Short Form

Tag: Fault

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
detail	vds_detail	Text	Fault detail

Description

None

Logger VMD: Errors

Message ID : VMD3203E

Severity

Error

Long Form

LDT: Live data transformation pause request from "{0}" failed

Short Form

LDT pause failed

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Description

None

Message ID : VMD3204E

Severity

Error

Long Form

LDT: Live data transformation resume request from "{0}" failed

Short Form

LDT resume failed

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Description

None

Message ID : VMD3503E

Severity

Error

Long Form

ReadBioPublicKey Bio_new failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3507E

Severity

Error

Long Form

PEM_read_X509 failed

Message ID : VMD3503E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3509E

Severity

Error

Long Form

X509_extract_key failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3507E

Message ID : VMD3510E

Severity

Error

Long Form

vm_generate_certificate: mkcert RSA_generate_key failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3514E

Severity

Error

Long Form

uname: bad machine name len {0}

Message ID : VMD3510E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3517E

Severity

Error

Long Form

ReadBioPublicKey X509_extract_key failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3514E

Message ID : VMD3520E

Severity

Error

Long Form

set process sid failed

Short Form

Set SID fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3525E

Severity

Error

Message ID : VMD3520E

Long Form

ReadBioX509cert Bio_read_filename failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3527E

Severity

Error

Long Form

PEM_read_PrivateKey {0} read

Short Form

No short form is provided for this message type

Message ID : VMD3525E

Description

None

Message ID : VMD3533E

Severity

Error

Long Form

ReadBioPublicKey failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3544E

Severity

Error

Message ID : VMD3527E

Long Form

The VMD failed to become a daemon.

Short Form

VMD daemonize fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3546E

Severity

Error

Long Form

Can't get NIS domain: {0}

Message ID : VMD3544E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3550E

Severity

Error

Long Form

ReadBioPrivateKey BIO_new failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3546E

Message ID : VMD3559E

Severity

Error

Long Form

ReadBioPublicKey PEM_read_bio_X509 failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3563E

Severity

Error

Long Form

File {0} open failed ({1})

Message ID : VMD3559E

Short Form

File open error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3572E

Severity

Error

Long Form

ReadBioPrivateKey PEM_read_bio_RSAPrivateKey failed {0}

Message ID : VMD3563E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3578E

Severity

Error

Long Form

WriteBioPublicKey PEM_write_bio_X509 failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3572E

Message ID : VMD3581E

Severity

Error

Long Form

WriteBioPrivateKey PEM_write_bio_RSAPrivateKey failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3596E

Severity

Error

Long Form

vm_generate_certificate: Error initializing openssl random number generator

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3597E

Severity

Error

Long Form

setmntent({0}, r) failed {1}({2})

Short Form

setmntent error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : VMD3596E

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3605E

Severity

Error

Long Form

sysinfo failed for uname errno {0} : {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3597E

Message ID : VMD3607E

Severity

Error

Long Form

WriteBioPublicKey Bio_new failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3611E

Severity

Error

Long Form

ReadBioPrivateKey BIO_read_filename failed {0}

Message ID : VMD3607E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3612E

Severity

Error

Long Form

{0}: check_mount({1}, {2}) malloc({3}) failed {4}

Short Form

No memory

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3616E

Severity

Error

Long Form

sysinfo failed for SI_HW_SERIAL errno[{0}][{1}]

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3617E

Severity

Error

Message ID : VMD3612E

Long Form

Failed to protect process {0}.

Short Form

Cannot protect process

Parameters

Label	CEF Label	Type	Usage
pid	dvcpid	Numeric	Numeric process ID

Description

None

Message ID : VMD3628E

Severity

Error

Long Form

WriteBioPrivateKey BIO_write_filename failed {0}

Message ID : VMD3617E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3629E

Severity

Error

Long Form

WriteBioPublicKey BIO_write_filename failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3628E

Message ID : VMD3633E

Severity

Error

Long Form

ReadBioX509cert PEM_read_bio_X509 failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3644E

Severity

Error

Long Form

NIS get group error: {0}

Message ID : VMD3633E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3645E

Severity

Error

Long Form

{0}: check_mount({1}, {2}) realloc({3}) failed {4}

Short Form

No memory

Parameters

No parameters are provided for this message type

Message ID : VMD3644E

Description

None

Message ID : VMD3651E

Severity

Error

Long Form

check_mount: mnttab open failed {0}

Short Form

Mnttab open error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3645E

Message ID : VMD3655E

Severity

Error

Long Form

vm_generate_certificate: mkcert EVP_PKEY_new failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3665E

Severity

Error

Long Form

WriteBioPrivateKey BIO_new failed {0}

Message ID : VMD3655E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3666E

Severity

Error

Long Form

ReadBioPrivateKey failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3665E

Message ID : VMD3667E

Severity

Error

Long Form

Error: can't load public key

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3674E

Severity

Error

Long Form

Failed to alloc mem for Host Key

Message ID : VMD3667E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3676E

Severity

Error

Long Form

ReadBioX509cert Bio_new failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3674E

Message ID : VMD3681E

Severity

Error

Long Form

Failed to open {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3683E

Severity

Error

Long Form

TEST HOST key failed {0}

Message ID : VMD3681E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3685E

Severity

Error

Long Form

ReadPrivateKey failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3683E

Message ID : VMD3686E

Severity

Error

Long Form

SET machine id failed {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3689E

Severity

Error

Long Form

X509 certificate file {0} open failed

Message ID : VMD3686E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3697E

Severity

Error

Long Form

vm_generate_certificate: mkcert failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3689E

Message ID : VMD3700E

Severity

Error

Long Form

Unable to create or write to file {0} as part of a policy update. Error code {1}.

Short Form

Policy update error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

Verify that the secfsd process is running; if not, restart it. If sesfsd is running, please call Thales support for assistance.

Message ID : VMD3702E

Severity

Error

Long Form

NIS get passwd error: {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3707E

Severity

Error

Long Form

vm_generate_certificate: mkcert EVP_PKEY_assign_RSA failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3713E

Severity

Error

Long Form

vm_get_pubkey_from_file: Read key file {0} failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3707E

Message ID : VMD3718E

Severity

Error

Long Form

vm_get_privkey_from_file: Read key file {0} failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3723E

Severity

Error

Long Form

ReadBioPublicKey Bio_read_filename failed {0}

Message ID : VMD3718E

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3724E

Severity

Error

Long Form

Private Key file {0} open failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3723E

Message ID : VMD3726E

Severity

Error

Long Form

mount_sec: {0} mount failed {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3730E

Severity

Error

Long Form

sysinfo: failed for SI_HW_SERIAL.

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3734E

Severity

Error

Long Form

sysinfo failed for SI_SYSNAME errno {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3730E

Message ID : VMD3736E

Severity

Error

Long Form

hpux_sysinfo: invalid buffer length

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3747E

Severity

Error

Long Form

can not write to file={0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3748E

Severity

Error

Long Form

Failed to read Host Private Key from file {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3747E

Message ID : VMD3750E

Severity

Error

Long Form

uname failed! errno[{0}][{1}]

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3758E

Severity

Error

Long Form

{0}: {1}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3759E

Severity

Error

Long Form

write() ssl error {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3758E

Message ID : VMD3760E

Severity

Error

Long Form

Server does not support required soap operation: {0}

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3761E

Severity

Error

Long Form

The server name could not be converted to an IP address. Service will restart.

Message ID : VMD3760E

Short Form

Cannot get server IP

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3779E

Severity

Error

Long Form

Unable to create a signature for file {0}; error code {1}.

Short Form

Sig creation error

Message ID : VMD3761E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3780E

Severity

Error

Long Form

Unable to encrypt file {0} with the session key; error code {1}.

Short Form

File encrypt error

Message ID : VMD3779E

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3782E

Severity

Error

Long Form

A new security configuration was received, but we failed to implement it. The current security configuration will continue to be used.

Short Form

Config update fail

Message ID : VMD3780E

Parameters

No parameters are provided for this message type

Description

An error occurred while attempting to process a policy push from a key manager. Details of the failure were logged in the preceding message.

Message ID : VMD3784E

Severity

Error

Long Form

Secfs component failed to provide initialization information to VMD.

Short Form

No config from secfs

Parameters

No parameters are provided for this message type

Message ID : VMD3782E

Description

None

Message ID : VMD3786E

Severity

Error

Long Form

Host file browsing for {0} failed.

Short Form

Host browse fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3784E

Message ID : VMD3787E

Severity

Error

Long Form

Unable to get status from secfs component. Error code {0}.

Short Form

Secfs config fetch error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3788E

Severity

Error

Long Form

Unable to send data to secfs component. Error code {0}.

Short Form

Kernel config send error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3789E

Severity

Error

Message ID : VMD3788E

Long Form

Unable to receive data from secfs component. Error code {0}.

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3790E

Severity

Error

Long Form

Secfs component did not confirm host-delete operation.

Short Form

No host-delete ACK

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3792E

Severity

Error

Long Form

Unable to write authorized file information to disk. Error code {0}.

Short Form

Write auth file error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Message ID : VMD3790E

Description

None

Message ID : VMD3795E

Severity

Error

Long Form

Query security config failed.

Short Form

Query config fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3792E

Message ID : VMD3796E

Severity

Error

Long Form

Secfs component reports failure on host-delete operation.

Short Form

Host delete fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3799E

Severity

Error

Long Form

Delete host operation failed.

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3801E

Severity

Error

Long Form

Cannot update service status. Error = {0}

Short Form

Service update error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3802E

Severity

Error

Long Form

Cannot set service status to stopped. Error = {0}

Short Form

Service stop error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Message ID : VMD3801E

Description

None

Message ID : VMD3807E

Severity

Error

Long Form

Cannot register service handler. Error = {0}

Short Form

Register server error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3802E

Message ID : VMD3809E

Severity

Error

Long Form

Cannot start service dispatcher. Error = {0}

Short Form

Start service error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3811E

Severity

Error

Long Form

User {0} in domain {1} failed to connect to network path {2}. Error code {3}.

Short Form

Net connect error

Parameters

Label	CEF Label	Type	Usage
user	suser	Text	User name
domain	dntdom	Text	A domain name (policy, network, users, etc)
url	request	Text	A uniform resource location
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3812E

Severity

Error

Long Form

Failed to enumerate network path {0}. Error code {1}.

Short Form

Net enumeration error

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3816E

Severity

Error

Long Form

Failed to initialize the signature request {0}

Short Form

Init sig req fail

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3819E

Severity

Error

Long Form

Failed to generate the file list for the signature request {0}

Short Form

Sig file list fail

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3822E

Severity

Error

Message ID : VMD3819E

Long Form

Failed to generate the signatures for the signature request {0}

Short Form

Sig gen fail

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3828E

Severity

Error

Long Form

Failed the signature request {0}

Message ID : VMD3822E

Short Form

Sig req fail

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3830E

Severity

Error

Long Form

Failed to read the file list for the signature request {0}, error code {1}

Short Form

Sig file list read error

Message ID : VMD3828E

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3831E

Severity

Error

Long Form

Failed to write the file list for the signature request {0}, error code {1}

Short Form

Sig file list write error

Message ID : VMD3830E

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3833E

Severity

Error

Long Form

Failed to create the signature disk object

Short Form

Create sig disk object fail

Message ID : VMD3831E

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3834E

Severity

Error

Long Form

Failed to add the signature {0} and name {1} into the signature disk object

Short Form

Add sig object error

Parameters

Label	CEF Label	Type	Usage
hex	vds_hex	Text	A hex string (e.g. a signature)
filePath	filePath	Text	Full path to file

Message ID : VMD3833E

Description

None

Message ID : VMD3835E

Severity

Error

Long Form

Failed to write the signature disk file

Short Form

Write sig object fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3834E

Message ID : VMD3837E

Severity

Error

Long Form

Failed to write the signature disk file header

Short Form

Sig write header fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3838E

Severity

Error

Message ID : VMD3837E

Long Form

Failed to read the signature disk file header

Short Form

Sig read hreader fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3840E

Severity

Error

Long Form

Failed to push a new signature database

Message ID : VMD3838E

Short Form

Sig push to secfs fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3843E

Severity

Error

Long Form

User browsing for {0} failed.

Short Form

User browse fail

Message ID : VMD3840E

Parameters

Label	CEF Label	Type	Usage
domain	dntdom	Text	A domain name (policy, network, users, etc)

Description

None

Message ID : VMD3844E

Severity

Error

Long Form

Failed to bind to {0}. Error code {1}.

Short Form

Domain bind error

Parameters

Label	CEF Label	Type	Usage
domain	dntdom	Text	A domain name (policy, network, users, etc)

Message ID : VMD3843E

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3845E

Severity

Error

Long Form

Failed to query the domain {0} by {1}. Error {2}: {3}.

Short Form

NIS query error

Parameters

Label	CEF Label	Type	Usage
domain	dntdom	Text	A domain name (policy, network, users, etc)
effect	vds_effect	Text	Policy effect

Message ID : VMD3844E

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3846E

Severity

Error

Long Form

Failed to query the group {0} in the domain {1} by {2}. Error {3}: {4}.

Short Form

NIS group query error

Parameters

Label	CEF Label	Type	Usage
group	vds_group	Text	Group name

Message ID : VMD3845E

Label	CEF Label	Type	Usage
domain	dntdom	Text	A domain name (policy, network, users, etc)
effect	vds_effect	Text	Policy effect
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3848E

Severity

Error

Long Form

Domain browsing failed.

Short Form

Domain browse fail

Message ID : VMD3846E

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3849E

Severity

Error

Long Form

Error getting common name: {0}

Short Form

Cannot determine common name

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : VMD3848E

Description

None

Message ID : VMD3855E

Severity

Error

Long Form

Failed to send {0} signatures for the signature request {1} to the Key Manager

Short Form

Send sigs error

Parameters

Label	CEF Label	Type	Usage
nsig	vds_nsig	Numeric	The number of signatures generated
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : VMD3849E

Description

None

Message ID : VMD3858E

Severity

Error

Long Form

The Secfs component was unable to implement the new security configuration

Short Form

New config to Secfs fail

Parameters

No parameters are provided for this message type

Description

An error occurred while attempting to apply a policy push from a key manager.

Message ID : VMD3855E

Message ID : VMD3864E

Severity

Error

Long Form

Unable to parse LDAP URL {0} - error "{1}"

Short Form

Bad LDAP url

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3865E

Severity

Error

Long Form

Unable to query LDAP server {0} - error "{1}"

Short Form

Bad LADP server

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3866E

Severity

Error

Long Form

Invalid LDAP posixAccount data returned

Short Form

Invalid LDAP account

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3867E

Severity

Error

Message ID : VMD3866E

Long Form

Invalid LDAP posixGroup data returned

Short Form

Invalid LDAP group

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3872E

Severity

Error

Long Form

Internal error: bad arguments to secfs component

Message ID : VMD3867E

Short Form

Bad args to Secfs

Parameters

No parameters are provided for this message type

Description

An internal error occurred. Please contact Thales Support

Message ID : VMD3873E

Severity

Error

Long Form

Internal error: the secfs component does not believe it's talking to the correct VMD

Short Form

Secfs rejecting VMD

Message ID : VMD3872E

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3874E

Severity

Error

Long Form

The secfs component is unable to read its private key

Short Form

Secfs priv key fail

Parameters

No parameters are provided for this message type

Message ID : VMD3873E

Description

None

Message ID : VMD3875E

Severity

Error

Long Form

The secfs component unable to obtain its PWD

Short Form

Secfs passwd fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3874E

Message ID : VMD3876E

Severity

Error

Long Form

The secfs component contains an invalid PWD

Short Form

Secfs passwd bad

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3877E

Severity

Error

Long Form

The secfs component was unable to extract the key-encrypting-key

Short Form

Secfs key extract fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3878E

Severity

Error

Long Form

The secfs component failed to pass internal sanity checks around the key-encrypting-key

Message ID : VMD3877E

Short Form

Secfs key sanity fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3879E

Severity

Error

Long Form

The secfs component was able to perform all of the crypto operations around the policy push, but was unable to actually apply the new policy configuration

Short Form

Secfs policy apply fail

Message ID : VMD3878E

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3888E

Severity

Error

Long Form

Unable to replicate coherent guardpoint info - {0}

Short Form

Unable to replicate coherent GuardPoint info -

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : VMD3879E

Description

None

Message ID : VMD3890E

Severity

Error

Long Form

Unable to commit configuration to GPFS cluster

Short Form

Unable to commit configuration to GPFS cluster

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3888E

Message ID : VMD3891E

Severity

Error

Long Form

Non-clustered GP {0} not allowed on clustered filesystem

Short Form

Non-clustered GP not allowed on clustered filesystem

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : VMD3892E

Severity

Error

Long Form

Clustered GP {0} not allowed on non-clustered filesystem

Short Form

Clustered GP not allowed on non-clustered filesystem

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : VMD3901E

Severity

Error

Message ID : VMD3892E

Long Form

Docker host browsing failed.

Short Form

Docker host browse fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3903E

Severity

Error

Long Form

Docker host browsing for image {0} failed.

Message ID : VMD3901E

Short Form

Docker host browse fail

Parameters

Label	Type	Usage
dockerid	Text	Docker image or container id

Description

None

Message ID : VMD3905E

Severity

Error

Long Form

Docker image {0} file browsing for {1} failed.

Short Form

Docker image file browse fail

Message ID : VMD3903E

Parameters

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3907E

Severity

Error

Long Form

Docker container {0} file browsing for {1} succeeded.

Short Form

Docker container file browse fail

Message ID : VMD3905E

Parameters

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3909E

Severity

Error

Long Form

User browsing for image {0} with {1} failed.

Short Form

Docker image user browse fail

Message ID : VMD3907E

Parameters

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id
domain	dntdom	Text	A domain name (policy, network, users, etc)

Description

None

Message ID : VMD3911E

Severity

Error

Long Form

User browsing for container {0} with {1} failed.

Short Form

Docker container user browse fail

Message ID : VMD3909E

Parameters

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id
domain	dntdom	Text	A domain name (policy, network, users, etc)

Description

None

Message ID : VMD3913E

Severity

Error

Long Form

Domain browsing for image {0} failed.

Short Form

Docker image domain browse fail

Message ID : VMD3911E

Parameters

Label	Type	Usage
dockerid	Text	Docker image or container id

Description

None

Message ID : VMD3915E

Severity

Error

Long Form

Domain browsing for container {0} failed.

Short Form

Docker container domain browse fail

Parameters

Label	Type	Usage
dockerid	Text	Docker image or container id

Message ID : VMD3913E

Description

None

Message ID : VMD3916E

Severity

Error

Long Form

The current docker version "{0} {1}" is not supported.

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3917E

Severity

Error

Message ID : VMD3915E

Long Form

Failed to connect to the Docker service at {0}. Please make sure the Docker service is up.

Short Form

Failed to connect to Docker

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

None

Message ID : VMD3918E

Severity

Error

Long Form

An unauthorized attempt to update the authentication signature for file {0} has been prevented

Message ID : VMD3917E

Short Form

Unauthorized signature change

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3922E

Severity

Error

Long Form

Internal error: unable to determine {0}.

Short Form

Unable to determine

Message ID : VMD3918E

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3923E

Severity

Error

Long Form

Error from data governance module: {0}

Short Form

DG error

Parameters

No parameters are provided for this message type

Message ID : VMD3922E

Description

None

Message ID : VMD3927E

Severity

Error

Long Form

An error occurred during certificate renewal: re-registration may be required

Short Form

Cert recovery failed

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3923E

Message ID : VMD3929E

Severity

Error

Long Form

Key manager failed to update CA certificate: {0}

Short Form

CA update failed

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3932E

Severity

Error

Long Form

The CTE client has failed attestation checks.

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD4245E

Severity

Error

Long Form

Key conversion failure when attempting to upgrade to fips-approved private key file format.

Message ID : VMD3932E

Short Form

Key conv fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD4594E

Severity

Error

Long Form

Failed to strengthen priority of the vmd, may face scheduling problems

Short Form

Cannot raise priority

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD4606E

Severity

Error

Long Form

vm_read_file: fstat failed {0}

Short Form

Stat error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Message ID : VMD4594E

Description

None

Message ID : VMD4607E

Severity

Error

Long Form

vm_read_file: fopen failed for {0} errno {1}

Short Form

Open error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD4608E

Severity

Error

Long Form

vm_read_file: malloc for size {0} failed {1}

Short Form

Out of memory

Parameters

Label	CEF Label	Type	Usage
slen	in	Numeric	Input byte count or length
ecode	cn1	Numeric	An error code

Message ID : VMD4607E

Description

None

Message ID : VMD4609E

Severity

Error

Long Form

vm_read_file: read() failed for {0}

Short Form

Read error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD4608E

1000

Message ID : VMD4610E

Severity

Error

Long Form

vm_write_file: fopen failed for {0} mode {1} errno {2}

Short Form

File open error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
mode	vds_mode	Text	File open mode
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD4612E

Severity

Error

Long Form

vm_write_file: fwrite() failed error {0}

Short Form

Write error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD4617E

Severity

Error

Long Form

The previous message {0} was repeated {1} times

Short Form

Repeat message

Parameters

Label	CEF Label	Type	Usage
msgid	vds_msgid	Text	A unique log message identifier
count	vds_count	Numeric	A generic count value

Description

None

Logger VMD: Fatal errors

Message ID : VMD3767F

Severity

Fatal error

Long Form

No attribute {0} was found in the configuration file located at {1}. Please supply this attribute or re-install the product and try again.

Short Form

Attribute missing

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3768F

Severity

Fatal error

Long Form

Unable to parse the URL {0}. This attribute is located in the config file at {1}. Please fix the URL or re-install this product.

Short Form

Bad URL in config file

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3769F

Severity

Fatal error

Long Form

Internal error: unable to set attribute {0}.

Short Form

Bad attribute

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3770F

Severity

Fatal error

Long Form

The VMD failed to establish a communication channel to the Key Manager.

Short Form

Cannot contact server

Parameters

No parameters are provided for this message type

Description

The agent is unable to reach the key manager. You may see any of the following error messages: COM4583F, COM4633W, VMD3770F, VMD3885I or VMD3886I. You may experience any of the following:

1. Connection to the key manager is down.
2. The VMD Host has been deleted from the key manager.
3. The host does not have "Communication Enabled" in the key manager UI.
4. The VMD's host may be deleted from the key manager. Run the register_host utility to re-register the VMD with the key manager.

Message ID : VMD3771F

Severity

Fatal error

Long Form

Logging setup failure. Error code {0}; "{1}"

Short Form

Log setup error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3772F

Severity

Fatal error

Long Form

Logging setup failure: VMD logger information not found in Key Manager response.

Short Form

Missing logger info

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3797F

Severity

Fatal error

Message ID : VMD3772F

Long Form

The VMD is unable to listen for requests from the Key Manager. Shutting down.

Short Form

Cannot list for server req.

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3894F

Severity

Fatal error

Long Form

The server does not support required oneway communications.

Message ID : VMD3797F

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD4595F

Severity

Fatal error

Long Form

The agent could not allocate enough memory. Contact support.

Short Form

Out of memory

Parameters

No parameters are provided for this message type

Message ID : VMD3894F

Description

None

Message ID : VMD4616F

Severity

Fatal error

Long Form

The previous message {0} was repeated {1} times

Short Form

Repeat message

Parameters

Label	CEF Label	Type	Usage
msgid	vds_msgid	Text	A unique log message identifier
count	vds_count	Numeric	A generic count value

Message ID : VMD4595F

Description

None

Logger VMD: Information

Message ID : VMD3201I

Severity

Information

Long Form

LDT: Live data transformation has been paused by "{0}"

Short Form

LDT paused

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Description

None

Message ID : VMD3202I

Severity

Information

Long Form

LDT: Live data transformation has been resumed by "{0}"

Short Form

LDT resumed

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Description

None

Message ID : VMD3548I

Severity

Information

Long Form

RSA key verification Failed

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3558I

Severity

Information

Long Form

RSA key verified

Message ID : VMD3548I

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3626I

Severity

Information

Long Form

{0} is MOUNTED

Short Form

Mount success

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Message ID : VMD3558I

Description

None

Message ID : VMD3640I

Severity

Information

Long Form

STARTED on {0} PORT {1} VERSION: {2}

Short Form

VMD Startup

Parameters

Label	CEF Label	Type	Usage
osname	cs2	Text	A name identifying the agent operating system
port	spt	Numeric	A socket port number
version	vds_version	Text	Software version string

Message ID : VMD3626I

Description

None

Message ID : VMD3663I

Severity

Information

Long Form

{0} is not mounted

Short Form

Mount fail

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3640I

Message ID : VMD3773I

Severity

Information

Long Form

The {0} is starting. It was invoked at the command line like this: "{1}"

Short Form

VMD startup

Parameters

Label	CEF Label	Type	Usage
agent	deviceProcessName	Text	The short identifier of the agent software
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3778I

Severity

Information

Long Form

The VMD is shutting down.

Short Form

VMD shutdown

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3781I

Severity

Information

Message ID : VMD3778I

Long Form

Successfully received and implemented a new security configuration.

Short Form

New Config OK

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3785I

Severity

Information

Long Form

Host file browsing for {0} succeeded.

Message ID : VMD3781I

Short Form

Host browse OK

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3794I

Severity

Information

Long Form

Query security config succeeded.

Short Form

Query config OK

Message ID : VMD3785I

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3798I

Severity

Information

Long Form

Delete host operation succeeded.

Short Form

Host delete OK

Parameters

No parameters are provided for this message type

Message ID : VMD3794I

Description

None

Message ID : VMD3800I

Severity

Information

Long Form

RESTARTED SDK Server at PORT {0}.

Short Form

SDK server restart

Parameters

Label	CEF Label	Type	Usage
port	spt	Numeric	A socket port number

Description

None

Message ID : VMD3798I

Message ID : VMD3803I

Severity

Information

Long Form

Shutting down file system service.

Short Form

Service stop

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3804I

Severity

Information

Long Form

Stopping file system service...

Short Form

Service shutdown

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3814I

Severity

Information

Long Form

Initializing the signature request {0}

Message ID : VMD3804I

Short Form

Init sig req start

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3815I

Severity

Information

Long Form

Finished initializing the signature request {0}

Short Form

Init sig req end

Message ID : VMD3814I

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3817I

Severity

Information

Long Form

Generating the file list for the signature request {0}

Short Form

Gen sig file list

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : VMD3815I

Description

None

Message ID : VMD3818I

Severity

Information

Long Form

Finished generating the file list for the signature request {0}. Number of files in the list: {1}

Short Form

Sig file list complete

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
nfile	vds_nfile	Numeric	The number of files processed

Message ID : VMD3817I

Description

None

Message ID : VMD3820I

Severity

Information

Long Form

Generating the signatures for the signature request {0}

Short Form

Generating sigs

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3818I

Message ID : VMD3821I

Severity

Information

Long Form

Finished generating the signatures for the signature request {0}. Number of processed files: {1}. Number of generated signatures: {2}. Number of failed files: {3}

Short Form

Generated sigs

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
nfile	vds_nfile	Numeric	The number of files processed
nsig	vds_nsig	Numeric	The number of signatures generated
nerror	vds_nerror	Numeric	The number of errors encountered

Description

None

Message ID : VMD3823I

Severity

Information

Long Form

Failed to get the file attributes for {0}, error code {1}, error message: {2}

Short Form

Sig file attr error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
ecode	cn1	Numeric	An error code
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : VMD3821I

Description

None

Message ID : VMD3825I

Severity

Information

Long Form

Generating the signatures for the signature request {0}, {1} out of {2} files have been processed

Short Form

Sig progress

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
nsig	vds_nsig	Numeric	The number of signatures generated
nfile	vds_nfile	Numeric	The number of files processed

Message ID : VMD3823I

Description

None

Message ID : VMD3827I

Severity

Information

Long Form

Completed the signature request {0} successfully

Short Form

Sig sig req done

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3825I

Message ID : VMD3829I

Severity

Information

Long Form

Canceled the signature request {0}

Short Form

Sig req cancelled

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3832I

Severity

Information

Long Form

Generating the file list for the signature request {0}, {1} files have been written to the list

Short Form

Sig file generation in progress

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
nfile	vds_nfile	Numeric	The number of files processed

Description

None

Message ID : VMD3836I

Severity

Information

Long Form

Finished writing the signature disk file

Short Form

Sig write complete

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3839I

Severity

Information

Message ID : VMD3836I

Long Form

Finished pushing a new signature database

Short Form

Sig push to secfs OK

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3841I

Severity

Information

Long Form

opendir failed for {0} for the signature request {1}, error code {2}

Message ID : VMD3839I

Short Form

Sig opendir error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3842I

Severity

Information

Long Form

User browsing for {0} succeeded.

Message ID : VMD3841I

1040

Short Form

User browse OK

Parameters

Label	CEF Label	Type	Usage
domain	dntdom	Text	A domain name (policy, network, users, etc)

Description

None

Message ID : VMD3847I

Severity

Information

Long Form

Domain browsing succeeded.

Short Form

Domain browse OK

Message ID : VMD3842I

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3851I

Severity

Information

Long Form

Canceling the signature request {0}

Short Form

Sig req cancelled

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : VMD3847I

Description

None

Message ID : VMD3852I

Severity

Information

Long Form

Querying the status of the signature request {0}

Short Form

Sig req status query

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3851I

Message ID : VMD3853I

Severity

Information

Long Form

Sending {0} signatures for the signature request {1} to the Key Manager

Short Form

Sending sigs

Parameters

Label	CEF Label	Type	Usage
nsig	vds_nsig	Numeric	The number of signatures generated
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3854I

Severity

Information

Long Form

{0} signatures of the signature request {1} have been sent to the Key Manager

Short Form

Sent sigs

Parameters

Label	CEF Label	Type	Usage
nsig	vds_nsig	Numeric	The number of signatures generated
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3856I

Severity

Information

Long Form

The Key Manager canceled the signature data push

Short Form

Send sigs cancelled

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3857I

Severity

Information

Message ID : VMD3856I

Long Form

Got the signature data push from the Key Manager. Number of signatures in the push: {0}. Total number of signatures from the Key Manager: {1}

Short Form

Sig push from server

Parameters

Label	CEF Label	Type	Usage
nsig	vds_nsig	Numeric	The number of signatures generated
nfile	vds_nfile	Numeric	The number of files processed

Description

None

Message ID : VMD3859I

Severity

Information

Message ID : VMD3857I

1047

Long Form

Completed the signature request {0} with some failed files

Short Form

Sig reg partially done

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3861I

Severity

Information

Long Form

The Key Manager canceled the signature sending for the signature request {0}

Message ID : VMD3859I

Short Form

Sig req cancelled

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3862I

Severity

Information

Long Form

Running in FIPS 140-2 mode, using {0}

Short Form

FIPS 140-2 mode

Message ID : VMD3861I

Parameters

Label	CEF Label	Type	Usage
version	vds_version	Text	Software version string

Description

None

Message ID : VMD3863I

Severity

Information

Long Form

Generating the file list for the signature request {0}, {1} files and directories have been scanned

Short Form

Sig scan in progress

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Message ID : VMD3862I

Label	CEF Label	Type	Usage
nfile	vds_nfile	Numeric	The number of files processed

Description

None

Message ID : VMD3868I

Severity

Information

Long Form

LDAP search of {0}/{1} for {2} returned "{3}"

Short Form

LDAP search error

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
filePath	filePath	Text	Full path to file

Message ID : VMD3863I

1051

Label	CEF Label	Type	Usage
effect	vds_effect	Text	Policy effect
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3870I

Severity

Information

Long Form

Configuration data was supplied by "{0}".

Short Form

Config source

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Message ID : VMD3868I

Description

None

Message ID : VMD3880I

Severity

Information

Long Form

The Key Manager was upgraded recently; informing it that this agent is challenge-response aware

Short Form

Try new host password req

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3870I

1053

Message ID : VMD3881I

Severity

Information

Long Form

The new certificate set has been activated

Short Form

New certs activated

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3883I

Severity

Information

Message ID : VMD3881I

Long Form

Certificates for the {0} agent expire in {1} days

Short Form

Certificate lifetime

Parameters

Label	CEF Label	Type	Usage
agent	deviceProcessName	Text	The short identifier of the agent software
daysleft	vds_daysleft	Numeric	Days until certificate expiry

Description

None

Message ID : VMD3885I

Severity

Information

Message ID : VMD3883I

1055

Long Form

The VMD failed to initialize with the Key Manager. This may indicate that the connection to the server is down, the VMD's host has been deleted from the Key Manager, or "Communication Enabled" for the host has not been enabled in the Key Manager UI.

Short Form

VMD/Server init fail

Parameters

No parameters are provided for this message type

Description

The agent is unable to reach the key manager. You may see any of the following error messages: COM4583F, COM4633W, VMD3770F, VMD3885I or VMD3886I. You may experience any of the following:

1. Connection to the key manager is down.
2. The VMD Host has been deleted from the key manager.
3. The host does not have "Communication Enabled" in the key manager UI.
4. The VMD's host may be deleted from the key manager. Run the register_host utility to re-register the VMD with the key manager.

Message ID : VMD3886I

Severity

Information

Long Form

The VMD's host may no longer be registered with a Key Manager. The VMD's host may have been deleted from the Key Manager. You may want to run the register_host utility to re-register the VMD with a Key Manager.

Short Form

VMD poss unregistered

Parameters

No parameters are provided for this message type

Description

The agent is unable to reach the key manager. You may see any of the following error messages: COM4583F, COM4633W, VMD3770F, VMD3885I or VMD3886I. You may experience any of the following:

1. Connection to the key manager is down.
2. The VMD Host has been deleted from the key manager.
3. The host does not have "Communication Enabled" in the key manager UI.
4. The VMD's host may be deleted from the key manager. Run the register_host utility to re-register the VMD with the key manager.

Message ID : VMD3893I

Severity

Information

Long Form

Clustered property of GP {0} is honored per Key Manager

Short Form

Clustered property of GP is honored per Key Manager

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Description

None

Message ID : VMD3895I

Severity

Information

Long Form

RSA certificates detected for the {0} agent, will renew with EC certificates

Short Form

Switching to EC certs

Parameters

Label	CEF Label	Type	Usage
agent	deviceProcessName	Text	The short identifier of the agent software

Description

None

Message ID : VMD3896I

Severity

Information

Long Form

RSA certificates detected for the {0} agent, will not renew with EC certificates as ports 8446/7 not open to Key Manager

Short Form

No Switch to EC certs due to missing 8446/7 ports

Parameters

Label	CEF Label	Type	Usage
agent	deviceProcessName	Text	The short identifier of the agent software

Description

None

Message ID : VMD3897I

Severity

Information

Message ID : VMD3896I

Long Form

New comms session with {0} using token {1}

Short Form

Comms session

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name
token	vds_token	Text	A token name (e.g. for one-time-passwords)

Description

None

Message ID : VMD3898I

Severity

Information

Message ID : VMD3897I

Long Form

STARTED on {0} VERSION: {1}

Short Form

VMD Startup

Parameters

Label	CEF Label	Type	Usage
osname	cs2	Text	A name identifying the agent operating system
version	vds_version	Text	Software version string

Description

None

Message ID : VMD3900I

Severity

Information

Message ID : VMD3898I

Long Form

Docker host browsing succeeded.

Short Form

Docker host browse OK

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3902I

Severity

Information

Long Form

Docker host browsing for image {0} succeeded.

Message ID : VMD3900I

Short Form

Docker host browse OK

Parameters

Label	Type	Usage
dockerid	Text	Docker image or container id

Description

None

Message ID : VMD3904I

Severity

Information

Long Form

Docker image {0} file browsing for {1} succeeded.

Short Form

Docker image file browse OK

Message ID : VMD3902I

Parameters

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3906I

Severity

Information

Long Form

Docker container {0} file browsing for {1} succeeded.

Short Form

Docker container file browse OK

Message ID : VMD3904I

1065

Parameters

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3908I

Severity

Information

Long Form

User browsing for image {0} with {1} succeeded.

Short Form

Docker image user browse OK

Message ID : VMD3906I

1066

Parameters

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id
domain	dntdom	Text	A domain name (policy, network, users, etc)

Description

None

Message ID : VMD3910I

Severity

Information

Long Form

User browsing for container {0} with {1} succeeded.

Short Form

Docker container user browse OK

Message ID : VMD3908I

1067

Parameters

Label	CEF Label	Type	Usage
dockerid	dockerid	Text	Docker image or container id
domain	dntdom	Text	A domain name (policy, network, users, etc)

Description

None

Message ID : VMD3912I

Severity

Information

Long Form

Domain browsing for image {0} succeeded.

Short Form

Docker image domain browse OK

Message ID : VMD3910I

1068

Parameters

Label	Type	Usage
dockerid	Text	Docker image or container id

Description

None

Message ID : VMD3914I

Severity

Information

Long Form

Domain browsing for container {0} succeeded.

Short Form

Docker container domain browse OK

Parameters

Label	Type	Usage
dockerid	Text	Docker image or container id

Message ID : VMD3912I

Description

None

Message ID : VMD3919I

Severity

Information

Long Form

Policy "{0}" version {1} received from Key Manager

Short Form

Policy update

Parameters

Label	CEF Label	Type	Usage
pol	cs1	Text	Policy name
verno	vds_verno	Numeric	A version number

Message ID : VMD3914I

1070

Description

None

Message ID : VMD3926I

Severity

Information

Long Form

An partial certificate renewal has been completed successfully

Short Form

Certs recovered OK

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3919I

Message ID : VMD3930I

Severity

Information

Long Form

Successfully received and implemented user space part of a new security configuration.

Short Form

Partial Config OK

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3934I

Severity

Information

Long Form

The CTE client has passed attestation checks.

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3935I

Severity

Information

Long Form

Attestation checks to be run on following adapters: {0}

Short Form

Attest run

Message ID : VMD3934I

1073

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD4246I

Severity

Information

Long Form

Detected upgrade situation from pre-FIPS (4.4.0) to post-FIPS (4.4.1). Converting the private key format now.

Short Form

Key converted

Parameters

No parameters are provided for this message type

Message ID : VMD3935I

Description

None

Message ID : VMD4611I

Severity

Information

Long Form

vm_write_file: Empty write buffer

Short Form

Empty write buf

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD4246I

1075

Message ID : VMD4619I

Severity

Information

Long Form

The previous message {0} was repeated {1} times

Short Form

Repeat message

Parameters

Label	CEF Label	Type	Usage
msgid	vds_msgid	Text	A unique log message identifier
count	vds_count	Numeric	A generic count value

Description

None

Message ID : VMD4620I

Severity

Information

Long Form

The space available for log files in {0} is low ({1} MB)

Short Form

Log space low

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
count	vds_count	Numeric	A generic count value

Description

None

Logger VMD: Warnings

Message ID : VMD3714W

Severity

Warning

Long Form

check_mount: {0} {1}{2} match failed({3})

Short Form

No short form is provided for this message type

Description

None

Message ID : VMD3762W

Severity

Warning

Long Form

Keys are not available at time of signing binaries. Check connection to Key Manager or run 'vmsec challenge'

Short Form

No Keys signing binaries.

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3805W

Severity

Warning

Long Form

Unhandled service opcode seen. Opcode = {0}

Message ID : VMD3762W

Short Form

Unhandled opcode

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3806W

Severity

Warning

Long Form

Unrecognized service opcode seen. Opcode = {0}

Short Form

Unknown opcode

Message ID : VMD3805W

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3813W

Severity

Warning

Long Form

The VMD is shutting down.

Short Form

VMD Shutdown

Parameters

No parameters are provided for this message type

Message ID : VMD3806W

Description

System shutdown, reboot or system re-registration will cause this message to display because the CTE daemon process was terminated.

Message ID : VMD3824W

Severity

Warning

Long Form

Failed to create the signature for {0} for the signature request {1}, error code {2}

Short Form

Sig creation error

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any
ecode	cn1	Numeric	An error code

Description

None

Message ID : VMD3826W

Severity

Warning

Long Form

{0} is invalid for the signature request {1}

Short Form

Bad sig file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3850W

Severity

Warning

Long Form

Could not find the signature request {0}

Short Form

Sig req mismatch

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3826W

Message ID : VMD3860W

Severity

Warning

Long Form

The signature request {0} is already initialized

Short Form

Sig req duplicated

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any

Description

None

Message ID : VMD3869W

Severity

Warning

Long Form

No LDAP server details were found (missing or incomplete ldap.conf)

Short Form

No LDAP server

Parameters

No parameters are provided for this message type

Description

No LDAP configuration data was found on the host system. This usually occurs because LDAP services have not been installed or configured properly.

Message ID : VMD3871W

Severity

Warning

Message ID : VMD3869W

1086

Long Form

Unauthorized communication attempt from "{0}" rejected

Short Form

Unauth comms rejected

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location

Description

None

Message ID : VMD3882W

Severity

Warning

Long Form

An error occurred with a new certificate set so the previous set has been restored

Message ID : VMD3871W

Short Form

Backup certs restored

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3887W

Severity

Warning

Long Form

Unable to initialize/join Vormetric Cluster Group - proceeding unclustered

Short Form

initialize/join CipherTrust Cluster Group - proceeding unclustered

Message ID : VMD3882W

1088

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3889W

Severity

Warning

Long Form

Cluster coherent GP {0} not allowed on unclustered node

Short Form

Cluster coherent GP not allowed on unclustered node

Parameters

Label	CEF Label	Type	Usage
gp	fileId	Text	GuardPoint base directory

Message ID : VMD3887W

Description

None

Message ID : VMD3899W

Severity

Warning

Long Form

The authentication signature for file {0} has changed

Short Form

Signature changed

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3889W

Message ID : VMD3920W

Severity

Warning

Long Form

Agent failing over to server "{0}"

Short Form

Failover

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Description

None

Message ID : VMD3921W

Severity

Warning

Long Form

Agent reverting to assigned server "{0}"

Short Form

Failover end

Parameters

Label	CEF Label	Type	Usage
shost	shost	Text	Source host name

Description

None

Message ID : VMD3924W

Severity

Warning

Message ID : VMD3921W

Long Form

Unknown key manager in URL {0} will be ignored. This attribute is located in the config file at {1}.

Short Form

Unknown URL in config file

Parameters

Label	CEF Label	Type	Usage
url	request	Text	A uniform resource location
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD3925W

Severity

Warning

Message ID : VMD3924W

Long Form

Certificate renewal not possible due to missing external cert directory and no saved CSR

Short Form

Cert renewal impossible

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3928W

Severity

Warning

Long Form

Certificate for "{0}" expires in {1} days

Message ID : VMD3925W

Short Form

CA cert expires

Parameters

Label	CEF Label	Type	Usage
agent	deviceProcessName	Text	The short identifier of the agent software
daysleft	vds_daysleft	Numeric	Days until certificate expiry

Description

None

Message ID : VMD3931W

Severity

Warning

Long Form

A required signature set update has not been received from the Key Manager - policy rules may not be enforced correctly.

Message ID : VMD3928W

Short Form

Missing sigset push

Parameters

No parameters are provided for this message type

Description

None

Message ID : VMD3933W

Severity

Warning

Long Form

The CTE client is unable to perform attestation checks.

Short Form

No short form is provided for this message type

Message ID : VMD3931W

Description

None

Message ID : VMD4618W

Severity

Warning

Long Form

The previous message {0} was repeated {1} times

Short Form

Repeat message

Parameters

Label	CEF Label	Type	Usage
msgid	vds_msgid	Text	A unique log message identifier
count	vds_count	Numeric	A generic count value

Message ID : VMD3933W

Description

None

Message ID : VMD4621W

Severity

Warning

Long Form

The space available for log files in {0} is dangerously low ({1} MB)

Short Form

Log space low

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file
count	vds_count	Numeric	A generic count value

Message ID : VMD4618W

Description

The directory used to process log files is low on space. The "filePath" field gives the path and directory. The "count" field gives the remaining space (in MB).

When space is low audit trails may become compromised, and error conditions may be unreported. This should be resolved immediately.

Message ID : VMD4622W

Severity

Warning

Long Form

Raising drop log message level to {0} because space consumed is now greater than {1}% and less than or equal to {2}%.

Short Form

Raise drop space level

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
count	vds_count	Numeric	A generic count value

Label	CEF Label	Type	Usage
count	vds_count	Numeric	A generic count value

Description

The space that holds log files uploaded to the key manager is increasing. Logging levels are automatically modified to accommodate the load. The "reason" field details the change being imposed, and the two "count" fields depict the lower and upper "percentage full" values that caused this condition. The following strings may occur on the "reason" field:

Reason	Meaning
Drop None	No adjustments currently in force
Speed Up	The agent will try to upload logs to the key manager in larger batches
Drop Info	No INFO level logs will be uploaded
Drop Warn	No WARN level logs will be uploaded
Drop Error	No ERROR level logs will be uploaded

Message ID : VMD4623W

Severity

Warning

Message ID : VMD4622W

1100

Long Form

Raising drop log message level to {0} because number of files is now greater than {1}% and less than or equal to {2}%.

Short Form

Raise drop file level

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
count	vds_count	Numeric	A generic count value
count	vds_count	Numeric	A generic count value

Description

Files pending upload to the key manager are increasing, so the agent has temporarily adjusted the logging parameters to handle the situation. The "reason" field details the change imposed, and the two "count" fields indicate the lower and upper percentages of the maximum permitted number of files. See VMD4622W for usage of the "reason" field.

Message ID : VMD4624W

Severity

Warning

Message ID : VMD4623W

1101

Long Form

Lowering drop log message level to {0} because space consumed is now greater than {1}% and less than or equal to {2}%.

Short Form

Lower drop space level

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
count	vds_count	Numeric	A generic count value
count	vds_count	Numeric	A generic count value

Description

The space used to hold log files for uploading to the key manager is decreasing, so the agent has temporarily adjusted the logging parameters to handle the situation. See VMD4622W for details about the fields used.

Message ID : VMD4625W

Severity

Warning

Message ID : VMD4624W

Long Form

Lowering drop log message level to {0} because number of files is now greater than {1}% and less than or equal to {2}%.

Short Form

Lower drop file level

Parameters

Label	CEF Label	Type	Usage
showStr	reason	Text	Code specifying reason for allowing access, if any
count	vds_count	Numeric	A generic count value
count	vds_count	Numeric	A generic count value

Description

The number of files pending upload to the key manager is decreasing, so the agent has temporarily adjusted the logging parameters to handle the situation. See VMD4623W for details about the fields used.

Message ID : VMD4636W

Severity

Warning

Message ID : VMD4625W

Long Form

Unable to determine expiry date from certificate {0}

Short Form

Cannot get expiry date

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD4639W

Severity

Warning

Long Form

Corrupt log data from Secfs in file {0} - some records lost

Message ID : VMD4636W

Short Form

Corrupt log file

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Message ID : VMD4640W

Severity

Warning

Long Form

Invalid directory in log directory. {0} Please remove.

Short Form

Invalid directory in log directory.

Message ID : VMD4639W

Parameters

Label	CEF Label	Type	Usage
filePath	filePath	Text	Full path to file

Description

None

Logger XFM: Errors

Message ID : XFM4501E

Severity

Error

Long Form

Decompression failure: the size of the data resulting from decompression is not the same size as before compression. Possible data corruption.

Short Form

Size mismatch

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4502E

Severity

Error

Long Form

Compression setup failure: module not initialized.

Short Form

Compression init fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4504E

Severity

Error

Long Form

Compression setup failure: no applicable module initialized.

Short Form

Compression setup fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4535E

Severity

Error

Long Form

Decompression got corrupted buffer (invalid size of encrypted data).

Message ID : XFM4504E

Short Form

Encryption buffer corrupt

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4568E

Severity

Error

Long Form

Compression failure: destination buffer too small: {0} < {1}.

Short Form

Buffer too small

Message ID : XFM4535E

1110

Parameters

Label	CEF Label	Type	Usage
slen	in	Numeric	Input byte count or length
dlen	out	Numeric	Output byte count or length

Description

None

Message ID : XFM4589E

Severity

Error

Long Form

Unable to initialize the message digest subsystem. The operation will fail.

Short Form

Digest setup fail

Message ID : XFM4568E

1111

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4590E

Severity

Error

Long Form

Unable to compute the message digest value.

Short Form

Cannot compute digest

Parameters

No parameters are provided for this message type

Message ID : XFM4589E

1112

Description

None

Message ID : XFM4591E

Severity

Error

Long Form

Unable to the retrieve the message digest value.

Short Form

Cannot extract digest

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4590E

1113

Logger XFM: Fatal errors

Message ID : XFM4508F

Severity

Fatal error

Long Form

Unable to find chunk headers; possible data corruption.

Short Form

Missing chunk hdr

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4509F

Severity

Fatal error

Long Form

Decompression/decryption failure: output buffer size ({0} bytes) is too small.

Short Form

Decomp/decrypt buffer too small

Parameters

Label	CEF Label	Type	Usage
dlen	out	Numeric	Output byte count or length

Description

None

Message ID : XFM4518F

Severity

Fatal error

Message ID : XFM4509F

Long Form

Invalid encryption key size received from Key Manager. The operation will fail.

Short Form

Invalid encr. key size

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4519F

Severity

Fatal error

Long Form

The agent could not allocate enough memory. Contact support.

Message ID : XFM4518F

1116

Short Form

Out of memory

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4525F

Severity

Fatal error

Long Form

Decryption fatal error: {0}. The restore operation will fail.

Short Form

Decryption error

Message ID : XFM4519F

1117

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : XFM4532F

Severity

Fatal error

Long Form

Decryption information mismatch; possible data corruption.

Short Form

Decryption info mismatch

Parameters

No parameters are provided for this message type

Message ID : XFM4525F

Description

None

Message ID : XFM4536F

Severity

Fatal error

Long Form

Compression module returned fatal error: {0}. The operation will fail.

Short Form

Compression error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : XFM4532F

Message ID : XFM4539F

Severity

Fatal error

Long Form

Unable to set up encryption subsystem. The operation will fail.

Short Form

Encryption setup fail

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4540F

Severity

Fatal error

Message ID : XFM4539F

Long Form

Decompression information mismatch; possible data corruption.

Short Form

Decompression info mismatch

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4541F

Severity

Fatal error

Long Form

Data read problem: corrupted buffer header. Data corruption has possibly occurred. The restore operation will fail.

Message ID : XFM4540F

Short Form

Corrupt buffer header

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4544F

Severity

Fatal error

Long Form

Unable to set up compression subsystem. The operation will fail.

Short Form

Compression setup fail

Message ID : XFM4541F

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4546F

Severity

Fatal error

Long Form

Compression module initialization failure. The backup operation will fail.

Short Form

Compression init fail

Parameters

No parameters are provided for this message type

Message ID : XFM4544F

Description

None

Message ID : XFM4561F

Severity

Fatal error

Long Form

Decompression fatal error: {0}. The restore operation will fail.

Short Form

Decompression error

Parameters

Label	CEF Label	Type	Usage
ecode	cn1	Numeric	An error code

Description

None

Message ID : XFM4546F

Message ID : XFM4565F

Severity

Fatal error

Long Form

Input data length does not match buffer length: {0} != {1}. Data corruption has possible occurred. The restore operation will fail.

Short Form

Data lenght mismatch

Parameters

Label	CEF Label	Type	Usage
slen	in	Numeric	Input byte count or length
dlen	out	Numeric	Output byte count or length

Description

None

Logger XFM: Information

Message ID : XFM4507I

Severity

Information

Long Form

Using no encryption.

Short Form

Using no encryption

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4517I

Severity

Information

Long Form

Shutting down compression/decompression subsystem.

Short Form

Comp/decomp shutdown

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4522I

Severity

Information

Message ID : XFM4517I

Long Form

Data transformation code now using single-threaded algorithm.

Short Form

Single-thread transform

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4526I

Severity

Information

Long Form

Using no compression.

Message ID : XFM4522I

Short Form

Using no compression

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4549I

Severity

Information

Long Form

Using compression.

Short Form

Using compression

Message ID : XFM4526I

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4557I

Severity

Information

Long Form

Using {0} encryption algorithm.

Short Form

Using enc algorithm

Parameters

Label	CEF Label	Type	Usage
key	cs3	Text	Name of key or key pair

Message ID : XFM4549I

Description

None

Message ID : XFM4559I

Severity

Information

Long Form

Shutting down encryption/decryption subsystem.

Short Form

Encrypt/decrypt shutdown

Parameters

No parameters are provided for this message type

Description

None

Message ID : XFM4557I

Logger XFM: Warnings

Message ID : XFM4550W

Severity

Warning

Long Form

Compression initialization failure: failed to initialize algorithm {0} upon startup.

Short Form

Compression init fail

Parameters

No parameters are provided for this message type

Description

None

CipherTrust Transparent Encryption

ADMINISTRATOR GUIDE



Document Information

Product Version	2.0.0
Release Date	11 September 2020

Trademarks and Copyrights

Copyright © 2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal, and personal use only provided that:

- > The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances,

shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

CONTENTS

Document Information	2
Preface: About this Document	10
Release Notes	10
Audience	10
What's in This Guide	10
Organization	11
Document Conventions	12
Command Syntax and Typeface Conventions	12
Notifications and Alerts	13
Related Documents	13
Support Contacts	14
Chapter 1: Interfaces	15
CLI	15
REST API	15
Acquiring an Authorization Token	15
Using the Token	16
Making an API Call	16
GUI	17
Header	17
Left Pane	18
Page	18
Notifications	20
Chapter 2: Licensing	21
Trialware	21
Time-limited Rental	21
Perpetual Licensing Model	21
Add-on Licenses	22
Installing CTE Licenses	22
Chapter 3: Concepts	24
Clients	24
Client Groups	24
GuardPoints	25
Policies	25
Security Rules	26
Security Rule Criteria	26
Actions	27
Security Rule Effects	28
How Security Policy Works	28

Resource Sets	29
User Sets	29
Signature Sets	29
Process Sets	30
Key Rules	30
Data Transformation Rules	30
Profiles	31
Learn Mode	31
User Roles	31
CTE Admins	32
CTE Clients	32
Chapter 4: Introduction to Data Transformation	33
The Data Transformation Process	33
Uses of Data Transformation	33
How CTE Protects Files	33
Components of the CTE Solution	34
Properties of Data Transformation	34
Data Transformation Techniques	35
The Copy Method	35
The Restore Method	37
The Dataxform Utility Method	37
Live Data Transformation	38
Summary	39
Protection Policies	40
Types of Policies	41
Chapter 5: Managing Profiles	42
Creating a Profile	42
Setting Client Log Configuration	43
Setting Client Syslog Configuration	48
Setting Quality of Service Configuration	50
Concise Logging	52
Advantages	53
Considerations	53
Modifying Profiles	53
Deleting Profiles	54
Deleting Individual Profiles	54
Deleting Multiple Profiles	54
Chapter 6: Managing Clients and Client Groups	55
Registering Clients	55
Searching Clients	56
Viewing Clients	56
Enabling Live Data Transformation	57
Prerequisites	58
Important Notes	58

Enable LDT	58
Setting Client Locks	59
Agent Lock	60
System Lock	61
Setting Locks on Individual Clients	62
Setting Locks on a Client Group	63
Verifying Locks on Clients	63
Unlocking Clients Manually	64
Disabling Locks	64
Administering Locking Issues	65
Client Settings	65
Client Settings for Linux	65
Client Settings for Windows	66
Oracle Database in a Guarded NFS Mount on AIX	68
Client Settings Keywords	68
Configuring Application Authentication Credentials	69
Re-Sign Settings	70
Modifying Client Configuration	71
Changing the Profile	72
Changing Client Password	72
Offline Password	72
Password Types	73
Changing the Password Manually	73
Changing the Password Dynamically	74
Managing Membership	74
Viewing Group Membership of a Client	74
Removing a Client from a Client Group	75
Deleting Clients	75
Deleting Clients with System Lock or Agent Lock	75
Deleted Client Indicators	76
Deleting Multiple Clients	76
Configuring Client Groups	77
Creating a Client Group	77
Adding Clients to a Client Group	78
Displaying Client Groups	79
Modifying Client Groups	79
Changing the Profile	80
Changing Client Group Password	81
Inheritance of Client Group Settings	82
Configuring Client Group Settings	84
Deleting Client Groups	84
Chapter 7: Managing Signature Sets	86
The Signing Process	87
Using Signature Sets in a Policy	87
Creating Signature Sets	88
Signing Files in a Signature Set	90

Checking Signing Completion Status	92
Stopping the Signing Process	92
Displaying Signatures of Files in a Signature Set	93
Displaying Signatures of All Files in the Signature Set	93
Displaying Specific Signed Files in the Signature Set	93
Detecting Duplicate Files	94
Deleting Signatures from Signature Sets	95
Deleting Single Signatures	95
Deleting Multiple Signatures	95
Deleting Source from Signature Sets	96
Deleting Single Sources	96
Deleting Multiple Sources	97
Deleting Signature Sets	97
Deleting Single Signature Sets	97
Deleting Multiple Signature Sets	98
Re-Signing Files in a Signature Set	98
Checking Agent Logs if Signing Fails	99
Chapter 8: Managing Policies	101
Overview	101
Policy Rule Criteria and Effects	102
Policy Rule Criteria	102
Policy Rule Effects	102
Creating Policy Elements	103
Creating Resource Sets	104
Creating User Sets	105
Creating Signature Sets	108
Creating Process Sets	110
Viewing Policy Elements	112
Creating Policies	114
Step 1: Specify General Information	115
Step 2: Add Security Rules	117
Step 3: Add Key Rules	119
Step 4: Add Data Transformation Rules	121
Step 5: Confirm Details	122
Creating a New Key	122
Displaying Policies	124
Viewing Policies	124
Viewing Details of Policies	125
Viewing Policy Version History	127
Modifying Policies and Rules	127
Updating Policy Description	128
Cloning a Policy	128
Adding New Security Rules	129
Adding New Key Rules	129
Adding New Data Transformation Rules	130
Modifying Security Rules	130

Modifying Key Rules	131
Modifying Data Transformation Rules	133
Deleting Policies	134
Chapter 9: Managing GuardPoints	135
Overview	135
Secure Start GuardPoints	136
Considerations Before Creating GuardPoints	136
When Changing a Policy or Rekeying a GuardPoint	137
Creating Standard GuardPoints on Clients	138
GuardPoint Status Information	140
Creating LDT GuardPoints on Clients	140
Creating Cloud Object Storage GuardPoints on Clients	143
Enabling Secure Start for GuardPoints	144
Creating GuardPoints on Client Groups	145
Create Standard GuardPoints on Client Groups	146
Creating LDT GuardPoints on Client Groups	148
Creating Cloud Object Storage GuardPoints on Client Groups	150
Automatic and Manual GuardPoints	151
Selecting a GuardPoint Mount Type	154
Viewing GuardPoints	154
Viewing GuardPoint Status	155
Viewing GuardPoint Status on the Client	155
Viewing GuardPoint Status on the GUI	155
Configuring Windows Network Drives	156
Deleting GuardPoints	157
Before Deleting GuardPoints	157
Deleting a GuardPoint	157
Chapter 10: Operations	158
Registering Clients	158
Using External CA Certificates	159
Reregistering CTE Clients	159
Protecting Data on Clients	159
GuardPoints	159
Policies	160
Policy Elements	163
Chapter 11: Common Scenarios	164
Prerequisites	164
User-based Access Privileges	164
Standard (Production) Policies	165
Standard (Dataxform) Policies	165
LDT Policies	167
Process-based Access Privileges	167
Signature-based Access Privileges for Processes	168
Different Access Privileges for Subdirectory or Different File Formats	169

Different Access Privileges for Combination of Users, Processes, and Resources	170
Appendix A: Troubleshooting	172
Connection Issues	172
Registration Issues	172
Licensing Issues	173
Configuration Issues	173
Index	174

PREFACE: About this Document

This introductory section identifies the audience, explains the importance of the release notes, provides a brief summary of the user guide's contents, explains how to best use the written material, and discusses the documentation conventions used. It contains the following sections:

- > "Release Notes" below
- > "Audience" below
- > "What's in This Guide" below
- > "Organization" on page 1
- > "Document Conventions" on page 1
- > "Related Documents" on page 13
- > "Support Contacts" on page 14

Release Notes

The release notes provide important information about this release that is not included in other customer documentation. It is strongly recommended that you read the release notes to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the release notes for this release at the following location:

<https://supportportal.thalesgroup.com>

Audience

This document is intended for CipherTrust Transparent Encryption (CTE) administrators responsible for deploying security policies on client machines.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with data security concepts.

What's in This Guide

This guide describes the CipherTrust Manager interfaces to use CTE. The document explains the CTE concepts such as clients and client groups, signature sets, security rules, and GuardPoints. Next, the document describes how to manage clients and client groups, signature sets, security policies on the CipherTrust Manager. Finally, the document describes how to manage GuardPoints.

- > It is assumed, for this document, that you have already configured the CipherTrust Manager appliance. Refer to the CipherTrust Manager product documentation for instructions.
- > The next step is to activate and install the CTE license. Refer to ["Licensing" on page 21](#) for details.
- > After the license is installed, you can configure CTE Agents. Refer to the CTE Agent Quick Start Guide specific to your platform for details. Installation of the CTE Agents is required for protecting directories and files stored on clients.

NOTE This document, may at times, abbreviate:

- > "CipherTrust Transparent Encryption" to "CTE"
- > "CipherTrust Manager" to "CM"

Organization

The CipherTrust Transparent Encryption Administrator Guide contains the following chapters:

1. ["Interfaces" on page 15](#)
Provides an overview of the CipherTrust Manager interfaces—Command Line Interface (CLI), REST Application Programming Interface (REST API), and Graphical User Interface (GUI).
2. ["Licensing" on page 21](#)
Describes the CTE licensing models.
3. ["Concepts" on page 24](#)
Describes CTE concepts such as clients, client groups, GuardPoints, policies, and security rules.
4. ["Introduction to Data Transformation" on page 33](#)
Provides an overview of the data transformation process.
5. ["Managing Profiles" on page 42](#)
Describes how to configure client log criteria and client Syslog settings.
6. ["Managing Clients and Client Groups" on page 55](#)
Describes how to add, register, and manage clients and client groups on the CipherTrust Manager appliance.
7. ["Managing Signature Sets" on page 86](#)
Describes how to create signature sets and how to sign and re-sign files in a signature set. The chapter also describes how to stop file signing and how to delete signatures and signature sets on the CipherTrust Manager appliance.
8. ["Managing Policies" on page 101](#)
Describes rules and effects of security policies, and provides instructions to create, configure, import, and export security policies on the CipherTrust Manager appliance.
9. ["Managing GuardPoints" on page 135](#)

Describes how to create, view, and delete GuardPoints on the CipherTrust Manager appliance. The chapter provides information on automatic and manual GuardPoints and provides steps to configure Windows network drives.

10. "Operations" on page 158

Describes the operations that the CTE Server Administrator performs on the CipherTrust Manager. These operations include registering CTE clients with the CipherTrust Manager, using external CA certificates, reregistering the clients, and protecting file system on a CTE client.

11. "Common Scenarios" on page 164

Describes the common encryption scenarios in which the paths can be encrypted using the CTE solution.

12. "Troubleshooting" on page 172

Describes how to handle the issues that you might face when using CTE with the CipherTrust Manager.

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Format	Convention
bold	The bold attribute is used to indicate the following: > Command-line commands and options that you enter verbatim (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Represent optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.

Format	Convention
<code>{a b c}</code> <code><a> <c></code>	Represent required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
<code>[a b c]</code> <code><a> <c></code>	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

Tips

Tips are used to highlight information that helps to complete a task more efficiently.

TIP This is some information that will allow you to complete your task more efficiently.

Notes

Notes are used to highlight important or helpful information.

NOTE Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

CAUTION! Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Related Documents

The following documents contain related or additional information:

- > CTE Release Notes
- > CTE Agent for Linux Quick Start Guide

- > CTE Agent for Windows Quick Start Guide
- > CTE Agent for AIX Advanced Configuration and Integration Guide
- > CTE Agent for Linux Advanced Configuration and Integration Guide
- > CTE Agent for Windows Advanced Configuration and Integration Guide
- > CTE-Live Data Transformation with CipherTrust Manager

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#).

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.

CHAPTER 1: Interfaces

This chapter provides an overview of the CipherTrust Manager interfaces

CLI

The CipherTrust Manager includes a CLI tool, named **ksctl**, that can be downloaded and run locally to control a remote CipherTrust Manager appliance. **ksctl** exclusively uses the REST API to communicate with the CipherTrust Manager, so anything that you can do with the tool, you can also do directly with the REST API. Conversely, **ksctl** exposes most of the functionality of the REST API. It can perform management functions, such as managing registration tokens and clients.

NOTE **ksctl** is designed to be run from a remote system, not on the CipherTrust Manager itself.

To use the CLI:

1. Open the **CipherTrust Manager** URL in a browser.
2. Click the **API & CLI Documentation** link. The API playground is displayed.
3. At the top left, click **CLI Guide**. The CLI documentation is displayed.
4. At the top right, click the **CLI** download button. This downloads the **ksctl_images.zip** file.
5. Unzip the **ksctl_images.zip** file. The extracted files contain platform specific files. For example, the file for Windows is **ksctl-win-amd64**, and for Linux, the file is **ksctl-linux-amd64**.
6. Set up the **ksctl-<os>** file for your system. Refer to the CipherTrust Manager CLI documentation for details.
7. Run **ksctl cte** to run CipherTrust Transparent Encryption specific commands.

Refer to the *CipherTrust Manager* documentation for details. For details on commands related to CipherTrust Transparent Encryption, refer to the online documentation of `ksctl cte`.

REST API

Use the REST interface from the *API playground* or through any REST client such as curl. The REST interface acquires an authorization token internally and uses it for making API calls.

Acquiring an Authorization Token

To acquire a token:

1. Open the **CipherTrust Manager** URL in a browser.

2. Click the **API & CLI Documentation** link. The API playground is displayed.
3. At the top right, click **Authenticate**.
4. Enter **username** and **password**.
5. Click **POST**.

NOTE This acquires an API token and prefills it in the playground examples. The token expires in 300 seconds (5 minutes). When it expires, use this tool again to acquire a new token.

On successful token generation, the remaining token expiry time in seconds is displayed. Two new buttons, **Clear Credentials** and **Re Authenticate**, are also displayed at the top right.

Using the Token

The authorization token acquired above is used in examples in the API playground. The token expires in 5 minutes; if expired, generate a new token, as described in ["Acquiring an Authorization Token" on the previous page](#).

Making an API Call

To make an API call, find the API in the left pane and click it. In the right pane, specify the required parameters, and click an appropriate button (for example, **POST**, **GET**, **DELETE**, or **Curl**). For example, to create a CTE policy on CipherTrust Manager:

1. In the left pane of the API playground, click **CTE/Policies**.
2. Under **cte/policies**, click **Create**. The **Create** section of the API playground is displayed in the right pane.
3. In the **body** field, specify required parameters with their values, as shown below.

```
{
  "name": "TestPolicy",
  "policy_type": "Standard",
  "never_deny": false,
  "security_rules": [
    {
      "effect": "permit",
      "action": "all_ops",
      "partial_match": false,
      "resource_set_id": "TestResourceSet",
      "exclude_resource_set": true
    }
  ]
}
```

Expand **schema** under the **body** field for names and types of fields. Hover your mouse over each field to view its description. The parameter names and casing in the **body** field must match with those shown in the schema. Also, ensure that parameters and their values are specified in double quotes.

4. Click **POST**.

Alternatively, to get an equivalent `curl` command, click the **Curl** button. The `curl` equivalent will be shown in the text field below. Use the `curl` tool to run the command to make the REST API call.

Similarly, all API calls can be made by referring to the schema shown in the playground.

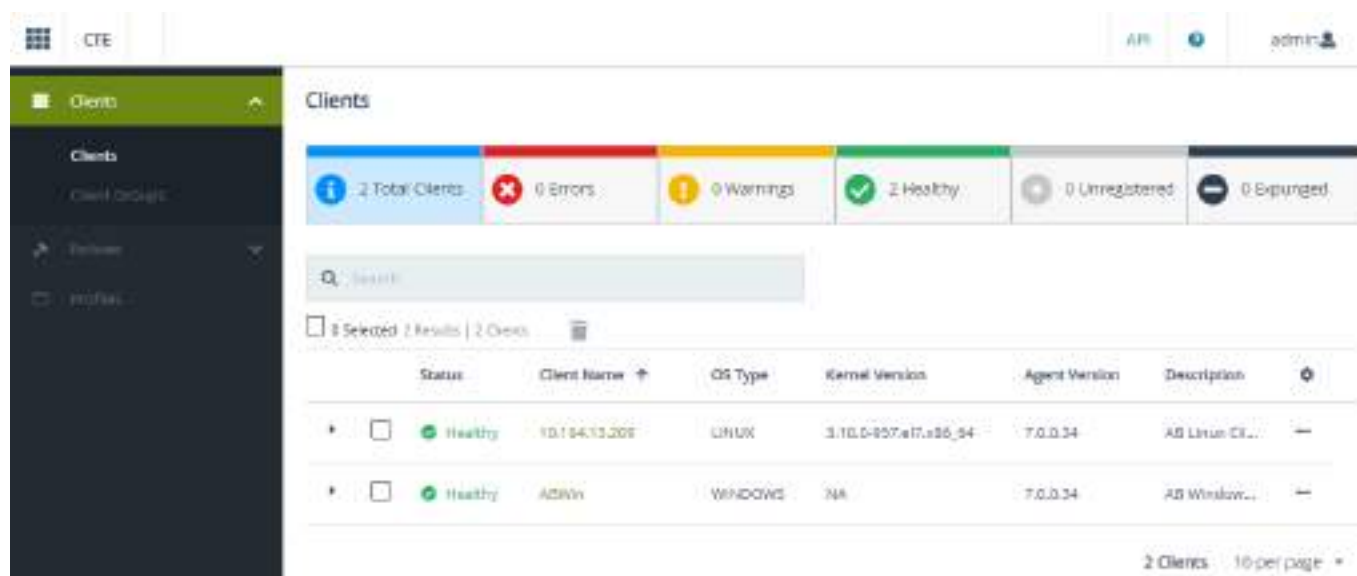
GUI

Use the CipherTrust Manager's GUI (also called the Management Console) to perform management functions such as managing profiles, policies, clients and client groups, and GuardPoints. These functions can also be performed using the CLI tool or the REST API.

To use the GUI:

1. Open the **CipherTrust Manager** URL in a browser.
2. Enter **Username** and **Password**.
3. Click **Log In**. By default, the Applications page is displayed.
4. Click **CTE** to open the application.

The Clients page of the CTE GUI is displayed, as shown below.



The main components of a CTE GUI are:

- > "Header" below
- > "Left Pane" on the next page
- > "Page" on the next page
- > "Notifications" on page 20

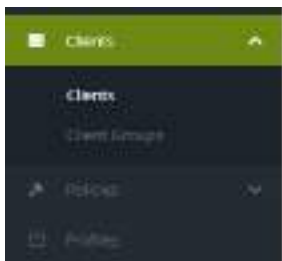
Header

Element	Description
	App switcher. Click to view and switch to another application such as Keys & Access Management and Admin Settings .
CTE	Application name. For CTE, CTE is displayed.

Element	Description
API	Link to the API playground.
	Link to the CipherTrust Manager product documentation.
	Logged in user. Click to switch domains, view and update user settings (Email address and password), and log out.

Left Pane

Contains links to manage CTE resources - clients, policies, and profiles.

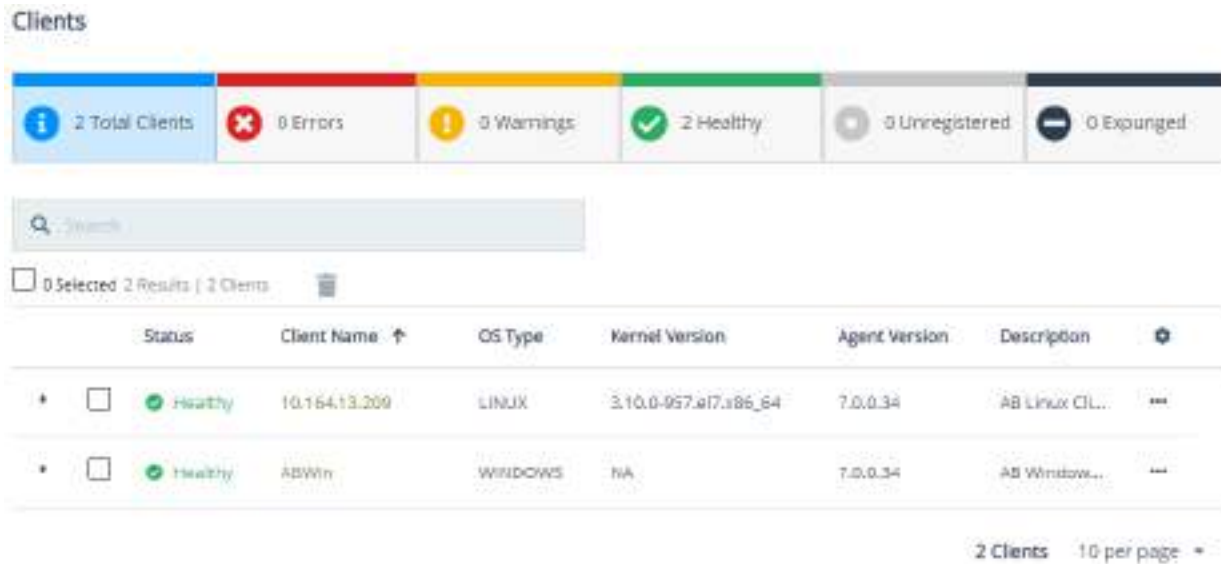


Element	Description
Clients	Click to manage clients and client groups. Clients > Clients is the option selected by default. Refer to "Managing Clients and Client Groups" on page 55 for details.
Policies	Click to manage policies and policy elements—resource sets, user sets, process sets, and signature sets. Refer to "Managing Policies" on page 101 for details.
Profiles	Click to manage profiles. Refer to "Managing Profiles" on page 42 for details.

Page

A page is the main working area that provides options to manage CTE resources. Depending on the selected option in the left pane, the page shows different types of information. These options are described in this document, where appropriate.

At any time, a page can either be in the list view or in the edit view. A sample screenshot of the list view of the Clients page is shown below. Most pages follow the similar pattern except that they show different content based on the resource being managed.



The sample page shown above can be divided into the following elements:

Element	Description
Title	Shows the page name.
Status bar	Shows the total number of clients added to the CipherTrust Manager, the number of clients with errors, warnings, healthy state. The status bar also shows the number of unregistered and expunged clients on the CipherTrust Manager. The status bar also acts as a filter. Click a health status to see the list of clients with that status.
Search box ()	Filters clients based on their partial or full names. Search is case-insensitive.
List	Shows the clients based on the selected health status. By default, all the clients added to the CipherTrust Manager are displayed.
Delete icon ()	Deletes the selected clients. A message is prompted to confirm the action.
Check box (☐)	Provides an option to select a client for deletion or modification. Multiple clients can be selected to perform the delete operation on them. Use the check box provided just under the Search box to select all clients visible on the page.
Expand icon ()	Shows mini detail view of a client in the clients list.

Element	Description
Custom View icon (⚙)	Hides/shows optional columns. For example, click this icon on the Clients page shows:  Select or clear the desired column and click OK.
Overflow icon (⋮)	Shows additional options. Depending on the current state of a client, the options can vary.
Pagination	Helps configure the number of records to display. By default, 10 records per page are displayed. 

Notifications

CTE prompts toast notifications at the top right corner of the main page area. These notifications are shown when operations such as creation or deletion of an entity is performed.

Green success toast notifications are displayed for successful operations.



Red error notifications are displayed for failed operations.



CHAPTER 2: Licensing

CTE base and LDT add-on licenses are offered through the following licensing models:

- > ["Trialware" below](#)
- > ["Time-limited Rental" below](#)
- > ["Perpetual Licensing Model" below](#)
- > ["Add-on Licenses" on the next page](#)
- > ["Installing CTE Licenses" on the next page](#)

Trialware

Provides the fully-functional CTE solution for 90 days with pre-installed trial license. After the trial period expires, CTE configurations on the CipherTrust Manager become read-only. Only decryption of GuardPoints is allowed; LDT-enabled registration is not allowed.

This is the default license shipped with the CipherTrust Manager.

Time-limited Rental

Provides the fully-functional CTE solution for a prepaid charge for a specific period of time, for a specific number of clients.

This license comes with a grace period of 90 days. After the license period expires, the grace period starts. During the grace period, CTE continues working normally. However, after the grace period is over, CTE configurations on the CipherTrust Manager become read-only. Only decryption of GuardPoints is allowed; LDT-enabled registration is not allowed.

The CipherTrust Manager GUI starts showing a notification about the remaining license time. The license renewal can be ordered before the license expires.

NOTE The number of clients that can be registered with the CipherTrust Manager is limited by the number of licenses purchased.

For example, if a 1-year license is purchased for 1000 clients, then only 1000 clients can be registered with the CipherTrust Manager.

Perpetual Licensing Model

Provides the fully-functional CTE solution for a prepaid charge with no time limit, for a specific number of clients.

NOTE The number of clients that can be registered with the CipherTrust Manager is limited by the number of licenses purchased.

For example, if a perpetual license is purchased for 1000 clients, then only 1000 clients can be registered with the CipherTrust Manager.

A CipherTrust Manager appliance administrator can install the CTE license.

Add-on Licenses

CTE offers the Live Data Transformation (LDT) feature as an add-on license. To use the LDT feature, you need a CTE base license activated on the CipherTrust Manager.

Installing CTE Licenses

Installing a CTE license requires a license string for the CipherTrust Manager with which the clients will be registered. This string is generated when a license is activated on the Sentinel EMS License Portal.

To install a CTE license:

1. Log on to the **CipherTrust Manager** GUI as administrator.
2. Click **Admin Settings** to open the application.
3. Click **Licensing**, if needed. A list of licenses is displayed on the right.
4. Click the **Lock codes** tab.
5. Click to expand **Connector Lock Code**.
6. Copy the **Connector Lock Code**. Every CipherTrust Manager appliance has a unique connector lock code. This lock code is needed to activate a CTE license for the CipherTrust Manager.

NOTE In a CipherTrust Manager cluster, the connector lock code is applicable to all nodes of the cluster to enforce connector licenses across the cluster nodes. When a CTE license is activated for one CipherTrust Manager appliance, the license is replicated on all the nodes of the cluster.

7. Activate the CTE license.

When you purchase a CipherTrust Manager and connectors, you receive an email after the Purchase Order (PO) is processed. Accompanying this email is a PDF attachment that contains the Entitlement ID (EID). This ID is needed to activate your license.

To activate the CTE license:

- a. Log on to the [License Portal](#). Use your EID when logging on for the first time.
- b. Register your account, if not already done. After registration, you can find the details about your EID and your available licenses.
- c. On the **Entitlements** tab, select the CTE license.
- d. Click **Activate**.

- e. In the **Quantity** field, specify the number of licenses to activate.
- f. In the **License Lock Code** field, paste the **Connector Lock Code** copied earlier.
- g. Click **Activate**.

NOTE

- > Based on the requirements, a CTE license is activated and a license string is generated.
- > The license string generated for one CipherTrust Manager cannot be used on any other CipherTrust Manager.

- h. Copy the **License String**. This license string is needed to install the CTE license on the CipherTrust Manager.
- 8. Return to the CipherTrust Manager GUI.
 - 9. Click the **Features** tab.
 - 10. Click **Add License**. The Add License dialog box is displayed.
 - 11. Paste the copied **License String** to the **License String** field.
 - 12. Click **Add**. The license is now installed.

The license is displayed in the installed licenses table with the feature name **CTE - TransparentEncryption**.

After the base CTE license is installed, an LDT add-on license can be activated and installed. The installed LDT license is displayed with the feature name **CTE - LiveDataTransformation**.

NOTE When a client is unregistered (unenrolled), the number of Used Clients on the Licensing page remains the same. To update the clients usage, the unregistered client must be deleted from the CipherTrust Manager. After the client is deleted, the license is released and can be used to register another client.

CHAPTER 3: Concepts

This chapter describes the following concepts:

- > ["Clients" below](#)
- > ["Client Groups" below](#)
- > ["GuardPoints" on the next page](#)
- > ["Policies" on the next page](#)
- > ["Security Rules" on page 26](#)
- > ["Resource Sets" on page 29](#)
- > ["User Sets" on page 29](#)
- > ["Signature Sets" on page 29](#)
- > ["Process Sets" on page 30](#)
- > ["Key Rules" on page 30](#)
- > ["Data Transformation Rules" on page 30](#)
- > ["Profiles" on page 31](#)
- > ["Learn Mode" on page 31](#)
- > ["User Roles" on page 31](#)

Clients

A client is a computer system where the data needs to be protected. A compatible CTE Agent software is installed on the client. The CTE Agent can protect data on the client or devices connected to it. A client can be associated with multiple GuardPoints for encryption of various paths (refer to ["Managing GuardPoints" on page 135](#) for details).

Client Groups

A client group is used to group one or more clients to simplify configuration and administration. GuardPoints created on a client group are applied to all members of the group. Additionally, you can apply client group configuration settings to all clients in a client group. A client can be a member of multiple client groups.

If you have created a group of one type of clients, then you should only add similar clients to the group. Same configuration settings can only be applied to clients of the type with which the client group is created. If a different type of client is added, configuration settings cannot be applied to that client.

Refer to ["Managing GuardPoints" on page 135](#) for details on creating GuardPoints on client groups.

GuardPoints

A GuardPoint specifies the list of folders that contains paths to be protected. Access to files and encryption of files under the GuardPoint is controlled by security policies.

Refer to ["Managing GuardPoints" on page 135](#) for details.

Policies

A policy is a collection of rules that govern data access and encryption. Think of a policy as an if-then statement. Policy rules are processed sequentially. If the criteria of rule one are not met, the policy enforcement engine moves on to the second rule and so on.

Policies specify:

- > **Actors:** Users, groups, and processes that are permitted/denied access to protected data.
- > **Actions:** What actions authorized actors are allowed to perform. For example create/delete, read/write, decrypt, modify permissions, and so on.
- > **Files acted upon:** Policy rules may apply to entire directories and mount points, or only to files named in a specific way (for example, .docx files may be encrypted and restricted to read only access by designated users, while other files may be stored clear and read and written by anyone).

Additionally, each CTE policy specifies one or more encryption keys used to encrypt blocks of file data when applications write them, and decrypt them when they are read.

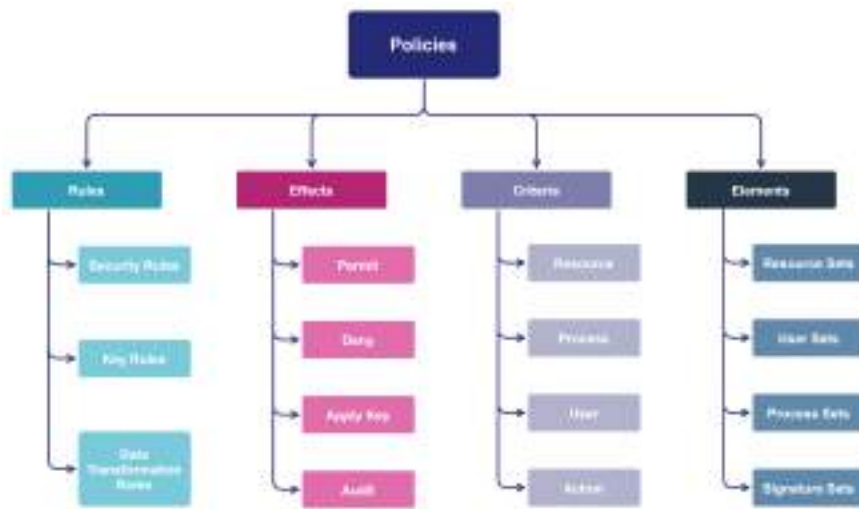
CTE encryption is transparent to applications. This means that the CTE Agent encrypts blocks of data as they are written, and decrypts data when they are read by authorized users and applications. This architecture separates administration of files from access to the data in them. Backup programs, for example, may be authorized to read files, but not view the data in them. Therefore, data can be backed up and taken offsite while remaining encrypted so that security is not breached.

A policy comprises ["Security Rules" on the next page](#), ["Key Rules" on page 30](#), and ["Data Transformation Rules" on page 30](#).

CTE supports the following policy types:

- > **Standard:** Access to data is blocked during initial encryption or rekeying of data.
- > **Live Data Transformation (LDT):** Encryption and rekeying of data takes place in the background, without disrupting user or application access to that data.
- > **Cloud Object Storage (COS):** Applicable to GuardPoints in Amazon S3 buckets. Access to data is blocked during initial encryption or rekeying of data.

The following diagram shows the main components of a policy:



Refer to ["Managing Policies" on page 101](#) for details.

Security Rules

A security rule defines:

- > Who can access the data (User or Group)
- > What they can do with the data (Action)
- > What applications or executables have access to the data (Process)
- > Where the data is located (Resource)
- > How the data can be accessed (Effect)
- > Whether it can be enforced on the subdirectories of the GuardPoint (Browsing)

Security Rule Criteria

Security rules consist of five criteria. They specify the attributes of an access attempt, and effects, which define whether that access is permitted or denied, and whether encryption/decryption is required. The following table lists policy rule criteria.

Criteria	Description
Resource	Specifies which files and/or directories in a GuardPoint are to be protected. For example, <code>/secure_dir/financials</code> .
User	Specifies a which users or groups of users can access the files.
Process	Specifies executables that can operate on the files.
Action	Specifies the allowed file action. Action could be read, write, remove, rename, and make directory. Refer to "Actions" on the next page for the complete list of supported actions.

Criteria	Description
Effect	Describes the type of access granted or denied according to the rule. Refer to "Security Rule Effects" on the next page for the list of supported effects.

Actions

Action specifies the type of access (read, write, copy, and move etc.) being made on the protected files. The following table lists all basic and advanced actions:

Basic Actions

Action	Description
read	read operations
write	write operations
all_ops	all operations
key_op	key operations

Advanced Actions

Action	Description
f_rd	read file
f_wr	write file
f_wr_app	write file appending
f_cre	create file
f_ren	rename file
f_link	link file
f_rm	remove file
f_rd_att	read file attribute
f_chg_att	change file attribute
f_rd_sec	read file security
f_chg_sec	change file security

Action	Description
d_rd	read directory
d_ren	rename directory
d_rd_att	read directory attribute
d_chg_att	change directory attribute
d_rd_sec	read directory security
d_chg_sec	change directory security
d_mkdir	make directory
d_rmdir	remove directory

Security Rule Effects

An effect describes the type of access granted or denied according to the rule. The following table lists policy effects that can be applied to GuardPoints.

Effect	Description
Permit	Allows access attempts to the resource. For example, you can specify an effect that allows writing to a directory.
Deny	Denies access attempts to the resource. For example, you can specify an effect that denies any attempts to access a resource.
ApplyKey	Applies an encryption key to the data in a GuardPoint. When applied, the data copied to the GuardPoint is encrypted with the specified key. When the data in the GuardPoint is accessed, it is decrypted using the same key.
Audit	Creates a message log entry for each qualifying event that records who is accessing what information and when.

How Security Policy Works

Every time a user's application tries to access a GuardPoint file, the security policy tests that access attempt against the criteria of each rule. For example, suppose a user, Harry, wants to access and modify a file called `secret`, using the command `cp`. For Harry to be successful, there must be a rule that allows access to `secret` (resource), by user Harry (user), using the command `cp` (process), and includes the permission `write` (action).

- > If criteria is not specified, a value of *All* is used.
- > If *resource* is not specified, the rule applies to all resources.
- > If *user* is not specified, the rule applies to all users.

- > If *process* is not specified, the rules apply to all executables, and so on.
- > *Effect* cannot be left unspecified. It must have at least a permit (allow access) or deny (disallow access).

A policy can have multiple rules. Rules are evaluated much like firewall rules. They are evaluated in order, from first to last. Evaluation stops when a rule is found for which all the criteria are met. The effect for that rule is then enforced. Therefore, you must carefully order a policy's rules to achieve the desired result.

Resource Sets

A resource is a combination of a directory, a file, and patterns or special variables. A resource set is a named collection of directories, files, or both, that a user or process will be permitted or denied access to.

Refer to ["Creating Resource Sets" on page 104](#) for details on creating resource sets.

User Sets

A user set is a collection of users and user groups that you want to grant or deny access to GuardPoints. User sets are configured in policies. Policies can be applied to user sets, not to individual users.

Refer to ["Creating User Sets" on page 105](#) for details on creating user sets.

Signature Sets

A signature set is a collection of hashes of processes and executables that you want to grant or deny access to GuardPoints. A signature set can be configured in a policy as part of a process set to verify the integrity of a process before it is allowed access to guarded data. Policies are applied to signature sets, not to individual signatures.

A cryptographic hash is created for each file in a signature set that meets a specific criterion. It would take longer, bloat the CipherTrust Manager database, and reduce performance to sign all the files in a signature set, especially when the set comprises top-level directories. The criteria is listed below. All other files are skipped.

Executables accessing a GuardPoint can be inside or outside the GuardPoint. If they are inside:

- > On a Windows client, *all* files in a signature set that are *inside* a GuardPoint are signed. Only the *compiled* Windows executables in the signature set that are *outside* the GuardPoint are signed. Non-executables outside the GuardPoint are not signed.
- > On a UNIX client, it makes no difference whether the files are inside or outside a GuardPoint. Only the files in a signature set with one or more execute bits set (for example, `-rwxrwxrwx-`) are signed.
- > File extension has no impact. Even files like the following are skipped:
 - [On Windows] `.bat` and Visual Basic programs if they are not inside a GuardPoint
 - [On Linux] `.so` files if they do not have an execute bit set

Every instance of a file that is copied to a different location or to a different name will have the same signature. This can be a convenient way to detect duplicate files on your system.

By default, a generic error message is displayed about a non-existent source being detected. The name of the offending file or directory is not specified. However, it is specified in the Agent log on the client. Review the logs to:

- > Identify the offending file or directory.
- > Determine how many files were affected, what file "is invalid for the signature request".
- > Identify the files that were not signed. Look for files with "is invalid for the signature request".

Refer to ["Managing Signature Sets" on page 86](#) for details on the signing process.

Process Sets

A process set is a collection of processes (executables) that you want to grant or deny access to GuardPoints. Like user sets, process sets can be configured in policies. Policies can be applied to process sets, not to individual processes.

Optionally, file signing can be configured to check the authenticity and integrity of executables and applications before they are allowed to access GuardPoint data. A signature set must already exist before you can configure file signing in a policy for a process set.

Refer to ["Creating Process Sets" on page 110](#) for details on creating process sets.

Key Rules

A key rule defines the encryption key to apply to a specific resource set or the encryption key to use as the default key, if no other key rule matches. The key rule defines the sequence in which the key rules are to be executed (Order), the location of the data to be encrypted (Resource), and the encryption key to be applied to the resource set (Key).

When defining a key rule for an LDT policy, you can select a key that is applied to the resource set (Current Key Name) and the key to use to rekey that resource set (Transformation Key Name).

NOTE Keys are created and stored on a CipherTrust Manager appliance.

Data Transformation Rules

Data transformation (dataxform) rules define:

- > Resources to be protected
- > Symmetric encryption key to use for
 - Rekeying the specified resources from one encryption key to a different key or
 - Rekeying resources into a plaintext format (also referred to as clear, unencrypted, or decrypted)

Profiles

A profile contains the CipherTrust Manager logging criteria for CTE clients, Syslog server configuration, default logging level, LDT Quality of Service (QoS) settings, and other settings that can be used for several CTE clients.

A default profile, `DefaultClientProfile`, is created automatically when either of the following happens:

- > On successful registration of the *first* client if no profile is specified during registration.
- > On creation of the *first* client group. A new client group is automatically linked to `DefaultClientProfile`.

When registering a CTE client, the installer prompts to specify a profile for the client. If not specified, `DefaultClientProfile` is automatically linked to the client on successful registration. The linked profile can be modified later. It is recommended to not delete or modify `DefaultClientProfile`.

Learn Mode

Learn Mode permits a policy to be tested without actually denying access to the GuardPoint. In Learn Mode, all actions that would have been denied are instead permitted, but logged. This allows you to test policies by tracking how rules are evaluated, without enforcing the policy. Monitor the log to determine how data is being accessed, then modify the policy accordingly.

In Learn Mode:

- > If the policy contains a security rule with the effect permission `Permit` and the effect option `ApplyKey`, then a security rule with the permission `Deny` **MUST** include the option `ApplyKey`. If it does not include the option `ApplyKey`, a user with the `Deny` permission can overwrite or edit data, which can corrupt the data.
- > Effect permission `Deny` has the same effect as `Permit`, and `Deny ApplyKey` has the same effect as `Permit ApplyKey`.

This option generates an `ERROR` log each time an access attempt is made that matches any security rule in the policy. The `ERROR` log is labeled `[LEARN MODE]` and can be viewed in the CTE Agent logs or under Records on the CipherTrust Manager GUI (if the log level is configured as `ERROR`).

Learn Mode is recommended for policies that restrict by application (process). Many applications use multiple binaries that may not be known to the creator of the policy at the time of creation. So, Learn Mode should be enabled when creating policies for such applications.

CAUTION! Use Learn Mode to analyze access patterns and make informed decisions about final encryption policies. Do not keep Learn Mode running for long time.

User Roles

CTE has the following users with different responsibilities in administering and using the system.

CAUTION! It is critical that credentials of these users are kept in a secure location. If a credential is compromised, an attacker could gain access to sensitive data.

CTE Admins

Initially, there is a System Defined Group named "CTE Admins". Users within the "CTE Admins" group are CTE Administrators.

A CTE Administrator is responsible for creating and managing the following resources:

- > Clients and client groups
- > Profiles, policy elements, and policies
- > GuardPoints
- > Client registration tokens

NOTE Only the users of the "CTE Admins" group can delete CTE keys.

CTE Clients

There is a System Defined Group named "CTE Clients". CTE clients registered with the CipherTrust Manager are part of this group.

CHAPTER 4: Introduction to Data Transformation

This chapter provides an overview of the data transformation process. It covers the following information:

- > ["The Data Transformation Process" below](#)
- > ["Data Transformation Techniques" on page 35](#)
- > ["Protection Policies" on page 40](#)

The Data Transformation Process

Data transformation is the process of transforming GuardPoint data from:

- > Plaintext (clear) to encrypted with a key
- > Encrypted with a key to plaintext
- > Encrypted with one (old) key to encrypted with another (new) key

This section covers the following information:

- > ["Uses of Data Transformation" below](#)
- > ["How CTE Protects Files" below](#)
- > ["Components of the CTE Solution" on the next page](#)
- > ["Properties of Data Transformation" on the next page](#)

Uses of Data Transformation

- > **Initial Data transformation:** Encrypting GuardPoint data for the first time.
- > **Rekeying:** Changing the encryption key for GuardPoint data, also called key rotation.
- > **Reverse Transformation:** Decrypting GuardPoint data to clear text (not a common procedure).
- > **Convert:** Non-LDT GuardPoints to LDT GuardPoints.

NOTE Data transformation is complex and disruptive to data center operations. It is strongly recommended that you read and understand this section before you proceed to the initial data transformation and rekey.

How CTE Protects Files

The CTE Agent encrypts the data within a file one block at a time. It does not encrypt file metadata such as a file's name or size. This enables administrators to manage files without being able to view or modify their contents. Whether initially encrypting files, rekeying them, or decrypting them, the CTE Agent must therefore:

- > **Read** each block of file data to be transformed.
- > **Transform** the block by encrypting, decrypting, or rekeying it.
- > **Write** the transformed block, either to its original location, or to an alternate one.

Components of the CTE Solution

CTE protects data either at the file level or at the storage device level. CTE file-level protection consists of two main components:

> CipherTrust Manager

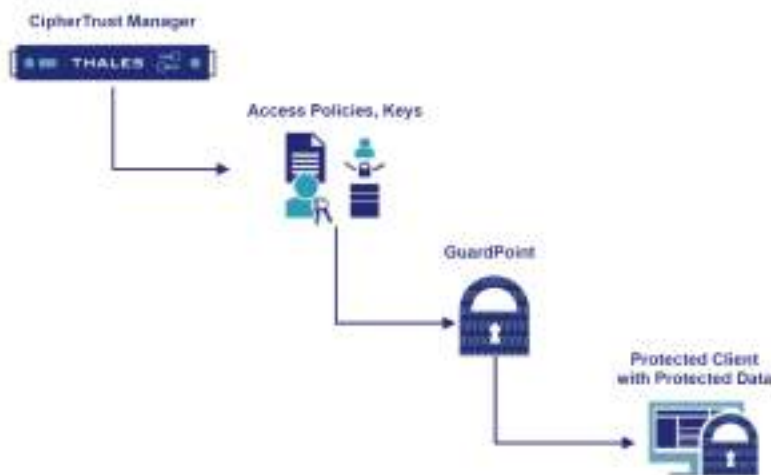
An appliance that manages a database of the file sets protected by CTE GuardPoints, the encryption keys that protect them, policies that specify access rights and encryption protections that can be applied to GuardPoints. The CipherTrust Manager is also a central point for logging events related to accessing protected files.

> CTE Agents

Software components that run on clients with file sets to be protected. A CTE Agent manages the files behind a GuardPoint by enforcing the policy associated with it, and communicates data access events to the CipherTrust Manager for logging.

A GuardPoint is usually associated with a Linux mount point or a Windows volume, but may also be associated with a directory subtree. The CTE Agent sits between applications and the file system that clients files within the GuardPoint. It intercepts every file access request, and enforces the access and encryption rules defined in the GuardPoint's policy.

Figure: CTE Operation



Properties of Data Transformation

For large file sets (hundreds of GBs or more), bulk transformation is time consuming. Managing transformation time is important, because file set content must be frozen (inaccessible to applications) throughout the transformation process. Once transformation starts, it must continue until complete. So transformation time determines the window of data unavailability. Two major components contribute to transformation time:

> Number of Blocks of File Data

Because CTE must read, transform, and rewrite each block of file data, this component can be estimated by multiplying the number of file blocks to be transformed by the average read, transformation, and write time for a block.

> Number of Files

Because the CTE Agent transforms data file by file, each file must be “looked up,” opened, and closed during transformation, using underlying file system mechanisms. This typically requires multiple disk accesses. Therefore, file sets that consist of many small files, per file overhead, can actually exceed file block transformation time.

Other factors, such as file system fragmentation, and load from concurrent applications, may also affect transformation time. Mainly, the number of blocks and number of files to be transformed are fundamental because they cannot be reduced or eliminated.

Data Transformation Techniques

Three methods to initially encrypt and rekey files are:

- > **The Copy/Restore Method:** Using the operating system file copy utility, the client administrator can copy unprotected files to a location protected by a CTE GuardPoint with a standard/production policy.
- > **The CTE Dataxform Utility Method:** Every CTE Agent includes a utility program that can encrypt or transform protected files. The dataxform utility encrypts, rekeys, or decrypts data in-place. Refer to the CTE Data Transformation Guide for details.
- > **The Live Data Transformation (LDT):** The CipherTrust Manager Security Administrators can encrypt or rekey GuardPoint data **without blocking** the user or application access to that data. Refer to the CTE-Live Data Transformation with CipherTrust Manager for details.

These methods have advantages and limitations that make them suitable in different scenarios. These are discussed in the subsequent sections.

Apart from encrypting data, you can reverse the transformation, that is, decrypt the data to plaintext. To **decrypt** protected files, copy them to an *unprotected* location.

NOTE CTE can also be configured to protect data at the disk level. For data protected in this way, only the copy transformation technique is available for encryption.

The Copy Method

Properties of the Copy Method

The copy method performs initial encryption, rekeying, and decryption by copying data from one directory, or GuardPoint, to another directory or GuardPoint.

> Initial Encryption

The client administrator encrypts a file set by copying it to a directory protected by a CTE GuardPoint with a standard policy. Encryption is transparent to the copy utility.

Figure: Initial Encryption



> Rekeying Protected Data

Encrypted files protected by a CTE GuardPoint are rekeyed by copying them to a directory protected by another GuardPoint with a different encryption key. Both decryption and re-encryption are transparent to copy utilities.

Figure: Rekeying Protected Data



> Decrypting Data by Copying

Decrypt a protected file set by copying files from their protected location to unprotected directories. The CTE Agent decrypts file blocks before delivery to the copy utility for rewriting.

Figure: Decrypt Data by Copying



CAUTION! If the governing policy does not authorize the copy utility user to access data, CTE delivers encrypted file blocks to it.

Advantages of the Copy Method

> Simplicity

After an Agent is installed and GuardPoints are activated on a client, the client's administrator can encrypt, decrypt, or rekey file sets simply by copying them from one location to another. There are no procedures to learn, and no requirements to coordinate with the CipherTrust Manager Security Administrator. Data transformation is simply another routine administrative task.

> Recoverability

If a copy-based transformation is interrupted, for example, by a power failure or a system crash, the transformation resumes at or prior to the point of interruption. This is because the source files remain available and can be recopied, overwriting files at the destination that may have been only partially re-encrypted.

Limitations of the Copy Method

> Storage Resource Consumption

Copying a file set requires that both source and destination files exist simultaneously. Storage capacity sufficient for both must be available during initial encryption. For very large protected data sets, “extra” temporary storage may be a significant expense. However, a greater concern is likely to be the impact of moving production file sets as they are transformed. File data is unprotected while in the copy utility’s buffers.

> Impact on Operating Procedures

Original and copied file sets have different path names and/or network addresses. After transformation, either both file sets must be renamed (the old path to a new name, and the new path to the old name), or applications must be adapted to process the transformed data set at the new directory. For a small data center with a few protected file sets, some combination of these options is usually practical. For data centers with hundreds of protected file sets, the administrative complexity and consequent chance of error make copying a complex option.

The Restore Method

A variation of the copy method is to make a backup of the files for transformation and restore the backup to the destination location. This works because:

- > Backing up data causes it to be read and decrypted.
- > Restoring data causes it to be written (re-encrypting it with an alternative key).
- > CTE protection is transparent to backup programs.

This technique also creates a backup of the data set. However, a disadvantage is the time required to copy data twice (once from the source location to backup, and once from backup to destination location).

These considerations suggest that copying data to transform it is more suitable for initial encryption (and final decryption), and less so for rekeying. Additionally, the simplicity of recovering an interrupted transformation makes the copy/restore method useful in situations where the probability of interruption during transformation is significant.

The Dataxform Utility Method

The CTE dataxform utility transforms data-in-place and contains two components:

- > User mode that controls the overall operation
- > Kernel mode that transforms files block-by-block

Figure: Offline Rekey



Advantages of the Dataxform Utility

Transforming data in place has two advantages:

> Minimal Storage Requirements

Because dataxform transforms files in place, where they reside, it does not require temporary file storage. However, the utility does need storage in which to create a list of files for transformation.

> Security

The period of time that the data transformed by the dataxform utility appears in memory, outside the GuardPoint and therefore, unprotected, is shorter than with copying. This is significant for rekeying (compared to copying), which holds clear file data in memory between reading and rewriting. Moreover, dataxform requires coordination between the client and CipherTrust Manager Security Administrators, so that no one individual can subvert security during transformation.

Limitations of the Dataxform Utility

Offsetting the advantages of the dataxform utility method is the complexity of recovering from an interrupted dataxform run. Because dataxform transforms files in-place, data in a file undergoing transformation at the time of a failure may be only partly transformed. There is no way to determine which blocks have been transformed and which have not. These files must be recreated after the dataxform runs from a backup copy. The client administrator must:

1. Determine (by examining dataxform logs) which files may have been incompletely transformed.
2. Delete them from the transformed file set.
3. Recreate them by selective copying from a backup.

Live Data Transformation

The CipherTrust Manager security administrators can encrypt or rekey the GuardPoint data without blocking the user or application access to that data.

After enabling GuardPoints, LDT performs initial encryption or rekeying in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block application and user access to data during encryption or rekey operations, which can seriously inconvenience users and affect operational efficiency.

Phases of LDT runtime operation:

1. Initial data transformation starts or key expires

Live Data Transformation begins when an LDT policy is first applied to a GuardPoint, or when a current key version expires. The CipherTrust Manager pushes the new policy, or the notification of a key version change, to the clients that are protected by those policies.

2. New key version triggers a rekey on the affected GuardPoints

On each client, CTE determines which GuardPoints are using the key that has just rotated to a new version. CTE starts an LDT rekey on each of those GuardPoints. (If another rekey is already underway on that GuardPoint, the new rekey is rejected).

3. Scan for files

On each GuardPoint where CTE has started a rekey, LDT determines which files to transform. LDT takes inventory of files encrypted with earlier versions of the rotated key and makes a persistent list of the files for transformation. During this phase, the rekey status of the GuardPoint becomes starting, then scanning.

The scan phase might be interrupted, such as by a client reboot. In this case, when the client reboots and the GuardPoint is enabled again, the scan operation starts over from the beginning.

4. Rekey/Key Rotation

a. Each file, from the persistent list of files, is decrypted using the old version of the key. The old key is applied to each file and then re-encrypted using the new version of the key. Note that new files created during the LDT process do not need to be rekeyed, as they inherit the new version of the key. Multiple files and multiple regions of files are rekeyed simultaneously.

b. The LDT extended attribute of each file is updated.

c. The LDT rekey operation can be suspended and resumed manually, or through the QoS schedule.

This manages the impact LDT has on other applications and processes. During this phase, the rekey status of the GuardPoint is rekeying or suspended.

If system errors occur during rekeying, such as IO errors or crashes, LDT can manage and recover from them after the system error is fixed.

5. Finish

When all of the required files in the GuardPoint have been rekeyed, the system and storage resources used by LDT are released, except for the storage required for the extended attributes. Upon completion of rekey, the rekey status of the GuardPoint is rekeyed.

Summary

The following table summarizes the strengths and weaknesses of the two file set transformation methods.

Factor	Copy Method	The dataxform Utility Method	Live Data Transformation
Temporary storage required	Equal to size of file set.	Sufficient to hold a list of path names of files in file set.	Additional space is required to store LDT metadata only.

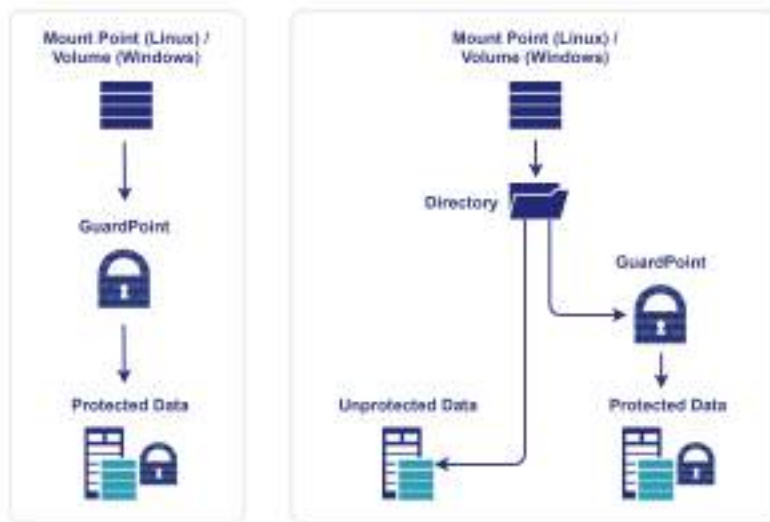
Factor	Copy Method	The dataxform Utility Method	Live Data Transformation
Security	File data is unprotected while in copy utility's buffers.	File data is never outside the CTE GuardPoint.	File data is never outside the CTE GuardPoint.
Initial encryption	Files can be copied directly from source directory to a CTE-protected directory.	Files must be in a protected location before transformation.	Files must be in a protected location before transformation.
Operational impact	No access to files during transformation. Path names or operating procedures must be adjusted after transformation.	No access to files during transformation. No other impact on operating procedures.	Encryption and rekeying of the data takes place in the background, without disrupting user or application access.
Recoverability	Restart copy operation at, or prior to, point of failure.	Files undergoing transformation at the point of failure must be discovered from dataxform logs and restored from backup.	Transformation process automatically restarts from the point of failure.

Protection Policies

The basic unit of CTE data protection policy application is the GuardPoint. GuardPoints are typically associated with file system mount points, but may also be associated with directory sub-trees.

NOTE Nested mount points within a directory, or mount points protected by a GuardPoint, are also protected in Linux environments.

Figure: CTE GuardPoints



All files in the directory hierarchy, below a GuardPoint, are subject to the GuardPoint's policy, which consists of rules that specify:

- > **Protected files:** Filenames or filename patterns (example: *.dat) to which the policy applies.
- > **Authorized users:** User(s) group(s), and application(s) permitted to access the protected files.
- > **Permissions:** Actions permitted to users (example: create/delete, read/write, rename, decrypt).

Policies also specify the name of an encryption algorithm and a key for encrypting protected files. For example, a policy might specify that all Excel workbooks protected by a GuardPoint be encrypted using an AES256 key called EXCEL KEY. Additionally, only users in group 128 have access to the files. All other files that are not encrypted, are freely accessible to all users.

Types of Policies

CTE Agents use two types of policies:

> Initial Data Transformation

Dataxform policies contain the elements listed above, plus a data transformation key, used by the dataxform utility to rekey file data. Transformation policies contain strict access control rules that prevent application and user access to files during transformation. CTE only uses dataxform policies for the initial transformation. Afterwards, you replace it with a production policy.

Dataxform operates on a per-GuardPoint basis. For initial encryption, the dataxform policy specifies a clear production key (meaning that the utility does not decrypt data because the data is unencrypted) and a new data transformation key to encrypt the data.

> Production/Standard

Production policies contain the elements listed above. They protect data within GuardPoint(s) during day-to-day IT operations.

For decryption, the policy specifies a clear data transformation key (that is, the utility does not re-encrypt files as it rewrites them) and the current production key.

A rekeying transformation policy specifies both a current production ("old") key and a transformation ("new") key.

CHAPTER 5: Managing Profiles

A profile contains the CipherTrust Manager logging criteria for CTE clients, Syslog server configuration, default logging level, LDT Quality of Service (QoS) settings, and other settings that can be used for several CTE clients.

A default profile, `DefaultClientProfile`, is created automatically when either of the following happens:

- > On successful registration of the *first* client if no profile is specified during registration.
- > On creation of the *first* client group. A new client group is automatically linked to `DefaultClientProfile`.

When registering a CTE client, the installer prompts to specify a profile for the client. If not specified, `DefaultClientProfile` is automatically linked to the client on successful registration. The linked profile can be modified later. It is recommended to not delete or modify `DefaultClientProfile`.

This section covers the following information:

- > ["Creating a Profile" below](#)
- > ["Setting Client Log Configuration" on the next page](#)
- > ["Setting Client Syslog Configuration" on page 48](#)
- > ["Setting Quality of Service Configuration" on page 50](#)
- > ["Concise Logging" on page 52](#)
- > ["Modifying Profiles" on page 53](#)
- > ["Deleting Profiles" on page 54](#)

Creating a Profile

To create a profile:

1. Open the **CTE** application.
2. In the left pane, click **Profiles**.
3. Click **Create Profile**.
4. Specify a unique **Name** for the profile. This is a mandatory field.
5. Provide a **Description** for the profile.
6. Click **Create**.

The newly created profile appears in the profiles list.



After you have created a profile, you can define client logging criteria, Syslog configurations, and QoS configurations. These configurations apply to the clients linked to this profile. Refer to the subsequent sections for details.

Setting Client Log Configuration

Client log configuration includes basic information such as the level of logs to capture, whether to enable the Syslog server, settings to upload logs to the CipherTrust Manager, and settings to store logs on clients.

To define client log configurations for a profile:

1. Open the **CTE** application.
2. In the left pane, click **Profiles**.
3. Under **Name**, click the desired profile. The edit view of the profile is displayed. Profile settings are divided into three categories, as shown below:



4. Click **CLIENT LOGGING CONFIGURATION** to expand it. The client log configuration settings are categorized into basic, log upload to key manager, and log to the file on the clients.

Basic Log Settings

Log Level: INFO

Duplicates: SUPPRESS

Threshold: 5

Suppress Interval (sec): 600

☐ Enable Concise Logging

☐ Syslog Enabled

☐ Log Upload to Key Manager

Upload Log Level: INFO

Connection Timeout (sec): 50

☐ Drop if Busy

Upload Timeout (sec) 1-900: 600

Max Interval (sec) 1-1000: 20

Min Interval (sec) 1-30: 10

Message Upload Range (100-1000): 1000

☐ Allow Purge

Cache Settings

Max Files: 200

Max Space (MB): 100

Basic Log Settings

5. Specify the basic settings:

Field	Description
Log Level	Level of logs to generate. It defines the detail and extent of information to be logged by the linked agents. In sequence, the options are: > DEBUG: Fine-grained informational events that are targeted towards support engineers and developers. > INFO: Informational messages that highlight the progress of the application at coarse-grained level. > WARN: Potentially harmful situations. > ERROR: Error events that might still allow the application to continue running. This is the default log level. > FATAL: Severe error events that will presumably lead the application to abort. Log levels are cumulative. The level that you select not only generates log entries for events that occur at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.
Duplicates	Treatment for duplicate logs. The options are: > SUPPRESS: Messages follow the configured Threshold as to how many times duplicate messages are sent to the CipherTrust Manager during the given Interval. > ALLOW: All duplicate messages are captured and displayed in the log.

Field	Description
Threshold	(Used when the Duplicates field is set to <code>SUPPRESS</code> .) Maximum number of duplicate messages the CTE Agent can send to the CipherTrust Manager within the time specified by <code>Suppress Interval</code> (see below). The default value is 5 messages.
Suppress Interval (sec)	(Used when the Duplicates field is set to <code>SUPPRESS</code> .) Time in which the number of duplicate messages, specified by <code>Threshold</code> , can be uploaded to the CipherTrust Manager. When <code>Suppress Interval</code> exceeds, the count specified by <code>Threshold</code> starts again. The default interval is 600 seconds (10 minutes).
Enable Concise Logging	Whether to enable Concise Logging for the linked clients. Select to enable, clear to disable. By default, Concise Logging is disabled. When enabled, a reduced number of audit log messages are captured. Refer to "Concise Logging" on page 52 for details.
Syslog Enabled	Whether the Syslog server is enabled. Select to enable, clear to disable. When you select Syslog Enabled, make sure that client Syslog configurations are defined. Refer to "Setting Client Syslog Configuration" on page 48 for details. When the Syslog server is disabled, the logs are sent to the client messages file such as <code>/var/adm/messages</code> . On a Windows client, the messages are sent to the Event Viewer (Application events).

Log Upload Settings

6. Configure settings to upload logs to the CipherTrust Manager:

Field	Description
Log Upload to Key Manager	Whether to enable log upload to the CipherTrust Manager. Select to enable, clear to disable. When this option is selected, you can configure the settings listed below. The logs are displayed under the Client Records page of the CipherTrust Manager GUI.

Field	Description
Upload Log Level	Level of logs to upload. In sequence, the options are: > DEBUG: Fine-grained informational events that are targeted towards support engineers and developers. > INFO: Informational messages that highlight the progress of the application at coarse-grained level. > WARN: Potentially harmful situations. > ERROR: Error events that might still allow the application to continue running. This is the default log level. > FATAL: Severe error events that will presumably lead the application to abort. Log levels are cumulative. The level that you select not only generates log entries for events that occur at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.
Connection Timeout (sec)	Interval after which the connection attempt to the key manager expires. The default value is 59 seconds.
Drop if Busy	Whether to slow log generation and drop log files during periods of extreme logging (that is, when the server is busy). Select to drop, clear to keep trying. This setting is clear by default.
Upload Timeout (sec) 1-900	Interval after which the log upload attempt expires. The default period is 600 seconds (10 minutes).
Max Interval (sec) 1-1000	Maximum interval to wait before the CTE Agent can upload messages to the CipherTrust Manager. Use this option to update the log viewer even when the Message Upload Range has not been reached. Lower the interval if there is little CTE Agent activity. The default maximum interval is 20 seconds.
Min Interval (sec) 1-30	Minimum interval to wait before the CTE Agent can upload messages to the CipherTrust Manager. Increase the interval if there is considerable CTE Agent activity, so the agents do not flood the network with log messages. The minimum interval is 10 seconds.
Message Upload Range (100-1000)	Maximum number of logs to upload at one time. When the specified number of logs is reached, they are uploaded to the CipherTrust Manager. The default number is 1000.
Cache Settings	Settings to cache logs. The options are: > Max Files: Maximum number of log files to cache. The default number is 200. > Max Space (MB): Maximum log size to cache. The default value is 100 MB.

Log to File Settings

7. Configure settings to gather logs in files on clients:

Field	Description
Log to File	Whether to write logs to files on clients. This option is selected by default. This means that, by default, the logs are written to files on clients. The logs are sent to the <code>/var/log/vormetric/vorvmd_root.log</code> file of a UNIX client, or a Windows equivalent, such as <code>\Documents and Settings\All Users or WINDOWS\Application\Data\Vormetric\DataSecurityExpert\agent\log\vorvmd.log</code>. When the Log to File option is selected, you can configure the settings listed below.
File Log Level	Level of logs to capture in the log file. In sequence, the options are: > DEBUG: Fine-grained informational events that are targeted towards support engineers and developers. > INFO: Informational messages that highlight the progress of the application at coarse-grained level. > WARN: Potentially harmful situations. > ERROR: Error events that might still allow the application to continue running. This is the default log level. > FATAL: Severe error events that will presumably lead the application to abort. Log levels are cumulative. The level that you select not only generates log entries for events that occur at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.
Max File Size (1-1000 MB)	Maximum size of a log file. The CTE Agent starts a new, empty log file when the specified limit is exceeded. The default maximum file size is 1000 MB.
Max Old Files (1-100)	The maximum number of old log files to keep. The default number is 100.
Allow Purge	Whether to allow purging the old log files. Select to allow purge, clear to disallow. This option works in conjunction with the Max Old Files option (see above). For example, set Max Old Files to 3 and select the Allow Purge check box. After 3 log files are generated, the first log file, log1, is deleted and a new log file, log4, is created. If Allow Purge check box is clear, log files continue to accumulate in the server database and you have to remove them manually.

8. Click **Apply**.

The changes are effective immediately and apply to the clients linked with the profile.

The CTE client logs can be seen on the **Keys & Access Management > Records > Client Records** page of the CipherTrust Manager GUI. Filter the records by **Client Type** and look for the **CTE** records, as shown below.

Client	Client Type	Timestamp	Severity	Event	Details
3.34.30.9	CTE	Aug 31st 2020 - 13:04:08	ERROR	BadGridPath NotFound	<pre>{ "log": "CGA", "uid": "CGA37348", "pid": 1013, "args": [["op": "/Non-Existent-Path"]], "message": "Not guarding path [/Non-Existent-Path] (Reason: Does not exist)", "version": "3.0.0.38", "filename": "SecFS_upload_3.04.05.9.343", "hostname": "3.04.30.9", "client_id": "70c511e-29c2-4f66-8b5d-0072aee5f585" }</pre>

Refer to the "Records" section in the CipherTrust Manager Administrator Guide for details.

Setting Client Syslog Configuration

When you have Syslog servers up and running in your environment, you can redirect your client logs to them. A CipherTrust Manager administrator can configure profiles to redirect client logs to Syslog servers.

To configure Syslog settings in a profile:

1. Open the **CTE** application.
2. In the left pane, click **Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **CLIENT SYSLOG CONFIGURATION**.

Log Level

INFO

☐ Local

Server 1

Hostname or IP

IP

Port

Port

Message Format

RFC5424

Protocol

TCP

Save

Server 2

Hostname or IP

IP

Port

Port

Message Format

RFC5424

Protocol

TCP

Save

Show Additional Servers

5. Specify the following details:

NOTE

- > You can configure up to four servers, labeled as **Server 1**, **Server 2**, **Server 3**, and **Server 4**. By default, Server 1 and Server 2 are visible. To view Server 3 and Server 4, click **Show Additional Servers**.
- > This document describes steps to configure one server, Server 1. Extend the steps to suit your setup requirements.

Field	Description
Log Level	Level of logs to redirect. In sequence, the options are: > DEBUG: Fine-grained informational events that are targeted towards support engineers and developers. > INFO: Informational messages that highlight the progress of the application at coarse-grained level. > WARN: Potentially harmful situations. > ERROR: Error events that might still allow the application to continue running. This is the default log level. > FATAL: Severe error events that will presumably lead the application to abort. Log levels are cumulative. The level that you select not only generates log entries for events that occur at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.
Local	Whether logs are sent to the client. If selected, the logs are saved on the client at <code>/var/log/messages</code> . By default, the option is clear.
Server 1	
Hostname or IP	Hostname or IP address of the Syslog server.
Port	Port of the Syslog server.
Message Format	Format in which the log messages are transferred to the Syslog server. The options are: > Plain Message > CEF > RFC5424 > LEEF The default log format is RFC5424. This format adheres to the Syslog Protocol RFC 5424 guidelines.

Field	Description
Protocol	Transport protocol for the Syslog connection. The options are UDP, TCP, and TLS. The default protocol is TCP. When you select TLS, the following fields appear: > CA Certificate: Click Browse to select the CA certificate. > Certificate: Click Browse to select the certificate. > Private Key: Click Browse to select the private key.

6. Click **Apply**.

The Syslog server settings are configured.

Setting Quality of Service Configuration

The QoS configuration settings apply to clients that have the LDT feature enabled on them. Administrators use these settings to maintain operational efficiencies in their systems in conjunction with LDT operations. They can specify percentage of CPU usage or a rekey rate and schedules for LDT operations. Refer to the CTE-Live Data Transformation with CipherTrust Manager for best practices about using LDT and QoS.

A CipherTrust Manager administrator can configure LDT QoS on the CipherTrust Manager.

To configure LDT QoS settings in a profile:

1. Open the **CTE** application.
2. In the left pane, click **Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **QUALITY OF SERVICE CONFIGURATION**.

5. Specify the rekey option. The options are:

- **Rekey by Rate:** Select to rekey by rate (in MB/s). This is the default setting. Specify the **LDT QoS Rekey Rate**. The default value is 0.

- **Rekey by CPU:** Select to rekey by CPU usage. By default, LDT operations use all of the available CPU memory.

Optionally, you can reserve percentage of the clients' CPU for LDT rekey operations. To do so:

- Select **Cap CPU Allocation**. The **CPU Percentage** field becomes editable.
- Enter the **CPU Percentage**. The value must be greater than 0.

- Specify a QoS schedule to run LDT. Under **QoS Schedules**, select an **LDT QoS Schedule**. The options are:

Name	Time Ranges	Description
ANYTIME	Sunday 12:00 AM - Saturday 11:59 PM	LDT runs any day at any time of the week
WEEKNIGHTS	Monday 12:00 AM - Monday 07:00 AM Monday 09:00 PM - Tuesday 07:00 AM Tuesday 09:00 PM - Wednesday 07:00 AM Wednesday 09:00 PM - Thursday 07:00 AM Thursday 09:00 PM - Friday 07:00 AM Friday 09:00 PM - Friday 11:59 PM	LDT runs between midnight to 7:00 AM from Monday to Friday
WEEKENDS	Sunday 12:00 AM - Monday 07:00 AM Friday 09:00 PM - Saturday 11:59 PM	LDT runs between 9:00 PM Friday to 7:00 AM on Monday
CUSTOM	<Custom Range>	LDT runs at a custom schedule (described below)

Creating a Custom LDT Schedule

To create a custom LDT schedule:

- Select **CUSTOM** from the **LDT QoS Schedule** drop-down list. Now, the **Create New QoS Schedule** button is available.

The screenshot shows the 'QoS Schedules' configuration area. Under the 'LDT QoS Schedule' dropdown, 'CUSTOM' is selected. A blue button 'Create New QoS Schedule' is visible. Below this, there are two input fields: 'Name' and 'Time Ranges'.

- Click **Create New QoS Schedule**. The Create QoS Schedule dialog box is displayed.

The screenshot shows a 'Create QoS Schedule' dialog box. It has a title bar with a close button (X). Inside, there are four input fields arranged in a 2x2 grid. The top row contains 'Starting Day:' with a dropdown menu showing 'Monday' and 'Ending Day:' with a dropdown menu showing 'Monday'. The bottom row contains 'Starting Time:' with three input fields (1, :, 00) and a dropdown menu (A...), and 'Ending Time:' with three input fields (2, :, 00) and a dropdown menu (A...).

- i. Select the **Starting Day**. The LDT process will start on this day of the week. The default starting day is Monday.
 - ii. Specify the **Starting Time** in the HH:MM AM/PM format. Use the arrows to select time in hours (1 to 11) and minutes (00 to 59). Select **AM** or **PM** from the drop-down list. The default starting time is 1:00 AM.
 - iii. Select the **Ending Day**. The LDT process will end on this day of the week. The default ending day is Monday.
 - iv. Specify the **Ending Time** in the HH:MM AM/PM format. The default ending time is 2:00 AM.
- c. Click **Create**. The custom LDT QoS schedule is displayed on the screen. The specified Time Ranges are also displayed.

The screenshot shows the 'QoS Schedules' section. At the top, there's a label 'QoS Schedules'. Below it, on the left, is 'LDT QoS Schedule:' with a dropdown menu showing 'CUSTOM'. To the right is a blue button labeled 'Create New QoS Schedule'. Below these is a table with two columns: 'Name' and 'Time Ranges'. The table has one row with 'CUSTOM' in the 'Name' column and 'Monday 1:00 AM - Friday 5:00 AM' in the 'Time Ranges' column. There is a three-dot menu icon to the right of the table row.

7. Click **Apply**. The configuration is saved successfully.

NOTE

- > To create a new custom schedule, click **Create New QoS Schedule**.
- > To delete a custom schedule, click **Delete** corresponding to the schedule you want to delete.

Concise Logging

CTE's standard operational logging sends audit messages for every file system operation. An audit message is sent every time a file is opened, read, updated, or written. Standard logging can generate high volumes of log data. Security administrators might not need most of these logs to monitor file system activities on the protected clients.

A CipherTrust Manager administrator can enable or disable Concise Logging for a profile. After Concise Logging is enabled or disabled, CTE Agent generates a log message to record that event:

```
"[CGA] [INFO] [CGA3201I] [08/07/2020 10:57:18] Concise logging enabled"
```

```
"[CGA] [INFO] [CGA3202I] [08/07/2020 10:57:27] Concise logging disabled"
```

Advantages

Concise Logging:

- > Helps security administrators to focus on relevant audit messages and important actionable messages such as errors and warnings.
- > Can eliminate repetitive and unimportant audit messages generated by read and write activities on a file, read and write directory attributes, and other file system activities.
- > Eliminates audit messages:
 - For each block read by a user or an application. Only one audit message is sent for every read/write activity.
 - That read the attributes, basic information of file set attributes, and other event-based messages.
 - For directory open, read directory attributes, and directory close.

Considerations

Concise Logging:

- > Changes the set of messages that are sent to Security Information and Event Management (SIEM) software systems. If this results in loss of data required for customer reports, then disable Concise Logging.
- > Applies to all GuardPoints and for all users of the clients linked with a profile. There is no fine-grained control such as per GuardPoint, user, or message type.
- > Applies to the existing clients and the new clients to be linked with the profile subsequently.
- > Is supported by CTE secfs only.
- > Should not be used with Learn Mode.

Modifying Profiles

To modify a profile:

1. Open the **CTE** application.
2. In the left pane, click **Profiles**.
3. Under **Name**, click the desired profile.
Alternatively, click the overflow icon () corresponding to the desired profile and click **Edit**.
4. Expand **CLIENT LOGGING CONFIGURATION**.
 - a. Modify the settings, as appropriate. Refer to ["Setting Client Log Configuration" on page 43](#) for details.
 - b. Click **Apply**.
5. Expand **CLIENT SYSLOG CONFIGURATION**.
 - a. Modify the settings, as appropriate. Refer to ["Setting Client Syslog Configuration" on page 48](#) for details.
 - b. Click **Apply**.
6. Expand **QUALITY OF SERVICE CONFIGURATION**.
 - a. Modify the settings, as appropriate. Refer to ["Managing Profiles" on page 42](#) for details.

- b.** Click **Apply**.

The profile settings are updated.

Deleting Profiles

Single or multiple profiles can be deleted from the CipherTrust Manager GUI in one go. Before deleting a profile make sure that no clients or client groups are linked to it.

Deleting Individual Profiles

To delete a profile:

1. Open the **CTE** application.
2. In the left pane, click **Profiles**.
3. Click the overflow icon () corresponding to the desired profile.
Alternatively, select the desired profile and click the delete icon ().
4. Click **Delete**.

The selected profile is removed from the profiles list.

Deleting Multiple Profiles

To delete multiple profiles:

1. Open the **CTE** application.
2. In the left pane, click **Profiles**.
3. Select the check boxes corresponding the desired profiles.
To select all profiles visible on the page for deletion, select the top check box to the left of the Name heading.
4. Click the delete icon (). A dialog box appears prompting to confirm the action.
5. Click **Delete**.

CHAPTER 6: Managing Clients and Client Groups

A client is a computer system where the data needs to be protected. A compatible CTE Agent software is installed on the client. The CTE Agent can protect data on the client or devices connected to it. A client can be associated with multiple GuardPoints for encryption of various paths (refer to ["Managing GuardPoints" on page 135](#) for details).

The Clients page of the CipherTrust Manager GUI displays all clients protected by encryption Agents. CipherTrust Manager Administrators can manage clients on this page.

NOTE Before proceeding, make sure that:

- > A compatible CTE Agent is installed on the client.
- > The client is registered with CipherTrust Manager.

Refer to the CTE Agent Quick Start Guide specific to your platform for information on installing and configuring CTE Agents.

This chapter covers the following sections:

- > ["Registering Clients" below](#)
- > ["Searching Clients" on the next page](#)
- > ["Viewing Clients" on the next page](#)
- > ["Enabling Live Data Transformation" on page 57](#)
- > ["Setting Client Locks" on page 59](#)
- > ["Client Settings" on page 65](#)
- > ["Modifying Client Configuration" on page 71](#)
- > ["Changing Client Password" on page 72](#)
- > ["Managing Membership" on page 74](#)
- > ["Deleting Clients" on page 75](#)
- > ["Configuring Client Groups" on page 77](#)

Registering Clients

When CTE clients are registered, they are added to the CipherTrust Manager GUI. Refer to the CTE Agent Quick Start Guide specific to your platform for information on installing and configuring CTE Agents.

NOTE Before proceeding, you must change the client password using the manual password creation method. Refer to ["Changing Client Password" on page 72](#) for details.

Searching Clients

The Clients page on the CipherTrust Manager GUI shows the list of registered clients.

To search for a registered client:

1. Log on to the CipherTrust Manager GUI as administrator.
2. Open the **CTE** application. The Clients page is displayed. This page lists the clients added to this CipherTrust Manager appliance.
3. In the **Search** box, enter the client name. Search is case-insensitive. You can enter all or part of a client name. A partial client name displays every client with a name that contains the specified string.



Viewing Clients

The Clients page shows the total number of clients, clients with errors, clients with warnings, healthy clients, unregistered clients. The Status Bar contains the following tabs:

- > **<N> Total Clients:** Shows the total number of registered and unregistered clients with all types of health status.
- > **<N> Errors:** Shows the number of clients with errors.
- > **<N> Warnings:** Shows the number of clients with warnings.
- > **<N> Healthy:** Shows the number of healthy clients.
- > **<N> Unregistered:** Shows the number of unregistered clients.
- > **<N> Expunged:** Shows the number of expunged clients.



Click each tab to filter the clients. The clients list displays names of clients in the CipherTrust Manager database and details about their configuration.

To view the clients registered with a CipherTrust Manager:

1. Open the **CTE** application.
2. Click **Clients > Clients**. The clients list shows the following details:

	Status	Client Name ↑	OS Type	Kernel Version	Agent Version	Description	⚙
+	☐  Healthy	P_1	LINUX	3.10.0-957.el7.x86_64	7.0.0.34	TestHost	⋮
+	☐  Healthy	P_10	LINUX	3.10.0-957.el7.x86_64	7.0.0.34	TestHost	⋮
+	☐  Healthy	P_11	LINUX	3.10.0-957.el7.x86_64	7.0.0.34	TestHost	⋮
+	☐  Healthy	P_12	LINUX	3.10.0-957.el7.x86_64	7.0.0.34	TestHost	⋮

Column	Description
Status	Health status of the client: > Healthy > Error > Warning > Unregistered > Expunged When a registered client is uninstalled, its status on the Clients page becomes Unregistered. The status of a deleted client becomes Expunged.
Client Name	Name link of the client on CipherTrust Manager.
OS Type	OS running on the client: > AIX > Linux > Windows
Kernel Version	Version of the kernel installed on the client. For Windows clients, NA is displayed.
Agent Version	Version of the CTE Agent installed on the client.
Description	(Optional) Description to identify the client.

Enabling Live Data Transformation

The Live Data Transformation (LDT) feature enables the CipherTrust Manager Security Administrators to encrypt or rekey GuardPoint data without blocking the user or application access to that data.

In standard CTE deployments, data access is blocked during the initial encryption or rekeying of the data, and each rekey operation requires guarding your data under separate production and offline data transformation policies. With LDT, encryption and rekeying of the data takes place in the background using one policy, without disrupting user or application access.

Prerequisites

To use LDT, you must have the following:

- > CTE Agent license. The feature is called TransparentEncryption on the Licensing page.
- > CTE LDT add-on license. The feature is called LiveDataTransformation on the Licensing page.
- > CTE Agent installed on a client. Refer to the CTE Clients Guide for information about installing and registering CTE clients.

Refer to the CTE LDT Guide and the CipherTrust Manager Compatibility Matrix for information about implementing LDT and the supported platforms.

Important Notes

- > If the CipherTrust Manager fails, all keys that were automatically rotated after the last backup would be lost, making all data encrypted with those keys unusable or unrecoverable. Therefore, it is recommended that the LDT feature is used in a high availability CipherTrust Manager deployment.
- > If LDT must be used in a single CipherTrust Manager configuration, it is recommended to:
 - Set "Persistent on Client" to "Yes" for all keys that are created.
 - Set the password creation method to "Manual" for all clients.
- > If the standalone CipherTrust Manager fails or is unavailable, the data on the client can still be accessed by entering the known passphrase. The data is accessible as the encryption keys are cached on the client.

Enable LDT

Enable the LDT support for a client either during registration or after registration with the CipherTrust Manager.

- > If LDT is enabled during registration, the Live Data Transformation check box appears selected by default on the CipherTrust Manager GUI.
- > If LDT is not enabled during registration, you can enable it on the CipherTrust Manager GUI, as described below.

To enable LDT on a client after CTE installation:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. In the mini detail view, select **Live Data Transformation**.



By default, LDT performs rekey operations on the LDT protected GuardPoints as soon as GuardPoints are enabled. To pause LDT rekey operations, click the Suspend Live Data Transformation icon (■). The icon changes to Resume Live Data Transformation (■).

5. Click **Apply.** LDT is now enabled on the client.

After LDT has been enabled, it cannot be disabled. To remove the feature, you must migrate existing data protected under LDT policies, unregister the client, and delete the client. Then, you can reregister the client without enabling the feature. This allows you reclaim the license for use on another client.

Refer to ["Managing GuardPoints" on page 135](#) for details on creating LDT GuardPoints. For details about how LDT works, guidelines, and best practices for using the feature, refer to the CTE-Live Data Transformation with CipherTrust Manager.

Setting Client Locks

Agent Lock and System Lock are used to protect the CTE Agent and certain system files. CTE Agent protection includes preventing:

- > Certain changes to the CTE Agent installation directory.
- > Unauthorized termination of the CTE Agent processes.

These locks can be applied to individual clients or client groups. By default, the Agent Lock and System Lock are disabled.

NOTE Uninstallation of the Agent software might fail when the Agent Lock and System Lock are enabled. It is recommended to disable the:

- > Agent Lock before uninstalling the Agent software on the client system.
- > Agent Lock before deleting the client records from the CipherTrust Manager GUI.
- > System Lock before updating, deleting, or modifying the protected system files.

This section covers the following information:

- > ["Agent Lock" on the next page](#)
- > ["System Lock" on page 61](#)
- > ["Setting Locks on Individual Clients" on page 62](#)
- > ["Setting Locks on a Client Group" on page 63](#)
- > ["Verifying Locks on Clients" on page 63](#)
- > ["Unlocking Clients Manually" on page 64](#)
- > ["Disabling Locks" on page 64](#)
- > ["Administering Locking Issues" on page 65](#)

Agent Lock

Agent Lock locks the contents of the CTE Agent directories on the client. These directories are `/<install root>/agent/secfs` and `/<install root>/agent/vmd`.

Files in these directories cannot be modified or removed when Agent Lock is enabled; however, the CipherTrust Manager can still propagate updates to the client system.

When Agent Lock is Disabled

- > CTE Agent software on the client is not protected

NOTE Do not unregister or delete the CTE Agent while locks are applied. The locks stay in effect after the Agent is unregistered, and without Agent credentials, the CipherTrust Manager can neither administer that Agent nor disable the locks. You must boot the client into single-user mode and manually modify the Agent configuration to disable the locks.

When Agent Lock is Enabled

- > Certificates are exchanged and the client is bound to the CipherTrust Manager
- > CTE Agent installation directory cannot be deleted or overwritten
- > CTE Agent services cannot be stopped
- > CTE Agent GuardPoints cannot be forcefully unmounted
- > On Linux systems:
 - All operations are permitted on the following directory:


```
/<install root>/agent/secfs/tmp
```
 - Following directories cannot be removed or renamed, and directory and file creation will fail.


```
/<install root>/agent/secfs/bin
/<install root>/agent/vmd
```
 - File creations and other operations will work for the following directory, but the directory cannot be removed or renamed.


```
/<install root>/agent/secfs/
```
- > On AIX systems:
 - Contents of the following directories cannot be changed or moved.


```
/<install root>/agent/vmd
```
 - Contents of the following files and directories can be modified, but not removed or renamed.


```
/<install root>/agent/secfs/
/<install root>/agent/secfs/tmp
```
- > On Windows systems:
 - Following folder cannot be moved and its contents cannot be modified.


```
C:\Program Files\Vormetric\DataSecurityExpert\Agent\secfs\sec
```
 - CTE Agent entries in the registry cannot be modified or deleted.

System Lock

System Lock applies an internal policy to the client to lock client system directories, such as `/var`, `/bin`, and `/etc`.

NOTE System Lock must be disabled before upgrading or installing third-party software, adding new applications, opening SSH sessions remotely, or modifying system directories.

NOTE (Windows only) Verify that the volume letter and the path for the Windows system are correct before proceeding. When the CTE Agent is installed, the volume letter defaults to "C:". The executables on the Client Settings tab may be on a different volume or in a different folder. If the volume or path information is incorrect, the CipherTrust Manager cannot sign the applications and apply Agent Lock and System Lock.

When System Lock is Disabled

- > The internal policy is disabled.
- > You can install or update system software.

When System Lock is Enabled

- > Agent Lock is automatically enabled.
- > Operating system directories on the client are protected.
- > Microsoft Update cannot be run on Windows systems to protect the client. Microsoft update and other installation-related executables are specifically blocked. Executables like `wuacult.exe` and `msiexec.exe` cannot be run.
- > The installation utility checks if System Lock is enabled on the client system. If it is, the utility aborts installation and displays a message telling you to "unlock system before running install/update program". Other third-party installation utilities do not check if System Lock is enabled and are not prevented from installing software.
- > New file or directory creation inside a protected directory is not allowed.

The following files, directories, and subdirectories are, by default, automatically protected when System Lock is enabled. Asterisks (*) indicate pattern matching.

- > On Linux systems:
 - Following files and the contents of the following directories cannot be changed or moved.
 - `/etc/pam.d`
 - `/etc/rc*`
 - `/etc/security`
 - `/usr/lib/security`
 - Contents of the following files and directories can be modified, but not removed or renamed.
 - `/etc`
 - `/etc/init.d/secfs`

- /usr
- /usr/bin/vmd
- /usr/bin/vmsec
- /usr/bin/secfsd
- /usr/bin/dataxform
- /usr/lib
- /usr/lib/*pam*
- /usr/lib/security
- /var/log/vormetric

> On AIX systems:

- Following files and the contents of the following directories cannot be changed or moved when System Lock is enabled.
 - /etc/rc.d
 - /etc/security
 - /usr/lib/security
 - /sbin/helpers/mount_secfs
- Contents of the following files and directories can be modified, but not removed or renamed when System Lock is enabled.
 - /var/log/vormetric

> On Windows systems:

- Files with the following extensions in the Windows OS installation folder (for instance: \Windows, \WinNT, and so on) cannot be moved or modified:
 - .exe
 - .dll
 - .sys
 - .cmd
 - .com

When System Lock is applied, a protected file or path cannot be renamed or deleted; however, if it is a directory, other files may be added to it. For example, /etc cannot be deleted nor renamed, though you can add files to it. A file that cannot be modified cannot be opened and edited in any way.

Setting Locks on Individual Clients

To apply locks to an individual client:

1. Make sure that no one is currently in or accessing the Agent installation directories; otherwise, the CipherTrust Manager might not lock the Agent software.
2. Open the **CTE** application.
3. Under **Client Name**, click the desired client.

- On the lock bar, click **Agent Lock**. This protects the CTE Agent files from modification and deletion.



- Click **System Lock**. This protects a set of system files from modification and deletion.



Agent Lock is automatically enabled when System Lock is enabled. You can manually enable or disable Agent Lock only when System Lock is disabled.

- Click **Apply**.
- Verify the locks. Refer to ["Verifying Locks on Clients" below](#).

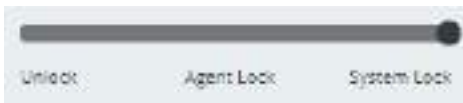
Setting Locks on a Client Group

To apply locks to a client group:

- Make sure that no one is currently in or accessing the Agent installation directories; otherwise, the CipherTrust Manager might not lock the Agent software.
- Open the **CTE** application.
- Click **Clients > Client Groups**.
- Under **Client Group Name**, click the desired client group.
- On the lock bar, click **Agent Lock**. This protects the CTE Agent files from modification and deletion.



- Click **System Lock**. This protects a set of system files from modification and deletion.



Agent Lock is automatically enabled when System Lock is enabled. You can manually enable or disable Agent Lock only when System Lock is disabled.

- Click **Apply**.
- Verify the locks. Refer to ["Verifying Locks on Clients" below](#).

NOTE To disable the locks on a client group, select the client, click **Unlock**, and click **Apply**.

Verifying Locks on Clients

A client administrator can verify that the locks are applied to the Agent on the client.

To verify the locks:

1. Log on to the client system.
2. Run the `secfsd` command with the `lockstat` argument:

```
# secfsd -status lockstat
FS Agent Lock: true
System Lock: true
```

NOTE Sometimes, the CipherTrust Manager reports the CTE Agent configuration different than the actual configuration. This can be because of the delay between log uploads to the CipherTrust Manager, or because a GuardPoint is in use when the lock is applied.

In some cases, when the locks are enabled, the CipherTrust Manager cannot administer the client. In such cases, after changing authentication credentials or removing the certificate fingerprint, the client administrator must unlock the client manually.

Unlocking Clients Manually

Unlocking Linux Clients

To unlock the client manually:

1. Boot the client into single-user mode.
2. Edit the `./secfs/.sec/conf/configuration/secfs_config` file.
3. Set both `coreguard_locked` and `system_locked` to `false`.
4. Save the file.
5. Boot the system into multi-user mode.

You can now administer the client again.

Unlocking Windows Clients

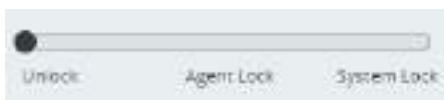
To unlock the client manually:

1. Boot in safe mode.
2. Rename `C:\Windows\system32\drivers\vmgmt.sys` and `.\drivers\vmfiltr.sys` to something else.
3. Boot in regular mode.

You can now administer the client again.

Disabling Locks

To disable the locks on a client or client group, select the client or client group, click **Unlock**, and click **Apply**. The lock bar should look like the following:



Administering Locking Issues

The client administrator must inform the Security Administrator of changes to the system hierarchy.

- > **Example 1:** The client system administrator can request to have the locks temporarily disabled to do administrative functions.
- > **Example 2:** The client system administrator can remove directories and files, then, later when the lock is reapplied, the CipherTrust Manager protects non-existent data.
- > Another common administrative issue pertains to mounted GuardPoints. The client system administrator can remove or unmount an unlocked, non-automounted GuardPoint. The CipherTrust Manager GUI is not aware of this change and does not issue a warning when you reapply the lock to the now non-existent mounted GuardPoint.
- > To recover an unmounted GuardPoint:
 - a. Disable the GuardPoint for the file system on the CipherTrust Manager GUI.
 - b. Mount the file system on the client.
 - c. Enable the GuardPoint for the file system.

Client Settings

Applications such as `su`, `sshd`, and `login` authenticate users' identity by requesting user credentials (user name and password). These are signed applications that identify and authenticate before a child process is executed.

GuardPoints can have an associated policy that restricts access to the data stored in them. For a process to access the data, the user's associated identity must be authorized. This authorization can be done by adding an entry to the Settings field on the Client Settings tab. This entry specifies a program, such as mentioned above, with a keyword that indicates the type of authorization that is applied.

Client settings configured on the CipherTrust Manager are pushed to the clients periodically.

Any changes to the client settings are not automatically signed. Signatures of the newly added processes are compared against the signatures in the existing settings. If they differ, an error message is generated. Refer to ["Re-Sign Settings" on page 70](#) for steps to configure this setting. Refer to the CTE Agent Advanced Configuration and Integration Guide specific to your platform for details about this feature.

Client settings can also be configured at the client group level, see ["Inheritance of Client Group Settings" on page 82](#) for details.

Client Settings for Linux

Specify the authentication mechanisms in place for certain binaries on the client machine.

Default Settings for Linux

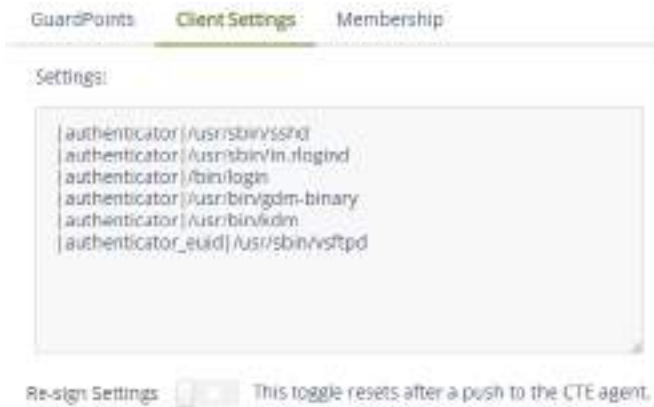
```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
|authenticator_euid|/usr/sbin/vsftpd
```

Add, edit, or modify authentication settings as appropriate.

Specify Authentication Settings

To specify authentication settings for the client:

1. Open the **CTE** application.
2. Under **Client Name**, click the desired client.
3. Click the **Client Settings** tab. The Settings text box contains the authentication settings.



Each line has the format:

```
|behavior|/path/to/binary
```

Refer to "[Client Settings Keywords](#)" on page 68 for keywords.

4. In the **Settings** box, specify the authentication mechanism.

NOTE

- > To delete the settings, delete the content and click **Apply**.
- > To edit the settings, modify the content and click **Apply**. When editing the setting strings, follow the format `|privilege|filename`.
- > To cancel any changes, click **Cancel**.

5. Click **Apply**.

Client Settings for Windows

For applications running under `WOW64` that require some form of user authentication, create entries on the Client Settings tab. The `syswow64` paths are created by default when the CTE Agent is installed. `\Windows` is for Windows XP and Windows Itanium operating systems.

In `WOW64`, all file access to `C:\Windows\System32` is redirected to `C:\Windows\syswow64`, and is implemented using the File System. Redirected `syswow64` paths are effective only for 64-bit Windows file agents. This is the path where programs compiled for 32-bits are stored to run on a 64-bit system.

Before proceeding, verify that the volume letter and the path for the Windows system are correct. When the CTE Agent is installed, the volume letter defaults to "C :". It is possible that the executables on the Client Settings tab are on a different volume or in a different folder. If the volume or path information is incorrect, the CipherTrust Manager cannot sign the applications, and it cannot apply Agent Lock and System Lock.

Default Settings for Windows

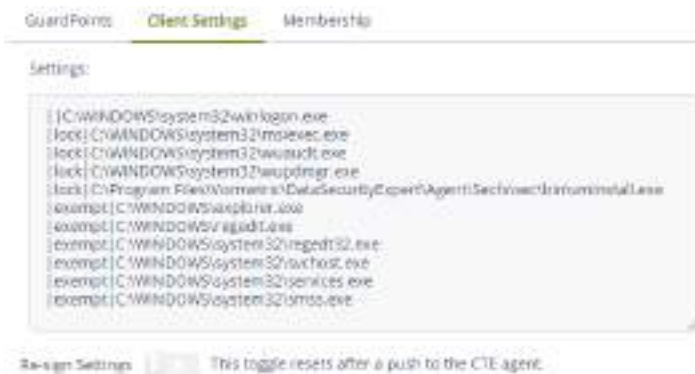
```
|C:\WINDOWS\system32\winlogon.exe
|lock|C:\WINDOWS\system32\msiexec.exe
|lock|C:\WINDOWS\system32\wuauclt.exe
|lock|C:\WINDOWS\system32\wupdmgr.exe
|lock|C:\Program Files\Vormetric\DataSecurityExpert\Agent\Secfs\sec\bin\vminstall.exe
|exempt|C:\WINDOWS\explorer.exe
|exempt|C:\WINDOWS\regedit.exe
|exempt|C:\WINDOWS\system32\regedt32.exe
|exempt|C:\WINDOWS\system32\svchost.exe
|exempt|C:\WINDOWS\system32\services.exe
|exempt|C:\WINDOWS\system32\smss.exe
```

Add, edit, or modify authentication settings as appropriate.

Specify Authentication Settings

To specify authentication settings for the client:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **Client Settings** tab. The Settings text box contains the authentication settings.



Each line has the format:

```
|behavior|/path/to/binary
```

Refer to "[Client Settings Keywords](#)" on the next page for keywords.

5. In the **Settings** box, specify the authentication mechanism.

NOTE

- > To delete the settings, delete the content and click **Apply**.
- > To edit the settings, modify the content and click **Apply**. When editing the setting strings, follow the format `|privilege|filename`.
- > To cancel any changes, click **Cancel**.

6. Click **Apply**.

Oracle Database in a Guarded NFS Mount on AIX

To locate your Oracle database in a guarded NFS mount:

1. Open the **CTE** application.
2. Under **Client Name**, click the desired client.
3. Click the **Client Settings** tab. The Settings text box contains the authentication settings. Each line has the format:

```
|behavior|/path/to/binary
```

4. In the **Settings** text box, add the following entries:

```
|vfsnumber|<path to>/oracle
```

```
|vfsnumber|<path to>/dbca
```

Example:

```
|vfsnumber|/u01/app/oracle/dbhome_1/bin/oracle
```

```
|vfsnumber|/u01/app/oracle/dbhome_1/bin/dbca
```

5. Click **Apply**.

Client Settings Keywords

The following table lists the keywords that you can enter on the Client Settings tab. These keywords override different authentication requirements:

Keyword	Description
authenticator	(UNIX only) Authenticates based upon the real user ID (<code>ruid</code>) credentials of a process. The indicates that the given binary is trusted to authenticate users. For example, the <code>sshd</code> process on UNIX is a good authenticator . It takes incoming network connections and authenticates the user that attempts to log on to the system. All child processes from this session are trusted as the original user.
authenticator_euid	(UNIX only) Authenticates based upon the effective user ID (<code>euid</code>) credentials of a process. The keyword is used to authenticate the credentials of a <code>setuid</code> process with the <code>euid</code> value rather than the <code>ruid</code> value.
vfsnumber	(AIX [all supported]/Oracle 10gR2) Use when Oracle RMAN backups fail on NFS as a result of not receiving underlying file system identifiers. Apply vfsnumber to the Oracle binaries directory.
realfsid	(AIX [All supported]) Use if the <code>cp</code> operation fails while copying files with extent attributes on guarded Veritas file systems. The failure occurs because the underlying file system identifier is not received.

Keyword	Description
lock	(Windows only) Specifies an application that cannot be executed on the client. An application defined with <code>lock</code> does not go through an internal policy check. The application is not allowed to run at all. A default set of applications is locked on Windows clients to prevent their execution and potential failure during bootup. The same effect can be achieved by configuring the resource and process security rule attributes in a policy. However, certain default applications are automatically locked on the Client Settings tab as a precautionary measure. Those applications must be included in the policy. Sometimes, problems such as installation failure or application lockup occur when installing software on a locked client. In such cases, identify the locked processes, unlock them, and retry installation. The failure goes away. For example: <pre> lock c:\winnt\system32\msiexec.exe</pre>
exempt	(Windows only) When processes or applications are started, the internal policy and regular policies are checked locally or by the CipherTrust Manager. When a policy check is performed and <code>exempt</code> is applied to the process, a six second timeout is imposed on the check. Without <code>exempt</code>, an application can wait indefinitely for a policy access check to complete, as when the CipherTrust Manager is required but is inaccessible. If the check times out because the CipherTrust Manager is unavailable for any reason, access is denied. Exempt client processes are also “exempt” from popup messages that describe the occurrence of access violations. An example of what causes such popups is an application that tries to memory map a file for which it does not have encryption permission (for instance, memory map with no view ability key on Windows). The only reasons to include <code>exempt</code> in the configuration are shorter wait periods and blocked popups.

The following table shows different results you get when using `authenticator` or `authenticator_euid` to verify user identities.

Product	Application	Client Setting	User
Oracle	oracle	authenticator_euid	"oracle"
Oracle	oracle	authenticator	*

* indicates the real `uid` of the user who starts the application. This means that if the policy is configured to check the user ID, a security rule must be generated for every possible user.

NOTE Apply the `|authenticator_euid|` keyword to the `oracle` binary on the Client Settings tab to authenticate the `oracle` user because regardless of who starts the `oracle` process, the `EUID` is always `oracle`.

Configuring Application Authentication Credentials

To configure application authentication credentials:

1. Open the **CTE** application.
2. Click **Clients > Clients**.

3. Under **Client Name**, click the desired client.
4. Click the **Client Settings** tab. The Settings box displays the default set of system applications that may require authentication entries.
5. In the **Settings** box, add, modify, or delete entries to control their access permissions. When you add more processes, you must include the entire path.

NOTE A keyword such as `|authenticator|` must be used in front of a process, otherwise, the entry is ignored by the CipherTrust Manager GUI.

6. Click **Apply**.

Client users currently logged on to the client must log off and log on again to refresh their user authentication credentials. They can verify the change by logging on to the client, accessing a GuardPoint, and checking the user information in the message logs.

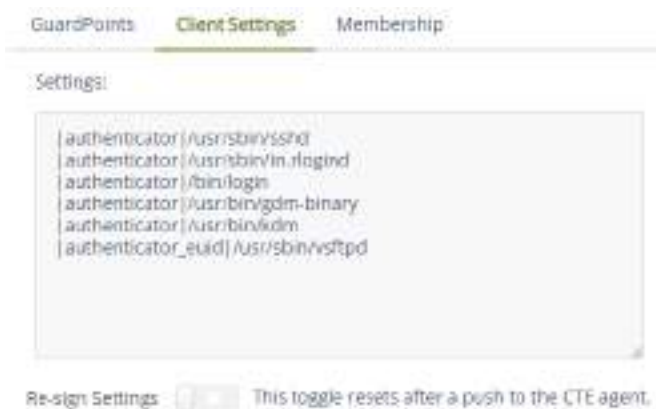
Re-Sign Settings

If you add another process to the set of trusted applications on the Client Settings tab, enable the Re-sign Settings toggle. This ensures that the new process is signed and authenticated by the client.

Subsequently, when the client settings are pushed to the CTE Agent, the updated settings are re-signed. The Re-sign Settings toggle is turned off (or reset).

To ensure that new processes are signed and authenticated by the client:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **Client Settings** tab.



5. In the **Settings** box, update settings as appropriate.
6. Turn on the **Re-sign Settings** toggle.



7. Click **Apply**.

Enabling the Re-sign Settings toggle forces a signature update. On subsequent push of the client settings to the CTE Agent, the updated settings are re-signed and the Re-sign Settings toggle is turned off (or reset). If you do not turn on this toggle after adding a new process, the client ignores the newly added process.

Modifying Client Configuration

To modify the client configuration:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client. The mini detail view of the client is displayed.

Linux Client



Windows Client



Alternatively, click the expand icon (▸) to the left of the desired client in the clients list.

4. Modify the following, as appropriate:
 - **Live Data Transformation:** Enable or disable LDT. By default, any ongoing rekey operations on the LDT GuardPoints on the client are resumed. To disable the setting, click the Suspend Live Data Transformation icon (■). The icon changes to Resume Live Data Transformation (■).
 - **Encryption Key Protection:** Enable or disable protection of encryption keys.
 - **Cloud Object Storage:** (Non-editable, Linux only) Enabled or disabled based on the feature selection during registration. From the GUI, you can neither disable nor enable the Cloud Object Storage feature. To enable or disable it, register the client again and opt or opt out of the Cloud Object Storage feature. Refer to the CTE Agent for Linux Quick Start Guide for details.
 - **Secure Start:** (Non-editable, Windows only) Enabled or disabled based on the installed Agent capability. If the Agent supports the Secure Start feature, then this option is enabled, otherwise, the option is disabled.
 - **Unlock:** Unlock Agent Lock and System Lock.
 - **Agent Lock:** Lock the contents of the CTE Agent directories on the client.
 - **System Lock:** Apply an internal policy to the client to lock client system directories, like /var, /bin, /etc. Enabling System Lock automatically enables Agent Lock.

- **Communication Enabled:** Whether to enable the client's communication with the CipherTrust Manager. Select to enable, clear to disable communication. By default, the communication is enabled.
- **Password Creation Method:** Set the password creation method—Manual or Generate. Refer to ["Changing Client Password" below](#) for details.
- **Client Profile:** Select a profile for the client. The default profile is DefaultClientProfile. If you did not specify a profile during registration, the client is linked with default profile. To change the client profile, refer to ["Changing the Profile" below](#) for details.

5. Click **Apply**.

Changing the Profile

To change the client profile:

1. Open the **CTE** application.
2. Under **Client Name**, click the desired client.
3. Next to **Client Profile**, click the profile link (for example, DefaultClientProfile). The Select Profile dialog box shows the current client profile and Rekey Option, Rekey Rate, and Schedule of the selected profile.



Profile	
DefaultClientProfile	
Rekey Option:	RekeyRate
Rekey Rate:	0
Schedule:	ANY_TIME

4. From the **Profile** drop-down list, select the desired profile.
5. Click **OK**. The selected profile is linked successfully.

Changing Client Password

Offline Password

CTE supports the offline password feature. This feature is designed to protect the data on a laptop or similar portable system from being accessed by unauthorized users. When the CTE Agent is unreachable from the CipherTrust Manager, then you must provide the offline password to decrypt/encrypt files that are encrypted with an offline key (cached or persistent on client).

The offline password feature controls access to encryption keys that are stored locally on a client. This keeps the data secure when the CipherTrust Manager is inaccessible. To access the data, provide the offline password. Then, the CTE Agent encrypts/decrypts the guarded data according to the applied policy.

Password Types

The client password is initially set when the client is added to the CipherTrust Manager. Passwords can be set on a client-by-client or client group basis. The CipherTrust Manager supports two types of offline passwords:

- > **Manual** (Static): A password is specified manually. After a client is registered, you must change the client password using this method.
- > **Generate** (Dynamic): A password is generated automatically by CipherTrust Manager. Support for dynamic method is limited in this release. Refer to the CipherTrust Manager Release Notes for details.

Changing the Password Manually

NOTE The manual password creation method is recommended for disaster recovery scenarios.

To change the password:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.



Alternatively, click the expand icon (▸) to the left of the desired client in the clients list.

4. From the **Password Creation Method** drop-down list, select **Manual**. The **Regenerate Password** button is replaced by **Change Password**.



5. Click **Change Password**.
6. Enter the new password in the **Password** and **Confirm Password** fields. The password must match in both the fields.

NOTE The password must contain minimum eight characters including at least:

- > One capital letter
- > One number
- > One of these special characters: ! @ # \$ % ^ & * () { } []

To cancel the password change, click **Cancel Change Password**.

7. Click **Apply**.

When changing a static password or changing a client from a dynamic password to a static password, provide the new static password to the client user(s). Without the password, they cannot access encrypted data when there is no network connection between the client and CipherTrust Manager.

Changing the Password Dynamically

To change the password:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.



Alternatively, click the expand icon (▸) to the left of the desired client in the clients list.

4. From the **Password Creation Method** drop-down list, select **Generate**. This is the default method.
5. Click **Regenerate Password**.

A new generated password is downloaded to the client.

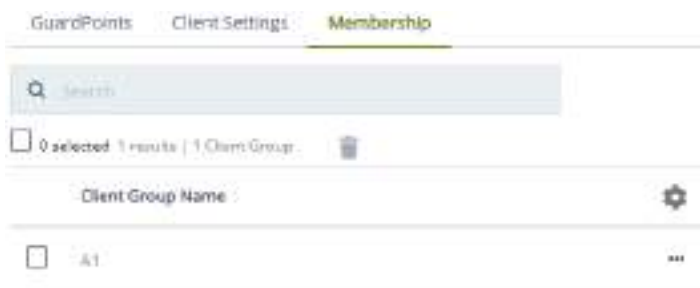
Managing Membership

View and manage the client group memberships of a client on the Membership tab. This tab provides option to remove the client from a group.

Viewing Group Membership of a Client

To view the groups of a client:

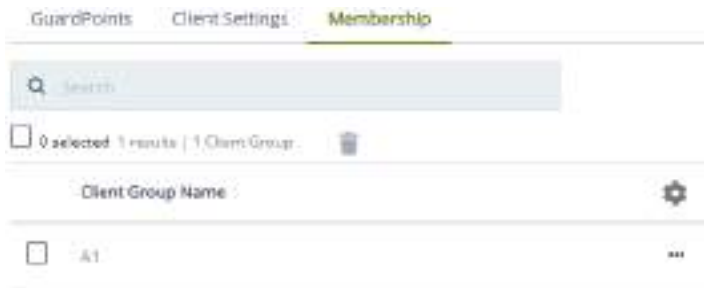
1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **Membership** tab. This tab shows the groups the client is a member of.



Removing a Client from a Client Group

To remove a client from a group:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **Membership** tab.



5. Select the group from which you want to remove the client.
6. Click the overflow icon (**...**) corresponding to the desired client.
7. Click **Remove**.

Deleting Clients

Only CipherTrust Manager administrators can delete clients. When a client is deleted from the CipherTrust Manager GUI, the client moves to the Expunged state and the CTE Agent is notified to drop client configuration. The CTE Agent installations on the client continue to run, complete with the applied policies. To completely remove a CTE Agent from the client, uninstall the Agent from the client system.

When Agent uninstallation is initiated, the client record is deleted from the CipherTrust Manager. The CipherTrust Manager pushes the configuration change to the CTE Agent running on that client. As a result, the following occur on the client:

- > CTE Agent certificates are deleted.
- > The `URL` line is removed from the `agent.conf` file.
- > The GuardPoints are removed.
- > The client is no longer recognized by the CipherTrust Manager. If the CTE Agent tries to communicate with the CipherTrust Manager, the connection is refused.

Deleting Clients with System Lock or Agent Lock

Do not unregister or delete the CTE client while locks are applied. The locks remain effective after the client is unregistered. Without client credentials, the CipherTrust Manager cannot administer that CTE Agent and cannot disable the locks. You must boot the client in single-user mode and manually modify the Agent configuration to disable the locks.

To remove everything associated with a client (including the CTE Agent):

1. Apply a rekey policy and run `dataxform` on the client to decrypt encrypted files.
2. Disable the locks on the client. Refer to ["Disabling Locks" on page 64](#).
3. Remove all the GuardPoints from the client.
4. Click **Clients > Clients**.
5. Under **Client Name**, click the overflow icon () corresponding to the desired client.
6. Click **Delete**. A dialog box appears prompting to confirm the action.
7. Click **Delete**.

The client administrator with root permissions must log on to the client system and uninstall the CTE Agent.

Deleted Client Indicators

A client is successfully deleted from the CipherTrust Manager GUI if:

- > CipherTrust Manager URL is deleted from the CTE Agent `agent.conf` file.
- > Certificates are removed from the `./agent/pem` directory.

However, if the client is deleted and its identity is changed while it is *offline*:

- > The GuardPoints are not removed
- > The certificates remain intact in the `./agent/pem` directory
- > The `agent.conf` file remains unchanged
- > But the Agent and CipherTrust Manager still cannot communicate with each other.

Logging for the CTE Agent on the CipherTrust Manager is also affected if an offline client is deleted. When the client comes online, log messages about the denied connection can be viewed only by CipherTrust Manager administrators of type System or All (when not in a domain). This is because the CipherTrust Manager:

- > No longer has the client's record.
- > Does not know which domain and the group the client belongs to.
- > Cannot send messages to the appropriate log service.

Deleting Multiple Clients

To delete multiple clients from the CipherTrust Manager GUI:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Select the check boxes corresponding the desired clients.
To select all clients visible on the page for deletion, select the top check box to the left of the Status heading.
4. Click the delete icon (). A dialog box appears prompting to confirm the action.
5. Click **Delete**.

Configuring Client Groups

A client group is used to group one or more clients to simplify configuration and administration. GuardPoints created on a client group are applied to all members of the group. Additionally, you can apply client group configuration settings to all clients in a client group. A client can be a member of multiple client groups.

If you have created a group of one type of clients, then you should only add similar clients to the group. Same configuration settings can only be applied to clients of the type with which the client group is created. If a different type of client is added, configuration settings cannot be applied to that client.

This section covers the following information:

- > ["Creating a Client Group" below](#)
- > ["Adding Clients to a Client Group" on the next page](#)
- > ["Displaying Client Groups" on page 79](#)
- > ["Modifying Client Groups" on page 79](#)
- > ["Changing Client Group Password" on page 81](#)
- > ["Inheritance of Client Group Settings" on page 82](#)
- > ["Configuring Client Group Settings" on page 84](#)
- > ["Deleting Client Groups" on page 84](#)

Creating a Client Group

To create a client group:

1. Open the **CTE** application.
2. Click **Clients > Client Groups**.
3. Click **Create Client Group**. The Create Client Group dialog box is displayed.
4. Enter a unique **Name** for the client group.
5. (Optional, displayed if a profile already exists) From the **Client Profile** drop-down list, select the desired client profile. The default profile is DefaultClientProfile.
6. (Optional) Provide **Description** to identify the client group. The maximum length can be 256 characters.



The screenshot shows a 'Create Client Group' dialog box with the following fields:

- Name:** A text input field containing 'testclientgroup'.
- Client Profile:** A dropdown menu with 'DefaultClientProfile' selected.
- Description:** A text input field containing 'test client group'.

7. Click **Create**. The client group is created.

The newly created client group appears in the client groups list. Now, you can add clients to the group, if needed. Refer to ["Adding Clients to a Client Group" on the next page](#) for details.

As soon as the first client group is created, DefaultClientProfile is also created, if it does not exist.

Adding Clients to a Client Group

Clients can be added a client group either manually or by specifying the group when registering clients with the CipherTrust Manager. If you specify a client group during client registration, the client automatically appears under the client group on the CipherTrust Manager GUI. Refer to the CTE Agent Clients Guide for information on the registration process.

To manually add clients to a client group:

1. Open the **CTE** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group.
4. In the mini detail view, click **Add Client**. The **Add Client To Client Group <ClientGroupName>** dialog box is displayed with the list of available clients, if any. At least, one client must already exist.

Add Client To Client Group A1



	Status	Name	OS Type	Description
☒	Healthy	P_1	LINUX	TestHost
☐	Healthy	P_10	LINUX	TestHost
☐	Healthy	P_11	LINUX	TestHost

5. Select the desired clients.
6. Click **Add**. A dialog box is displayed asking you to confirm settings inheritance.
7. Confirm whether the selected clients should inherit settings from the client group. The options are:
 - **Inherit Client Group Settings:** This is the default and recommended option. Clients inherit the following properties of the group *except the password*:
 - Client Settings
 - Agent Lock
 - System Lock
 - Communication Enabled
 - Profile Settings
 - QoS Settings
 - GuardPoints

Refer to ["Inheritance of Client Group Settings" on page 82](#) for details.

- **Do not Inherit Client Group Settings:** Clients retain their individual settings. Selecting this option can introduce configuration conflicts. This is not the recommended option. Read the instructions carefully before selecting this option.

8. Click **OK**.

The selected clients are added to the group. They are displayed in the mini view of the client group. Also, the client group is now displayed on the Membership tab of the client. You can remove the client from the group by clicking **Remove**.

Displaying Client Groups

To view the list of client groups:

1. Open the **CTE** application.
2. Click **Clients > Client Groups**. The list of available client groups is displayed.



The client groups list shows the following details:

Column	Description
Client Group Name	Name link of the client group on CipherTrust Manager. Click the link to open client group details in edit mode. The edit mode shows additional details and configuration settings. In the edit mode, you can also view and add clients, GuardPoints, and Client Group Settings.
Description	(Optional) Description to identify the client group.

Modifying Client Groups

After you have created a client group, you can update group details and configuration settings. You can make the following changes:

- > Enable or disable Agent communication for the clients in the group
- > Lock or unlock the CTE Agent files on the clients in the group
- > Change the CTE Agent password for the clients in the group
- > Change the linked profile
- > Add new clients to the group

> Remove clients from the group

To modify a client group:

1. Open the **CTE** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group. The mini view of the client group is displayed.



4. In the mini detail view, modify the required details:
 - **Unlock:** Unlock Agent Lock and System Lock.
 - **Agent Lock:** Lock the contents of the CTE Agent directories on the clients.
 - **System Lock:** Apply an internal policy to the clients to lock system directories like `/var`, `/bin`, and `/etc`. Enabling System Lock automatically enables Agent Lock.
 - **Communication Enabled:** Whether to enable clients' communication with the CipherTrust Manager. Select to enable, clear to disable communication.
 - **Password Creation Method:** Set the password creation method—Generate or Manual. Refer to ["Changing Client Group Password" on the next page](#) for details.
 - **Client Profile:** Select a profile for the client group. The default profile is DefaultClientProfile. To change the client profile, refer to ["Changing the Profile" below](#) for details.
5. Click **Apply**.

Additionally, you can define GuardPoints for the clients in the group. Refer to ["Managing GuardPoints" on page 135](#).

Changing the Profile

To change the profile:

1. Open the **CTE** application.
2. Under **Client Group Name**, click the desired client group.
3. Next to **Client Profile**, click the profile link (for example, DefaultClientProfile). The Select Profile dialog box shows the current client profile and Rekey Option, Rekey Rate, and Schedule of the selected profile.



4. From the **Profile** drop-down list, select the desired profile.
5. Click **OK**. The selected profile is linked successfully.

Changing Client Group Password

The CipherTrust Manager allows for client password management using client groups. For large scale deployments where the CipherTrust Manager must manage several hundreds or thousands of agents, administering passwords on a per-client basis becomes untenable and burdensome. Using a common password across all the clients in a client group mitigates the administrative burden.

This feature is also useful for offline agent recovery. If a remote agent reboots (planned or unplanned) and cannot communicate with the CipherTrust Manager in the central office, it prompts the administrator at the remote site to enter the client password. The remote site administrator typically calls the corporate help desk for the password. Using the password provided by the help desk personnel, the remote site administrator enables offline agent recovery and the resumption of services. As the password is now known to the remote site administrator and the help desk personnel, it may result in a breach of security and/or render the IT operations non-compliant with respect to guaranteeing data privacy.

To remedy the compromised situation, the security administrators should change the password—rotate the password—according to existing security practices. The client group password management feature allows changing the password on all the clients in the client group when the password is compromised.

The use cases for client group password feature can be summarized as follows:

1. Set a common password for all clients in a client group.
2. Reset the common password for all clients in a client group (if the password is provided to a remote CTE Agent administrator for offline agent recovery).

This feature is best suited for large scale deployments when many agents are under the management of a CipherTrust Manager cluster.

Changing the Password Manually

NOTE The manual password creation method is recommended for disaster recovery scenarios.

To change the password:

1. Open the **CTE** application.
2. Click **Clients > Client Groups**
3. Under **Client Group Name**, click the desired group.



Alternatively, click the expand icon (▶) to the left of the desired client group in the client groups list.

4. From the **Password Creation Method** drop-down list, select **Manual**. The **Regenerate Password** button is replaced by **Change Password**.



5. Click **Change Password**.
6. Enter the new password in the **Password** and **Confirm Password** fields. The password must match in both the fields.

NOTE The password must contain minimum eight characters including at least:

- > One capital letter
- > One number
- > One of these special characters: ! @ # \$ % ^ & * () { } []

To cancel the password change, click **Cancel Change Password**.

7. Click **Apply**.

When the new password is applied, the server pushes the password to all clients in the client group. Clients that are removed from the client group retain the password set for the group. Clients added to the group later do not receive the new password.

Changing the Password Dynamically

To change the password:

1. Open the **CTE** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired group.



Alternatively, click the expand icon (▶) to the left of the desired client group in the client groups list.

4. From the **Password Creation Method** drop-down list, select **Generate**. This is the default method.
5. Click **Regenerate Password**.
6. Click **Apply**.

A new generated password is downloaded to the client.

Inheritance of Client Group Settings

Instead of specifying settings for applications running on multiple clients individually, configure them at the client group level. Those settings can be automatically applied to all clients in the group. Refer to "[Client Settings](#)" on page 65 for details on client settings.

CAUTION! Take care when defining client settings at the client group level. If a group contains clients running different operating systems (for example, Linux and Windows) that inherit client settings from the group, conflicts and issues may be observed with file and user access permissions.

- > A client that joins a client group can opt to inherit client group configuration including the client settings.
 - If the client settings are not defined at the group level, the client retains its own settings.
 - If the client settings at the group level are modified later, the updated settings apply to all group members that inherit configuration from the group.
 - Individual clients in the group have client settings overwritten by the group's client settings.

For example:

- a. `clientA` has client settings defined, joins `clientGroup1` and inherits its group configuration. `clientB` also joins `clientGroup1` but does not inherit its group configuration. `clientGroup1`, however, does not have any client settings defined. In this case, both `clientA` and `clientB` retain their own client settings.
 - b. Now, client settings of `clientGroup1` are modified. This overwrites the client settings of all clients that inherit group configuration from `clientGroup1`. So `clientA` inherits the modified group configuration but `clientB` does not, as it does not inherit client group configuration.
 - c. `clientB` is modified to inherit settings from `clientGroup1`. The next time `clientGroup1` updates its client settings, the changes apply to both `clientA` and `clientB`.
- > A client can be a member of more than one client groups. If the client inherits client group configuration from the first client group it joins, and the next groups it joins subsequently, the client inherits the client settings from the last group that it joins.

For example:

- a. `clientC` joins `clientGroup2` and inherits the client group configuration. `clientC` now has `clientGroup2` client settings.
 - b. `clientC` is added to `clientGroup1` and set to inherit client group configuration. So, `clientC` gets `clientGroup1` client settings.
- > If client settings of a client group are emptied, member clients that inherit settings from the group retain the last defined client settings.

For example:

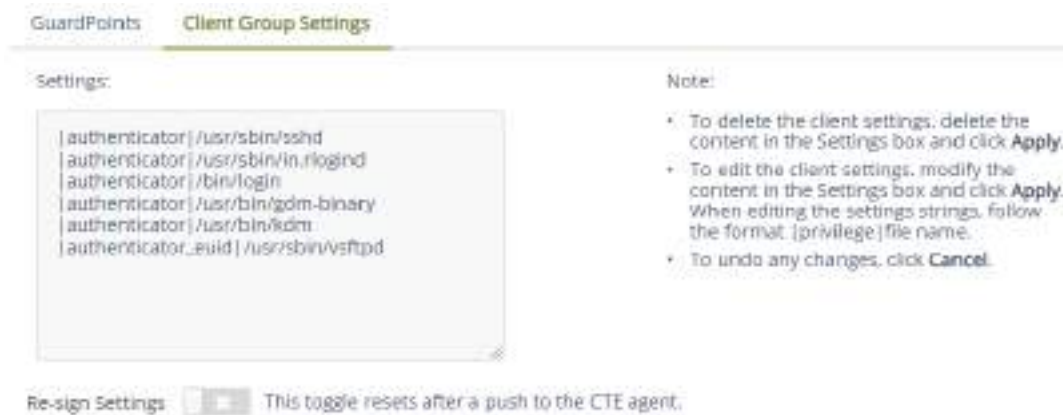
- a. `clientGroup1` deletes its client settings. All member clients (`clientA`, `clientB`, and `clientC`) retain the last client settings defined for `clientGroup1`—blank client settings are not passed to members of the group.
 - b. `clientB` leaves `clientGroup1`. Now, `clientB` retains the client settings it last inherited from `clientGroup1`.
- > If the client settings of a member of a client group are modified, that client no longer inherits client settings from the client group.

For example, client settings on `clientB` are modified. Then, the client settings for `clientGroup1` are modified, all members except `clientB` inherit the changes made to the client settings for `clientGroup1`.

Configuring Client Group Settings

To configure client settings at group level:

1. Open the **CTE** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group.
4. Click the **Client Group Settings** tab. Scroll down the screen, if needed.



5. In the **Settings** text box, add `|authenticator|` before the path of the binary. For example, `|authenticator|/bin/su` to allow `su` to be a trusted method of authentication. For further consideration of authentication options, refer to ["Client Settings" on page 65](#).
6. (Optional, if you add another process to the set of trusted applications) Select **Re-sign Settings** to ensure that the new process is signed and authenticated by the client. The next time the client settings are pushed to the CTE Agent, the updated client settings are re-signed and the **Re-sign Settings** check box is cleared (or reset).

If, after adding a new process, you do not select **Re-sign Settings**, the client ignores the newly added process. See ["Re-Sign Settings" on page 70](#) for more information.

7. Click **Apply**.

Deleting Client Groups

As part of CipherTrust Manager maintenance, you occasionally must remove client groups from the CipherTrust Manager.

- > When you delete a client group, only the group is removed from the CipherTrust Manager GUI. Individual clients that are members of the group remain intact.
- > If you configured a client group password, the individual clients retain the group password.

Deleting a Client Group

To remove a client group:

1. Make sure that no GuardPoints is applied on the group.
2. Open the **CTE** application.
3. Click **Clients > Client Groups**.

4. Under **Client Group Name**, click the overflow icon () corresponding to the desired group.
5. Click **Delete**. A dialog box appears prompting to confirm the action.
6. Click **Delete**.

The client group is removed from the client groups list. Also, the client group is removed from the Membership tab of the linked clients.

Deleting Multiple Client Groups

To remove single or multiple client groups:

1. Make sure that no GuardPoints are applied on the groups.
2. Open the **CTE** application.
3. Click **Clients > Client Groups**.
4. Select the check boxes corresponding to the desired groups.

To select all client groups visible on the page for deletion, select the top check box to the left of the Client Group Name heading.

5. Click the delete icon (). A dialog box appears prompting to confirm the action.
6. Click **Delete**.

The selected client groups are removed from the client groups list. Also, the client groups are removed from the Membership tab of the linked clients.

CHAPTER 7: Managing Signature Sets

File signing checks the authenticity and integrity of executables and applications before they are allowed to access GuardPoint data. When you initiate file signing on the CipherTrust Manager, the CTE Agent calculates the cryptographic signatures of the executables that are eligible to access GuardPoint data. Files are individually signed as part of a set and the set is configured in a policy that defines the processes to allow.

When an executable tries to access a GuardPoint, the secfs service checks the fingerprint, a SHA-2 (Secure Hashing Algorithm) message digest, of the executable against the fingerprint stored in the CTE database. If they match, the executable's authenticity is verified and it can be allowed to access protected data. A hostile or compromised executable, such as a Trojan application, malicious code, or rogue process, with a missing or mismatched signature, is denied access.

Once a set of files to be signed is created, the executables are signed on a selected client and a copy of each signature is stored on the CTE. This is done as a background process on the selected client. The time it takes to complete signing depends upon the number of files to be signed, the response time of the client system, and other load factors. The completion status is indicated in the Signature Sets window.

Completed signature sets are configured in a (CTE Agent) policy so that not only are the executables attempting GuardPoint access identified, but their signatures are checked to ensure that they had not been compromised.

This chapter covers the following information:

- > ["The Signing Process" on the next page](#)
- > ["Using Signature Sets in a Policy" on the next page](#)
- > ["Creating Signature Sets" on page 88](#)
- > ["Signing Files in a Signature Set" on page 90](#)
- > ["Checking Signing Completion Status" on page 92](#)
- > ["Stopping the Signing Process" on page 92](#)
- > ["Displaying Signatures of Files in a Signature Set" on page 93](#)
- > ["Detecting Duplicate Files" on page 94](#)
- > ["Deleting Signatures from Signature Sets" on page 95](#)
- > ["Deleting Source from Signature Sets" on page 96](#)
- > ["Deleting Signature Sets" on page 97](#)
- > ["Re-Signing Files in a Signature Set" on page 98](#)
- > ["Checking Agent Logs if Signing Fails" on page 99](#)

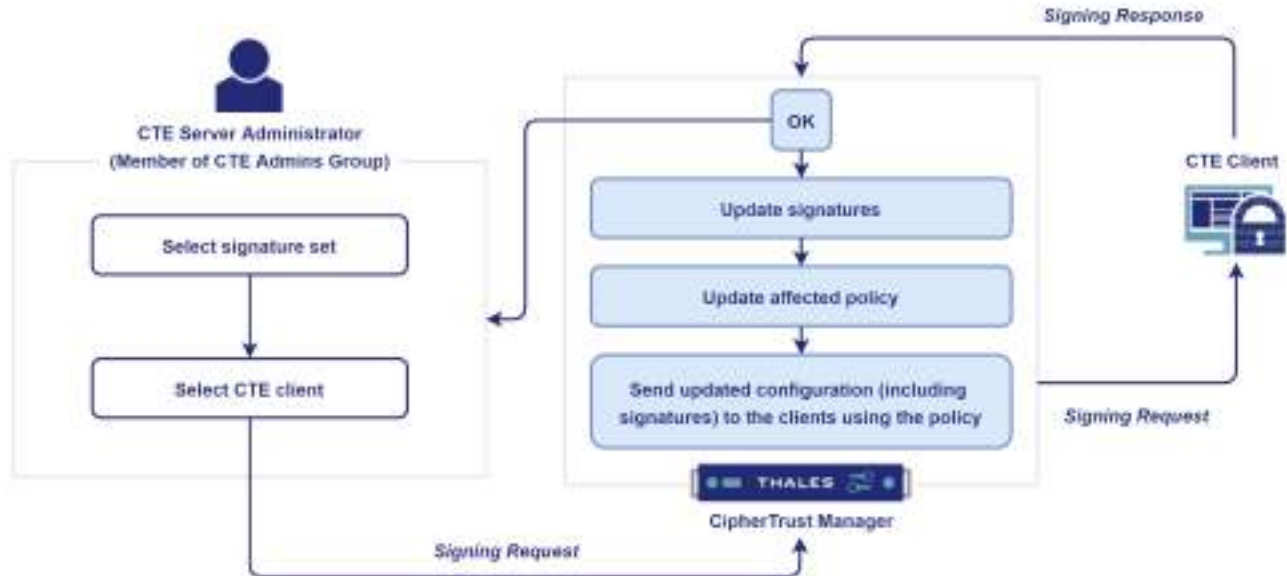
The Signing Process

The basic steps involved in the signature signing process are:

1. The CTE Server Administrator creates signature sets. Refer to ["Creating Signature Sets" on the next page](#) for details.
2. The CTE Server Administrator initiates the signature signing request. The administrator selects the signature set to be signed and the CTE client that will sign the set. Refer to ["Signing Files in a Signature Set" on page 90](#) for details.
3. The CipherTrust Manager forwards the request to the selected CTE client.
4. The CTE client signs the set and sends it to the CipherTrust Manager.
5. The CipherTrust Manager:
 - a. Updates the signatures in the set.
 - b. Updates the affected policies.
 - c. Sends the updated configuration files including the signatures to the clients that are using the affected policies.

In future, if any processes in the signature set are updated, the signature set should be signed again. The CTE Server Administrator can initiate the signature signing process again. This is referred to as the signature re-signing process.

The following diagram shows the high level signature signing process:



Using Signature Sets in a Policy

Policies can be configured to identify the executables trying to access GuardPoint data and to verify that the executables themselves are unchanged since they were signed. You must, however, anticipate the effect of encryption on file signatures.

When a file inside a GuardPoint is copied to a location outside the GuardPoint, the two files have different signatures. The file in the GuardPoint is encrypted, but the file outside the GuardPoint is not.

- > Encryption makes the two files different. The VMD process does not decrypt guarded files before checking their signatures. So, when you rekey guarded files, their signatures also change. Re-sign the files that use the signatures of those files in process sets.
- > If both files must access the GuardPoint data, add both files to the signature set and sign them. If encryption is not applied, both files have the same signature; a signature mismatch should not occur.

Creating Signature Sets

A signature set is a collection of file names and/or directory names. You can enter the full path of files and directories manually or use the browser to locate and select them. Specify a directory to sign all the files in that directory and all the subdirectories that it may contain.

Signing many files can take a while. To shorten processing time, verify that the files and directories in the signature set exist. It takes longer to process non-existent files. If they do not exist, it is recommended that you delete them as sources from the signature set. Refer to ["Deleting Source from Signature Sets" on page 96](#) for details.

To create a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click **Create Signature Set**. The Create Signature Set wizard is displayed.
5. On the **General Info** screen:
 - a. Enter a unique **Name** for the set.

NOTE

- > The name must start with a character. The maximum length can be 64 characters.
- > The name can contain alphanumeric characters, underscores (_), and dashes (-).
- > The name cannot contain the following special characters:
 ? : ; | ! @ # \$ % ^ & * < = > + () { } ~ , \ / [] ' "

- b. Provide a **Description** for the set.
- c. Click **Next**. The Add Sources screen is displayed. On this screen, you can add files to be signed, as described below.

Adding Files to a Signature Set

6. Specify path of the directory or file to be signed. If a directory is specified, all files in the directory and its subdirectories are signed.
 - a. Click **Select Client**. The list of registered clients is displayed.
 - b. Select the desired client.

Status	Name	OS Type	Description
Healthy	10.164.13.209	LINUX	ABLinux
Healthy	ABWin	WINDOWS	AB Windows Client

- c. Click **Select**. The selected client appears next to Select Client.
- d. Click **Add Source**. The file system of the selected client is displayed. The file system of a client marked for deletion cannot be browsed.

The Client drop-down box shows the selected client. If needed, change the client from the list.

- e. Select the path to be signed. Select the path either typing manually or by using the browser.

To jump to a specific directory, enter the directory path in the **Start Directory** field and click **Apply**. The browser shows the subdirectories and files, as shown below.

You cannot browse above the Start Directory. Enter a start point that is higher in the directory hierarchy than all the directories and files that you want to select, or you will have to re-enter start points to locate and select the desired files. The default is the top-level, either slash (Linux) or backslash (Windows).

Alternatively, if you know the directory path, you can enter it manually in the **Path** field.

- f. Click **Add**. The selected source is displayed in the Source Directory list.

Optionally, you can add a new source by clicking **Add Source**. To remove a source, click the overflow icon () corresponding to the source and click **Remove**.

7. Click **Next**. The Confirmation screen shows general information about the set and the selected sources.
8. Verify the set details. If the details are incorrect or you want to modify them, click **Back** and update the details.
9. Click **Save**.

The newly created set appears on the Signature Sets tab. By default, the signature set has the status **UNSIGNED**.

	Name	Signing Status	Updated At: 	Description	
☐	testsigset	Unsigned	18 Aug 2020, 07:54	Test signature set	
☐	test	Unsigned	18 Aug 2020, 00:55		

It is recommended that the signature set is signed before you apply policies to processes. This ensures that a tampered with or compromised process executable is not granted permissions to access protected GuardPoints. Refer to ["Signing Files in a Signature Set" below](#) for details.

Signing Files in a Signature Set

Signing involves calculating a hash value for a file and storing the value on the CipherTrust Manager. Later, when a policy checks signatures, the signature of the process or executable accessing the GuardPoint is calculated and compared against the value in the CipherTrust Manager. If the two values match, the process or executable satisfies the Process requirement of a policy and may be granted access to the guarded data.

NOTE If the executable itself is volatile, or subject to frequent change, it may not be worthwhile to use a file signature as a criteria in a policy because you have to re-sign the executable after each change. If the volatile executables are members of a large signature set, it can take a while to re-sign the files because the signature of every file in the signature set is recalculated. If the volatile files are few, it might be quicker to add the volatile files to a different signature set and sign that set, rather than re-sign all the files in the original signature set.

To sign the files in a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Click the desired signature set.



5. Select a client to sign the signature set. A signing client is required to start the signing process.
 - a. On the **Source** tab, click **Select Client**. The list of registered clients is displayed. Select any client to sign the signature set.
 - b. Select the client.
 - c. Click **Select**. The selected client appears next to the Select Client button. The Sign icon (▶) is now enabled.



CAUTION! Do not select check boxes when signing a signature set. They are used to select source directories to be deleted from the set.

6. Click the Sign icon (▶). The signing process starts.



The signing status of the signature set becomes `InProgress`.

- > To view the percent completion of the signing process, hover over the Spinner (⌂) progress bar.
- > To stop the signing process before it completes, click the Stop Signing icon (●). Refer to ["Stopping the Signing Process" on the next page](#) for details.

The time for the signing process to complete depends on the number of files being processed. Signing occurs as a background process. So, you can use the CipherTrust Manager GUI for other administrative functions during this process.

When the signing completes, the signing status of the signature set becomes `Finished`. Refer to ["Checking Signing Completion Status" on the next page](#) for details about the signing status.

The resulting signatures are available on the Signature tab of the signature set.

Checking Signing Completion Status

To view the signing completion status of a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.

Name	Signing Status	Updated At ↓	Description
☐ testSigned	Finished	18 Aug 2020, 08:04	Test signature set
☐ test	Unsigned	18 Aug 2020, 08:55	

4. View the **Signing Status** for the signature set.

The Signing Status can be:

Status	Description
Unsigned	Signature set is unsigned. Either no files exist in the set or no attempt is made to sign them yet.
InProgress	The CipherTrust Manager is actively signing the files in the set. This can take some time depending on the system load, accessibility, and the number of files being signed at one time.
Finished	All the files in the set are signed successfully. The set is ready for use.
FinishedWithWarning	All the files in the set are processed, but one or more files in the set could not be signed. Possible causes are missing files or inadequate access permissions. Check the VMD logs for details: > On Unix, <code>vorvmd_root.log</code>. > On Windows, <code>vorvmd.log</code>. Alternatively, view the logs in Event Viewer > CipherTrust Encryption Expert. Refer to "Checking Agent Logs if Signing Fails" on page 99 for details.
Aborted	Signing was started but stopped before completion.

Stopping the Signing Process

Interrupt the signing process at any time before it completes. Click the Stop Signing (●) icon on the Source tab of the Signature Sets tab. The CipherTrust Manager does prompt you to verify your choice.

It takes a while for the signing process to stop. After the process is stopped, the Signing Status displayed on the Signature Sets tab is set to `abort`. All the files that were signed until you stopped the process remain intact and can be viewed on the Signature tab of the signature set.

Displaying Signatures of Files in a Signature Set

CipherTrust Manager provides options to display signatures of all or specific files in a signature set.

Displaying Signatures of All Files in the Signature Set

To display the signatures of all files in a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Under **Name**, click the desired signature set.
5. Click the **Signature** tab.



	Program	Signature	
☐	/usr/bin/crash	8840AA3A71BD1D2C3C0A347032E93F7A17F65553B06095409758B55E28E1CA62	...
☐	/usr/bin/vortc	56FE294800C98989D589D1983A550807DA1E06E227E63D611325F81803A9123D	...
☐	/usr/bin/voradmin	7BB14D0AAAFF0DED8FCD55D445AEAF4C2418F8B30CA3EA90844A613906E3029	...

The list of all files (programs) in the signature set with their signatures is displayed. By default, 10 records per page are displayed. Adjust the pagination to view more records.

Displaying Specific Signed Files in the Signature Set

To display specific signed files in a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Under **Name**, click the desired signature set.
5. Click the **Signature** tab. By default, all signed files in the set are displayed in alphanumeric order.
6. In the **Search** box, enter the string that matches the partial or full name of the program whose signature you are searching for.



The search is case-insensitive. All files that contain the string in their names are displayed.

Detecting Duplicate Files

Unless the content of a file is modified, its signature remains the same regardless of the file name and location. Also, the signature of all copies of a file remains the same.

So, to determine the duplicates of a file, display the files based on their signature. If you search using a signature, it is recommended to enter the complete signature.

To detect the duplicates of a file:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Under **Name**, click the signature set in which you want to detect duplicate files.
5. Click the **Signature** tab. The signatures of the files in the set are displayed.
6. Copy the signature of a file from the **Signature** column.
7. Paste the signature in the **Search** box. Remove any extra space, if inserted when pasting.
8. Notice the search result.
 - If multiple records are displayed, duplicates of the file exist.
 - If a single record is displayed, duplicates of the file do not exist.

For example, the following figure shows two files with different names and locations, but with identical content based on their signature.



Source **Signature**

7724722A749EA44B83B8ACE63C20E08DD9C4805EE34D039E1

0 selected 2 results | 2 Signatures

Program	Signature	
☐ /bin/mv_r	7724722A749EA44B83B8ACE63C20E08DD9C4805EE34D039E1B754A85E900D02	...
☐ /bin/ls	7724722A749EA44B83B8ACE63C20E08DD9C4805EE34D039E1B734A88E900D02	...

2 Signatures 10 per page

Deleting Signatures from Signature Sets

Delete either individual signatures from a set or the complete signature sets. Refer to ["Deleting Signature Sets" on page 97](#) for information on deleting complete signature sets.

Delete signatures from a signature set when you want to continue to use the signature set to authenticate processes, but you no longer want to authenticate the files that you are deleting from the set.

You can delete signatures individually or one page at a time.

Deleting Single Signatures

To delete a single signature from a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click the desired signature set.
5. Click the **Signature** tab. The list of signatures in the signature set is displayed.
6. Click the overflow icon (**...**) corresponding to the desired signature.



Program	Signature	
☒ /usr/bin/crash	8829A43A71BD1D3CE3CDA847932E8F7A17F862538D99B51D9756853E2981CA82	...
☐ /usr/bin/wdtt	56FE294800C9E0805589D1983A556887D41E06E227E63D611325F31B93A9723D	...

Delete

7. Click **Delete**. A dialog box appears prompting you to confirm the action.
8. Click **Delete**.

The selected signature is removed from the list and the CipherTrust Manager database.

Deleting Multiple Signatures

To delete single or multiple signatures from a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click the desired signature set.
5. Click the **Signature** tab.
6. Select the check boxes corresponding to the signatures you want to delete.



Program	Signature
☒ /usr/bin/crash	8840AA3A71BD1D2C9C0A3
☒ /usr/bin/vort	56FE204800C9B0805580D1

To select all signatures for deletion, select the top check box to the left of the Signature heading.

7. Click the delete icon (🗑️). A dialog box appears prompting you to confirm the action.
8. Click **Delete**.

The selected signatures are removed from the list and the CipherTrust Manager database.

Deleting Source from Signature Sets

Signing many files can take a while. To shorten processing time, verify that the files and directories in the signature set exist. It takes longer to process non-existent files. If they do not exist, it is recommended that you delete them as sources from the signature set.

Deleting Single Sources

To delete a single source from a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click the desired signature set. The Source tab shows the list of source directories.
5. Click the overflow icon (⋮) corresponding to the desired source directory.



6. Click **Delete**. A dialog box appears prompting you to confirm the action.
7. Click **Delete**.

The selected source is removed from the list and the CipherTrust Manager database.

Deleting Multiple Sources

To delete single or multiple sources from a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click the desired signature set. The Source tab shows the list of source directories.
5. Select the check boxes corresponding to the desired source directories.



To select all sources for deletion, select the top check box to the left of the Source Directory heading.

6. Click the delete icon (🗑️). A dialog box appears prompting you to confirm the action.
7. Click **Delete**.

The selected sources are removed from the list and the CipherTrust Manager database.

Deleting Signature Sets

Delete either individual signatures from a set or the complete signature sets. Refer to ["Deleting Signatures from Signature Sets" on page 95](#) for information on deleting individual signatures.

An active (in use) signature set cannot be deleted. Before deleting a signature set from the CipherTrust Manager, make sure that no policies are using it.

CipherTrust Manager provides options to delete single or multiple signature sets.

Deleting Single Signature Sets

To delete a single signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Click the overflow icon (⋮) corresponding to the desired signature set.

Name	Signing Status	Updated At	Description
☐ testsigset	Finished	18 Aug 2020, 08:12	Test signature set
☐ test	Unsigned	18 Aug 2020, 08:55	

Edit
Delete

5. Click **Delete**. A dialog box appears prompting you to confirm the action.

6. Click **Delete**.

The selected signature set is removed from the list.

Deleting Multiple Signature Sets

To delete single or multiple signature sets:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Select the check boxes corresponding to the desired signature sets.

2 Selected 2 Results | 2 Signature Sets

Name	Signing Status
☒ testsigset	Finished
☒ test	Unsigned

To select all sets for deletion, select the top check box to the left of the Name column.

5. Click the delete icon (🗑️). A dialog box appears prompting you to confirm the action.

6. Click **Delete**.

The selected signature sets are removed from the list.

Re-Signing Files in a Signature Set

Signatures are computed values. Unless the files in a signature set are compromised or modified, the signature always remains the same for a given file. If the files are modified, they must be re-signed to ensure that their signatures match the signatures on the CipherTrust Manager.

To re-sign the files, you can:

- > Create and sign a new signature set with the files and directories to be signed. Use this option if the set contains only a few files and directories.
- > Create and sign a new signature set with the paths of the directories that contain the files to be signed. Use this option if the directories contain only a few files or most files in the directories need re-signing.

- > Open and re-sign the existing signature set that is originally used to sign the files. Use this option if you have the time or the signature set is small.

Computing the signature of every file in a large signature set takes a long time.

Re-signing the files in a set takes longer than signing the files the first time. It requires additional handling to update information on the CipherTrust Manager. If you plan to re-sign a large number of files (say hundreds of thousands), it can be quicker to:

1. Delete the existing signature set. Refer to ["Deleting Signature Sets" on page 97](#) for details.
2. Create the signature set again, from scratch. Refer to ["Creating Signature Sets" on page 88](#) for details.
3. Sign the files of the signature set again. Refer to ["Signing Files in a Signature Set" on page 90](#) for details.

Checking Agent Logs if Signing Fails

If signing fails, or you want more information about the signing process such as which files were skipped, check the CTE Agent logs captured on the client.

Messages are logged to:

- > (UNIX) `/var/log/vormetric/vorvmd_root.log` with Log to File enabled and to a Syslog server with Syslog enabled.
- > (Windows) `\Documents and Settings\...\agent\log\vorvmd.log` with Log to File enabled.

In the `vorvmd_root.log`/`vorvmd.log` file on the client, look for messages like:

```
[VMD] [WARN ] [3732] [VMD3824W] Failed to create the signature for
E:\apps\lib\dx1\aa_dir\dataxform_auto_config for the signature request 9, error
code 3
```

The following table lists error codes with their description:

Code	Description
0	System is okay.
1	Does not exist.
2	DO NOT USE.
3	Invalid argument.
4	Operation not supported.
5	Out of memory.
6	No space left on device.
7	Timeout reached.
8	I/O error.

Code	Description
9	Interrupted.
10	Permission denied.
11	Too many keys in key group.
12	Error in soap rpc layer.
13	Returned buffer is partially full.
14	Given target buffer is too small.
15	Unable to compress buffer.
16	Internal test failed.
17	Overflow.
18	Error setting up logging.
19	Overloaded error.
20	Server responded to a file upload with "bad request".
21	Unknown user name or bad password.
22	The directory service is not available.

CHAPTER 8: Managing Policies

The primary job of a CipherTrust Manager Security Administrator is to create policies that protect data. Policies govern access to, and encryption of, the files in GuardPoints.

This chapter covers the following information:

- > ["Overview" below](#)
- > ["Policy Rule Criteria and Effects" on the next page](#)
- > ["Creating Policy Elements" on page 103](#)
- > ["Creating Policies" on page 114](#)
- > ["Displaying Policies" on page 124](#)
- > ["Modifying Policies and Rules" on page 127](#)

Overview

A policy is a collection of rules that govern data access and encryption. Think of a policy as an if-then statement. Policy rules are processed sequentially. If the criteria of rule one are not met, the policy enforcement engine moves on to the second rule and so on.

Policies specify:

- > **Actors:** Users, groups, and processes that are permitted/denied access to protected data.
- > **Actions:** What actions authorized actors are allowed to perform. For example create/delete, read/write, decrypt, modify permissions, and so on.
- > **Files acted upon:** Policy rules may apply to entire directories and mount points, or only to files named in a specific way (for example, .docx files may be encrypted and restricted to read only access by designated users, while other files may be stored clear and read and written by anyone).

Additionally, each CTE policy specifies one or more encryption keys used to encrypt blocks of file data when applications write them, and decrypt them when they are read.

CTE encryption is transparent to applications. This means that the CTE Agent encrypts blocks of data as they are written, and decrypts data when they are read by authorized users and applications. This architecture separates administration of files from access to the data in them. Backup programs, for example, may be authorized to read files, but not view the data in them. Therefore, data can be backed up and taken offsite while remaining encrypted so that security is not breached.

The following criteria are processed by the policy enforcement engine:

Criteria	Description
Order	Security rule enforcement sequence.

Criteria	Description
Resource	Files and/or directories to which the policy will apply, plus key rules that govern those files and directories.
User	Users and user groups authorized to access the resources.
Process	Executables which will access the files.
Action	Type of user access being made (read, write, copy, move etc.). Before you can define Data Transformation Rules, you must select an Action type of Key_op.
Effect	When all the other rules match, this describes the type of access granted or denied per the rule.
Browsing	Allow browsing is enabled by default, while the Enable Communication check box is enabled on the client. This allows the server to browse the client's file system. This option can be deselected even if client communication is still enabled.

A policy comprises ["Security Rules" on page 26](#), ["Key Rules" on page 30](#), and ["Data Transformation Rules" on page 30](#).

Policy Rule Criteria and Effects

Policy Rules consist of five criteria, which specify the attributes of an access attempt, and effects, which define whether that access is permitted or denied, and whether encryption/decryption is required.

Policy Rule Criteria

Criteria	Action
Resource	Files and/or directories in a GuardPoint to be blocked. Example: <code>/secure_dir/financials</code> .
User	Users or groups of users that can access the files.
Process	Executables that can operate on the files.
Action	Allowed file action. Example: read, write, remove, rename, and make directory.

Policy Rule Effects

Effect	Action
Permit	Allows access to the data.

Effect	Action
Deny	Disallows access to the data.
Apply Key	Encrypts data written to a GuardPoint with the specified key. Decrypts data that is accessed using the same key.
Audit	Creates an entry in the Message Log that describes what is being accessed, when it is being accessed, and the security rule being applied.

Every time a user's application tries to access a GuardPoint file, the security policy tests that access attempt against the criteria of each rule. For example, suppose a user, Harry, wants to access and modify a file called `secret`, using the command `cp`. For Harry to be successful, there must be a rule that allows access to the `secret` (resource), by the user `Harry` (user), using the command `cp` (process), and includes the permission `write` (action).

A blank criteria field specifies a value of `All`. If `User` is blank, the rule applies to all users; if `Process` is blank, the rule applies to all executables, and so on. `Effect` can never be blank. It must have at least a `permit` (allow access) or `deny` (disallow access).

A policy can have multiple rules. Rules are evaluated much like firewall rules. They are evaluated in order, from first to last, and evaluation stops when a rule is found for which all the criteria are met. The effect for that rule is then enforced. So, carefully order a policy's rules to achieve the desired result.

Creating Policy Elements

Policy rule criteria consist of resource sets, user sets, signature sets, process sets, action, and effect, and are called policy elements. These elements should exist on the CipherTrust Manager before you can use them in security policies.

Although you can add policy elements when creating policies, it may be a better approach to have them created in advance. This document describes creation of policy elements separately, before creating policies.

A CipherTrust Manager administrator can create, modify, and delete resource sets, user sets, process sets, and signature sets on the CipherTrust Manager. Actions and effects are preconfigured on the CipherTrust Manager.

This section covers the following information:

- > ["Creating Resource Sets" on the next page](#)
- > ["Creating User Sets" on page 105](#)
- > ["Creating Signature Sets" on page 108](#)
- > ["Creating Process Sets" on page 110](#)

After you have created policy elements, you can use them in creating and configuring policies. Refer to ["Creating Policies" on page 114](#) for details.

Creating Resource Sets

A resource is a combination of a directory, a file, and patterns or special variables. A resource set is a named collection of directories, files, or both, that a user or process will be permitted or denied access to.

Use the Create Resource Set wizard to create resource sets.

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. On the Resource Sets tab, click **Create Resource Set**. The Create Resource Set wizard is displayed.
4. On the **General Info** screen:
 - a. Enter a unique **Name** for the set.

NOTE

- > The name must start with a character. The maximum length can be 64 characters.
- > The name can contain alphanumeric characters, underscores (_), and dashes (-).
- > The name cannot contain the following special characters:

? : ; | ! @ # \$ % ^ & * < = > + () { } ~ , \ / [] ' "

- b. Provide a **Description** for the set.
 - c. Click **Next**. The Add Resources screens is displayed.
5. Specify the resource **Directory**.
The path must end with a slash. For example, a Windows path must end with a \ (backward slash). A Linux path must end with a / (forward slash).
6. Specify a **File** or enter the asterisk. The asterisk acts as a wild card character.
7. (Optional) Specify whether to include subfolders in the set. Turn on **Include Sub Folders**. By default, the subfolders are not included.

Directory: /opt/cte-test/

File: *

include Sub Folders: ☒

8. Click **Next**. The Confirmation screen is displayed.
The screen shows general information about the set and the selected sources.

Directory	File	include Sub Folders	File System Type	
/opt/cte-test/	*	Yes	Local FileSystem	...

9. Verify the resource set details.

If the details are incorrect or you want to modify them, click **Back** and update the details. To add another resource, click **Add Another Resource**, and specify the details, as described above.

10. Click **Save**. The resource set is created.

The newly created resource set appears on the Resource Sets tab.

Name	Updated At ↓	Description
☐ resourceSet	18 Aug 2020, 11:47	Resource set
☐ SG-ResourceSet	18 Aug 2020, 11:38	

Creating User Sets

A user set is a collection of users and user groups that you want to grant or deny access to GuardPoints. User sets are configured in policies. Policies can be applied to user sets, not to individual users.

Use the Create User Set wizard to create user sets. The wizard provides two options to add user sets. Specify a user set either by querying the registered client or by manually entering the members (individual members, groups, or group members). If needed, you can manually add AD users to a user set.

Creating User Sets by Browsing the Client

To create a user set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **User Sets** tab.
4. Click **Create User Set**. The Create User Set wizard is displayed.
5. On the **General Info** screen:
 - a. Enter a unique **Name** for the set.

NOTE

- > The name must start with a character. The maximum length can be 64 characters.
- > The name can contain alphanumeric characters, underscores (_), and dashes (-).
- > The name cannot contain the following special characters:
 ? : ; | ! @ # \$ % ^ & * < = > + () { } ~ , \ / [] ' "

- b. Provide a **Description** for the set.
- c. Click **Next**. The Add Users screen is displayed.

By default, the **Browse to Add Users** tab is active. This tab allows you to browse the client for members. To add members manually, refer to ["Creating User Sets by Adding Members Manually" on page 107](#).

6. Select the **Agents** option.
7. Click **Select**. The list of registered clients is displayed.

8. Select the desired client. Members, groups, or group members of this client will be added to the set.
9. Click **Select**. The IP address or hostname of the selected client is displayed next to the Select button. The Member Choice and Max Entries to Return fields are also displayed.

Agents

Select 10.164.13.209

Member Choice
Members

Max Entries to return
300

10. From the **Member Choice** drop-down list, select members. The options are:
 - **Members**: Retrieves members (users) of the client. This is the default setting.
 - **Groups**: Retrieves user groups of the client.
 - **Group Members**: Retrieves group members of the client. When you select this option, the Select Groups field appears. This is a mandatory field. Select a group from the drop-down list. Search will retrieve members of the selected group.
11. Specify the **Max Entries to Return**. This is a mandatory field. The default number is 300.
12. Click **Submit**. The search result based on the specified criteria is displayed on the right. By default, five entries per screen are displayed. Use the on-screen pagination to view more entries.
13. Select the desired members from the list.

☐	uname	UID	gname	GID
☒	root		root	
☐	bin	1	bin	1
☐	daemon	2	daemon	2

14. Click **Next**. The Confirmation screen shows general information about the set and the selected members.

uname	UID	gname	GID	OS domain	
root		root			Remove
testuser_1	1003	testuser_1	1003		Remove

15. Verify the set details.
If the details are incorrect or you want to modify them, click **Back** and update the details.
16. Click **Save**. The user set is created.

The newly created set appears on the User Sets tab.

	Name	Updated At ↓	Description	
☐	userset	18 Aug 2020, 12:10	A test user set	...
☐	testuserset	18 Aug 2020, 12:09	Test user set	...

Creating User Sets by Adding Members Manually

This method is useful when you already know the names of users and groups that should be added to a user set. Also, use this method to add AD users and groups to the user set.

To create a user set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **User Sets** tab.
4. Click **Create User Set**. The Create User Set wizard is displayed.
5. On the **General Info** screen:
 - a. Enter a unique **Name** for the set.

NOTE

- > The name must start with a character. The maximum length can be 64 characters.
- > The name can contain alphanumeric characters, underscores (_), and dashes (-).
- > The name cannot contain the following special characters:

? : ; | ! @ # \$ % ^ & * < = > + () { } ~ , \ / [] ' "

- b. Provide a **Description** for the set.
- c. Click **Next**. The Add Users screen is displayed.

By default, the **Browse to Add Users** tab is active. This tab allows you to browse the client for members. Refer to ["Creating User Sets by Browsing the Client" on page 105](#) for details.

6. Click the **Manually Add Users** tab.
7. Specify the following details, as appropriate:

Element	Description
uname	Login name of the user.
UID	(AIX/Linux only) ID of the user.
gname	Comma-separated list of group names.

Element	Description
GID	(AIX/Linux only) Group ID of the user. Specify only the primary group ID.
OS domain	(Windows only) Network domain of the user. Multiple domain names, separated by commas, can be entered. Specify the string <code>localhost</code> to configure a generic domain.

8. Click **Next**. The Confirmation screen shows general information about the set and the selected members.

9. Verify the set details.

If the details are incorrect or you want to modify them, click **Back** and update the details.

10. Click **Save**. The user set is created.

The newly created set appears on the User Sets tab.

Creating Signature Sets

A signature set is a collection of hashes of processes and executables that you want to grant or deny access to GuardPoints. A signature set can be configured in a policy as part of a process set to verify the integrity of a process before it is allowed access to guarded data. Policies are applied to signature sets, not to individual signatures.

To create a signature set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click **Create Signature Set**. The Create Signature Set wizard is displayed.
5. On the **General Info** screen:
 - a. Enter a unique **Name** for the set.

NOTE

- > The name must start with a character. The maximum length can be 64 characters.
- > The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
- > The name cannot contain the following special characters:

? : ; | ! @ # \$ % ^ & * < = > + () { } ~ , \ / [] ' "

b. Provide a **Description** for the set.

c. Click **Next**. The Add Sources screen is displayed. On this screen, you can add files to be signed, as described below.

Adding Files to a Signature Set

6. Specify path of the directory or file to be signed. If a directory is specified, all files in the directory and its subdirectories are signed.
 - a. Click **Select Client**. The list of registered clients is displayed.

- b. Select the desired client.

Status	Name	OS Type	Description
 Healthy	10.164.13.209	LINUX	ABLinux
 Healthy	ABWin	WINDOWS	AB Windows Client

- c. Click **Select**. The selected client appears next to Select Client.
- d. Click **Add Source**. The file system of the selected client is displayed. The file system of a client marked for deletion cannot be browsed.

The Client drop-down box shows the selected client. If needed, change the client from the list.

- e. Select the path to be signed. Select the path either typing manually or by using the browser.



To jump to a specific directory, enter the directory path in the **Start Directory** field and click **Apply**. The browser shows the subdirectories and files, as shown below.



You cannot browse above the Start Directory. Enter a start point that is higher in the directory hierarchy than all the directories and files that you want to select, or you will have to re-enter start points to locate and select the desired files. The default is the top-level, either slash (Linux) or backslash (Windows).

Alternatively, if you know the directory path, you can enter it manually in the **Path** field.

- f. Click **Add**. The selected source is displayed in the Source Directory list.

Optionally, you can add a new source by clicking **Add Source**. To remove a source, click the overflow icon () corresponding to the source and click **Remove**.

7. Click **Next**. The Confirmation screen shows general information about the set and the selected sources.
8. Verify the set details. If the details are incorrect or you want to modify them, click **Back** and update the details.
9. Click **Save**.

The newly created set appears on the Signature Sets tab. By default, the signature set has the status **UNSIGNED**.

	Name	Signing Status	Updated At: 	Description	
☐	testsignset	Unsigned	18 Aug 2020, 07:54	Test signature set	
☐	test	Unsigned	18 Aug 2020, 00:55		

It is recommended that the signature set is signed before you apply policies to processes. This ensures that a tampered with or compromised process executable is not granted permissions to access protected GuardPoints. Refer to ["Signing Files in a Signature Set" on page 90](#) for details.

Creating Process Sets

A process set is a collection of processes (executables) that you want to grant or deny access to GuardPoints. Like user sets, process sets can be configured in policies. Policies can be applied to process sets, not to individual processes.

Optionally, file signing can be configured to check the authenticity and integrity of executables and applications before they are allowed to access GuardPoint data. A signature set must already exist before you can configure file signing in a policy for a process set.

Use the Create Process Set wizard to create process sets.

To create a process set:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**.
3. Click the **Process Sets** tab.
4. Click **Create Process Set**. The Create Process Set wizard is displayed.
5. On the **General Info** screen:
 - a. Enter a unique **Name** for the set.

NOTE

- > The name must start with a character. The maximum length can be 64 characters.
- > The name can contain alphanumeric characters, underscores (_), and dashes (-).
- > The name cannot contain the following special characters:

? : ; | ! @ # \$ % ^ & * < = > + () { } ~ , \ / [] ' "

- b. Provide a **Description** for the set.
 - c. Click **Next**. The Add Processes screen is displayed.
6. Specify the process path.
- a. Click **Browse** next to the Directory field. The list of registered clients is displayed.
 - b. Select the desired client.
 - c. Click **Next**. The Browse Path dialog box is displayed.
 - d. Browse the process.

Alternatively, specify the process name (with its path) in the **Path** field. For a Windows path, use \ (backward slashes), for a Linux path, use / (forward slashes). A directory path must end with a slash.

- e. Click **Add**.

The selected directory and process appear in the **Directory** and **File** fields. If a process is not selected, the **File** field shows an (*) asterisk. The asterisk acts as a wild card character.

Alternatively, specify the directory and process in the **Directory** and **File** fields. For a Windows path, use \ (backward slashes), for a Linux path, use / (forward slashes). A directory path must end with a slash.

7. Link the desired signature set to the process set.
 - a. Click **Select** next to the Signature field. The list of signature sets is displayed.
 - b. Select the desired signature set.
 - c. Click **Next**.

The selected signature set appears in the **Signature** field.

8. Click **Next**. The Confirmation screen shows general information about the set.

Directory	File	Signature	
/usr/bin/	*	testsigset	***

9. Verify the set details.

If the details are incorrect or you want to modify them, click **Back** and update the details. To add another process, click **Add Another Process**, and specify the details, as described above.

10. Click **Save**. The process set is created.

The newly created set appears on the Process Sets tab.

	Name	Updated At ↓	Description	
☐	testprocessset	18 Aug 2020, 12:34	Test process set	...
☐	aprocesstest	18 Aug 2020, 12:34	A process set	...

After you have created policy elements, you can use them in creating and configuring policies. Refer to ["Creating Policies" on page 114](#) for details.

Viewing Policy Elements

The Policy Elements page shows the list of configured policy elements.

To view the policy elements:

1. Open the **CTE** application.
2. Click **Policies > Policy Elements**. The Policy Elements page contains the following tabs:

Column	Description
Resource Sets	Displays the list of configured resource sets. This is the default tab.
User Sets	Displays the list of configured user sets.
Process Sets	Displays the list of configured process sets.
Signature Sets	Displays the list of configured signature sets.

3. Click the **Resource Sets** tab. This tab displays the following details:

	Name	Updated At ↓	Description	
☐	resourceSet	18 Aug 2020, 11:47	Resource set	...
☐	SG-ResourceSet	18 Aug 2020, 11:38		...

Column	Description
Name	Name of the resource set.
Updated At	Time when the set is created or updated.
Description	Optional description of the resource set.

By default, the records are displayed in descending order by Updated At. To add a new resource set, refer to ["Creating Resource Sets" on page 104](#).

To modify an existing resource set, click the desired set, modify the **Description**, and click **Apply**. The edit view also provides the **Add Resource** button to add new resources to the set.

4. Click the **User Sets** tab. This tab displays the following details:

Name	Updated At ↓	Description	
☐ userset	18 Aug 2020, 12:10	A test user set	...
☐ testuserset	18 Aug 2020, 12:09	Test user set	...

Column	Description
Name	Name of the user set.
Updated At	Time when the set is created or updated.
Description	Optional description of the user set.

By default, the records are displayed in descending order by Updated At. To add a new user set, refer to ["Creating User Sets" on page 105](#).

To modify an existing user set, click the desired set, modify the **Description**, and click **Apply**. The edit view also provides the **Browse for users** and **Manually add user** buttons to add new users to the set.

5. Click the **Process Sets** tab. This tab displays the following details:

Name	Updated At ↓	Description	
☐ testprocessset	18 Aug 2020, 12:34	Test process set	...
☐ aprocessset	18 Aug 2020, 12:34	A process set	...

Column	Description
Name	Name of the process set.
Updated At	Time when the set is created or updated.
Description	Optional description of the process set.

By default, the records are displayed in descending order by Updated At. To add a new process set, refer to ["Creating Process Sets" on page 110](#).

To modify an existing process set, click the desired set, modify the **Description**, and click **Apply**. The edit view also provides the **Add Process** button to add new processes to the set.

6. Click the **Signature Sets** tab. This tab displays the following details:

	Name	Signing Status	Updated At ↓	Description	
☐	testsigset	Unsigned	18 Aug 2020, 07:54	Test signature set	...
☐	test	Unsigned	18 Aug 2020, 00:55		...

Column	Description
Name	Name of the signature set.
Signing status	Signing status of the signature set. Refer to "Checking Signing Completion Status" on page 92 for details.
Updated At	Time when the set is created or updated.
Description	Optional description of the signature set.

By default, the records are displayed in descending order by Updated At. To add a new signature set, refer to ["Creating Signature Sets" on page 108](#).

To add a new source to an existing signature set, click the desired set, and click **Add Source** on the **Source** tab.

Creating Policies

A policy is a collection of rules that govern data access and encryption. Think of a policy as an if-then statement. Policy rules are processed sequentially. If the criteria of rule one are not met, the policy enforcement engine moves on to the second rule and so on.

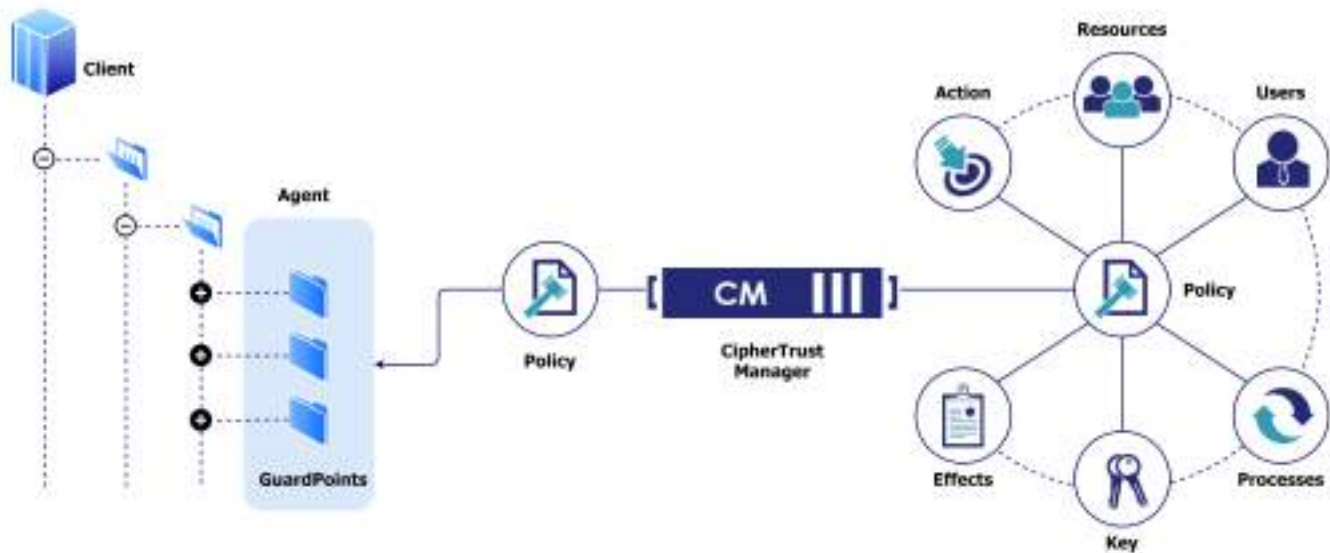
Policies specify:

- > **Actors:** Users, groups, and processes that are permitted/denied access to protected data.
- > **Actions:** What actions authorized actors are allowed to perform. For example create/delete, read/write, decrypt, modify permissions, and so on.
- > **Files acted upon:** Policy rules may apply to entire directories and mount points, or only to files named in a specific way (for example, .docx files may be encrypted and restricted to read only access by designated users, while other files may be stored clear and read and written by anyone).

Additionally, each CTE policy specifies one or more encryption keys used to encrypt blocks of file data when applications write them, and decrypt them when they are read.

CTE encryption is transparent to applications. This means that the CTE Agent encrypts blocks of data as they are written, and decrypts data when they are read by authorized users and applications. This architecture separates administration of files from access to the data in them. Backup programs, for example, may be authorized to read files, but not view the data in them. Therefore, data can be backed up and taken offsite while remaining encrypted so that security is not breached.

The following diagram shows policies and how they relate to the GuardPoints, clients, and the CipherTrust Manager.



Before you can create a policy, policy elements should exist on the CipherTrust Manager. This section assumes that you have already created policy elements, as described in ["Creating Policy Elements" on page 103](#).

When creating a policy, you can specify security rules, key rules, and data transformation (dataxform) rules that apply to the policy. At least one key or security rule must be added to a policy. Use the Create Policy wizard to create a policy.

To create and configure policies:

- > ["Step 1: Specify General Information" below](#)
- > ["Step 2: Add Security Rules" on page 117](#)
- > ["Step 3: Add Key Rules" on page 119](#)
- > ["Step 4: Add Data Transformation Rules" on page 121](#)
- > ["Step 5: Confirm Details" on page 122](#)

Step 1: Specify General Information

To specify general information about policy:

1. Open the **CTE** application.
2. Click **Policies**. The Policies page shows the list of available policies.
3. Click **Create Policy**.
4. Specify a unique **Name** for the policy. For example, `basic-access-policy` or `ldt-policy`.

NOTE

- > The name must start with a character. The maximum length can be 64 characters.
- > The name can contain alphanumeric characters, underscores (_), and dashes (-).
- > The name cannot contain the following special characters:
 ? : ; | ! @ # \$ % ^ & * < = > + () { } ~ , \ / [] ' "

5. Select a **Policy Type**. The options are:

- **Standard:** Access to data is blocked during initial encryption or rekeying of data. This is the default policy type.
- **Live Data Transformation:** Encryption and rekeying of data takes place in the background, without disrupting user or application access to that data. The LDT policy is available if you have a valid LDT license.

If you select an LDT policy type, then the first security rule for the policy is created by default. This rule permits key operations on all resources for that policy, without denying user or application access to resources. This allows a rekey operation whenever the encryption key is versioned. This rule is always the first rule in an LDT policy and cannot be edited.

- Refer to ["Enabling Live Data Transformation" on page 57](#) for more information about LDT.
- An LDT policy is needed for creating LDT GuardPoints. Refer to ["Creating LDT GuardPoints on Clients" on page 140](#) for details.

- **Cloud Object Storage:** Access to data is blocked during initial encryption or rekeying of data. This policy type is needed for creating GuardPoints for cloud storages. Refer to ["Creating Cloud Object Storage GuardPoints on Clients" on page 143](#) for details.

6. (Optional) Turn on the **Learn Mode** toggle. A warning message is displayed indicating that the policy is in Learn Mode.



Refer to ["Learn Mode" on page 31](#) for details. By default, the toggle is turned off.

7. (Optional, applicable to Standard policies) Turn on the **Data Transformation** toggle. This option is used to create a [dataxform](#) policy. By default, the toggle is turned off.

NOTE The Data Transformation option is not applicable to LDT and Cloud Object Storage policies. For a dataxform policy, the Create Policy wizard shows *five* steps including the Data Transformation step, as shown below.



8. Click **Next**. The Security Rules screen is displayed.

- > For a standard dataxform policy, a security rule with the Action `key_op` and the Effect `permit, applykey` and Browsing set to Yes is added automatically. Edit or delete the rule, as appropriate. Click the overflow icon (`...`) for options.

Resource Set	User Set	Process Set	Action	Effect	Browsing	
			key_op	permit,applykey	Yes	⋮

- > For an LDT policy, the default security rule with the Action `key_op` and the Effect `permit, applykey` and Browsing set to No added automatically. The rule is *read only*.

Resource Set	User Set	Process Set	Action	Effect	Browsing	
			key_op	permit,applykey	No	

Step 2: Add Security Rules

1. Click **Create Security Rule**. The Create Security Rule dialog box is displayed. This dialog box contains the following fields:

Field	Description
Resource Set	(Applicable to Standard and LDT policies) Resource set for the rule.
User Set	User set for the rule.
Process Set	Process set for the rule.
Action	Actions for the rule. Refer to "Actions" on page 27 for the complete list of supported actions.
Effect	Effect permission and options for the rule. This is a mandatory field.
Browsing	(Applicable to Standard and LDT policies) Whether browsing of directories under the GuardPoint down to the resources in the rule is allowed.

2. (Optional, applicable to Standard and LDT policies) Select a **Resource Set**.
 - a. Click **Select** next to the Resource Set field. The list of available resource sets is displayed.
Optionally, you can add a new resource set by clicking **Create Resource Set**. Walk through the Create Resource Set wizard, as described in ["Creating Resource Sets"](#) on page 104. The newly created resource set appears in the resource sets list.
 - b. Select a resource set.
 - c. (Optional) Select **Exclude Rule** to exclude the resource set from the policy. The security rule does not apply to this resource set.
 - d. Click **Select**. The selected resource set appears in the Resource Set field.
3. (Optional) Select a **User Set**.
 - a. Click **Select** next to the User Set field. The list of available user sets is displayed.

- **ApplyKey:** Applies an encryption key to data in a GuardPoint. When applied, data copied to the GuardPoint is encrypted with the key specified on the Create Key Rule screen and data that is accessed in the GuardPoint is decrypted using the same key. It allows the access attempt to the resource. For example, you can specify an effect that allows writing to a directory.

NOTE If you select ApplyKey, you must also specify the key rules to apply for encrypting and decrypting the resources. Refer to ["Step 3: Add Key Rules" below](#) for details.

- **Audit:** Creates a message log entry for each qualifying event. It records what, when, and who is accessing the information.

d. Click **Select**. The selected effects appear in the Effect field.

7. (Optional, applicable to Standard and LDT policies) Specify whether to **Allow Browsing** the directories under the GuardPoint down to the resources in the rule.

By default, the **Allow Browsing** toggle is on. Users that match the criteria set by the security rule can access the directories between the GuardPoint and the resource. If you define a resource, then that resource should exist in the GuardPoint. The files in these directories can be listed like any file in a browser, but they cannot be modified, copied, or deleted.

To prevent users from browsing the directories under the GuardPoint, turn off the **Allow Browsing** toggle.

8. Click **Add**. The newly created security rule appears in the list of security rules.

Similarly, you can add multiple security rules to the policy by clicking **Create Security Rule**. To delete a security rule, click **Delete** next to the rule.

NOTE A security rule with the ApplyKey Effect must be supported by at least one key rule. Refer to ["Step 3: Add Key Rules" below](#).

9. Click **Next**. The Key Rules screen is displayed.

Step 3: Add Key Rules

If you added a security rule with the Effect ApplyKey on the Security Rule screen, then you must add at least one key rule.

To add a key rule:

1. Click **Create Key Rule**. The Create Key Rule dialog box is displayed.
2. (Optional, applicable to Standard and LDT policies) Select a **Resource Set**.
 - a. Click **Select** next to the Resource Set field. The list of available resource sets is displayed.
Optionally, you can add a new resource set by clicking **Create Resource Set**. The newly created resource set will appear in the resource sets list.
 - b. Select a resource set.
 - c. Click **Select**. The selected resource set appears in the Resource Set field.
3. Select a **Key Name**. This is a mandatory field. For LDT and Data Transformation policies, the field name is **Current Key Name** instead of Key Name.
 - a. Click **Select** next to the field. The list of available keys is displayed.

Optionally, you can create a new key by clicking **Create a New Key**. Optionally, specify a **Name** for the key and click **Create**. The newly created key will appear in the keys list.

Alternatively, encryption keys for CTE can be created on the **Keys** page of the **Keys & Access Management** application. Refer to ["Creating a New Key" on page 122](#) for details.

- b. Select the desired key.

NOTE The CTE keys must be:

- > AES128, AES-256, ARIA-128, or ARIA-256
- > Shared with the CTE Clients group
- > Set as exportable

Only the clients that support the CBC CS1 encryption mode can have GuardPoints that use a policy with a CBC CS1 key.

- c. Click **Select**. The selected key appears in the Key Name / Current Key Name field.

The next two steps are specific to LDT policies.

4. (Applicable to LDT policies) Select a **Transformation Key Name**. This is a mandatory field.

- a. Click **Select** next to the field. The list of available keys is displayed.

Optionally, you can create a new key by clicking **Create a New Key**. Optionally, specify a **Name** for the key and click **Create**. The newly created key will appear in the keys list.

Alternatively, encryption keys for CTE can be created on the **Keys** page of the **Keys & Access Management** application. Refer to ["Creating a New Key" on page 122](#) for details.

- b. Select the desired key.

NOTE The CTE keys must be:

- > AES128, AES-256, ARIA-128, or ARIA-256
- > Shared with the CTE Clients group
- > Set as exportable

Only the clients that support the CBC CS1 encryption mode can have GuardPoints that use a policy with a CBC CS1 key.

- c. Click **Select**. The selected key appears in the Transformation Key Name field.

5. Click **Add**. The newly created key rule appears in the list of key rules.

Similarly, you can add multiple key rules to the policy by clicking **Create Key Rule**. To delete a key rule, click **Delete** next to the rule.

6. Click **Next**.

- > For Live Data Transformation and Cloud Object Storage policies, the Confirmation screen is displayed. Verify policy details, as described in ["Step 5: Confirm Details" on page 122](#).
- > For Standard policies, the following screen is displayed:

- **Data Transformation:** If you selected the Data Transformation check box on the General Info screen of the Create Policy wizard. Add data transformation rules, as described in ["Step 4: Add Data Transformation Rules"](#) below.
- **Confirmation:** If you cleared the Data Transformation check box. Verify policy details, as described in ["Step 5: Confirm Details"](#) on the next page.

Step 4: Add Data Transformation Rules

This step is applicable to Standard policies if you selected the Data Transformation check box on the General Info screen of the Create Policy wizard.

1. Click **Create Data Transformation Rule**. The Create Data Transformation Rule dialog box is displayed.
2. (Optional) Select a **Resource Set**.
 - a. Click **Select** next to the Resource Set field. The list of available resource sets is displayed.
Optionally, you can add a new resource set by clicking **Create Resource Set**. The newly created resource set will appear in the resource sets list.
 - b. Select a resource set.
 - c. Click **Select**. The selected resource set appears in the Resource Set field.
3. Select the **Transformation Key Name**. This is a mandatory field.
 - a. Click **Select** next to the Transformation Key Name field. The list of available keys is displayed.
Optionally, you can create a new key by clicking **Create a New Key**. Optionally, specify a **Name** for the key and click **Create**. The newly created key will appear in the keys list.
Alternatively, encryption keys for CTE can be created on the **Keys** page of the **Keys & Access Management** application. Refer to ["Creating a New Key"](#) on the next page for details.
 - b. Select the desired key.

NOTE The CTE keys must be:

- > AES128, AES-256, ARIA-128, or ARIA-256
 - > Shared with the CTE Clients group
 - > Set as exportable

Only the clients that support the CBC CS1 encryption mode can have GuardPoints that use a policy with a CBC CS1 key.
- c. Click **Select**. The selected key appears in the Transformation Key field.
4. Click **Add**. The newly created data transformation rule appears in the list of rules.
Similarly, you can add multiple rules to the policy by clicking **Create Data Transformation Rule**. To delete a rule, click **Delete** next to the rule.
5. Click **Next**. The Confirmation screen is displayed.

Step 5: Confirm Details

1. Verify the policy details. The Confirmation screen displays general information about the policy and details of the security and key rules added to the policy.

If the details are incorrect or you want to modify them, click **Back** and update the details.

Sample confirmation

2. Click **Save**.

The newly created policy appears in the policies list on the Policies page. Similarly, add as many policies as required. A sample list of policies is shown below:

	Name	Type	Version	Updated At	Description	
☐	testcospic	Cloud Object Storage	1	18 Aug 2020, 17:35	Test COS policy	...
☐	ldtpic	Live Data Transformation	1	18 Aug 2020, 17:32		...
☐	testpolicy	Standard	1	18 Aug 2020, 17:30		...

Creating a New Key

When creating a key rule for a policy, you can either select an existing key or create a new key. The list of available keys is displayed on the Select Key dialog box. The new keys that you create on this dialog box appear under the keys list.

Alternatively, encryption keys for CTE can be created on the **Keys** page of the **Keys & Access Management** application, as described below.

NOTE The CTE keys must be:

- > AES128, AES-256, ARIA-128, or ARIA-256
- > Shared with the CTE Clients group
- > Set as exportable

Only the clients that support the CBC CS1 encryption mode can have GuardPoints that use a policy with a CBC CS1 key.

To create a new key:

1. Open the **Keys & Access Management** application.
2. On the Keys page, click **Create a New Key**.
3. Specify the **Key Name**.
4. Select the **Algorithm** from the drop-down list. The default algorithm is AES. CTE supports AES and ARIA algorithms.
5. Select the key **Size** from the drop-down list. The default size is 256.

6. Under the **Key Metadata** section, type **CTE** in the **Groups for Key sharing** box to filter the groups. The CTE Admins and CTE Users groups are displayed.

Groups for Key sharing

Group Names	Key Shared?	
CTE Admins	☐	<button>Add</button>
CTE Clients	☐	<button>Add</button>

7. Click **Add** next to the **CTE Clients** group.
8. Select the **CTE Key Properties** check box. The following fields appear:

☒ CTE Key Properties

☒ CTE Versioned ☐ Persistent on Client

Encryption Mode

- **CTE Versioned:** Specify whether the key is versioned. By default, the key is set as versioned.
 - For Standard and COS policies, clear the **CTE Versioned** check box. This makes sure that the is displayed in the keys list when you add the key rule to the policy.
 - For LDT policies, make sure that the **CTE Versioned** check box is selected.
- **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.
 - When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.
 - When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.
- **Encryption Mode:** Encryption mode of the key. The options are:
 - CBC
 - CBC CS1
 - XTS

Encryption using the XTS and CBC CS1 keys is known as enhanced encryption. Refer to the CTE Agent Advanced Configuration and Integration Guide specific to your platform for details.

9. Scroll down to the **Key Behaviors** section.
10. Clear **Prevent this key from being exported**. This makes sure that the is displayed in the keys list when you add the key rule to the policy.

Key Behaviors

☒ Prevent this key from being deleted ☐ Prevent this key from being exported

11. Click **Create**.

The newly created key appears in the keys list.

NOTE

- > Only CTE Administrators (users of the CTE Admins group) can delete the CTE keys.
- > An in-use CTE key cannot be deleted. Before you delete a CTE key, make sure that no security rule is using the key.

Displaying Policies

The Policies page shows the list of configured policies with their details such as names, types, and versions. You can view the version history of policies from the Policies page. Additionally, you can delete policies from this page. In the detail view, you can view types of rules linked with the policies.

Name	Type	Version	Updated At: ↓	Description	
☐ testcospic	Cloud Object Storage	0	18 Aug 2020, 17:35	Test COS policy	---
☐ ldtplc	Live Data Transformation	0	18 Aug 2020, 17:32		---
☐ testpolicy	Standard	0	18 Aug 2020, 17:30		---

This section covers the following information:

- > ["Viewing Policies" below](#)
- > ["Viewing Details of Policies" on the next page](#)
- > ["Viewing Policy Version History" on page 127](#)

Viewing Policies

To view the complete list of configured policies:

1. Open the **CTE** application.
2. Click **Policies**. The Policies page shows the following details:

Column	Description
Name	Unique name of the policy.

Column	Description
Type	Type of the policy can be: > STANDARD > LDT > CLOUD OBJECT STORAGE
Version	Version of the policy. Click to view the version history of the policy. Refer to " Viewing Policy Version History " on page 127 for details.
Updated At	Time when the policy is created or updated.
Description	Optional description of the policy.

By default, the policies are displayed in descending order by Updated At. By default, 10 records per page are displayed. Adjust pagination and/or the number of records to display per page to view more records.

To add a new policy, click **Create Policy**. Refer to "[Creating Policies](#)" on page 114 for details.

Viewing Details of Policies

To view the details of a policy:

1. Open the **CTE** application.
2. Click **Policies**. The list of configured policies is displayed.
3. Under **Name**, click the desired policy. The rules linked with the policy are displayed on the following tabs:
 - Security Rules
 - Key Rules
 - Data Transformation Rules (Applicable to Standard policies that contain data transformation rules)

NOTE If a policy is in Learn Mode, a warning banner stating the following is displayed at the top of the page:

Warning: This Policy is in Learn Mode

To disable the Learn Mode, turn off the **Learn Mode** toggle on the right.

4. Click the **Security Rules** tab. This tab displays the following details:

Column	Description
Order	Sequence to enforce security rules. Rules higher in the order take higher priority.
Resource Set	(Not applicable to Cloud Object Storage policies) Resource set linked with the rule.
User Set	User set linked with the rule.

Column	Description
Process Set	Process set linked with the rule.
Action	Action applied to the rule. Refer to "Actions" on page 27 for the complete list of supported actions.
Effect	Effect applied to the rule.
Browsing	Whether browsing of directories under the GuardPoint down to the resources in the rule is allowed. For Cloud Object Storage policies, No is displayed.

To add a new security rule, refer to ["Step 2: Add Security Rules" on page 117](#) for details.

- Click the **Key Rules** tab. This tab displays the following details:

NOTE For Cloud Object Storage policies, only **Key Id** is displayed.

Column	Description
Order	Sequence to enforce key rules. Rules higher in the order take higher priority.
Resource Set	Resource set linked with the key rule.
Key Name / Current Key Name	Encryption key currently applied to the resource. For LDT and Data Transformation policies, the name is Current Key Name.
Transformation Key Name	(Applicable to LDT policies) Encryption key to perform data transformation for LDT policies.
Exclusion Rule	(Applicable to LDT policies) Whether to exclude the resource set from the policy.

To add a new security rule, refer to ["Step 3: Add Key Rules" on page 119](#) for details.

- Click the **Data Transformation Rules** tab. This tab is displayed if the policy contains data transformation rules. This tab displays the following details:

Column	Description
Order	Sequence to enforce key rules. Rules higher in the order take higher priority.
Resource Set	Resource linked with the key rule.
Transformation Key Name	Transformation key to use for rekeying.

To add a new data transformation rule, refer to ["Step 4: Add Data Transformation Rules" on page 121](#) for details.

Viewing Policy Version History

The policy version defines the number of times a policy has been changed. This number indicates the current revision only. It cannot be used to roll back to a previous version. Restore a backup to revert to a previous online policy version. The version count starts at zero when the policy is initially created and increments by one each time it is saved thereafter.

Policy Version History

Version	Date	Author	Comment
4	07/28/20	admin	Delete LDT Key Rule
2	07/28/20	admin	LDT Key Rule Created
2	07/28/20	admin	Dataform Rule Created
1	07/28/20	admin	Key Rule Created
0	07/28/20	admin	Policy Created
0	07/28/20	admin	LDT Key Rule Created
0	07/28/20	admin	Dataform Rule Created
0	07/28/20	admin	Key Rule Created
0	07/28/20	admin	Security Rule Created

9 Policy Audit Records 10 per page +

To view the version history of a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the version number of the policy. The Policy Version History popup displays the following details:

Field	Description
Version	Version of the policy.
Date	Date when the version is created.
Author	User who changed the policy.
Comment	Description of change.

4. Click **OK**.

Modifying Policies and Rules

On the Policies page, you can update the description of policies and delete policies that are no longer needed. Additionally, you can modify the key and security rules linked to the policy. Information in this section is divided into the following topics:

- > ["Updating Policy Description" on the next page](#)

- > "Cloning a Policy" below
- > "Adding New Security Rules" on the next page
- > "Adding New Key Rules" on the next page
- > "Adding New Data Transformation Rules" on page 130
- > "Modifying Security Rules" on page 130
- > "Modifying Key Rules" on page 131
- > "Modifying Data Transformation Rules" on page 133
- > "Deleting Policies" on page 134

Updating Policy Description

To update the description of a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the overflow icon () corresponding to the desired policy.
4. Click **Edit**.
5. Add or modify the **Description**. The policy Name and Type cannot be modified.
6. Click **Update**.

The updated description appears in the policies list.

Cloning a Policy

Cloning is an efficient and simple method to create a copy of an existing policy. The clone is a separate policy and contains all the configurations of its parent policy. When cloning a policy, specify a new unique name for the clone. Also, enable or disable Learn Mode for the clone, if required.

To duplicate a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the overflow icon () corresponding to the desired policy.



4. Click **Clone**.
5. Enter a unique **Name** for the clone.
6. (Optional) Provide a **Description** for the clone.

7. (Optional) Turn on/off the **Learn Mode** toggle. Refer to ["Learn Mode" on page 31](#) for details.

Duplicating policy ldtpic

Name *

clone-pic

Description

A copy of ldtpic

Learn Mode: ☐

The clone with the specified name appears at the top of the policies list.

	Name	Type	Version	Updated At	Description	
☐	clone-pic	Live Data Transformation	1	18 Aug 2020, 20:12	A copy of ldtpic	⋮

Adding New Security Rules

To add a new security rule to a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. On the **Security Rules** tab, click **Add Security Rule**. The Add Security Rule dialog box is displayed.
5. Specify the required details. The fields on the Add Security Rule dialog box are same as the fields on the Create Security Rule dialog box. Refer to ["Step 2: Add Security Rules" on page 117](#) for details.
6. Click **Add**.

The newly added security rule appears in the security rules list. Similarly, you can add more security rules to the policy.

Adding New Key Rules

To add a new key rule to a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Key Rules** tab.
5. Click **Add Key Rule**.
6. Specify the required details. The fields on the Add Key Rule dialog box are same as the fields on the Create Key Rule dialog box. Refer to ["Step 3: Add Key Rules" on page 119](#) for details.
7. Click **Add**.

The newly added key rule appears in the key rules list. Similarly, you can add more key rules to the policy.

Adding New Data Transformation Rules

To add a new data transformation rule to a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Data Transformation Rules** tab.
5. Click **Add Data Transformation Rule**. The Add Data Transformation Rule dialog box is displayed.
6. Specify the required details. The fields on the Add Data Transformation Rule dialog box are same as the fields on the Create Data Transformation Rule dialog box. Refer to ["Step 4: Add Data Transformation Rules" on page 121](#) for details.
7. Click **Add**.

The newly added data transformation rule appears in the data transformation rules list. Similarly, you can add more rules to the policy.

Modifying Security Rules

- > ["Editing Security Rules" below](#)
- > ["Changing Order of Security Rules" below](#)
- > ["Deleting Security Rules" on the next page](#)

Editing Security Rules

To edit a security rule in a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Security Rules** tab.
5. Click the overflow icon () corresponding to the desired rule.
6. Click **Edit**. The Edit Security Rule dialog box is displayed.
7. Change the required fields. The fields on the Edit Security Rule dialog box are the same the fields on the Create Security Rule dialog box. Refer to ["Step 2: Add Security Rules" on page 117](#) for details.
8. Click **Update**.

The updated details appear in the security rules list.

Changing Order of Security Rules

To change the order of a security key rule in a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.

3. Click the desired policy.
4. Click the **Security Rules** tab.
5. Select the desired rule. Depending on the current order, the following ordering icons are activated.

Icon	Description
Bottom (⇓)	Move the rule to the bottom. Unavailable for the rule at the bottom.
Down (↓)	Move the rule one place lower. Unavailable for the rule at the bottom.
Up (↑)	Move the rule one place higher. Unavailable for the rule at the top.
Top (⇑)	Move the rule to the top. Unavailable for the rule at the top.

6. Click the desired icon.

The rules list shows the updated order.

Deleting Security Rules

To delete security rules from a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Security Rules** tab.
5. Select the check boxes corresponding to the desired rules.

To select all rules visible on the page for deletion, select the top check box to the left of the Order heading.

6. Click the delete icon (■).

The selected rules are removed from the security rules list.

Modifying Key Rules

Modifying key rules linked with a policy involves:

- > ["Editing Key Rules" below](#)
- > ["Changing Order of Key Rules" on the next page](#)
- > ["Deleting Key Rules" on the next page](#)

Editing Key Rules

To edit a key rule in a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Key Rules** tab.

5. Click the overflow icon () corresponding to the desired rule.
6. Click **Edit**. The Edit Key Rule dialog box is displayed.
7. Change the required fields. The fields on the Edit Key Rule dialog box are the same the fields on the Create Key Rule dialog box. Refer to ["Step 3: Add Key Rules" on page 119](#) for details.
8. Click **Update**.

The updated details appear in the key rules list.

Changing Order of Key Rules

To change the order of a key rule in a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Key Rules** tab.
5. Select the desired rule. Depending on the current order, the following ordering icons are activated.

Icon	Description
Bottom ()	Move the rule to the bottom. Unavailable for the rule at the bottom.
Down ()	Move the rule one place lower. Unavailable for the rule at the bottom.
Up ()	Move the rule one place higher. Unavailable for the rule at the top.
Top ()	Move the rule to the top. Unavailable for the rule at the top.

6. Click the desired icon.

The key rules list shows the updated order.

Deleting Key Rules

To delete key rules from a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Key Rules** tab.
5. Select the check boxes corresponding to the desired rules.

To select all rules visible on the page for deletion, select the top check box to the left of the Order heading.

6. Click the delete icon ()

The selected rules are removed from the key rules list.

Modifying Data Transformation Rules

Modifying data transformation rules linked with a policy involves:

- > ["Editing Data Transformation Rules" below](#)
- > ["Changing Order of Data Transformation Rules" below](#)
- > ["Deleting Data Transformation Rules" on the next page](#)

Editing Data Transformation Rules

To edit a data transformation rule in a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Data Transformation Rules** tab.
5. Click the overflow icon () corresponding to the desired rule.
6. Click **Edit**. The Edit Data Transformation Rule dialog box is displayed.
7. Change the required fields. The fields on the Edit Data Transformation Rule dialog box are the same the fields on the Create Data Transformation Rule dialog box. Refer to ["Step 4: Add Data Transformation Rules" on page 121](#) for details.
8. Click **Update**.

The updated details appear in the data transformation rules list.

Changing Order of Data Transformation Rules

To change the order of a data transformation rule in a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Data Transformation Rules** tab.
5. Select the desired rule. Depending on the current order, the following ordering icons are activated.

Icon	Description
Bottom ()	Move the rule to the bottom. Unavailable for the rule at the bottom.
Down ()	Move the rule one place lower. Unavailable for the rule at the bottom.
Up ()	Move the rule one place higher. Unavailable for the rule at the top.
Top ()	Move the rule to the top. Unavailable for the rule at the top.

6. Click the desired icon.

The rules list shows the updated order.

Deleting Data Transformation Rules

To delete data transformation rules from a policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Data Transformation Rules** tab.
5. Select the check boxes corresponding to the desired rules.

To select all rules visible on the page for deletion, select the top check box to the left of the Order heading.

6. Click the delete icon ().

The selected rules are removed from the data transformation rules list.

Deleting Policies

CipherTrust Manager provides options to delete single or multiple policies.

Deleting Single Policies

To delete a single policy:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Click the overflow icon () corresponding to the desired policy.
4. Click **Delete**.

The selected policy is removed from the policies list.

Deleting Multiple Policies

To delete single or multiple policies:

1. Open the **CTE** application.
2. In the left pane, click **Policies**.
3. Select the check boxes corresponding to the desired policies.

To select all policies visible on the page for deletion, select the top check box corresponding to the left of the Name heading.

4. Click the delete icon ().

The selected policies are removed from the policies list.

CHAPTER 9: Managing GuardPoints

A GuardPoint specifies the list of folders that contains paths to be protected. Access to files and encryption of files under the GuardPoint is controlled by security policies.

This chapter contains the following sections:

- > ["Overview" below](#)
- > ["Secure Start GuardPoints" on the next page](#)
- > ["Considerations Before Creating GuardPoints" on the next page](#)
- > ["Creating Standard GuardPoints on Clients" on page 138](#)
- > ["Creating LDT GuardPoints on Clients" on page 140](#)
- > ["Creating Cloud Object Storage GuardPoints on Clients" on page 143](#)
- > ["Enabling Secure Start for GuardPoints" on page 144](#)
- > ["Creating GuardPoints on Client Groups" on page 145](#)
- > ["Automatic and Manual GuardPoints" on page 151](#)
- > ["Viewing GuardPoints" on page 154](#)
- > ["Viewing GuardPoint Status" on page 155](#)
- > ["Configuring Windows Network Drives" on page 156](#)
- > ["Deleting GuardPoints" on page 157](#)

Overview

Before you apply GuardPoints:

- > A CTE Agent must be installed on the client system and registered with CipherTrust Manager. Refer to the CTE Agent Quick Start Guide specific to your platform for details.
- > A client must be added to the CipherTrust Manager. The client is automatically added to the CipherTrust Manager on successful registration with the CipherTrust Manager.
- > Policies must be created using the encryption keys on the CipherTrust Manager. This involves creation of policy elements and encryption keys. Refer to ["Managing Policies" on page 101](#) for details.
- > A GuardPoint must be created. No one must be using the directory to be guarded before making it a GuardPoint.

If users are working on the directory when it is made a GuardPoint, they can continue to use data in memory rather than use the actual data in the GuardPoint. Inform users to:

- > Save their work
- > Close applications that are running on the directory
- > Exit the directory before applying the GuardPoint

When the users re-enter the directory, they will use protected data and the CTE Agent will work appropriately.

Secure Start GuardPoints

NOTE The Secure Start feature is supported on Windows clients.

Secure Start offers a new type of GuardPoint that offers data protection for applications that start earlier in the boot sequence than VMD (CTE Agent daemon). For example, an AD (Active Directory) or a SQL Server service starts very early. A Secure Start GuardPoint starts before the AD and SQL services, and can, therefore, encrypt those services.

For more information on protecting such applications using Secure Start, refer to the CTE Agent for Windows Advanced Configuration and Integration Guide. To determine whether other applications qualify for Secure Start, contact Thales Customer Support.

Considerations Before Creating GuardPoints

- > If a client is to be added to a client group, do not apply a GuardPoint at the client level, rather, apply the GuardPoint at the client group level. You can do both, but it is harder to keep track of GuardPoints applied at the client group level and custom GuardPoints applied at the client level.
- > Certain directories are protected against guarding. So plan your GuardPoints accordingly:

Windows Platforms

- The following folders cannot be guarded because a GuardPoint cannot be applied to a folder that contains open files.
 - The top-level "Program Data" folder on Windows Vista and Windows 2008
 - The top-level "Documents and Settings" folder on all other Windows platforms
 - The "Users" folder
- The CTE Agent opens and continually maintains log files in subfolders under "ProgramData" and "Documents and Settings". Other subfolders below these folders can be guarded as long as no files are open in any subfolder at the time the GuardPoint is applied.
- Be especially careful when specifying paths for Windows agents. Cross-guarding the same folder with different policies and encryption keys returns unexpected results and corrupts the files in that folder.
- GuardPoint paths must use standard Windows path notation and delimiters.
 - Incorrect notation and delimiters are ignored and discarded by the Windows agent. Therefore, it is possible to enter two paths that resolve to the same Windows folder and successfully guard both of them. The CipherTrust Manager reports that it is guarding two unique folders when, in fact, it is guarding the same folder twice.
 - Do not use any of the following characters as path delimiters: | ? < > : * " / ,
For example, both `C : \gp\` and `C : \gp\/` are allowed by the CipherTrust Manager. When the second GuardPoint is applied, the extraneous "/" is discarded by the Windows CTE Agent and the Windows CTE Agent applies a GuardPoint to `C : \gp\` a second time.

Linux Platforms

- The following directories cannot be guarded:
 - `<secfs install root>/agent/secfs/`
 - `<install root>/agent/secfs/bin` and everything under it
 - `<secfs install root>/agent/vmd` and everything under it
 - `/etc/vormetric` and everything under it
 - `/etc`
 - `/etc/pam.d` and everything under it
 - `/etc/security` and everything under it
 - `/usr`
 - `/usr/lib`
 - `/usr/lib/pam`
 - `/usr/lib/security` and everything under it
 - `/etc/rc*` and everything under it
 - `/var/log/vormetric`
- You cannot apply CTE Agent protection to already mounted and guarded directories, nor can you nest GuardPoints.
 - The `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec` directory is automatically mounted and guarded by `secfs` when the CTE Agent process starts on the client.
 - You cannot apply a GuardPoint to `/opt` because it contains the existing GuardPoint, `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec`; however, you can guard a directory like `/opt/myapps` because it is in a different hierarchy and has no impact on `/opt/vormetric`.
 - Mounted and guarded directories can be displayed using the `df` command.
- > Both CipherTrust Manager and CTE support a new enhanced encryption mode (CBC-CS1). If your client groups contain clients with older versions of CTE, you cannot apply policies containing keys that use this new encryption mode. The action fails with an error message informing you that all clients in the client group do not support the key's encryption mode. Refer to the CTE Agent Advanced Configuration and Integration Guide specific to your platform for details.

When Changing a Policy or Rekeying a GuardPoint

- > To change a policy or rekey a GuardPoint, be prepared to temporarily stop access to the GuardPoint. Changing policies for a GuardPoint requires an interruption of service because the transition process entails disabling one policy and then enabling another policy. The GuardPoint must be inactive during the transition period to ensure GuardPoint integrity. The same rule applies to moving a client between client groups when it includes a change in policies. Coordinate policy changes during a maintenance outage window.
- > If LDT is enabled on your clients, encryption and rekeying of GuardPoint data is done without blocking user or application access to the data. LDT is a separately licensed feature, refer to ["Enabling Live Data Transformation" on page 57](#).

Creating Standard GuardPoints on Clients

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

To create a GuardPoint:

1. Open the **CTE** application.
2. Click **Clients > Clients**. The list of registered clients is displayed.
3. Under **Client Name**, click the client on which you want to create a GuardPoint.
4. On the **GuardPoints** tab, click **Create GuardPoint**.
5. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field.
 - b. Select a *Standard* policy. If no policy exists, create one, as described in ["Creating Policies" on page 114](#).

Name	Type	Version
☐ testcosplc	Cloud Object Storage	0
☒ testpolicy	Standard	1
☐ ldtplc	Live Data Transformation	0

- c. Click **Select**.
6. Select the **Type** of device to protect. This is a mandatory field. Depending on the platform, the options for the standard policy are:

Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system directories to be guarded manually.
Auto Raw or Block Device	Yes	Yes	Select for standard policies for raw (block) devices.
Manual Raw or Block Device	No	Yes	Select for standard policies for raw (block) devices to be guarded manually.

NOTE Manual Directory and Manual Raw or Block Device are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd -unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

7. Specify the **Path** to be protected. This is a mandatory field.

- Click **Browse** to select a path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify the path.
- Alternatively, if you know the path, manually enter full paths of one or more directories. Enter one path per line.

NOTE

- > If a manually entered path does not exist yet, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.
- > See ["Considerations Before Creating GuardPoints" on page 136](#) for what to be aware of before creating a GuardPoint.
- > If multiple paths are specified, they will all be protected by the same policy.

8. (Optional, Linux only) Select **Auto Mount** to specify an automount path. For a regular (non-auto) mount path, make sure that the check box is clear.

The screenshot shows the 'Create GuardPoint' dialog box. It has a title bar with a close button (X). The dialog contains three main sections: 'Policy' with a text field containing 'testpolicy' and a 'Select' button; 'Type' with a dropdown menu showing 'Auto Directory'; and 'Path' with a text area containing '/opt/cie-test/Files' and a 'Browse' button. At the bottom, there is an 'Auto Mount' checkbox which is checked.

9. (Optional, Windows only) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in ["Enabling Secure Start for GuardPoints" on page 144](#).

10. Click **Create**. A message appears prompting to confirm the reuse the GuardPoint settings on another path.

- Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:
 - i. Specify a new **Path**.
 - ii. Click **Add Path**.
 - iii. Click **OK**.
- Click **No** if you do not want to use the same settings on another path.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to ["GuardPoint Status Information" on the next page](#) for details.

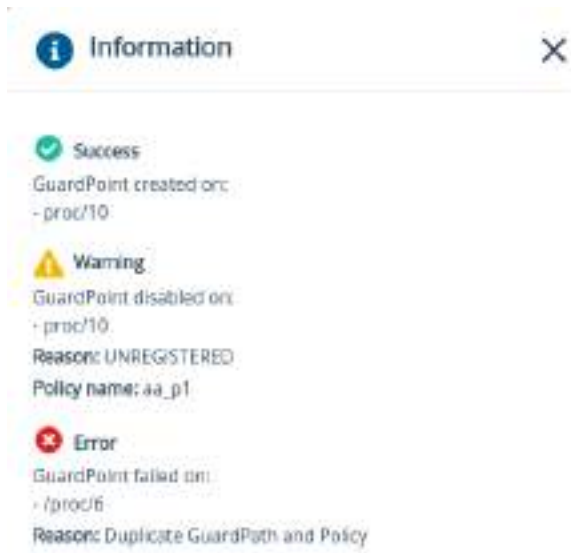
The newly created GuardPoint appears on the GuardPoints tab. The status remains `Unknown` until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon (↻) to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to "[Viewing GuardPoint Status](#)" on page 155 for details.

GuardPoint Status Information

> When you add multiple paths to a GuardPoint:

- If GuardPoint is created successfully for all paths, a message is displayed at the top right corner of the screen.
- If GuardPoint is disabled or failed for at least one of the paths (for example, when a path is already guarded), a warning message similar to the following appears:



> When you add only one path, and the GuardPoint for that path fails, then an error message is displayed stating the reason of failure.

Creating LDT GuardPoints on Clients

To create an LDT GuardPoint on a client:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the LDT client on which you want to create a GuardPoint.
4. On the **GuardPoints** tab, click **Create GuardPoint**.
5. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field. The Select Policy dialog box is displayed.
 - b. Select a *Live Data Transformation* policy. If no policy exists, create one, as described in "[Creating Policies](#)" on page 114.

Name	Type	Version
☐ testcospic	Cloud Object Storage	0
☐ testpolicy	Standard	1
☒ ldtpic	Live Data Transformation	0

c. Click **Select**.

6. Select the **Type** of device to protect. This is a mandatory field. Depending on the platform, the options for an *LDT* policy are:

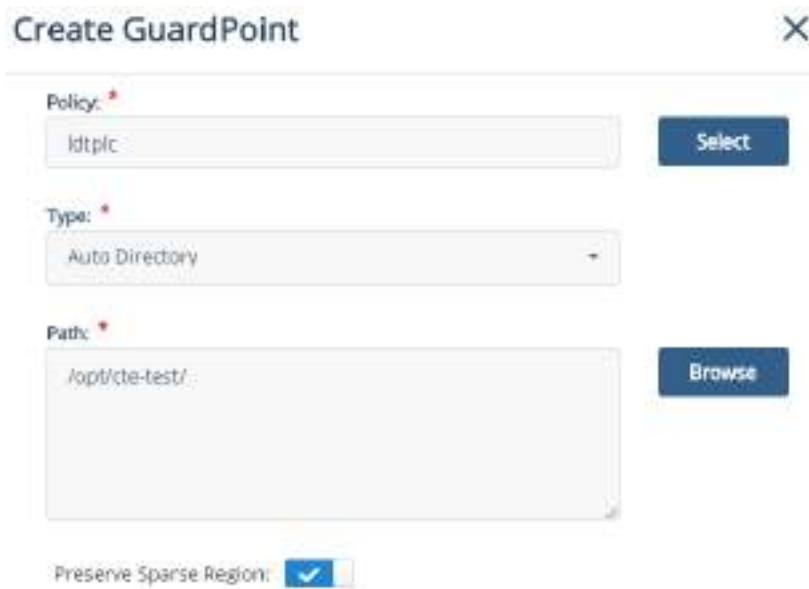
Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system directories to be guarded manually.

NOTE Manual Directory is guarded and unguarded (for example, `mounted` and `unmounted`) by running the `secfsd -guard` and `secfsd-unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

7. Specify the **Path** to be protected. This is a mandatory field.
- Click **Browse** to select a path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify the path.
 - Alternatively, if you know the path, manually enter full paths of one or more directories. Enter one path per line.

NOTE

- > If a manually entered path does not exist yet, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.
- > See "[Considerations Before Creating GuardPoints](#)" on page 136 for what to be aware of before creating a GuardPoint.
- > If multiple paths are specified, they will all be protected by the same policy.



8. Configure the **Preserve Sparse Region** toggle. The toggle is turned on by default.

CAUTION! If you turn off the **Preserve Sparse Region** toggle, you are prompted to confirm the action. This is an irreversible action.

9. (Optional, Windows only) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in ["Enabling Secure Start for GuardPoints" on page 144](#).

10. Click **Create**. A message appears prompting to confirm the reuse the GuardPoint settings on another path.

- Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:
 - i. Specify a new **Path**.
 - ii. Click **Add Path**.
 - iii. Click **OK**.
- Click **No** if you do not want to use the same settings on another path.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to ["GuardPoint Status Information" on page 140](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon (↻) to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to ["Viewing GuardPoint Status" on page 155](#) for details.

An LDT GuardPoint is applied automatically according to the QoS settings configured in the linked profile. Refer to ["Creating a Profile" on page 42](#) and ["Setting Quality of Service Configuration" on page 50](#).

Creating Cloud Object Storage GuardPoints on Clients

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

To create a Cloud Object Storage GuardPoint:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the client on which you want to create a GuardPoint.
4. On the **GuardPoints** tab, click **Create GuardPoint**.
5. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field. The Select Policy dialog box is displayed.
 - b. Select a *Cloud Object Storage* policy. If no policy exists, create one, as described in "[Creating Policies](#)" on page 114.

Name	Type	Version
☒ testcoospic	Cloud Object Storage	0
☐ testpolicy	Standard	1
☐ idtpic	Live Data Transformation	0

- c. Click **Select**.
6. Select the **Type** of device to protect. This is a mandatory field. The options are:
 - **Auto Cloud Storage**: Select for Cloud Storage policies.
 - **Manual Cloud Storage**: Select for Cloud Storage policies to be guarded manually.

NOTE Manual Cloud Storage are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd-unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

7. Select the **Cloud Storage Type**. The available option is **Amazon S3 Bucket**.
8. Specify the **URL** of the S3 bucket to be protected. The URL format is `http://s3.amazonaws.com/[bucket_name]`.

9. Click **Validate** to check whether the S3 bucket exists. The Create GuardPoint - Validate Connection dialog box is displayed.
 - a. Enter your AWS account credentials:
 - **Access Key**: Key to access the bucket.
 - **Secret Key**: Secret key to access the bucket.
 - **Region Code**: Code of your AWS region.
 - **URL**: S3 bucket URL that you entered (populated automatically).
 - b. Click **Connect**.
 - c. Click **OK**.

10. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to "[GuardPoint Status Information](#)" on page 140 for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains `Unknown` until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon (↻) to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to "[Viewing GuardPoint Status](#)" on page 155 for details.

Enabling Secure Start for GuardPoints

NOTE Information in this section is applicable to Windows clients.

Access to a Secure Start GuardPoint is permitted only during the boot sequence and for a short period. After the VMD is up and running, it performs normal agent initialization and communicates with the CipherTrust Manager to access files within a GuardPoint location.

A CipherTrust Manager administrator can enable Secure Start either when creating a GuardPoint or later by modifying the GuardPoint.

To enable Secure Start for a GuardPoint:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired Windows.
4. Click the **GuardPoints** tab.
5. Click the overflow icon () corresponding to the desired GuardPoint.
6. Click **View/Edit**. The Edit GuardPoint dialog box is displayed. In the edit mode, you can enable or disable the Secure Start and Preserve Sparse Region toggles.
7. Turn on the **Secure Start** toggle. By default, the toggle is off.



8. Click **Save**.

Refer to the CTE Agent for Windows Advanced Configuration and Integration Guide for details about using the Secure Start feature.

NOTE To disable Secure Start for a GuardPoint, clear the **Secure Start** check box in the Edit GuardPoint dialog box.

Creating GuardPoints on Client Groups

GuardPoints created on a client group are applied to all members of the group. Additionally, you can apply client group configuration settings (except the password, Agent Lock, System Lock, and Communication Enabled settings) to all clients in a client group. It is important to keep this in mind when adding clients to a client group.

For example, if you create a Linux file system GuardPoint on a client group, and then you add a Windows client to that client group, the Windows client will not be protected by that GuardPoint.

If you create a client group and add a non-LDT client to the group but you create LDT GuardPoints on the client group, then those GuardPoints are not propagated to the non-LDT client. However, if you subsequently enable LDT on the client in that group (assuming you have a license for this feature), the LDT GuardPoint is now propagated to the client.

This section covers the following information:

- > ["Create Standard GuardPoints on Client Groups" on the next page](#)
- > ["Creating LDT GuardPoints on Client Groups" on page 148](#)
- > ["Creating Cloud Object Storage GuardPoints on Client Groups" on page 150](#)

Create Standard GuardPoints on Client Groups

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups. Client group GuardPoints apply to all clients in the group.

To create a standard GuardPoint:

1. Open the **CTE** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the client group on which you want to create a GuardPoint.
4. On the **GuardPoints** tab, click **Create GuardPoint**.
5. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field.
 - b. Select a *Standard* policy. If no policy exists, create one, as described in ["Creating Policies" on page 114](#).

Name	Type	Version
☐ testcosplc	Cloud Object Storage	0
☒ testpolicy	Standard	1
☐ ldtplc	Live Data Transformation	0

- c. Click **Select**.
6. Select the **Type** of device to protect. This is a mandatory field. Depending on the platform, the options for the standard policy are:

Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system directories to be guarded manually.
Auto Raw or Block Device	Yes	Yes	Select for standard policies for raw (block) devices.
Manual Raw or Block Device	No	Yes	Select for standard policies for raw (block) devices to be guarded manually.

NOTE Manual Directory and Manual Raw or Block Device are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd -unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

7. Specify the **Path** to be protected. This is a mandatory field.

- Click **Browse** to select a path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify the path.
- Alternatively, if you know the path, manually enter full paths of one or more directories. Enter one path per line.

NOTE

- > If a manually entered path does not exist yet, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.
- > See ["Considerations Before Creating GuardPoints" on page 136](#) for what to be aware of before creating a GuardPoint.
- > If multiple paths are specified, they will all be protected by the same policy.

8. (Optional, Linux only) Select **Auto Mount** to specify an automount path. For a regular (non-auto) mount path, make sure that the check box is clear.

The screenshot shows the 'Create GuardPoint' dialog box. It has a title bar with a close button (X). The dialog contains three main sections: 'Policy:' with a text field containing 'testpolicy' and a 'Select' button; 'Type:' with a dropdown menu showing 'Auto Directory'; and 'Path:' with a large text area containing '/opt/cie-test/Files' and a 'Browse' button. At the bottom, there is an 'Auto Mount:' checkbox which is checked.

9. (Optional, Windows only) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in ["Enabling Secure Start for GuardPoints" on page 144](#).

10. Click **Create**. A message appears prompting to confirm the reuse the GuardPoint settings on another path.

- Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:
 - i. Specify a new **Path**.
 - ii. Click **Add Path**.
 - iii. Click **OK**.
- Click **No** if you do not want to use the same settings on another path.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to ["GuardPoint Status Information" on page 140](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains `Unknown` until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon (↻) to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to ["Viewing GuardPoint Status" on page 155](#) for details.

Creating LDT GuardPoints on Client Groups

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups. Client group GuardPoints apply to all clients in the group.

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Group Name**, click the LDT client group on which you want to create a GuardPoint.
4. On the **GuardPoints** tab, click **Create GuardPoint**.
5. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field. The Select Policy dialog box is displayed.
 - b. Select a *Live Data Transformation* policy. If no policy exists, create one, as described in ["Creating Policies" on page 114](#).

Name	Type	Version
☐ testosplc	Cloud Object Storage	0
☐ testpolicy	Standard	1
☒ ldtplc	Live Data Transformation	0

- c. Click **Select**.
6. Select the **Type** of device to protect. This is a mandatory field. Depending on the platform, the options for an *LDT* policy are:

Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system directories to be guarded manually.

NOTE Manual Directory is guarded and unguarded (for example, `mounted` and `unmounted`) by running the `secfsd -guard` and `secfsd-unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

7. Specify the **Path** to be protected. This is a mandatory field.

- Click **Browse** to select a path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify the path.
- Alternatively, if you know the path, manually enter full paths of one or more directories. Enter one path per line.

NOTE

- > If a manually entered path does not exist yet, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.
- > See ["Considerations Before Creating GuardPoints" on page 136](#) for what to be aware of before creating a GuardPoint.
- > If multiple paths are specified, they will all be protected by the same policy.

Create GuardPoint

Policy:

Type:

Path:

Preserve Sparse Region: ☒

8. Configure the **Preserve Sparse Region** toggle. The toggle is turned on by default.

CAUTION! If you turn off the **Preserve Sparse Region** toggle, you are prompted to confirm the action. This is an irreversible action.

9. (Optional, Windows only) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in ["Enabling Secure Start for GuardPoints" on page 144](#).

10. Click **Create**. A message appears prompting to confirm the reuse the GuardPoint settings on another path.
 - Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:
 - i. Specify a new **Path**.
 - ii. Click **Add Path**.
 - iii. Click **OK**.

- Click **No** if you do not want to use the same settings on another path.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to ["GuardPoint Status Information" on page 140](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains `Unknown` until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon (↻) to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to ["Viewing GuardPoint Status" on page 155](#) for details.

An LDT GuardPoint is applied automatically according to the QoS settings configured in the linked profile. Refer to ["Creating a Profile" on page 42](#) and ["Setting Quality of Service Configuration" on page 50](#).

Creating Cloud Object Storage GuardPoints on Client Groups

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups. Client group GuardPoints apply to all clients in the group.

To create a Cloud Object Storage GuardPoint:

- Open the **CTE** application.
- Click **Clients > Clients**.
- On the **GuardPoints** tab, click **Create GuardPoint**.
- Select a **Policy**. This is a mandatory field.
 - Click **Select** next to the Policy field. The Select Policy dialog box is displayed.
 - Select a *Cloud Object Storage* policy. If no policy exists, create one, as described in ["Creating Policies" on page 114](#).

Name	Type	Version
☒ testcosplc	Cloud Object Storage	0
☐ testpolicy	Standard	1
☐ ldtplc	Live Data Transformation	0

- Click **Select**.
- Select the **Type** of device to protect. This is a mandatory field. The options are:
 - Auto Cloud Storage**: Select for Cloud Storage policies.
 - Manual Cloud Storage**: Select for Cloud Storage policies to be guarded manually.

NOTE Manual Cloud Storage are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd-unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

- Select the **Cloud Storage Type**. The available option is **Amazon S3 Bucket**.

7. Specify the **URL** of the S3 bucket to be protected. The URL format is `http://s3.amazonaws.com/[bucket_name]`.

8. Click **Validate** to check whether the S3 bucket exists. The Create GuardPoint - Validate Connection dialog box is displayed.
- Enter your AWS account credentials:
 - **Access Key**: Key to access the bucket.
 - **Secret Key**: Secret key to access the bucket.
 - **Region Code**: Code of your AWS region.
 - **URL**: S3 bucket URL that you entered (populated automatically).
 - Click **Connect**.
 - Click **OK**.
9. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to ["GuardPoint Status Information" on page 140](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains `Unknown` until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon (🔄) to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to ["Viewing GuardPoint Status" on page 155](#) for details.

Automatic and Manual GuardPoints

The following table lists the type of GuardPoints depending on the platform and type of the policy type:

Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system directories to be guarded manually.
Auto Raw or Block Device	Yes	Yes	Select for standard policies for raw (block) devices.
Manual Raw or Block Device	No	Yes	Select for standard policies for raw (block) devices to be guarded manually.
Auto Cloud Storage	No	Yes	Select for Cloud Storage policies.
Manual Cloud Storage	No	Yes	Select for Cloud Storage policies to be guarded manually.

A GuardPoint is usually applied immediately after it is configured on the CipherTrust Manager GUI; however, it can be applied later on the client system.

When would you want to apply the GuardPoint later? Consider the case of a 2-node cluster configured as active/passive in a cluster environment, such VCS, HACMP, or MSCS. There are two nodes, one which is currently active and the other that is currently inactive. Both nodes are locked.

Apply GuardPoint protection to active nodes only. You should never apply a GuardPoint to a passive node. If the active node develops a problem and tries to switch over to the inactive node, the cluster process fails to switch over because the mirror directory on the inactive node is currently mounted on the active node.

The solution is, for the cluster process to unmount (for example, unguard) the currently active node:

1. Place it in an inactive state.
2. Place the old inactive node in an active state.
3. Mount (for example, guard) the mirror directory on the newly active node.

Generally, when you get error messages, check that only active nodes are properly guarded.

When an auto GuardPoint is applied, regardless of whether it is a file system directory or a raw device, the change is pushed to the client system, and the GuardPoint is applied immediately.

Use the `df` command to display `secfs` mounts (for example, GuardPoints) or `secfsd` to display the GuardPoints themselves. The `secfsd` output shows a guard type of local for directories configured with Directory (Auto Guard).

For example:

```
# df
Filesystem      1K-blocks      Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol100
40123784        11352236        26733380      30% /
/dev/sda1       101086 14590      81277      16% /boot

none          254492 0          254492 0% /dev/shm
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec
40123784        11352236        26733380      30%
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec
/opt/apps/apps1/tmp      40123784      11352236      26733380      30% /opt/apps/apps1/tmp
/opt/apps/apps1/lib      40123784      11352236      26733380      30% /opt/apps/apps1/lib
```

```

/opt/apps/apps1/doc      40123784      11352236      26733380      30% /opt/apps/apps1/doc
# secfsd -status guard
GuardPoint      Policy      Type      ConfigState      Status      Reason
-----
/opt/apps/apps1/tmp allowAllOps_fs      local      guarded guarded N/A
/opt/apps/apps1/lib allowAllRootUsers_fs      local      guarded guarded N/A
/opt/apps/apps1/doc      allowAllOps-winusers1_fs      local      guarded guarded N/A
#

```

When a manual GuardPoint is applied, regardless if it is a file system directory or a raw device, the change is pushed to the client system only. The client is aware of the GuardPoint but the client does not mount it. This is indicated in the `Type` column of the `secfsd -status guard` command output.

For example, the GuardPoint `/opt/apps/apps2/bin` has been configured with Manual Directory, so the guard type is set to `manual`.

```

# secfsd -status guard
GuardPoint      Policy      Type      ConfigState      Status      Reason
-----
/opt/apps/apps1/tmp allowAllOps_fs      local      guarded guarded N/A
/opt/apps/apps1/lib allowAllRootUsers_fs      local      guarded guarded N/A
/opt/apps/apps1/doc      allowAllOps-winusers1_fs      local      guarded guarded N/A
/opt/apps/apps2/bin      HR_policy01      manual      unguarded      not guarded Inactive
#

```

Note the `Type` value. A `Type` of `manual` indicates a manual GuardPoint. A `Type` of `local` indicates an automatic GuardPoint.

A manually applied GuardPoint remains Inactive until the GuardPoint is applied on the client. After the GuardPoint is applied on the client, and the client communicates the change to the server, the status changes to Active. It returns to the Inactive state when the GuardPoint is manually unguarded.

Use the `secfsd` command to guard and unguard Manual GuardPoints. The `secfsd` syntax is:

```

secfsd -guard path
secfsd -unguard path

```

Example

To manually guard and unguard a file system directory:

1. As CipherTrust Manager administrator, configure a GuardPoint with the type `Manual Directory`.
2. Log on to the client as an administrator with root permissions.
3. Wait until the configuration change is downloaded to the Agent system.
4. Run the status command until the manual GuardPoint is displayed.

For example:

```

# secfsd -status guard
GuardPoint      Policy      Type      ConfigState      Status      Reason
-----
/opt/apps/etc      allowAllOps_fs      manual      unguarded      not guarded N/A
/opt/apps/lib/dx3 allowAllOps_fs      local      guarded guarded N/A
#

```

5. Enable the GuardPoint.

```

# secfsd -guard /opt/apps/apps2/bin
secfsd: Guard initiated
#

```

The manual GuardPoint is active and the policy is enforced.

6. Disable the GuardPoint.

```
# secfsd -unguard /opt/apps/apps2/bin
secfsd: Unguard initiated
#
```

Selecting a GuardPoint Mount Type

- > Under random circumstances, NFS file systems can be mounted before the CTE Agent drivers are loaded. When this occurs, the CTE Agent is unable to protect GuardPoints on the file system. The **Auto Mount** feature prevents this from occurring. Select the **Auto Mount** toggle in the Edit Client window when the GuardPoint is in an automounted file system.
- > When applying file system protection to an automounted file system, do not apply the GuardPoint to the link-target directory. Rather, apply the GuardPoint to the full path to the directory underneath it. For example, if the automounted directory `"/Auto"` mounts a link-target directory named `"/documents"`, do not set the GuardPoint to `"/documents"`. Instead, set the GuardPoint to `"/Auto/documents"`.
- > Do not configure Linux 64-bit clients to automount directories with the `"/net"` option. The automounter uses the automount map associated with each mount point to locate each file system as it is accessed. The CTE Agent cannot resolve file system selections for GuardPoints, including any directories below a GuardPoint, that are configured with the `"/net"` option.

Viewing GuardPoints

The Status Bar on the GuardPoints tab of a client shows the total number of GuardPoints on the client, and inactive, active, and unknown GuardPoints. The Status Bar contains the following tabs:

- > **<N> Total GuardPoints**: Shows the total number of GuardPoints with all types of health status.
- > **<N> Inactive**: Shows the number of inactive GuardPoints.
- > **<N> Active**: Shows the number of active GuardPoints.
- > **<N> Unknown**: Shows the number of GuardPoints whose status is unclear.

Click each tab to filter the GuardPoints. The GuardPoints list displays details of the GuardPoints on the client.

To view the GuardPoints created on a client:

1. Open the **CTE** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client. The GuardPoints tab shows the GuardPoints configured on the client.

Status	Policy	Protected Path	Type	Client Group	Rekey Status	Enabled
Active	Idtpic	C:\AnunB	directory_auto		Rekeyed	Yes

The GuardPoints list shows the following details:

Column	Description
Status	Status of the GuardPoint. The status can be: > Inactive > Active > Unknown A status "Processing" is displayed for a brief period until an operation on the GuardPoint completes.
Policy	Policy applied to the GuardPoint.
Protected Path	Path of the protected directory.
Type	Type of the GuardPoint.
Origin	Origin of the GuardPoint. The origin can be: > Client: GuardPoint is created on an individual client. > Client group: GuardPoint is created on a client group.
Rekey Status	Rekey status of the GuardPoint.
Enable	Whether the GuardPoint is enabled.

Viewing GuardPoint Status

Status of GuardPoints can be seen on the CipherTrust Manager and on the client running the CTE Agent. The CipherTrust Manager GUI shows the GuardPoint status as it is configured on the CipherTrust Manager. It is not a real-time indication of the actual status.

Viewing GuardPoint Status on the Client

To view the actual status:

1. Log on to the CTE client as root/administrator.
2. Run the CTE Agent utilities.
3. Compare the GuardPoint status on the client with the status on the CipherTrust Manager GUI. If they do not match, go with the status on the CTE client.

Viewing GuardPoint Status on the GUI

The GuardPoints tab of the Clients page shows the total number of configured GuardPoints with their status. Similarly, status of GuardPoints on a client group can viewed on its GuardPoints tab.

To view the status on the GUI:

1. Open the **CTE** application.
2. Click **Clients > Clients**.

3. Under **Client Name**, click the desired client.
4. Click the **GuardPoints** tab. This tab shows the list of configured GuardPoints.
5. View the **Status** of the GuardPoint. The status can be:
 - **Active**: GuardPoint is deployed successfully and connection to the CTE Agent is healthy.
 - **Inactive**: GuardPoint is enabled but is not yet applied. Possible reasons are:
 - The GuardPoint is manual and is not mounted on the client. To apply manual GuardPoints, the client administrator needs to run the `secfsd -guard` command on the client.
 - A communication error has occurred between the CipherTrust Manager and CTE client.
 - **Unknown**: GuardPoint is created. Awaiting response from the CTE Agent on the GuardPoint request.

To view more details about an **Active** or **Inactive** GuardPoint, click the corresponding status link.

A status "Processing" is displayed for a brief period until an operation on the GuardPoint completes.

Configuring Windows Network Drives

Windows network drives may need user credentials and domain information for the CipherTrust Manager to configure GuardPoints and to push configuration changes to the CTE Agent. The Remote File Browser window enables you to automatically supply the user credentials.

Guard network mapped drives on a Windows client using the complete Universal Naming Convention (UNC) name for each file path. For example:

```
> \\1.2.3.4\ShareName\dirpath
> \\ServerName.DomainName.com\ShareName\dirpath
> \\ServerName\ShareName\dirpath
```

We recommend that you use the CipherTrust Manager IP address instead of the DNS name. GuardPoint protection is still enforced even when the CipherTrust Manager name is used.

To configure a network drive:

1. Open Guard File System window.
2. Click **Browse**. The Remote File Browser window opens.
3. Enable **Network Drive**. Three text-entry boxes are displayed. They are **Username**, **Password**, and **Windows Domain**.
4. Enter the network name of the user who has access permission to the network drive in the **Username** text-entry box.
5. Enter the password for the specified user in the **Password** text-entry box.
6. Enter the domain name of the system hosting the network drive in the **Windows Domain** text-entry box.
7. Select the GuardPoint and apply the policy as you would a non-network resource.

Deleting GuardPoints

GuardPoints can be removed (deleted) from entire client groups or individual clients. When a GuardPoint is removed from a client group, the GuardPoint is automatically removed from all clients in the group.

Before Deleting GuardPoints

The following preliminary steps need to be taken before deleting a GuardPoint:

- > Encrypted data in a GuardPoint will still be encrypted when the GuardPoint is removed. If you are not going to reuse the GuardPoint for any reason, such as uninstalling the CTE Agent software from a client, do either of the following:
 - Copy the encrypted files out of the GuardPoint so that they are saved as unencrypted files.
 - Rekey the encrypted files while the GuardPoint is still applied.
- > Take the GuardPoint out of service so that no user or application is accessing the directories and files in the GuardPoint. A GuardPoint is a mounted file system. Removing a GuardPoint involves unmounting the file system. File systems cannot be unmounted when in use.
- > Delete all the GuardPoints and disable the locks for a client before deleting the client from the CipherTrust Manager. This ensures that there are no residual GuardPoints in effect on the client.
- > For LDT GuardPoints, refer to procedures described in the CTE-Live Data Transformation with CipherTrust Manager to ensure that the data in those GuardPoints remains available.

Deleting a GuardPoint

To delete a GuardPoint:

1. Open the **CTE** application.
2. Select the client or client group from which you want to remove the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, select the GuardPoint to be deleted.
4. Click the overflow icon () corresponding to the desired GuardPoint.
5. Click **Remove**. The GuardPoint status becomes Processing. While processing the GuardPoint removal:
 - a. CipherTrust Manager notifies the CTE Agent that the GuardPoint is removed from the CipherTrust Manager.
 - b. CTE Agent removes the mount point from the client.
 - c. CTE Agent notifies the CipherTrust Manager about the GuardPoint removal.
 - d. CipherTrust Manager removes the GuardPoint from the GuardPoints tab.
6. Click the **Refresh GuardPoints** icon () to update the tab.
7. Verify the mount points on the CTE Agent client.
 - On UNIX, run the command `df` or `secfsd -status guard`.
 - On Windows, click the Vormetric icon and **View > File System > GuardPoints**.

CHAPTER 10: Operations

This chapter provides information on operations that the CTE Server Administrator performs on the CipherTrust Manager. These operations include registering CTE clients with the CipherTrust Manager, and protecting file system on a CTE client.

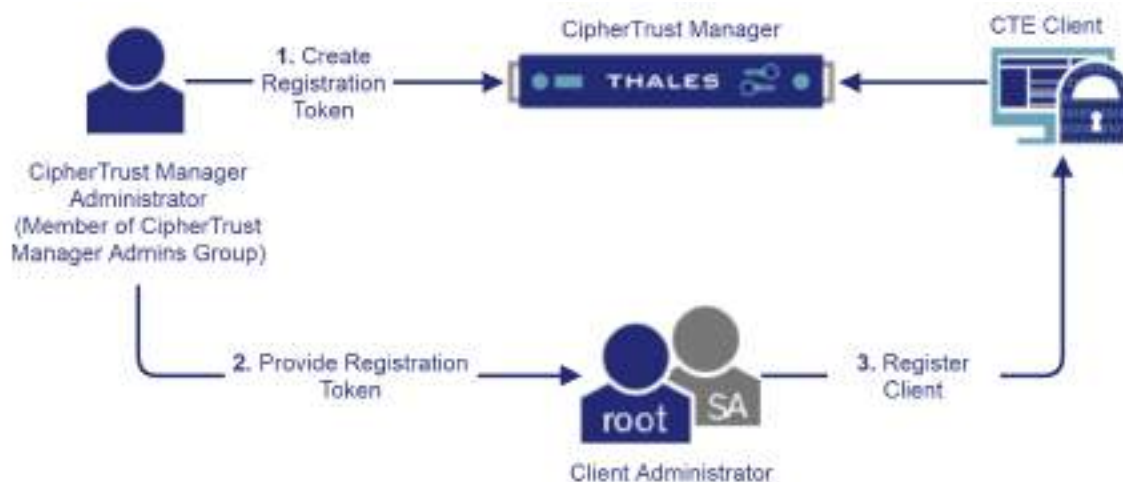
Registering Clients

Registration is the process of configuring a CTE client with a CipherTrust Manager. This process creates SSL certificates for further communication between the CipherTrust Manager and the CTE client.

Registering a CTE client with the CipherTrust Manager requires a registration token. Single registration token can be used to register any number of CTE clients. Refer to the CTE Agent Quick Start Guide specific to your platform for details.

NOTE After a client is registered, you must change the client password using the manual password creation method. Refer to ["Changing Client Password" on page 72](#) for details.

The following diagram shows the process of registering CTE clients with the CipherTrust Manager:



By default, CipherTrust Manager issues a Local CA with Common Name "KeySecure Root CA" which is used by CTE for signing client certificates. This Local CA is, by default, marked as trusted by the "web" interface which is also used by CTE for client authentication. Make sure that the CA whose signature is used for registering CTE clients is trusted by the "web" interface. Refer to the Interfaces section in the CipherTrust Manager documentation for details.

Third party (external) CA certificates can also be used for securing communication between the CipherTrust Manager and CTE clients. Refer to ["Using External CA Certificates" on the next page](#) for details.

Using External CA Certificates

All local and external CAs that participate in securing communication between the CipherTrust Manager and CTE clients must be added to the list of trusted CAs for the "web" interface on the CipherTrust Manager. Refer to the "Operation > Certificate Authority" section in the CipherTrust Manager Administrator Guide for details.

To use an external CA certificate:

1. Create a registration token using the ID of the Local CA signed by the external CA. Refer to "Client Management > Tokens" in the CipherTrust Manager Administrator Guide for details.
2. Register the CTE clients using this registration token. The registration process will automatically use the Local CA signed by the external CA. Refer to the CTE Agent Quick Start Guide specific to your platform for details.

Reregistering CTE Clients

In some cases, you need to change the CA certificate that was used to register a client with the CipherTrust Manager. For example, when the existing CA certificate expires or the certificate needs to be renewed to meet security requirements of your organization, the client must be reregistered with the CipherTrust Manager.

To reregister a client with the CipherTrust Manager:

1. Create a new registration token. Use the ID of the trusted CA that will be used to sign the client certificate. By default, a local CA will be used to issue certificates. Refer to "Client Management > Tokens" in the CipherTrust Manager Administrator Guide for details.
2. Register the client again using the new registration token created in step 1. The client administrator reregisters the client with the CipherTrust Manager. Steps are similar to registering a new client with the CipherTrust Manager.

Protecting Data on Clients

After registration, the client can communicate with the CipherTrust Manager, and is ready for data protection using CTE. This section describes how CTE GuardPoints, policies, and policy elements work together to encrypt file systems.

Refer to ["Common Scenarios" on page 164](#) for prerequisites and procedures to encrypt data in the most common scenarios.

GuardPoints

A GuardPoint specifies the path on the client that is to be protected with different access and encryption policies. GuardPoint is configured by specifying the guard path, policy, and other policy/path specific configuration parameters.

A sample configuration of a GuardPoint is shown below::



Refer to ["Managing GuardPoints" on page 135](#) for details.

Policies

A policy is the resource where all the access privileges and key configuration is done to achieve the required use cases. Policies are categorized as:

> Standard Policies

Depending on the availability of data in GuardPoints, standard policies can be applied in two different scenarios.

- **The GuardPoint does not contain any data.** The data would be created after the GuardPoint is applied. These policies are also called production policies.

A sample production policy is shown below:



- **The GuardPoint already contains data.** The existing data is migrated to encrypted form by using the data transformation (dataxform) policy.

A sample dataxform policy is shown below:

1 General Info

Name: dataxform.plc

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key.op	permit,applykey	Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	key1

After the data is migrated, unguard the dataxform policy, apply the standard policy with same key (as used by the dataxform policy). A sample standard policy applied after unguarding a dataxform policy is shown below:

1 General Info

Name: UC1-Standard

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
	User1		all_ops	permit,applykey	Yes
	User2		all_ops	permit	Yes
				deny	Yes

3 Key Rules

Resource Set	Key Name
	key1

Dataxform policies are created by turning on the Data Transformation toggle when creating a Standard policy. These policies require downtime, so they are referred to as offline policies. If you do not want downtime, you can deploy LDT policies.

> LDT Policies

As their name implies, LDT policies perform live transformation of data. They do not require any time downtime, so they are referred to as online policies. You can continue to work while the transformation of your data in GuardPoints is in progress. To benefit from LDT, you need to purchase an Add-On LDT license with the CTE Base license.

LDT policies can handle both these cases:

- The GuardPoint **does not contain** any data. No data is migrated. A production policy is applied to encrypt/decrypt the future data.
- The GuardPoint already **contains** data. The existing data is automatically migrated. After the data is migrated, the data is encrypted/decrypted like a production policy.

A sample LDT policy is shown below:

Name: UC1-LDT
Policy Type: ldt
Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit,applykey	No
	User1		all_ops	permit,applykey	Yes
	User2		all_ops	permit	Yes
				deny	Yes

3 Key Rules

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule
	clear_key	testldt	No

> COS Policies

These policies are used to encrypt data and apply access rules on the GuardPoints on cloud. CTE supports Amazon S3 buckets.

A sample COS policy is shown below:

Name: RS3-COSPolicy
Policy Type: cloud_object_storage
Description:

2 Security Rules

User Set	Process Set	Action	Effect	Browsing
		all_ops	permit,applykey	No

3 Key Rules

Key Name
key2

Refer to ["Creating Policies" on page 114](#) for details.

Policy Elements

To achieve different access privileges based on users, processes, and different resources (sub-directory/specific file formats), create these policy elements:

- > **User Sets:** Groups of single or multiple users that can be used as individual entities in policies to grant user specific privileges. A sample user set is shown below:

1 General Info

Name: UserSet1

Description:

2 Users / Groups

uname	UID	gname	GID	OS domain	
User1	1000	group1	1000		 Remove

- > **Process Sets:** Groups of single or multiple processes that can be used as individual entities in policies to grant process specific privileges.

1 General Info

Name: ProcessSet

Description:

2 Processes

Directory	File	Signature
/usr/bin	vi	

- > **Resource Sets:** Groups of single or multiple resources (sub-directory or specific file formats) that can be used as individual entities in policies to grant resource specific privileges.

1 General Info

Name: ResourceSet1

Description:

2 Resources

Directory	File	Include Sub Folders	File System Type
/	*.txt	Yes	Local File System

Refer to ["Creating Policy Elements" on page 103](#) for details.

CHAPTER 11: Common Scenarios

This chapter describes the common encryption scenarios in which paths can be encrypted using the CTE solution. Similarly, you can configure different types of policies with different combinations of policy elements to suit your requirements.

This chapter describes encryption using:

- > ["User-based Access Privileges" below](#)
- > ["Process-based Access Privileges" on page 167](#)
- > ["Signature-based Access Privileges for Processes" on page 168](#)
- > ["Different Access Privileges for Subdirectory or Different File Formats" on page 169](#)
- > ["Different Access Privileges for Combination of Users, Processes, and Resources" on page 170](#)

Prerequisites

- > The CipherTrust Manager is up and running. Refer to the [CipherTrust Manager Deployment Guide](#) for details.
- > A CTE base license is activated and installed. Refer to ["Licensing" on page 21](#) for details.
- > (Optional) Add-on LDT license is activated and installed. This license is needed only if you want to deploy LDT policies. A CTE base license must be activated on the CipherTrust Manager. Refer to ["Licensing" on page 21](#) for details.
- > The CTE Agent is installed on client machines where data is to be protected. The client machines are running a supported platform. Refer to the CTE Agent Quick Start Guide specific to your platform for details.

NOTE Policy elements can be created either in advance or when creating the policy. Refer to ["Creating Policy Elements" on page 103](#) for details.

User-based Access Privileges

Encrypt a local path with the following access privileges:

- > User set `UserSet1` can encrypt/decrypt data in the GuardPoint.
- > User set `UserSet2` can access the ciphertext data but cannot encrypt or decrypt.
- > All other user sets are denied access to the GuardPoint data.

Depending on the data availability (or downtime) and storage requirements in your setup, you can apply any of these policies:

- > ["Standard \(Production\) Policies" on the next page](#)
- > ["Standard \(Dataxform\) Policies" on the next page](#)

> ["LDT Policies" on page 167](#)

Refer to ["Data Transformation Techniques" on page 35](#) for advantages and limitations of data transformation techniques. LDT policies require an add-on license to use them.

Standard (Production) Policies

If the GuardPoint does not contain any existing data, and the data would be created after the GuardPoint is applied:

1. Create a standard policy. Refer to ["Creating Policies" on page 114](#) for details.

The screenshot shows a policy configuration interface with two main sections: 'General Info' and 'Security Rules'.

General Info:

- Name: ProductionPolicy
- Policy Type: Standard
- Description:

Security Rules:

Resource Set	User Set	Process Set	Action	Effect	Browsing
	User1		all_ops	permit,applykey	Yes

Key Rules:

Resource Set	Key Name
	key1

2. Apply a GuardPoint using the standard policy. Refer to ["Creating Standard GuardPoints on Clients" on page 138](#) for details.

Standard (Dataxform) Policies

If the GuardPoint already contains data, and the existing data needs to be migrated to encrypted form by using the dataxform utility:

1. Create a dataxform policy. Refer to ["Creating Policies" on page 114](#) for details.

1 General Info

Name: dataxform.plc

Policy Type: standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit,applykey	Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	key1

- Apply a GuardPoint using the dataxform policy. Refer to ["Creating Standard GuardPoints on Clients" on page 138](#) for details.
- After the existing data is migrated, unguard the dataxform policy from the GuardPoint. Refer to ["Deleting GuardPoints" on page 157](#) for details.
- Create a standard policy with same key (as used by the dataxform policy in the first step). Refer to ["Creating Policies" on page 114](#) for details.

1 General Info

Name: UC1-Standard

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
	User1		all_ops	permit,applykey	Yes
	User2		all_ops	permit	Yes
				deny	Yes

3 Key Rules

Resource Set	Key Name
	key1

- Apply the GuardPoint using the standard policy created in the previous step. Refer to ["Creating Standard GuardPoints on Clients" on page 138](#) for details.

LDT Policies

If you have an add-on LDT license, you can achieve the combined effects of the standard production and standard dataxform policies by applying the LDT policies.

- > If the GuardPoint already contains data, the policy migrates the existing data automatically. No need to run the dataxform utility manually. Later, the policy automatically encrypts/decrypts the data similar to a standard policy.
- > If the GuardPoint does not contain any existing data, migration is not required. A standard (production) policy of encryption/decryption is applied automatically.

To apply an LDT policy:

1. Create an LDT policy. Refer to ["Creating Policies" on page 114](#) for details.

Name: UC1-LDT
Policy Type: ldt
Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit,applykey	No
	User1		all_ops	permit,applykey	Yes
	User2		all_ops	permit	Yes
				deny	Yes

3 Key Rules

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule
	clear_key	testldt	No

2. Apply the GuardPoint using the LDT policy. Refer to ["Creating LDT GuardPoints on Clients" on page 140](#) for details.

Process-based Access Privileges

Encrypt a local path with the following access privileges:

- > Process set `ProcessSet1` can encrypt/decrypt data in the GuardPoint.
- > Process set `ProcessSet2` can access the ciphertext data but cannot encrypt or decrypt.
- > All other process sets are denied access to the GuardPoint data.

Process-based policies are configured in exactly the same way the user-based policies are configured, as described in ["User-based Access Privileges" on page 164](#). The only difference is that instead of adding user sets add process sets to the Security Rules tab of the policy.

Depending on the data availability (or downtime) and storage requirements in your setup, you can apply any of these policies:

- > ["Standard \(Production\) Policies" on page 165](#)

- > ["Standard \(Dataxform\) Policies" on page 165](#)
- > ["LDT Policies" on the previous page](#)

Refer to ["Data Transformation Techniques" on page 35](#) for advantages and limitations of data transformation techniques. LDT policies require an add-on license to use them.

Signature-based Access Privileges for Processes

Encrypt a local path with the following access privileges:

- > Process `Process1` with a particular signature can encrypt/decrypt data in the GuardPoint.
- > All other processes are denied access to the GuardPoint data.

To apply a signature-based access policy for a process:

1. Create a signature set. When creating the set, add the source path of `Process1`. This process will be signed. Refer to ["Creating Signature Sets" on page 88](#).

The screenshot shows the 'General Info' and 'Sources' tabs of a signature set configuration. Under 'General Info', the 'Name' is 'SignSet1' and the 'Description' is empty. Under 'Sources', the 'Source Directory' is '/usr/bin/xi'.

2. Sign the signature set. Use a CTE client having the desired process to sign the process. Refer to ["Signing Files in a Signature Set" on page 90](#) for details.

The screenshot shows the 'Source' and 'Signature' tabs of the signing interface. The 'Source' tab is active, showing a 'Change Client' button, a client IP address '10.154.13.209', and a 'Sign' button. Below, there is a search bar and a list of sources with checkboxes. The list shows '0 selected | 1 results | 1 source' and includes 'Source Directory' and '/usr/bin/xi'.

3. Create a process set. When creating the set, add the newly created signature set. Refer to ["Creating Process Sets" on page 110](#) for details.

1 General Info

Name: UC-3-ProcessSet

Description:

2 Processes

Directory	File	Signature	
/usr/bin/	vi	signed	...

4. Configure process-based access policies. Refer to ["Process-based Access Privileges" on page 167](#) for details.

Different Access Privileges for Subdirectory or Different File Formats

Encrypt a local path with the following access privileges:

- > Encrypt/decrypt only a subdirectory, `subdir1`, under the GuardPath.
- > Deny access to all other files and directories under the GuardPoint.

To achieve this use case, you need to add a resource set to the policy. In a resource set, you can provide details about the subdirectories or specific file formats that need to be handled differently under a GuardPoint.

To achieve this use case:

1. Create a resource set. Specify the details of the subdirectory (`subdir1`) in the resources. Refer to ["Creating Resource Sets" on page 104](#) for details.

1 General Info

Name: UC4_ResourceSet_SubDir1

Description:

2 Resources

Directory	File	Include Sub Folders	File System Type
/subdir1/	*	Yes	Local File System

NOTE Paths specified in a resource set should be relative to the GuardPath. Do not provide absolute path for the resources.

2. Create the desired policy type. Make sure to add the resource set created in the previous step. This is done to enforce the desired access policy. Refer to ["Creating Policies" on page 114](#) for details.

1 General Info

Name: UC4-Policy

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
UC4_ResourceSet_SubDir1			all_ops	permit,applykey	Yes
				deny	Yes

3 Key Rules

Resource Set	Key Name
UC4_ResourceSet_SubDir1	Key1

3. Apply the GuardPoint using the policy created in the previous step. Refer to ["Managing GuardPoints" on page 135](#) for details.

Different Access Privileges for Combination of Users, Processes, and Resources

Encrypt a local path with the following access privileges:

- > Allow only the process `usrbin.exe` being run by `User1` to encrypt/decrypt text files (*.txt) present under the GuardPath.
- > Deny access to all other users and processes.

To achieve this use case:

1. Created the required resource set. Refer to ["Creating Resource Sets" on page 104](#) for details.
2. Create the required user set. Refer to ["Creating User Sets" on page 105](#) for details.
3. Create the required process set. Refer to ["Creating Process Sets" on page 110](#) for details.
4. Create the desired policy type using the resource set, the user set, and the process set created above. Refer to ["Creating Policies" on page 114](#) for details.

1 General Info**Name:** UCS-Combination-Policy**Policy Type:** Standard**Description:****2 Security Rules**

Resource Set	User Set	Process Set	Action	Effect	Browsing
Text_ResourceSet	User1	UsrBin_ProcessSet	allOps	permitApplyKey	Yes
				deny	Yes

3 Key Rules

Resource Set	Key Name
Text_ResourceSet	Key1

5. Apply the GuardPoint using the policy created in the previous step. Refer to ["Managing GuardPoints" on page 135](#) for details.

APPENDIX A: Troubleshooting

This chapter describes how to handle the issues that you might face when using CTE with the CipherTrust Manager. These issues are categorized as:

- > ["Connection Issues" below](#)
- > ["Registration Issues" below](#)
- > ["Licensing Issues" on the next page](#)
- > ["Configuration Issues" on the next page](#)

Connection Issues

Symptoms	Possible Cause and Remediation
> Client status is Error > Configuration changes are not pushed to the client > Requests like Browse file system are failing	Analyze the CTE logs, identify connection failure reasons, and rectify them: 1. Look for the issues in the <code>/var/log/vormetric/server_comms.log</code> file on the CTE agent. This file contains information about the CipherTrust Manager's communication with the client. 2. Identify the cause of the issue. 3. Take appropriate action to resolve the issue. For example, you might need to: • Restart <code>vmd</code> to get the latest <code>init</code>. • Enable the connection timeout on the CipherTrust Manager to resolve registration token related errors.

Registration Issues

Symptoms	Possible Cause and Remediation
Registration fails with conflict errors	Conflict errors occur when a client with the given name already exists on the CipherTrust Manager. To fix these issues: > Delete the existing client entry from the CipherTrust Manager. > Unenroll the existing client if you want to register it with another CipherTrust Manager.
Reregistration fails with capabilities related errors	Reregistration requires the state of the CTE Agent capabilities such as LDT and COS is the same as it was before unenrollment. After a client is registered, these capabilities can be enabled on the CipherTrust Manager GUI. To disable the CTE Agent capabilities, delete the client from the CipherTrust Manager and register again with these capabilities disabled.

Licensing Issues

Symptoms	Possible Cause and Remediation
> Registration fails with licensing errors > LDT feature cannot be used > CTE configurations are read-only	> Registration can fail if the number of purchased licenses are consumed or the validity of a license is expired. This is applicable for both types of licenses: the base license (CTE - TransparentEncryption) and the add-on license (CTE - LiveDataTransformation). > To enable LDT at the time of registration (or later), make sure that you have a valid base license and a valid add-on LDT license. > After a license is expired: • A new client cannot be registered. • Existing operations on registered clients remain in tact. Their existing security configurations are pushed as and when required. • Creation of new GuardPoints with decryption policies is allowed. • Existing resources on the CipherTrust Manager become read only. Only existing records can be viewed.

Configuration Issues

Symptoms	Possible Cause and Remediation
Mismatched log levels between the CipherTrust Manager configuration and client logs	Try these: > Check the configuration in the linked profile on the CipherTrust Manager. > Validate the <code>vmd</code> configuration on the CTE client by running: <code>vmsec vmdconfig</code>

Index

C

- Changing password
 - Clients 72
- CLI 15
- client group 24, 77
- Client Group
 - modify configuration 80
- Client Group GuardPoints
 - Cloud Object Storage 150
 - COS 150
 - LDT 148
 - Standard 146
- Client Group Settings
 - Inherit settings 82
- Client Groups
 - Adding clients 78
 - Client settings 84
 - configure 24, 77
 - Creating 77
 - Deleting 84
 - Displaying 79
 - Editing 79
 - Modifying 79
- Client Groups GuardPoints
 - Creating 145
- Client locks
 - Agent lock 59-60
 - client groups 63
 - Disabling 64
 - individual clients 62
 - System Lock 61
- Client settings
 - Application Authentication Credentials 69
 - keywords 68
 - Re-sign 70
- Client Settings
 - linux 66-68
- Clients
 - Client Settings 65
 - delete 75
 - deleted client indicator 76
 - deleting 75
 - Group membership 74
 - Health status 57
 - Modifying configuration 71
 - register 55
 - search 56
 - status bar 56
 - view 56
 - Viewing 56
- Clients settings
 - Linux 65
 - Windows 66
- Common Scenarios 164
- Concise Logging 52
- configure policies 115
- CTE
 - How it protects files 33
- CTE client 24, 55
- CTE components 34
 - Agent 34
 - CipherTrust Manager 34

D

Data transformation

- Copy/Restore 35
- dataxform utility 37
- process 33
- Properties 34
- techniques 35
- Uses 33

Data transformation rules 30

dataxform 30

G

guarded NFS mount 68

GuardPoint 25, 135

GuardPoints 135

- Automatic and Manual 151
- Cloud Object Storage 143
- Considerations 136
- COS 143
- Deleting 157
- Enable Secure Start 144
- LDT 140
- Overview 135
- Rekeying 137
- Secure Start 136
- Standard on Clients 138
- Status 140, 155
- Viewing 154
- Windows Network Drives 156

GUI 17

I

Interfaces 15

K

key rule 30

L

LDT

- enable 57
- Enabling 58

Learn Mode 31

Licensing 21

- Add-on Licenses 22
- Installing CTE Licenses 22
- Perpetual Licensing Model 21
- Sentinel EMS License Portal 22
- Time-limited Rental 21
- Trialware 21

Live Data Transformation

- Enabling 58

Log configuration

- Client logs 43
- Client Syslog 48
- QoS 50
- Quality of Service 50

M

Managing Clients and Client Groups 24, 55

O

offline password 72

Operations

- Protecting Client Data 159
- Registering 158
- Reregistering Clients 159
- Using External CA Certificates 159

P

Password

- Client groups 81
- Dynamic 74, 82
- Manual 73, 81
- Types 73

playground 15

Policies 101

- Cloning 128
 - Cloud Object Storage (COS) 25
 - components 25
 - Creating 114
 - Data Transformation Rules 121
 - Deleting 134
 - elements 25
 - Elements 163
 - General Information 115
 - Key Rules 119
 - LDT 25
 - Live Data Transformation 25
 - Modifying Policies and Rules 127
 - Policy Elements 103
 - Process Sets 110
 - Resource Sets 104
 - Rule Criteria 102
 - Rule Effects 102
 - Security Rules 117
 - Signature Sets 108
 - Standard 25
 - User Sets 105
- policy 25, 101, 114
- Policy elements
- pocess set 30, 110

resource set 29, 104

signature set 29, 108

user set 29, 105

profile 31, 42

DefaultClientProfile 31, 42

Profile

- Changing 72
- Client log configuration 43
- creating 42
- Deleting 54
- Modifying 53
- QoS configuration 50

Q

QoS

LDT schedule 51

R

resource 29, 104

REST API 15

S

security rule 26

Security rule

- actions 27
- criteria 26
- effect 28

Selecting a GuardPoint Mount Type 154

Setting Client Locks 59

Signature sets

Detecting duplicate files 94

Signature Sets 86

- Checking agent logs 99
- Creating 88
- Deleting 97

- Deleting signatures 95
- Deleting source 96
- Re-signing 98
- Signature of all files in a set 93
- Signature of specific files in a set 93
- Using in a policy 87

Signature signing

- Checking status 92
- Files in a set 90
- Stopping 92
- The process 87

T

Troubleshooting 172

- configuration issues 173
- connection issues 172
- licensing issues 173
- registration issues 172

U

User Roles 31

- CTE Admins 32
- CTE Clients 32

CipherTrust Transparent Encryption



Challenge: securing sensitive data across changing environments and increasing threats

Safeguarding sensitive data requires much more than just securing a data center's on-premises databases and files. The typical enterprise today uses three or more IaaS or PaaS providers, along with fifty or more SaaS applications, big data environments, container technologies, and their own internal virtual environments and private clouds.

To further complicate the problem, cyber-attacks have grown in sophistication and power. New compliance and regulatory mandates around protection of sensitive information keep on coming, and existing regulations have become more stringent.

Solution: CipherTrust Transparent Encryption

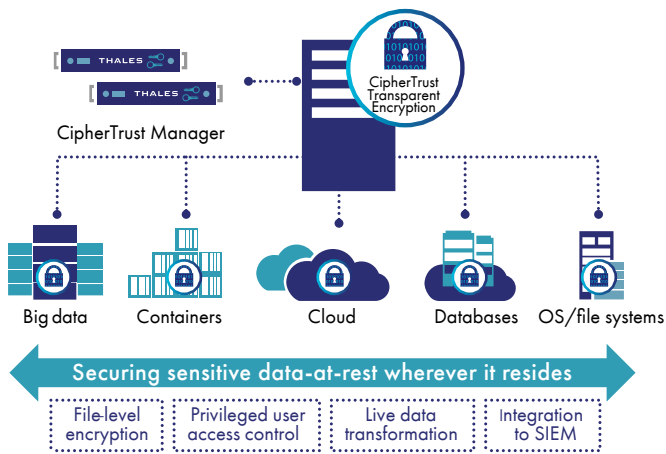
CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control, and detailed data access audit logging that helps organizations meet compliance and best practice requirements for protecting data, wherever it resides. The FIPS 140-2 compliant CipherTrust Transparent Encryption agent resides at the operating file-system or device layer, and encryption and decryption is transparent to all applications that run above it. CipherTrust Transparent Encryption

provides rich access controls, which allow organizations to determine who can access data, when they can access it, and what type of access they have.

Securing sensitive data-at-rest wherever it resides

- Meet compliance and best practice requirements for encryption, access control, and data access logging using a proven hardware accelerated encryption solution, that secures files, volumes and linked cloud storage while enabling access control and data access audit logging in physical, virtual, and cloud environments.
- Deployment is simple, scalable and fast with centralized key management, encryption, and access policies that reach across multiple clouds, on-premises, and within big data, and container environments.
- Easily implement privileged user access controls to enable administrators to work as usual but protect against users and groups that are potential threats to data.

CipherTrust Transparent Encryption



- Leverage detailed, actionable security event logs that provide unprecedented insight into file access activities to identify and stop threats faster.
- Broadest platform support in the industry. Protects structured and unstructured data accessed by Linux, AIX and Windows systems, as well as transparent encryption and access control for data residing in S3 buckets.
- Eliminate the downtime required for initial encryption and re-keying operations by adding the Live Data Transformation option. There is no other data encryption solution that offers this unique capability.

Key advantages

Transparent data protection. Continuously enforces file-level encryption that protects against unauthorized access by users and processes and creates detailed data access audit logs of all activities without requiring changes to applications, infrastructure, systems management tasks, or business practices.

Seamless and easy to deploy. CipherTrust Transparent Encryption agents are deployed on servers at the file system or volume-level and support both local disks as well as cloud storage environments, such as Amazon S3 and Azure Files.

Define granular access controls. Apply granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop and containers. Controls also include access by process, file type, time of day, and other parameters.

High-performance hardware accelerated encryption. CipherTrust Transparent Encryption only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs.

Comprehensive security intelligence. Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance requirements, but also enable data security analytics.

In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.

Broadest system and environment support. The agent is available for a broad selection of Windows, Linux, and AIX platforms, and can be used in physical, virtual, cloud, container, and big data environments, regardless of the underlying storage technology.

Advanced security

Zero-downtime data transformation. Live Data Transformation option eliminates the downtime required for initial encryption and scheduled rekeying operations. This patented technology allows for databases or files to be encrypted or re-keyed with a new encryption key while the data is in use without taking applications off-line.

Advanced access controls for big data (Hadoop). When implemented in Hadoop environments, access controls are extended to Hadoop users and groups.

SAP HANA qualified. SAP has qualified CipherTrust Transparent Encryption with HANA v2.0 to deliver data encryption, key management, privileged user access control, and granular file access audit logs.

CipherTrust Transparent Encryption UserSpace. Provides scalable and robust file encryption solution based on Linux FUSE that is not affected by kernel upgrades on Linux servers.

Solution architecture

Deployments consist of CipherTrust Transparent Encryption agents and CipherTrust Manager appliances. Policy and key management is centralized at the CipherTrust Manager. The CipherTrust Manager is available as a FIPS 140-2 level 1, 2 or 3 compliant appliance.

CipherTrust Data Security Platform

CipherTrust Transparent Encryption is part of the CipherTrust Data Security Platform. The CipherTrust platform unifies data discovery, classification, data protection, and provides unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations, and reduces risk across your business. You can rely on Thales CipherTrust Data Security Platform to help you discover, protect and control your organization's sensitive data, wherever it resides.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <     

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

CipherTrust Transparent Encryption

Advanced data-at-rest encryption, access control and data access audit logging



Contents

3	Introduction
4	The CipherTrust Data Security Platform from Thales
4	Simplify Data Security
4	Accelerate Time to Compliance
4	Secure Cloud Migrations
5	The CipherTrust Transparent Encryption Solution
5	Introduction
5	Meet compliance requirements for encryption and access control
5	Scalable encryption
5	Protect data on-premises or in-cloud
7	CipherTrust Transparent Encryption Agent
8	Powerful protection against root and privileged user risks
8	CipherTrust Manager
9	Strong Separation of Duties
10	CipherTrust Security Intelligence
11	Live Data Transformation Extension
11	CipherTrust Transparent Encryption for SAP HANA
12	Secure Import of Data Encryption Keys
13	Use cases
13	Databases and Unstructured Files – Across Data Centers and Cloud Environments
14	Big Data
15	Advanced data protection for Amazon S3
16	Summary
16	Appendix: Performance benchmarks
16	About Thales

Introduction

Enterprise digital transformation and increasingly sophisticated IT security threats have resulted in a progressively more dangerous environment for enterprises with sensitive data, even as compliance and regulatory requirements for sensitive data protection rise. With attacks adapting on a daily or even hourly basis, even next-generation network and endpoint defenses consistently fail to stop enterprise network penetration. At the same time, digital transformation is expanding the attack surface available to adversaries beyond traditional enterprise boundaries, as organizations embrace the business advantages available from these new solutions.

Just as no single attack method is responsible for all increased threats to enterprise data, no single digital transformation technology is responsible for all increased risks from these new environments – as each technology adopted presents unique data security challenges. However, the number and complexity of these new technologies and the individualized approach required to secure data throughout each environment combine to compound the problem.

Within this environment of increased risks to sensitive data, enterprises require the ability to limit access to sensitive information to only those users, groups, and processes that require the use of the data – and no more. This need extends across traditional data centers, cloud environments, SaaS implementations, and to the data stores of every digitally transformative environment. What is required is a way to make sensitive data useless (and valueless) when not in use and then to control access to the levers that make the data useful again, when it is needed by a legitimate user. This is what transparent encryption with user access control does.

CipherTrust Transparent Encryption enables quick, effective and transparent protection of data at the system level without derailing business processes, user tasks, and administrative workflows. With a single set of data security controls, information stored within physical and virtual systems, big data environments, containers, and linked cloud storage are protected at the file system or volume level across data centers and cloud environments. The result is greatly reduced risk, and an enhanced capability to meet compliance and regulatory data security requirements.

The CipherTrust Data Security Platform from Thales

The CipherTrust Data Security Platform is composed of an integrated suite of products built on a common, extensible infrastructure with efficient, centralized key and policy management. As a result, your security teams can address your data security policies, compliance mandates, and best practices, while reducing administration effort and total cost of ownership. The platform offers capabilities for protecting and controlling access to databases, files and containers—and can secure assets residing in cloud, virtual, big data and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements, and it prepares your organization to nimbly respond when the next security challenge or compliance requirement arises.

Simplify Data Security

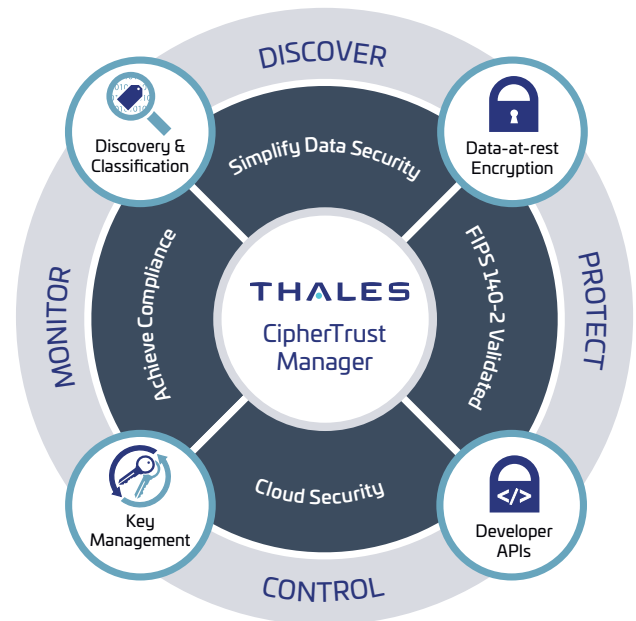
Discover, protect, and control sensitive data anywhere with next-generation unified data protection. The CipherTrust Data Security Platform simplifies data security administration with 'single pane of glass' centralized management console that equips organizations with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud or in any external provider's infrastructure. Organizations can easily uncover and close privacy gaps, prioritize protection, and make informed decisions about privacy and security mandates before a digital transformation implementation.

Accelerate Time to Compliance

Regulators and auditors require organizations to have control of regulated and sensitive data and reports to prove it. CipherTrust Data Security Platform capabilities, such as data discovery and classification, encryption, access control, audit logs, tokenization, and key management support ubiquitous data security and privacy requirements. These controls can be quickly added to new deployments or in response to evolving compliance requirements. The centralized and extensible nature of the platform enables new controls to be added quickly through the addition of licenses and scripted deployment of the needed connectors in response to new data protection requirements.

Secure Cloud Migrations

The CipherTrust Data Security Platform offers advanced encryption and centralized key management solutions that enable organizations to safely store sensitive data in the cloud. The platform offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management. Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager. The CipherTrust Cloud Key Manager supports Bring Your Own Key (BYOK) use-cases across multiple cloud infrastructures and SaaS applications. With the CipherTrust Data Security Platform, the strongest safeguards protect an enterprise's sensitive data and applications in the cloud, helping the organization meet compliance requirements and gain greater control over data, wherever it is created, used, or stored.



The CipherTrust Transparent Encryption Solution

Introduction

CipherTrust Transparent Encryption software for enterprises delivers data-at-rest encryption with centralized key management, privileged user access control, and detailed data access audit logging. This protects data wherever it resides -- on-premises, across multiple clouds and within big data and container environments.

The deployment is simple, scalable and fast, with agents installed at operating file system or device layer, and encryption and decryption is transparent to all applications that run above it. CipherTrust Transparent Encryption is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost. Implementation of the encryption software is seamless keeping both business and operational processes working without changes even during deployment and roll out.

Meet compliance requirements for encryption and access control

Encryption, access controls, and data access logging are basic requirements or recommended best practices for almost all compliance and data privacy standards and mandates, including PCI DSS, HIPAA/Hitech, GDPR and many others. CipherTrust Transparent Encryption delivers the controls required without operational or business process changes.

Scalable encryption

The CipherTrust Transparent Encryption agent runs at the file system or volume level on a server. The agent is available for a broad selection of Windows, Linux, and AIX platforms and can be used in physical, virtual, cloud, container, and big data environments – regardless of the underlying storage technology. Administrators perform all policy and key administration through the CipherTrust Manager. Encryption takes place on the server, eliminating bottlenecks that plague legacy, proxy-based solutions. Performance and scalability are further enhanced by leveraging cryptographic hardware modules that are built into such modern CPUs as Intel AES-NI and IBM POWER9.

Protect data on-premises or in-cloud

Keep control of your data by managing encryption keys and access policies from your local data center for both your on-premises and cloud data, even in hybrid environment deployments.

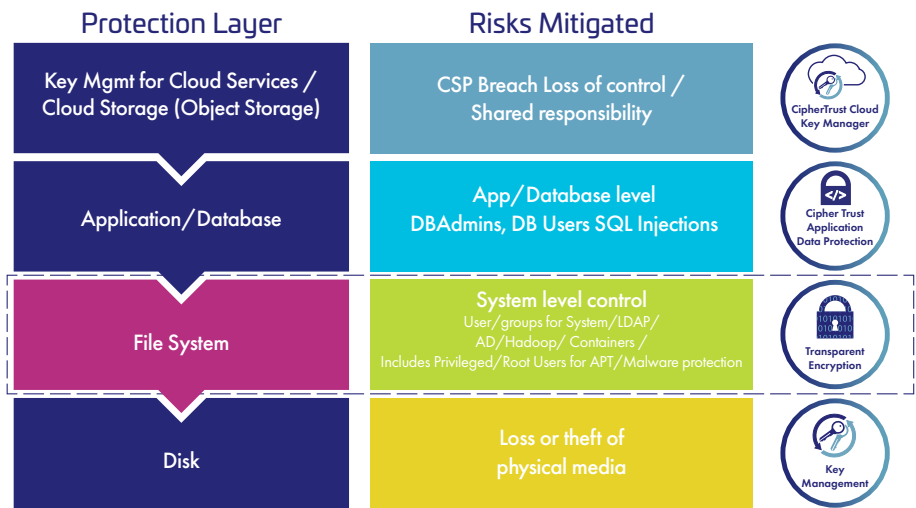


Figure 2. CipherTrust Data Security Platform – Risks and Protection Layers for Transparent Encryption

Advanced capabilities

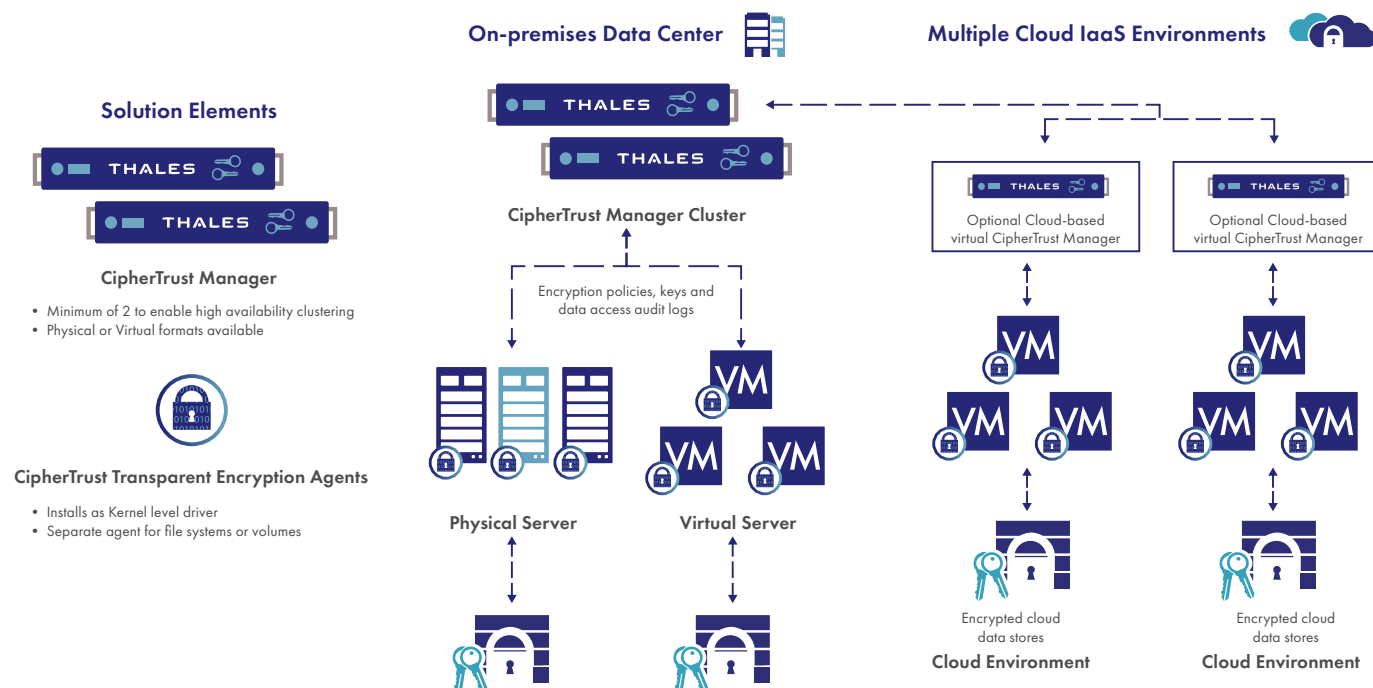
- **Zero-downtime data transformation.** The Live Data Transformation option eliminates the downtime required for initial encryption and scheduled rekeying operations. This patented technology allows for databases or files to be encrypted or re-keyed with a new encryption key while the data is in use without taking applications off-line.
- **Advanced access controls for big data (Hadoop).** When implemented in Hadoop environments, access controls are extended to Hadoop users and groups.
- **SAP HANA reviewed and qualified.** SAP has qualified CipherTrust Transparent Encryption with HANA v2.0 to deliver data encryption, privileged user access control, and granular file access audit logs.

Key features

- **Transparent data protection.** Continuously enforces file-level encryption that protects against unauthorized access by users and processes and creates detailed data access audit logs of all activities without requiring changes to applications, infrastructure, systems management tasks, or business practices.
- **Seamless and easy to deploy.** CipherTrust Transparent Encryption agents are deployed on servers at the file system or volume level and support both local disks as well as cloud storage environments, such as Amazon S3 and Azure Files.
- **Define granular access controls.** Apply granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop and containers. Controls also include access by process, file type, time of day, and other parameters.
- **High-performance hardware accelerated encryption.** CipherTrust Transparent Encryption only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs.
- **Comprehensive security intelligence.** Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance requirements, but also enable data security analytics. In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.
- **Broadest system and environment support.** The agent is available for a broad selection of Windows, Linux, and AIX platforms and can be used in physical, virtual, cloud, container, and big data environments, regardless of the underlying storage technology.

Optional extensions and additions:

- **Live Data Transformation.** Perform initial encryption and data re-keying without taking applications using data stores offline. This extension is enabled with an additional license.
- **SAP HANA qualified.** CipherTrust Transparent Encryption provides a proven approach to safeguarding SAP HANA data. This solution meets rigorous security, data governance, and compliance requirements. The solution can be quickly deployed, requiring no changes to SAP HANA or the underlying database or hardware infrastructure. With the solution, organizations can encrypt SAP HANA data and log volumes and establish strong governance and separation of duties.



A simple CipherTrust Transparent Encryption deployment scenario for file system or volume data within a local data center includes:

- A CipherTrust Transparent Encryption agent deployed to the host systems or virtual machines
- Two CipherTrust Manager appliances. Two appliances are required for clustering and failover capabilities that enable solution uptime.

Additional options extend the solution's functionality.

CipherTrust Transparent Encryption Agent

CipherTrust Transparent Encryption agents are kernel level drivers that sit above file systems or volumes in the OS stack. Agents perform encryption, decryption, policy-based access control, and data access audit logging.

Policies administered by agents employ logic and fine-grained access control settings configured at the CipherTrust Manager to evaluate attempts to access protected data, and then either grant or deny access.

Controls include who is enabled to access data, what and where information is available to them, when access can be performed, and what processes are allowed to access plaintext, copy encrypted files, or even view file system metadata.

This fine-grained policy control enables operation that lets administrators and system level users perform their work (such as system backups, updates, and hardware maintenance), without having access to decrypted sensitive information.

All activities are logged. Logs are available from the local system or the CipherTrust Manager and can be integrated with leading SIEM systems. See the section of this white paper on Security Intelligence for further detail.

Application uptime, for the solutions whose data CipherTrust Transparent Encryption protects, is supported with an easily available failover capability. Simply deploy agents at the primary and failover locations and keep encrypted data stores in sync with standard processes. When top level application failover is required, enable the same policy used at the primary location at the failover location. Sensitive information is continuously protected, and business operations continue with standard failover operation.

CipherTrust Transparent Encryption is designed to minimize impact on overall system performance. The AES-256 hardware-accelerated encryption capabilities available from modern CPUs are used by the agent regardless of the environment. AIX, Linux, and Windows deployments to physical servers, virtual environments, cloud, and even container environments all benefit from the extremely low overhead on encryption and decryption available from hardware acceleration.

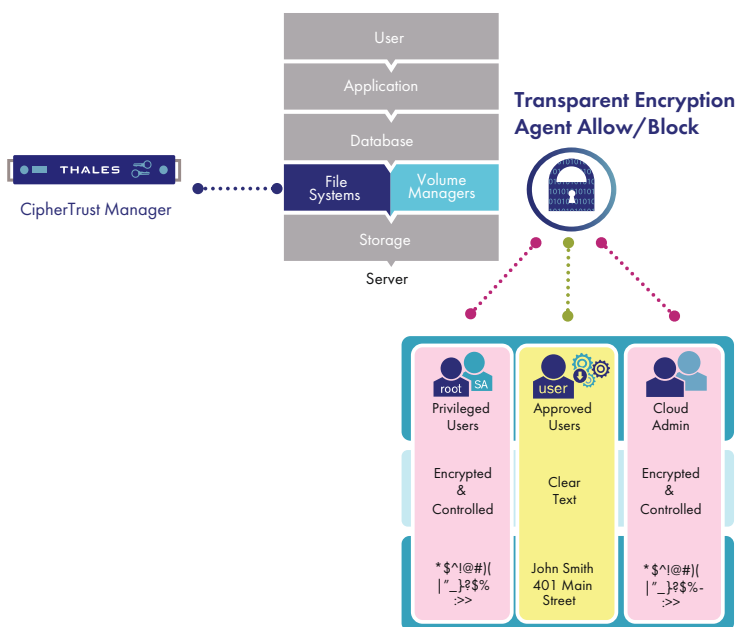


Figure 4. CipherTrust Transparent Encryption encrypts, enforces access policies, and logs all file, volume and linked cloud storage access

Environment Support

OS Support Microsoft: Windows Server 2012, 2016, and 2019 Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, AWS Linux and Ubuntu, UNIX: IBM AIX	Big Data Support Hadoop: Cloudera, Hortonworks, IBM NoSQL: Couchbase, DataStax, MongoDB, SAP HANA
Database Support IBM DB2, Microsoft SQL Server, MySQL, NoSQL, Oracle, Sybase, and others	Encryption Hardware Acceleration AMD and Intel AES-NI, IBM P9 cryptographic coprocessor
Application Support Transparent to all applications, including Documentum, SAP, SharePoint, custom applications, and more	Agent Certification FIPS 140-2 Level 1
File systems Supports most standard file systems for each OS – See your Thales sales representative for a complete and current listing. Cloud Storage Amazon AWS – EBS, EFS, and via the AWS Storage Gateway also supports S3 Standard, S3 Infrequent and S3 Glacier Microsoft Azure – Disk Storage, Azure Files	Users and Groups System, LDAP/AD, Hadoop and Containers

Powerful protection against root and privileged user risks

CipherTrust Transparent Encryption includes highly intelligent protection against root user attacks. The solution will log and control access based on user roles and groups (system, LDAP/AD, Hadoop, Containers), but also has additional capabilities to combat root user attacks. The root user role has the capability to both create system level accounts and to log in to other system level accounts. When root users use these capabilities to change to an account that has access to sensitive data, access to the data will still be denied if the root user is not specifically allowed access by CipherTrust Transparent Encryption policy (as defined at the CipherTrust Manager). The solution will be aware of the original login account as root and deny or allow access based on the policies for that root account.

CipherTrust Manager

The CipherTrust Manager is the common centralized management environment for all CipherTrust Data Security Platform products. It provides policy control as well as secure management and storage of encryption keys, includes a web-based console as well as CLI and REST APIs. The CipherTrust Manager is available as FIPS 140-2 compliant virtual and physical appliances.

The CipherTrust Manager also provides a unified way to manage keys for third-party platforms, such as IBM Guardium Data Encryption (GDE), Oracle Transparent Data Encryption (TDE), Microsoft SQL Server TDE, and KMIP-compliant encryption products. The CipherTrust Manager can also store and manage X.509 certificates, symmetric keys, and asymmetric keys.

Strong Separation of Duties

The CipherTrust Manager can be configured as a multi-tenant device that runs many different virtual CipherTrust Managers, which are called “domains.” The CipherTrust Manager can enforce strong separation of duties by requiring more than one data security administrator to manage or change key and policy permissions. CipherTrust Manager administration can be broken into three categories: system, domain, and security. In this manner, no one person has complete control over security activities, encryption keys, or administration. Also, the CipherTrust Manager supports two-factor authentication for administrative access.

Users and groups for data security management tasks can be based on locally defined users or groups, or imported via LDAP from Active Directory or other directory services and identity management environments.

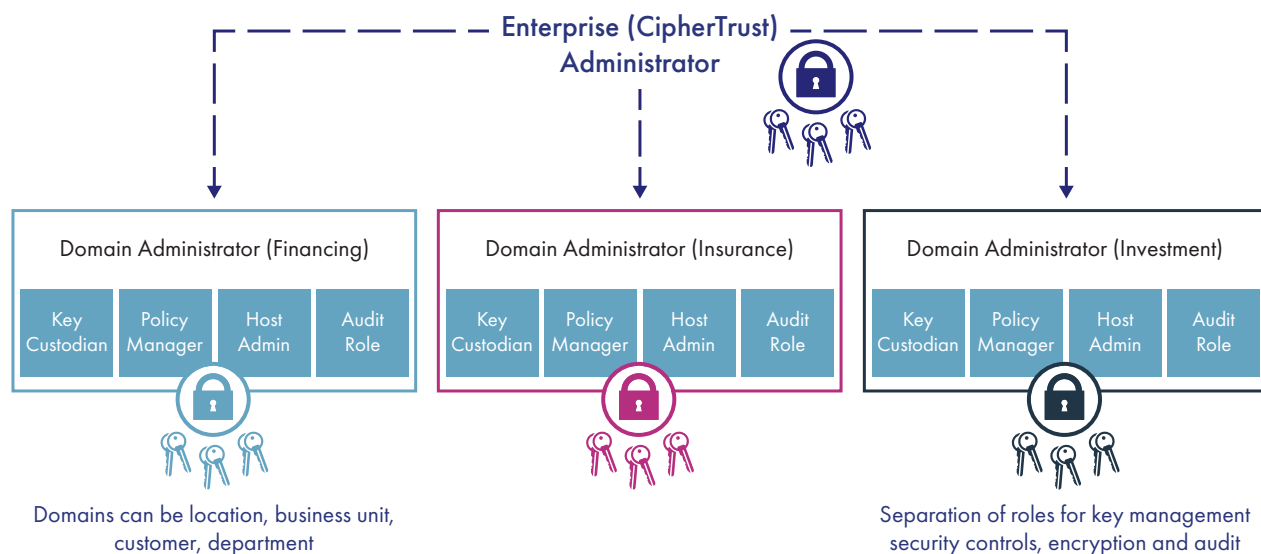


Figure 5. Multitenant Key Management and Strong Separation of Duties

To further isolate and protect sensitive data, the CipherTrust Manager and CipherTrust Transparent Encryption work in tandem to allow security administrators to create a strong separation of duties between data owners and privileged IT administrators. Users and groups used in policies for access control to data can be based on system level roles, LDAP/AD, Hadoop users/groups/zones as well as container environment users and groups.

If desired, CipherTrust Transparent Encryption can encrypt files while leaving their metadata in the clear. This capability enables IT administrators to perform system administration tasks (such as replication, backup, migration, snapshots, and system updates), without exposure to sensitive data. The CipherTrust Manager also can control basic system commands such as copy, write, and directory listings.

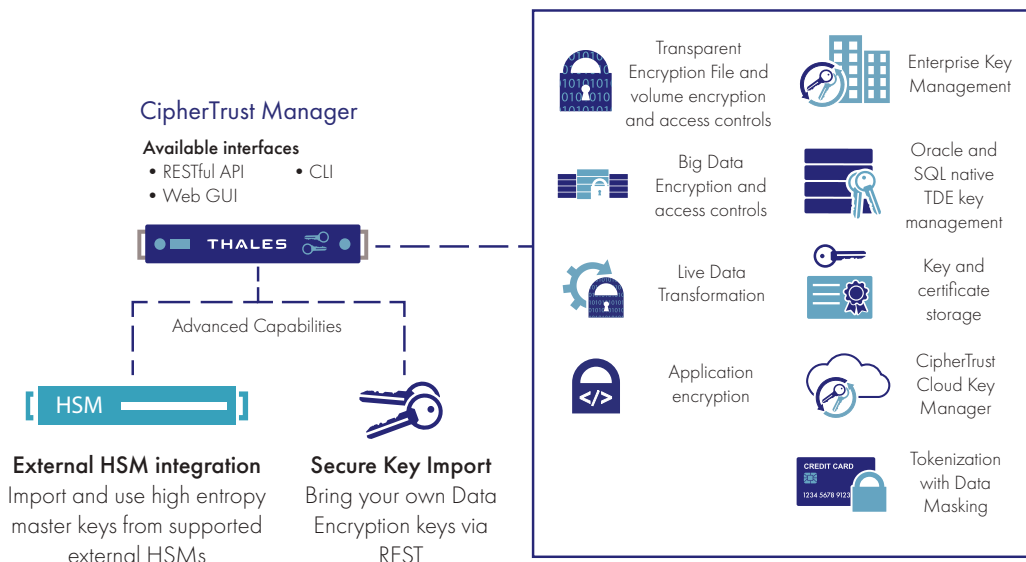


Figure 6. Centralized, integrated policy and encryption key management for all CipherTrust Data Security Platform products

CipherTrust Manager High Availability

CipherTrust Managers can be clustered for High Availability (HA), and Thales recommends this configuration for all implementations with a minimum deployment of two CipherTrust Managers. When configured for HA, one CipherTrust Manager acts as the primary and others are used for failover, scalability, or in additional locations where latency is a concern, such as a remote data center or cloud location.

All configuration settings, including changes to administrators, domains, hosts, keys, and policies, are made on the primary CipherTrust Manager, other CipherTrust Managers are read-only. Configuration changes and updates on the primary CipherTrust Manager are pushed to the other CipherTrust Managers at set intervals using replication.

APIs and interfaces

A web-based UI console and RESTful APIs are available. APIs make it possible to manage CipherTrust Manager functions remotely and are designed to operate in environments that require high levels of automation, such as service providers with cloud environments or highly automated data centers.

CipherTrust Security Intelligence

CipherTrust Transparent Encryption agents and CipherTrust Manager provide extensive logging capabilities detailing successful and attempted access attempts to protected data and the CipherTrust Manager management environment, agent interactions and key operations, as well as the actions of administrators at the CipherTrust Manager. Logs are designed to meet a range of needs for information from the solution. These include:

- Audit level information required by compliance, regulatory mandates, and best practice security reports
- Immediate insight into attempted access events by users and processes that may represent threats
- Detailed historical usage data that can be used to create baselines of expected operation from access pattern recognition

Logs are available in standard formats used by security information and event management (SIEM) systems (RFC5424, CEF and LEEF), and are available from CipherTrust Managers as well as from systems hosting CipherTrust Transparent Encryption agents. The primary CipherTrust Manager can be used as a collection point for all logs from CipherTrust Managers and CipherTrust Transparent Encryption agents if desired.

These logs provide deep visibility into data access, which can be used to alert administrators to unauthorized access attempts to protected data that may represent a threat, and to build typical access patterns when combined with other infrastructure and access information. For instance, a user that typically accesses information in small quantities from within a local network, if seen to be accessing large volumes of data from a remote location, would represent a threat that should generate an alert and be investigated.

Detailed logs include information about when users and processes accessed data, under which policies, and if access requests were allowed or denied. The logs will even expose when a privileged user leverages a command like "switch user" to imitate another user. Logs are designed to be able to easily meet the auditing requirements of compliance mandates and regulations as well by delivering the detailed evidence needed to prove to an auditor the encryption, key management, and access policies are appropriate and operating correctly.

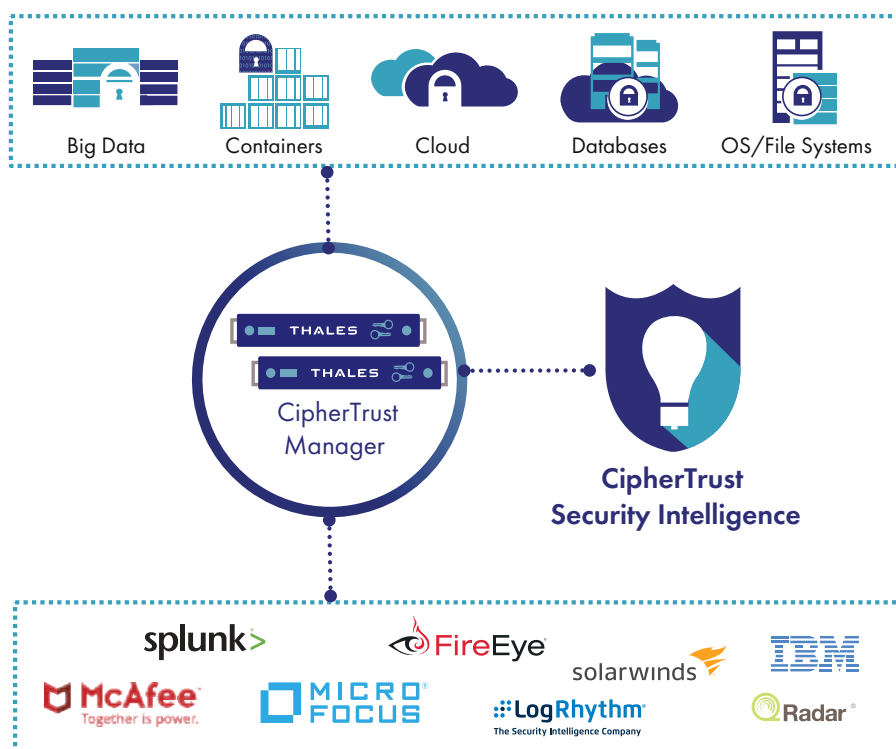
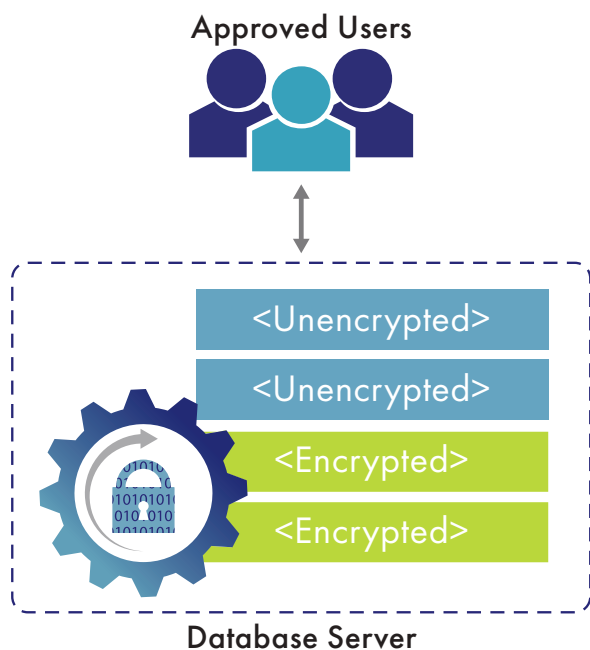


Figure 7. CipherTrust Security Intelligence



Live Data Transformation Extension

Deployment and management of data-at-rest encryption can present challenges when transforming clear-text to cipher-text, or when rekeying data that has already been encrypted. Traditionally, these efforts either required planned downtime or labor-intensive data cloning and synchronization efforts. CipherTrust Transparent Encryption Live Data Transformation Extension eliminates these hurdles, enabling encryption and rekeying with unprecedented uptime and administrative efficiency.

Zero-downtime encryption and key rotation.

Live Data Transformation delivers these key capabilities:

- Zero-downtime encryption deployments. The solution enables administrators to encrypt data without downtime or disruption to users, applications or workflows. While encryption is underway, users and processes continue to interact with databases or file systems as usual.
- Seamless, non-disruptive key rotation. Both security best practices and many regulatory mandates require periodic key rotation. Live Data Transformation makes it fast and efficient to address these requirements.

With the solution you can perform key rotation without having to duplicate data or take associated applications offline.

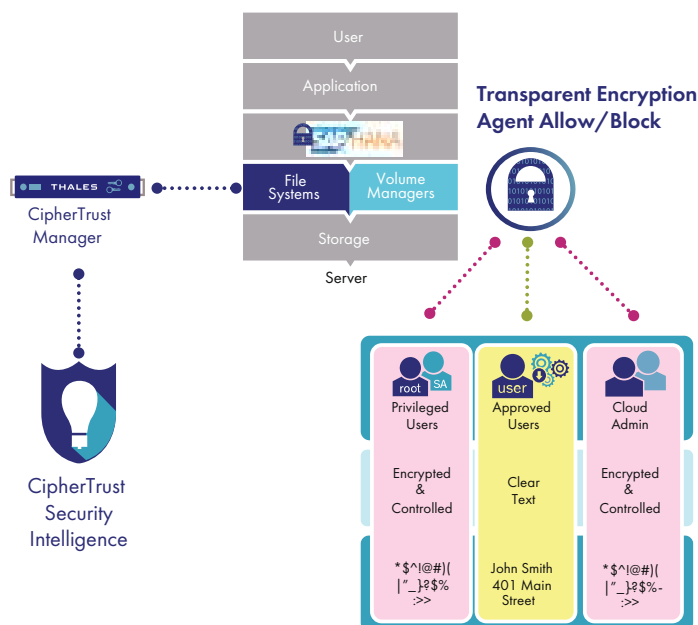
Figure 8. CipherTrust Transparent Encryption with CipherTrust Live Data Transformation Enabled

- Intelligent resource management. Encrypting large data sets can require significant CPU resources for an extended time. Live Data Transformation provides sophisticated CPU use and I/O rate management capabilities so administrators can balance between the resource demands of encryption and other business operations. For example, an administrator can define a resource management rule specifying that, during business hours, encryption can only consume 10% of system CPU, while on nights and weekends, encryption can consume 70% of CPU.
- Versioned backups and archives. With key versioning management, Live Data Transformation offers efficient backup and archive recovery that enable more immediate access. In a data recovery operation, archived encryption keys recovered from the CipherTrust Manager are automatically applied to an older data set. Restored data is encrypted with the current cryptographic key.

CipherTrust Transparent Encryption for SAP HANA

CipherTrust Transparent Encryption provides a proven approach to safeguarding SAP HANA data that meets rigorous security, data governance, and compliance requirements. The solution can be quickly deployed, requiring no changes to SAP HANA, the underlying database, or hardware infrastructure. With this solution, organizations can encrypt SAP HANA data and log volumes, and establish strong governance and separation of duties.

- Enforce strong data encryption on all SAP HANA data and log partitions
- Protect and control access to the SAP HANA persistence layer
- Use granular access controls to prevent privileged users and system administrators from accessing unauthorized data
- Facilitate compliance with new and existing data security mandates
- Maintain key and security policy custody on tenant/customer premises



Secure Import of Data Encryption Keys

As organizations increasingly place business-critical data within multiple cloud environments, the question of who controls the encryption keys that protect sensitive data becomes increasingly important. Enterprises prefer to control and even create the data encryption keys protecting their cloud environment data. Those with the highest levels of IT security requirements may even wish to control the creation of their in-house keys for maximum complexity, randomness, and assurance.

The CipherTrust Data Security platform provides the capability for cloud service providers and enterprises to offer multi-tenanted access to CipherTrust Managers that enables them to create and bring in data encryption keys used with CipherTrust Transparent Encryption agents rather than use the data encryption keys generated by the CipherTrust Manager. Data encryption keys can be created by a trusted hardware device (such as a Thales or third-party Hardware Security Module) or from an existing key management and creation application. Keys imported for use with CipherTrust Transparent Encryption agents can then be used as needed with policies created within the CipherTrust Manager.

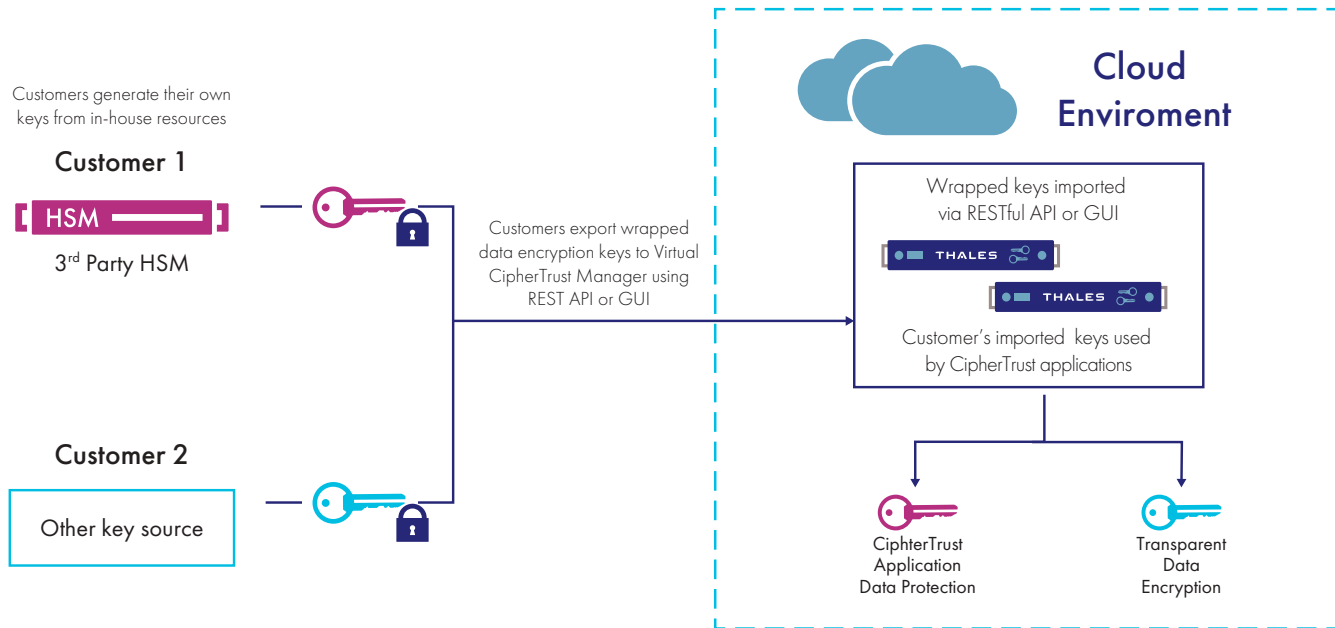


Figure 9. Maintain complete control of encryption keys, even within multi-tenant cloud environments

Use cases

Databases and Unstructured Files – Across Data Centers and Cloud Environments

As organizations continue to grow their infrastructure and data sets, they have to deal with a mix of in-house and cloud-based data assets and applications. Regardless of where this data is located, it requires the same level of data security and protection. CipherTrust Transparent Encryption enables enterprises to choose their implementation mode for data security based on their risk tolerance, compliance, and privacy requirements.

Most enterprises will opt for a solution that includes managing and controlling from their local data center encryption keys and access policies for both local data center resources and cloud environments. This approach keeps control of keys firmly within the enterprise, eliminating the risk of remote legal access or compromise at the cloud provider. Enterprises that are “all in” the cloud and make no use of local data center compute resources may opt for a cloud-based deployment of key and policy management. Such organizations can either co-locate cloud key management in the same cloud with data protected by CipherTrust Transparent Encryption, using a secondary cloud environment for the CipherTrust Manager to provide a greater degree of separation and lower risk, or use a co-location or hosting provider for hardware versions of CipherTrust Managers. All of these scenarios are easily supported with CipherTrust Transparent Encryption by locating physical or virtual CipherTrust Managers in local data centers, co-location vendors, hosting solutions, or cloud environments as needed.

Regardless of the deployment model, a typical database protection scenario includes a CipherTrust Transparent Encryption agent deployed to database servers with a simple policy – a signed database process and the database user are allowed cleartext access to the protected data store, all others will only see file metadata and ciphertext. This effectively shields the database access from compromise by root and privileged user-based attacks, local system, and LDAP users and groups while also meeting compliance and best practice requirements for safeguarding the data set with encryption.

For larger data sets, customers will typically purchase the Live Data Transformation extension to CipherTrust Transparent Encryption, enabling immediate encryption of the database without taking critical applications offline and periodic rekeying to meet compliance and best practice requirements without downtime.

We will use a directory for a typical unstructured file system protection example. The CipherTrust Transparent Encryption agent is deployed to the server with separate policies for LDAP/Active Directory user groups. For instance, allowing only finance department members to access critical accounting data, HR to access confidential employee information, and Engineering to access development documents. Each data store section is encrypted with an individual key by policy, effectively limiting the access to only those who require it for their work.

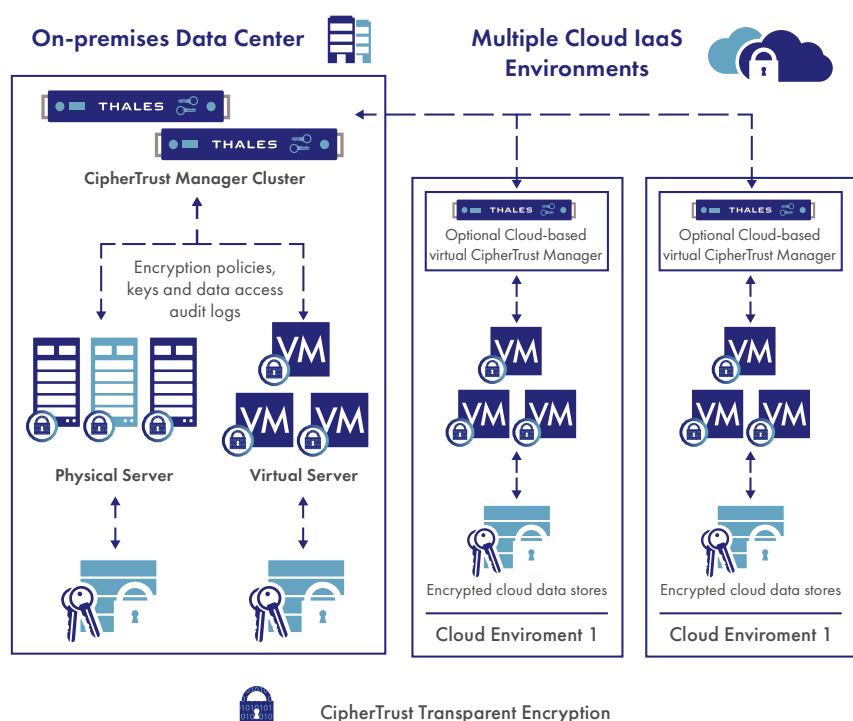


Figure 10. Fully integrated enterprise on-premises and cloud environment deployment

Big Data

With nearly every enterprise embracing big data environments, and with large numbers of these environments implemented in the cloud, the security of the sensitive data within the data lake, source data environments, and the reports that hold high-value correlated results have become an insistent concern.

CipherTrust Transparent Encryption safeguards this information. The solution can be used to protect data at the file system level within compute nodes (and underlying storage), source data locations, as well as the repositories used for logs and reports. And, this protection extends beyond the system level users/ groups and LDAP/AD users and groups that are enforced by CipherTrust Transparent Encryption on a typical server. The solution also enforces policy-based encryption, access controls and data access logging by Hadoop users, groups and zones. This capability provides further protection against privileged users within the big data lake or users within the environment.

A typical deployment includes agents installed on compute nodes, source data servers, and servers accessing log/report repositories. Data is encrypted throughout the environment with appropriate access policies and data access logging controls provided by the CipherTrust Manager. Further, the use of hardware encryption capabilities in underlying compute infrastructure results in minimal overhead from encrypt/decrypt operations. This makes it possible to use the solution even where speed and compute capability are critical.

Further, Thales works with leading big data environment vendors as a partner to ensure solution capability and operation. At the time of this writing, these partners include DataStax, MongoDB, Teradata, IBM, Cloudera, Couchbase, SAP HANA, and Hortonworks.

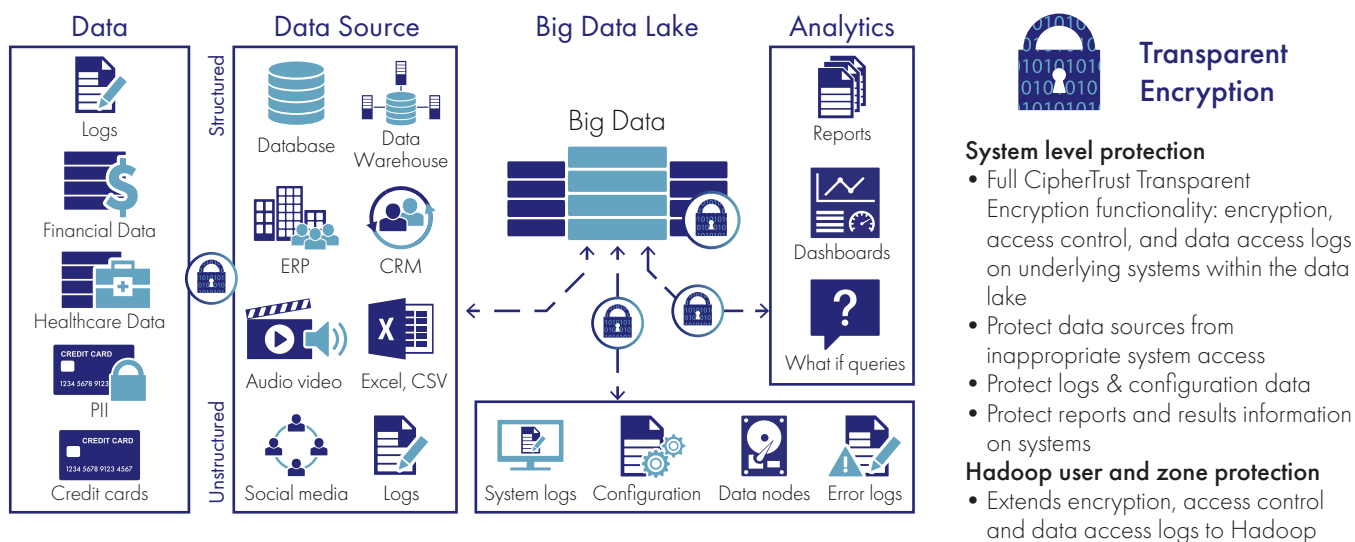
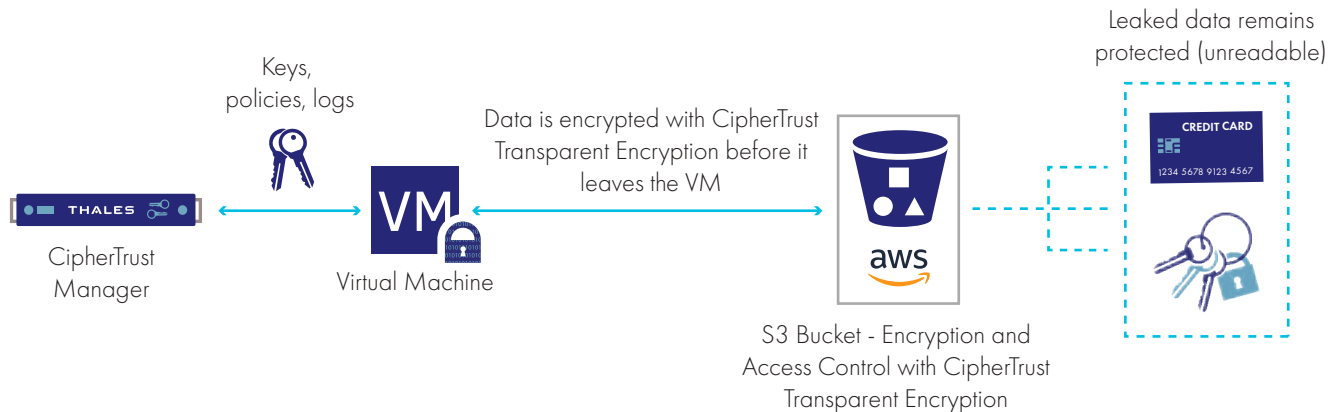


Figure 11. Protecting data within big data environments using CipherTrust Transparent Encryption

Advanced data protection for Amazon S3

As organizations increasingly use Amazon S3 cloud storage as part of their implementation strategy, as well as for backups and failover environments, they need to protect data within these S3 buckets just as they would if the storage were located within their own data centers.

With advanced data protection for Amazon S3, organizations can apply transparent encryption and access controls to sensitive data in S3 buckets. The CipherTrust Transparent Encryption solution encrypts unstructured files, semi-structured data, or structured databases before they are written to Amazon S3 buckets. This assures that the data is always encrypted in-flight, for example from on-premises hosts or Amazon EC2 instances to the S3 buckets. Decryption only occurs once the data is on the server where it will be used. In addition, CipherTrust Transparent Encryption protection for Amazon S3 features enhanced granular access controls, which, when deployed with custom AWS IAM policies, can enforce additional access controls to limit S3 access only to hosts running the CipherTrust Transparent Encryption for Amazon S3 agent.



Key features of CipherTrust Transparent Encryption for Amazon S3 include:

- **Transparent to applications and Amazon S3 administrators.** Encryption and access controls are completely transparent to applications while Amazon S3 administrative procedures remain unchanged after software agent deployment. The encryption offered by this solution is independent of Amazon S3 server-side encryption.
- **Continuous protection even with misconfigured S3 buckets.** Continuously enforces policies that protect against unauthorized access by users and processes even in the case of Amazon misconfigurations. Data access to protected S3 buckets is tracked through detailed audit logs.
- **Granular controls.** Applies granular, least-privileged user access policies that protect sensitive data in S3 buckets from external attacks and misuse by other privileged users. Security administrators can set up access controls on bucket creation, deletion, and enumeration, as well as for object creation, deletion, and updates. Optional S3 server-side access controls can be enabled with custom IAM policies to restrict S3 bucket access only to hosts configured with CipherTrust Transparent Encryption.
- **Strong data security.** Employs strong, standards-based encryption protocols, such as Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. TLS 1.3 and other NIST recommendations adopted to enforce strong key and data security. The agent is FIPS 140-2 Level 1 validated. The encryption keys are always created and managed by the CipherTrust Manager, a FIPS 140-2 Level 3 compliant appliance.
- **Security intelligence logs.** Identify and stop threats faster with detailed data access audit logs that produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented insight into file access activities.

Summary

The urgent need for data-at-rest encryption continues to grow. Compliance requirements proliferate. Digital transformation expands attack surfaces. And every day we see new internal and external threats to critical IP, PII, customer and citizen information, and more. With CipherTrust Transparent Encryption, organizations can secure their file and volume data wherever it is stored in a wide range of environments and use cases. And, CipherTrust Transparent Encryption is an integral part of a single platform solution that provides comprehensive data-at-rest security across the entire enterprise. The solution helps organizations address their security mandates while minimizing costs and administrative efforts.

Appendix: Performance benchmarks

Intel®, AMD, and PowerPC processor family all include hardware accelerated encryption capabilities that are leveraged by CipherTrust Transparent Encryption agents. For Intel, this includes Intel® Data Protection Technology with Advanced Encryption Standard New Instructions (AES-NI). AES-NI accelerates AES encryption and has been optimized for fast throughput and low latency.

CipherTrust Transparent Encryption uses AES-NI instructions for hardware-based acceleration of data encryption and decryption. In fact, CipherTrust Transparent Encryption has a proprietary encryption engine that is designed to take full advantage of the parallelism that can be achieved with multi-core processor chipsets and it specifically leverages the pipelining capabilities of AES-NI. As a result, the solution delivers the maximum performance possible.

In addition to leveraging hardware-based encryption capabilities, CipherTrust Transparent Encryption is tightly integrated with, and optimized for, each supported operating system kernel. Consequently, CipherTrust Transparent Encryption leverages the latest features available for every platform supported, rather than being coded to a lowest common denominator across multiple platforms. With each new release, Thales continues to add new capabilities that enable the solution to exploit the latest operating system features.

For many applications, the performance overhead that CipherTrust Transparent Encryption introduces is negligible. However, as loads associated with input/output (I/O) increase, there will be increased overhead associated with encryption. Even with demanding, I/O heavy applications, such as databases or big data processing, CipherTrust Transparent Encryption generally introduces less than 10% overhead.

One example can be seen in the chart below. In this example, the Yahoo Cloud Serving Benchmark (YCSB) was run against MongoDB 4.0.3, with the WiredTiger storage engine running on top of CipherTrust Transparent Encryption. YCSB is a generally available open source framework that has a common set of workloads for evaluating the performance of different “key-value” and “cloud” serving stores. The workload was configured so that less than one-half of the data set could fit in memory, causing a heavy I/O load. As the chart illustrates, CipherTrust Transparent Encryption only introduced minimal overhead.

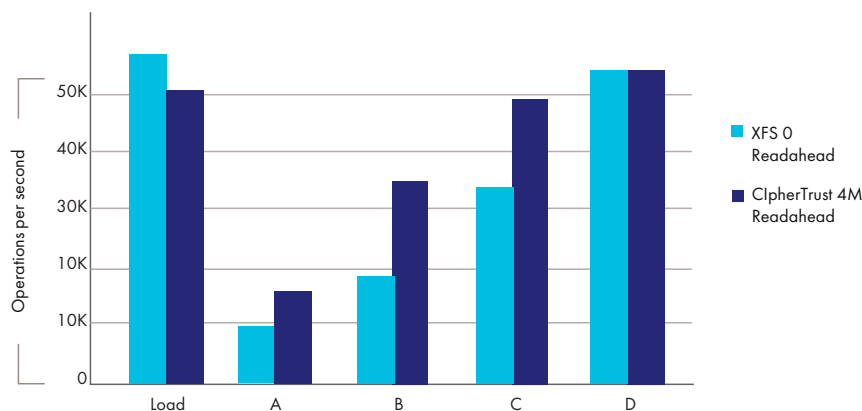


Figure 12. Even when testing in a scenario with a heavy I/O load, CipherTrust Transparent Encryption introduces minimal performance overhead.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

CipherTrust Transparent Encryption [White Paper](#)



Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <





CipherTrust Manager

Version: v2.22 (latest)

30 January 2026

Contents

CipherTrust Transparent Encryption (CTE)	5
Overview	7
Interfaces	10
Concepts	18
Data Transformation	28
Managing Profiles	39
Managing Clients	60
Enabling Live Data Transformation	73
Setting Client Locks	75
Client Settings	83
CTE Linux Authentication and Client Settings	100
Changing Client Password	106
Managing Membership	110
Deleting Clients	114
Kernel Compatibility Matrix	116
Collecting Agent Information	118
Fetching Latest Capabilities from Clients	121
Managing LDT Communication Groups	122
Managing Client Groups	126
Managing Signature Sets	147
Managing Policies	167
Creating Policy Elements	169
Viewing Policy Elements	188
Creating Policies	191
Modifying Policies and Rules	208
Managing FAM Policies and Rules	226
Managing GuardPoints	227
Secure Start GuardPoints	228
Considerations Before Creating GuardPoints	228
Creating GuardPoints	230
Creating Standard GuardPoints	230
Creating LDT GuardPoints	240
Creating Cloud Object Storage GuardPoints	250
Creating IDT GuardPoints	252
Creating Ransomware Protection GuardPoints	256
Enabling Secure Start for GuardPoints	259
Protecting Teradata Appliances	260
Automatic and Manual GuardPoints	260
Viewing GuardPoints	264
Viewing GuardPoint Status	266
Changing Designated Primary Set Connection	267
Changing SMB Connection	267

Removing GuardPoints	267
Disabling GuardPoints	270
Enabling GuardPoints	271
Enabling and Disabling MFA on GuardPoints	272
Managing Kubernetes Storage Groups and Clients	274
Managing Kubernetes Storage Groups	274
Managing Kubernetes Clients	278
Protecting Kubernetes Clients	281
Collecting Kubernetes Agent Information	284
Sharing Resources Across Domains	287
Multifactor Authentication	291
Communication with CipherTrust Manager	294
Communication Workflow with CipherTrust Manager Behind a Load Balancer	295
Configuring Cluster Node Preference	295
Backup and Restore	296
Integrating CTE Logging with Splunk	299
Migrating CTE Configuration from Data Security Manager	304
Migration Summary	309
Permissions	315
Quorum Control	330
Confidential Computing	335
Ransomware Protection	337
File Activity Monitoring (FAM)	340
Unique to Client Keys	340
Load Balancer	342
Operations	344
Certificate Renewal	352
Common Scenarios	358
Reports	366
Clients Health Report	368
Clients Keys Report	371
Clients Profiles Report	374
Clients Policies Report	377
Policies Keys Report	380
GuardPoints Report	383
Clients GuardPoint Status Report	386
Troubleshooting	388
API Examples	391
Creating Keys	391
Creating Policy Elements	399
Creating Policies	403
LDT Use Cases	408
Creating GuardPoints	414
API Response Codes	416
How to Configure the External CA for CTE	418

How to Change Local CA or External CA for CTE	420

CipherTrust Transparent Encryption (CTE)

This document describes the CipherTrust Manager interfaces to use CTE. The document explains the CTE concepts such as clients and client groups, signature sets, security rules, and GuardPoints. Next, the document describes how to manage clients and client groups, signature sets, security policies on the CipherTrust Manager. Finally, the document describes how to manage GuardPoints.

- It is assumed, for this document, that you have already configured the CipherTrust Manager appliance. Refer to the CipherTrust Manager product documentation for instructions.
- The next step is to activate and install the CTE license. Refer to [Licensing](#) for details.
- After the license is installed, you can configure CTE Agents. Refer to the [CTE Agent Quick Start Guide](#) specific to your platform for details. Installation of the CTE Agents is required for protecting directories and files stored on clients.

Organization

This document contains the following sections:

- [Overview](#): Provides a high-level overview of the CTE solution.
- [Interfaces](#): Provides an overview of the CipherTrust Manager interfaces—Command Line Interface (CLI), REST Application Programming Interface (REST API), and Graphical User Interface (GUI).
- [Concepts](#): Describes CTE concepts such as clients, client groups, GuardPoints, policies, and security rules.
- [Data Transformation](#): Provides an overview of the data transformation process.
- [Managing Profiles](#): Describes how to configure client log criteria, client Syslog settings, Quality of Service (QoS), multifactor authentication (MFA), ransomware protection (RWP), and server settings etc.
- [Managing Clients](#): Describes how to add, register, and manage clients on the CipherTrust Manager.
- [Managing LDT Communication Groups](#): Describes how to manage LDT communication groups on the CipherTrust Manager.
- [Managing Client Groups](#): Describes how to manage client groups on the CipherTrust Manager.
- [Managing Signature Sets](#): Describes how to create signature sets and how to sign and re-sign files in a signature set. The chapter also describes how to stop file signing and how to delete signatures and signature sets on the CipherTrust Manager.
- [Managing Policies](#): Describes rules and effects of security policies, and provides instructions to create, configure, import, and export security policies on the CipherTrust Manager.
- [Managing GuardPoints](#): Describes how to create, view, and delete GuardPoints on the CipherTrust Manager. The chapter provides information on automatic and manual GuardPoints and provides steps to configure

Windows network drives.

- **Managing Kubernetes Storage Groups and Clients:** Describes how to manage Kubernetes (K8s) storage groups, manage K8s clients, apply GuardPolicies to storage groups, and protect K8s clients.
- **Sharing Resources Across Domains:** Describes how to share CTE resources across CipherTrust Manager domains.
- **Multifactor Authentication:** Describes how Multifactor Authentication (MFA) works for CTE clients and GuardPoints.
- **Communication with CipherTrust Manager:** Describes how communication takes place between the CTE clients and CipherTrust Manager.
- **Configuring Cluster Node Preference:** Describes how to configure preferred nodes of a CipherTrust Manager cluster for sending status updates from CTE clients.
- **Backup and Restore:** Describes how to back up CTE policies and restore them to other CipherTrust Managers.
- **Integrating CTE Logging with Splunk:** Describes how to integrate the CTE audit logging with Splunk.
- **Migrating CTE Configuration from Data Security Manager:** Describes how to migrate CTE configuration from the DSM to the CipherTrust Manager.
- **Migration Summary:** Provides a summary of the CTE resources migrated from the DSM to CipherTrust Manager, mapping of the resources that are handled differently between the two key managers. Also, the section provides any constraints applicable to the migrated resources and describes how to interpret the migration status.
- **Migrating ProtectFile to CipherTrust Transparent Encryption:** Thales CipherTrust Transparent Encryption solutions provide state-of-the-art encryption solutions that cover all of the use cases for ProtectFile and other legacy applications. This guide helps you to migrate from ProtectFile and legacy applications, to CipherTrust Transparent Encryption or CipherTrust Transparent Encryption Userspace. The PFMigrate docs have been moved to their own site. This site contains the documentation for all use cases for PFMigrate.
- **Permissions:** Describes the complete permissions required to perform create, read, update, and delete operations on CTE resources.
- **Quorum Control:** Describes the quorum control for CTE operations and resources.
- **Confidential Computing:** Describes support for Confidential Computing with Intel Trust Domain Extensions (TDX) attestation.
- **Ransomware Protection:** Describes how to protect CTE clients from Ransomware.
- **Unique to Client Keys:** Describes how to make a key unique to a client.
- **Load Balancer:** Describes how to configure the load balancer for CTE on CipherTrust Manager.

-
- **Operations:** Describes the operations that the CTE Server Administrator performs on the CipherTrust Manager. These operations include registering CTE clients with the CipherTrust Manager, using external CA certificates, re-registering the clients, and protecting file system on a CTE client.
 - **Certificate Renewal:** Describes how the CTE clients are automatically notified of any changes in the client certificate or the web interface certificate.
 - **Common Scenarios:** Describes the common encryption scenarios in which the paths can be encrypted using the CTE solution.
 - **Reports:** Describes how to generate and download CTE reports.
 - **Troubleshooting:** Describes how to handle the issues that you might face when using CTE with the CipherTrust Manager.
 - **API Examples:** Provides examples to use CTE APIs to perform tasks such as decrypting LDT-protected GuardPoints.
 - **API Response Codes:** Describes the response codes returned by the CTE APIs with corresponding messages, and possible corrective actions to be taken for them.
 - **How to Configure the External CA for CTE:** Describes how to configure an external CA for CTE.
 - **How to Change Local CA or External CA for CTE:** Describes how to change a local or an external CA for CTE.

Overview

CTE protects data at rest, residing on Direct Attached Storage (DAS), Network Attached Storage (NAS), and Storage Area Networks (SAN). This can be a mapped drive or mounted disk, as well as through Universal Naming Convention paths.

CTE secures data with little impact to application performance. It requires no changes to your existing infrastructure and supports separation of duties between data owners, system administrators, and security administrators.

The CTE solution consists of two parts:

- The CTE Agent software that resides on each protected virtual or physical machine (client). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the CipherTrust Manager. The communication between the CTE Agent and the CipherTrust Manager is encrypted and secure.

The clients contain the directories and drives you want to protect. These clients can be onsite, in the cloud, or a hybrid of both.

- The CipherTrust Manager that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a client and register it with a CipherTrust Manager, you can use the CipherTrust Manager to specify which devices on the client you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

How CTE Protects Data

CTE uses policies created in the CipherTrust Manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your clients. These directories or devices are called GuardPoints. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of GuardPoints.

Policies specify:

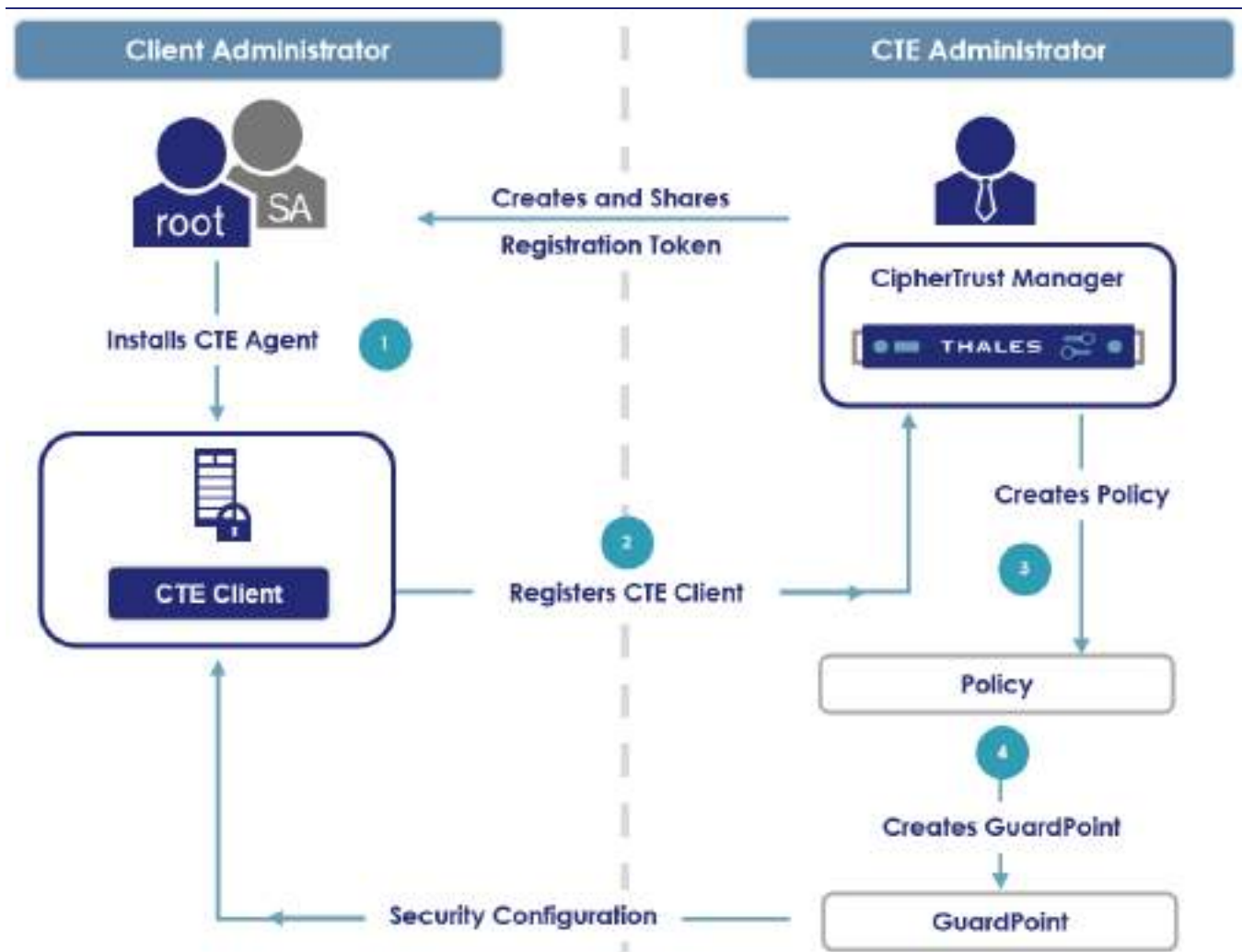
- Whether or not the resting files are encrypted.
- Who can access decrypted files.
- What level of file access auditing is applied when generating fine-grained audit trails.

A security administrator accesses the CipherTrust Manager through a web browser. You must have administrator privileges to create policies using the CipherTrust Manager. The CTE Agent then implements the policies once they are pushed to the client.

CTE can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

Workflow

The following diagram shows the basic flow of the CTE solution:



1. A client administrator installs the CTE Agent on the client machine. Refer to these sections in the [CTE Agent Quick Start Guide](#) for your platform:
 - [Installation Prerequisites](#)
 - [Installing and Registering CTE](#)

2. The client administrator registers the client with the CipherTrust Manager. Refer to the "Installing and Registering CTE" section in the [CTE Agent Quick Start Guide](#) for your platform:

A registration token is required to register the client with the CipherTrust Manager. The CTE administrator creates the registration token. Refer to [Creating a Registration Token](#) for details.

After successful registration, the client is added to the CipherTrust Manager. Alternatively, you can manually create a client on the CipherTrust Manager without registration, and register it later. Refer to [Adding Clients Manually](#) for details.

3. The CTE administrator identifies and creates a policy for the device or directory that specifies the access controls and the encryption keys to use for the device or directory. Refer to [Creating Policies](#) for details.

When creating the policy, the CTE administrator identifies and creates the encryption key that CTE will use to encrypt the data on the device or directory. Alternatively, encryption keys for CTE can be created on the Keys page of the CipherTrust Manager GUI. Refer to [Creating a New Key](#) for details.

4. The CTE administrator assigns a GuardPoint to the device or directory. When a GuardPoint is created, the security configuration is prepared and pushed to the CTE client. Refer to [Managing GuardPoints](#) for details.

The above workflow shows high-level and mandatory steps of the CTE solution. It is recommended to read related sections thoroughly (refer to [Organization](#)). These sections provide useful information to help you customize/configure the CTE solution to suit your requirements.

Interfaces

This section provides an overview of the CipherTrust Manager interfaces.

CLI

The CipherTrust Manager includes a CLI tool, named `ksctl`, that can be downloaded and run locally to control a remote CipherTrust Manager appliance. `ksctl` exclusively uses the REST API to communicate with the CipherTrust Manager, so anything that you can do with the tool, you can also do directly with the REST API. Conversely, `ksctl` exposes most of the functionality of the REST API. It can perform management functions, such as managing registration tokens and clients.

Note

`ksctl` is designed to be run from a remote system, not on the CipherTrust Manager itself.

To use the CLI:

1. Open the **CipherTrust Manager** URL in a browser.
2. Click the **API & CLI Documentation** link. The API playground is displayed.
3. At the top left, click **CLI Guide**. The CLI documentation is displayed.
4. At the top right, click the **CLI** download button. This downloads the **ksctl_images.zip** file.
5. Unzip the **ksctl_images.zip** file. The extracted files contain platform specific files. For example, the file for Windows is **ksctl-win-amd64**, and for Linux, the file is **ksctl-linux-amd64**.
6. Set up the `ksctl<os>` file for your system. Refer to the CipherTrust Manager CLI documentation for details.
7. Run `ksctl cte` to run CipherTrust Transparent Encryption specific commands.

Refer to the CipherTrust Manager documentation for details. For details on commands related to CipherTrust Transparent Encryption, refer to the online documentation of `ksctl cte`.

Authenticating to the Embedded API Guide

The embedded API Guide shares authentication with the CipherTrust Web UI. To authenticate to both the API Guide and the CipherTrust Web UI, visit `https://<ciphertrust_manager_IP_or_hostname>` in a web browser. Alternatively, click the **Log In** link in the top right corner of the API Guide when you are unauthenticated.

The simplest login is with a username and password. This authenticates a local user to the root domain. There can be additional login options to [authenticate to another domain](#), [authenticate with a certificate](#), [authenticate using LDAP](#), or [authenticate using OIDC](#). These options require additional user management configuration from a user in the User Admins group.

After login, the API Guide is accessible through the **API** button in the upper right corner.

There, you can make API calls in the established authentication context. You are logged out after 10 minutes of inactivity with the API Guide open. If you close the browser window, you are logged out after 30 minutes of your last login.

Manual API Token Generation for User Credentials

You can generate an API token with a user's username and password for a given domain, outside of the embedded API guide. This is useful if you have created a custom REST API client.

To copy and paste the following example commands, set an environment variable to point to your CipherTrust Manager instance:

```
$ export KSCTL_URL=https://{addr}          # sh/bash
$ set -x KSCTL_URL=https://{addr}         # fish
```

For example, this command will use the root admin's credentials to create an API token:

```
$ curl -k -X POST $KSCTL_URL/api/v1/auth/tokens/ \
  -H "Content-Type: application/json" \
  -d '{"name":"admin","password":"admin"}'
```

Note

By default, this command creates a token for the root domain. You can specify a [child domain](#) to log in to with `'{"name":"domain_user","password":"domain_user_password","domain":"domain_name"}'`

The response:

```
{
  "jwt": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJkMzEzZjJ0ZlNy1hN2ZlLTQ1YzEtOWU1OS0zYmUxNTRkMTZjYmQiLCJpc3MiOiJreWxvIiwiaWF0IjoiYXNja3lsbyIsImN1c3QiOi0nsiZ3JvdXBzIjpbImFkbWwluI191LCJpYXQiOiJ0e00DExMjQxMzcsImV4cCI6Ij00MTQ4MTEyNDQzN30.Z9GU0Yy0ImHmdPmbZx66vL0NLQfeLvNGkyGkZpVbfx4",
  "duration": 300
}
```

```
}
```

Copy the value of the `jwt` property into another environment variable:

```
(sh) $ export KSCTL_JWT=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdwQiOiJkMzEzYzcwZS01NmYyLTQ5MTU0OGJkNy01ZmMyYmUyNzk2YzEiLCJzdwIiOiJsb2Nhbmh4Im2ZjOGZlNy1hN2ZlLTQ1YzEtOWU1OS0zYmUxNTRkMTZjYmQiLCJpc3MiOiJreWxvIiwiaWVhbnJlIjoia3lsbyIsImN1c3QiOi0nsiZ3JvdXBzIjpbImFkbWluIl19LCJpYXQiOiJE00DEXMjQxMzcsImV4cCI6MTQ4MTEyNDQzN30.Z9GU0Yy0ImHMDPmbZx66vL0NLQfeLvNGkyGkZpVbfx4
(fish)$ set -x KSCTL_JWT eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdwQiOiJkMzEzYzcwZS01NmYyLTQ5MTU0OGJkNy01ZmMyYmUyNzk2YzEiLCJzdwIiOiJsb2Nhbmh4Im2ZjOGZlNy1hN2ZlLTQ1YzEtOWU1OS0zYmUxNTRkMTZjYmQiLCJpc3MiOiJreWxvIiwiaWVhbnJlIjoia3lsbyIsImN1c3QiOi0nsiZ3JvdXBzIjpbImFkbWluIl19LCJpYXQiOiJE00DEXMjQxMzcsImV4cCI6MTQ4MTEyNDQzN30.Z9GU0Yy0ImHMDPmbZx66vL0NLQfeLvNGkyGkZpVbfx4
```

Using the `jq` tool, we can fetch, extract, and export the token in a single shell command:

```
(sh) $ export KSCTL_JWT=$(curl -k -X POST $KSCTL_URL/api/v1/auth/tokens/ \
-H "Content-Type: application/json" \
-d '{"name":"admin","password":"admin"}' | jq -r '.jwt')
(fish)$ set -x KSCTL_JWT (curl -k -X POST $KSCTL_URL/api/v1/auth/tokens/ \
-H "Content-Type: application/json" \
-d '{"name":"admin","password":"admin"}' | jq -r '.jwt')
```

We can use that API token to make other calls:

```
$ curl -k "$KSCTL_URL/api/v1/vault/keys2?limit=20" \
-H "Authorization: Bearer $KSCTL_JWT"
```

Making an API Call

To make an API call, find the API in the left pane and click it. In the right pane, specify the required parameters, and click an appropriate button (for example, **POST**, **GET**, **DELETE**, or **Curl**). For example, to create a CTE policy on CipherTrust Manager:

1. In the left pane of the API playground, click **CTE/Policies**.
2. Under **cte/policies**, click **Create**. The Create section of the API playground is displayed in the right pane.
3. In the **body** field, specify required parameters with their values, as shown below.

```
{
  "name": "TestPolicy",
  "policy_type": "Standard",
  "never_deny": false,
  "security_rules": [
    {
```

```

        "effect": "permit",
        "action": "all_ops",
        "partial_match": false,
        "resource_set_id": "TestResourceSet",
        "exclude_resource_set": true
    }
]
}

```

Expand **schema** under the **body** field for names and types of fields. Hover your mouse over each field to view its description. The parameter names and casing in the **body** field must match with those shown in the schema. Also, ensure that parameters and their values are specified in double quotes.

4. Click **POST**.

Alternatively, to get an equivalent `curl` command, click the **Curl** button. The `curl` equivalent will be shown in the text field below. Use the `curl` tool to run the command to make the REST API call.

Similarly, all API calls can be made by referring to the schema shown in the playground.

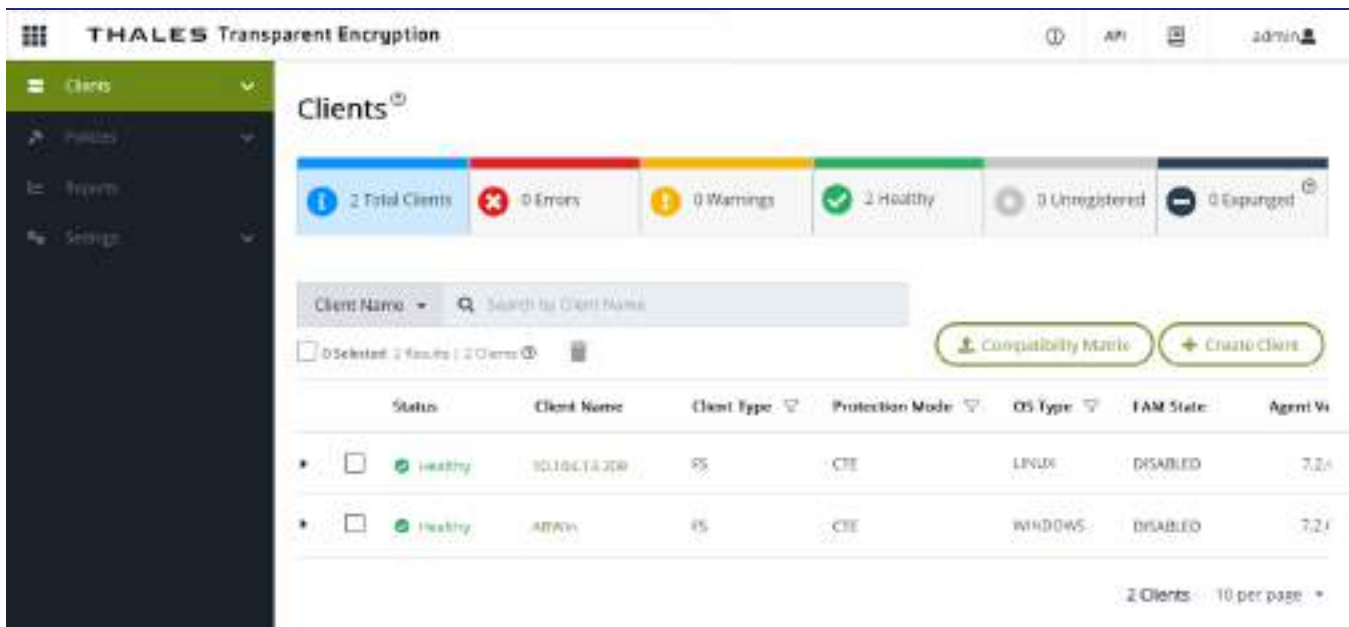
GUI

Use the CipherTrust Manager's GUI (also called the Management Console) to perform management functions such as managing profiles, policies, clients and client groups, and GuardPoints. These functions can also be performed using the CLI tool or the REST API.

To use the GUI:

1. Open the **CipherTrust Manager** URL in a browser.
2. Enter **Username** and **Password**.
3. Click **Log In**. By default, the Products page is displayed.
4. Click **Transparent Encryption** to open the application.

The Clients page of the Transparent Encryption GUI is displayed, as shown below.



The main components of a Transparent Encryption GUI are:

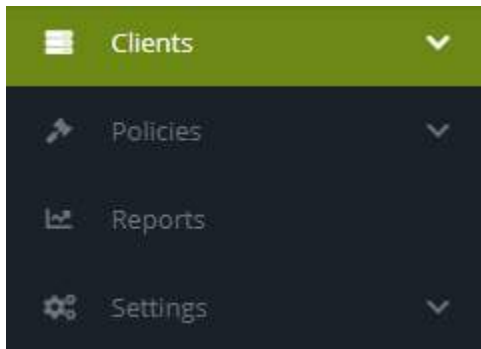
- Header
- Left Pane
- Page
- Notifications

Header

Element	Description
	App switcher. Click to view and switch to another application such as Access Management and Admin Settings .
THALES	Thales logo.
Transparent Encryption	Application name. For CTE, Transparent Encryption is displayed.
	Version and Server Info icon. Click to view the name, appliance name, and version of the CipherTrust Manager.
API	Link to the API playground.
	Link to the CipherTrust Manager product documentation.
admin	Logged in user. Click to switch domains, view and update user settings (Email address and password), and log out.

Left Pane

Contains links to manage CTE resources - clients, policies, reports, and settings etc.



Element	Description
Clients	Click to manage clients and client groups. The Clients page is the displayed by default. Refer to Managing Clients and Managing Client Groups for details.
Policies	Click to manage policies and policy elements—resource sets, user sets, process sets, and signature sets. Refer to Managing Policies for details.
Reports	Click to manage reports. Refer to Reports for details.
Settings	Click to manage settings such as profiles. Refer to Managing Profiles for details.

Page

A page is the main working area that provides options to manage CTE resources. Depending on the selected option in the left pane, the page shows different types of information. These options are described in this document, where appropriate.

At any time, a page can either be in the list view or in the edit view. A sample screenshot of the list view of the Clients page is shown below. Most pages follow the similar pattern except that they show different content based on the resource being managed.

Client Name Search by Client Name

☐ 0 Selected 2 Results | 2 Clients

[Compatibility Matrix](#) [+ Create Client](#)

	Status	Client Name	Client Type	Protection Mode	OS Type	FAM State	Agent Ver
	☐ Healthy	10.154.13.209	FS	CTE	LINUX	DISABLED	7.2.1
	☐ Healthy	AGWin	FS	CTE	WINDOWS	DISABLED	7.2.1

2 Clients 10 per page

The sample page shown above can be divided into the following elements:

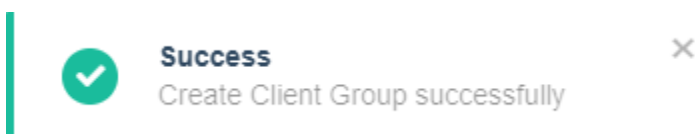
Element	Description
Title	Shows the page name.
Status bar	Shows the total number of clients added to the CipherTrust Manager, the number of clients with errors, warnings, healthy state. The status bar also shows the number of unregistered and expunged clients on the CipherTrust Manager. The status bar also acts as a filter. Click a health status to see the list of clients with that status.
Search box (Search)	Filters clients based on their partial or full names. Search is case-insensitive.
List	Shows the clients based on the selected health status. By default, all the clients added to the CipherTrust Manager are displayed.
Compatibility Matrix button	Provides an option to upload the kernel compatibility matrix.
Create Client button	Provides an option to add a new client even before a CTE Agent is installed on it.
Delete icon ()	Deletes the selected clients. A message is prompted to confirm the action.
Check box (☐)	Provides an option to select a client for deletion or modification. Multiple clients can be selected to perform the delete operation on them. Use the check box provided just under the Search box to select all clients visible on the page.
Expand icon ()	Shows mini detail view of a client in the clients list.
Custom View icon ()	Hides/shows optional columns. For example, click this icon on the Clients page shows:

Element	Description
	 ☒ Status ☒ OS type ☒ Kernel Version ☒ Agent Version ☒ Description ☐ Encryption Modes ☐ Upgrade On Reboot OK Reset Select or clear the desired column and click OK.
Overflow icon ()	Shows additional options. Depending on the current state of a client, the options can vary.
Pagination	Helps configure the number of records to display. By default, 10 records per page are displayed. 
Tooltip icon()	Shows the basic description about an element when the mouse pointer is moved over the tooltip icon. Click the Learn More link in the tooltip to view the related documentation.

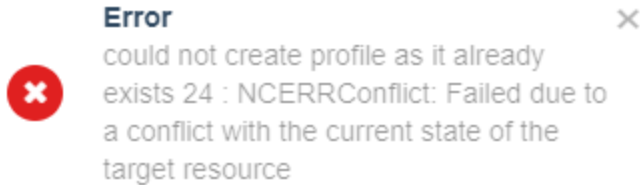
Notifications

CTE prompts toast notifications at the top right corner of the main page area. These notifications are shown when operations such as creation or deletion of an entity is performed.

Green success toast notifications are displayed for successful operations.



Red error notifications are displayed for failed operations.



Concepts

This section describes important concepts for CTE.

Clients

A client is a computer system where the data needs to be protected. A compatible CTE Agent software is installed on the client. The CTE Agent can protect data on the client or devices connected to it. A client can be associated with multiple GuardPoints for encryption of various paths (refer to [Managing GuardPoints](#) for details).

CTE also supports Kubernetes (K8s) clients. Refer to [Kubernetes Clients](#).

Client Groups

A client group is used to group one or more clients to simplify configuration and administration. GuardPoints created on a client group are applied to all members of the group. Additionally, you can apply client group configuration settings to all clients in a client group. A client can be a member of multiple client groups.

If you have created a group of one type of clients, then you should only add similar clients to the group. Same configuration settings can only be applied to clients of the type with which the client group is created. If a different type of client is added, configuration settings cannot be applied to that client.

Refer to [Managing GuardPoints](#) for details on creating GuardPoints on client groups.

Kubernetes Clients

Unlike a traditional CTE Agent, a Kubernetes (K8s) client runs as a K8s pod. Multiple pods can run on a single K8s node. Every pod protects the K8s persistent volumes attached to it using a CTE for Kubernetes policy received from the CipherTrust Manager.

The name of a K8s client is a combination of:

- The node on which the K8s client is running
- The linked K8s StorageClass
- The namespace where the K8s client pod runs
- A random string attached automatically

So, the format of K8s client name is `<node-name>_<csi-storage-class>_<csi-namespace>_<random-string>`, for example, `node1_K8sStorageClass1_K8sNamespace1_f2eaa752`.

Kubernetes Storage Groups

A Kubernetes (K8s) storage group is a logical group of multiple K8s clients with the same K8s namespace and K8s StorageClass. The group helps simplify K8s configuration and administration across K8s clients. GuardPolicies created on a storage group are applied to all members of the group.

A K8s client can be a member of one storage group only.

GuardPoints

A GuardPoint specifies the list of folders that contains paths to be protected. Access to files and encryption of files under the GuardPoint is controlled by security policies.

Refer to [Managing GuardPoints](#) for details.

GuardPolicies

A GuardPolicy, which is similar to a CTE GuardPoint, can be attached to a K8s storage group only. It is inherited by the K8s clients attached to the storage group.

Only the policies of type [CTE for Kubernetes](#) can be included in a K8s GuardPolicy. As CTE for K8s protects a volume not a specific path, the GuardPath is automatically set to the CTE for Kubernetes policy name prefixed with a slash (/).

Policies

A policy is a collection of rules that govern data access and encryption. Think of a policy as an if-then statement. Policy rules are processed sequentially. If the criteria of rule one are not met, the policy enforcement engine moves on to the second rule and so on.

Policies specify:

- **Actors:** Users, groups, and processes that are permitted/denied access to protected data.
- **Actions:** What actions authorized actors are allowed to perform. For example create/delete, read/write, decrypt, modify permissions, and so on.
- **Files acted upon:** Policy rules may apply to entire directories and mount points, or only to files named in a specific way (for example, .docx files may be encrypted and restricted to read-only access by designated users, while other files may be stored clear and read and written by anyone).

Additionally, each CTE policy specifies one or more encryption keys used to encrypt blocks of file data when applications write them, and decrypt them when they are read.

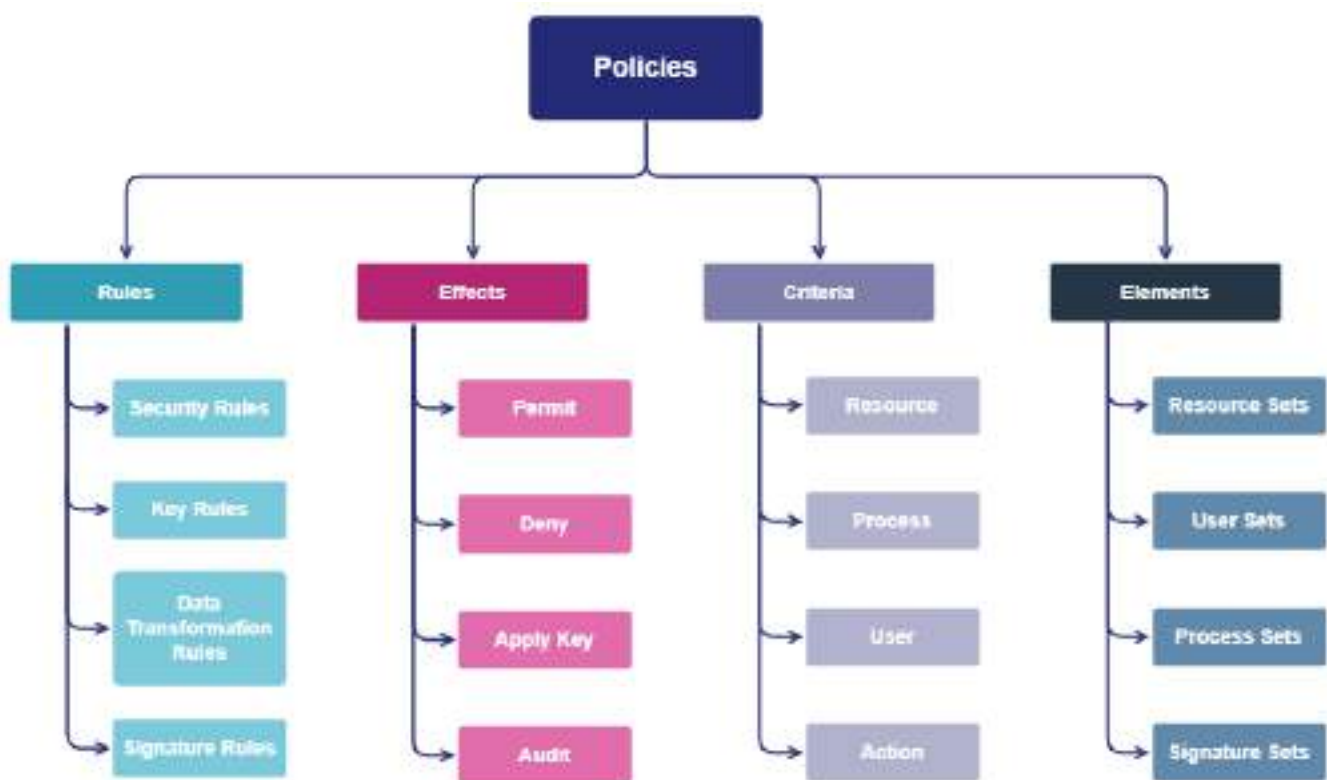
CTE encryption is transparent to applications. This means that the CTE Agent encrypts blocks of data as they are written, and decrypts data when they are read by authorized users and applications. This architecture separates administration of files from access to the data in them. Backup programs, for example, may be authorized to read files, but not view the data in them. Therefore, data can be backed up and taken offsite while remaining encrypted so that security is not breached.

A policy comprises Security Rules, Key Rules, and Data Transformation Rules.

CTE supports the following policy types:

- **Standard:** Access to data is blocked during initial encryption or rekeying of data.
- **Live Data Transformation (LDT):** Encryption and rekeying of data takes place in the background, without disrupting user or application access to that data.
- **Cloud Object Storage (COS):** Applicable to GuardPoints in Amazon S3 buckets. Access to data is blocked during initial encryption or rekeying of data.
- **In-place Data Transformation (IDT):** Access to data is blocked during encryption or rekeying of data. This policy type is needed for creating GuardPoints for Teradata clusters.
- **CTE for Kubernetes:** Applicable to GuardPolicies for CTE for Kubernetes clients. Access to data is blocked during initial encryption or rekeying of data.

The following diagram shows the main components of a policy:



Refer to [Managing Policies](#) for details.

Security Rules

A security rule defines:

- Who can access the data (User or Group)
- What they can do with the data (Action)
- What applications or executables have access to the data (Process)

- Where the data is located (Resource)
- How the data can be accessed (Effect)
- Whether it can be enforced on the subdirectories of the GuardPoint (Browsing)

Security Rule Criteria

Security rules consist of five criteria. They specify the attributes of an access attempt, and effects, which define whether that access is permitted or denied, and whether encryption/decryption is required. The following table lists policy rule criteria.

Criteria	Description
Resource	Specifies which files and/or directories in a GuardPoint are to be protected. For example, /secure_dir/financials.
User	Specifies a which users or groups of users can access the files.
Process	Specifies executables that can operate on the files.
Action	Specifies the allowed file action. Action could be read, write, remove, rename, and make directory. Refer to Actions for the complete list of supported actions.
Effect	Describes the type of access granted or denied according to the rule. Refer to Security Rule Effects for the list of supported effects.

Actions

An action is an attempt to access protected data in some way. Action specifies the type of file and directory action (read, write, delete, and rename etc.) allowed on a GuardPoint. A policy provides a wide range of access methods to specify the action required for the security rule. The action is identified, evaluated, and used as a factor in determining whether or not to grant access. Specifying an access method is optional. If you do not specify one, the policy defaults to **all_ops**, or "all operations".

Any action that starts with **d_** applies to directories. Any action that starts with **f_** applies to files. Only a few actions are available for COS and IDT policies.

The following table lists all basic and advanced actions:

Basic Actions

Action	Description	Policy Types
all_ops	All operations. Users can access the data using any method. all_ops is the default action (when no action is specified).	All
read	Read operations. This is a collection of actions related to reading files, directories, and their	Standard, IDT, LDT

Action	Description	Policy Types
	attributes. The read action comprises f_rd , f_rd_attr , f_rd_sec , d_rd , d_rd_attr , and d_rd_sec .	
write	Write operations. This is a collection of actions related to writing to files, directories, and their attributes. The write action comprises f_wr , f_cre , f_ren , f_rm , f_link , f_chg_attr , f_chg_sec , d_ren , d_chg_attr , d_chg_sec , d_mkdir , and d_rmdir .	Standard, IDT, LDT
key_op	Key operations. It requires <i>two</i> keys. One key is specified on the Add Security Rules screen and the other on the Add Data Transformation Rules screen. The encryption keys for the <i>current</i> security rule are specified on the Add Security Rules screen. The keys to migrate data from an encrypted form to a non-encrypted form or to change the encryption keys used to access the data are specified on the Data Transformation Rules screen.	Standard, LDT

Advanced Actions

Action	Description	Policy Types
f_rd	Read a file.	Standard, LDT, COS
f_wr	Write to an existing file.	Standard, LDT, COS
f_wr_app	Append data to a file.	Standard, LDT
f_cre	Create a new file.	Standard, LDT
f_ren	Rename a file.	Standard, LDT
f_link	Link to a file (for example, <code>ln file_name link_name</code>).	Standard, LDT
f_rm	Remove/delete a file.	Standard, LDT, COS
f_rd_attr	Read the attributes of a file (for example, <code>ls -l file</code>).	Standard, LDT
f_chg_attr	Change file attributes (for example, <code>chmod</code>).	Standard, LDT
f_rd_sec	View the security properties of a file.	Standard, LDT

Action	Description	Policy Types
f_chg_sec	Change any security property of a file.	Standard, LDT
d_rd	View directory contents (for example, <code>ls dir; cd dir</code>).	Standard, LDT, COS
d_ren	Rename a directory (for example, <code>mv dir1 dir2</code>).	Standard, LDT
d_rd_att	Read the attributes of a directory (for example, <code>ls -la dir1</code>).	Standard, LDT
d_chg_att	Change directory attributes (for example, <code>chown usr dir1</code>).	Standard, LDT
d_rd_sec	View the security properties of a directory.	Standard, LDT
d_chg_sec	Change any security property of a directory.	Standard, LDT
d_mkdir	Make a new directory.	Standard, LDT
d_rmdir	Delete a directory (for example, <code>rm -r dir1</code>).	Standard, LDT

Security Rule Effects

An effect describes the type of access granted or denied according to the rule. The following table lists policy effects that can be applied to GuardPoints.

Effect	Description
Permit	Allows access attempts to the resource. For example, you can specify an effect that allows writing to a directory.
Deny	Denies access attempts to the resource. For example, you can specify an effect that denies any attempts to access a resource.
ApplyKey	Applies an encryption key to the data in a GuardPoint. When applied, the data copied to the GuardPoint is encrypted with the specified key. When the data in the GuardPoint is accessed, it is decrypted using the same key.
Audit	Creates a message log entry for each qualifying event that records who is accessing what information and when.

How Security Policy Works

Every time a user's application tries to access a GuardPoint file, the security policy tests that access attempt against the criteria of each rule. For example, suppose a user, Harry, wants to access and modify a file called secret, using the command `cp`. For Harry to be successful, there must be a rule that allows access to secret (resource), by user Harry (user), using the command `cp` (process), and includes the permission write (action).

-
- If criteria is not specified, a value of All is used.
 - If resource is not specified, the rule applies to all resources.
 - If user is not specified, the rule applies to all users.
 - If process is not specified, the rules apply to all executables, and so on.
 - Effect cannot be left unspecified. It must have at least a permit (allow access) or deny (disallow access).

A policy can have multiple rules. Rules are evaluated much like firewall rules. They are evaluated in order, from first to last. Evaluation stops when a rule is found for which all the criteria are met. The effect for that rule is then enforced. Therefore, you must carefully order a policy's rules to achieve the desired result.

Resource Sets

A resource is a combination of a directory, a file, and patterns or special variables. A resource set is a named collection of directories, files, or both, that a user or process will be permitted or denied access to.

Refer to [Creating Resource Sets](#) for details on creating resource sets.

User Sets

A user set is a collection of users and user groups that you want to grant or deny access to GuardPoints. User sets are configured in policies. Policies can be applied to user sets, not to individual users.

Refer to [Creating User Sets](#) for details on creating user sets.

Signature Sets

A signature set is a collection of hashes of processes and executables that you want to grant or deny access to GuardPoints. A signature set can be configured in a policy as part of a process set to verify the integrity of a process before it is allowed access to guarded data. Policies are applied to signature sets, not to individual signatures.

A cryptographic hash is created for each file in a signature set that meets a specific criterion. It would take longer, bloat the CipherTrust Manager database, and reduce performance to sign all the files in a signature set, especially when the set comprises top-level directories. The criteria is listed below. All other files are skipped.

Executables accessing a GuardPoint can be inside or outside the GuardPoint. If they are inside:

- On a Windows client, all files in a signature set that are inside a GuardPoint are signed. Only the compiled Windows executables in the signature set that are outside the GuardPoint are signed. Non-executables outside the GuardPoint are not signed.
- On a UNIX client, it makes no difference whether the files are inside or outside a GuardPoint. Only the files in a signature set with one or more execute bits set (for example, `-rwxrwxrwx-`) are signed.
- File extension has no impact. Even files like the following are skipped:
 - [On Windows] `.bat` and Visual Basic programs if they are not inside a GuardPoint

- [On Linux] `.so` files if they do not have an execute bit set

Every instance of a file that is copied to a different location or to a different name will have the same signature. This can be a convenient way to detect duplicate files on your system.

By default, a generic error message is displayed about a non-existent source being detected. The name of the offending file or directory is not specified. However, it is specified in the Agent log on the client. Review the logs to:

- Identify the offending file or directory.
- Determine how many files were affected, what file "is invalid for the signature request".
- Identify the files that were not signed. Look for files with "is invalid for the signature request".

Refer to [Managing Signature Sets](#) for details on the signing process.

Process Sets

A process set is a collection of processes (executables) that you want to grant/deny access to GuardPoints or exempt from RWP monitoring. Like user sets, process sets can be configured in policies. Policies can be applied to process sets, not to individual processes.

In a process set, you can also specify processes with and without signatures and directories to be exempted from RWP monitoring. This process set can be used as a Trusted Process Set in the [Ransomware Protection Configuration](#).

Optionally, file signing can be configured to check the authenticity and integrity of executables and applications before they are allowed to access GuardPoint data. A signature set must already exist before you can configure file signing in a policy for a process set.

Refer to [Creating Process Sets](#) for details on creating process sets.

Key Rules

A key rule defines the encryption key to apply to a specific resource set or the encryption key to use as the default key, if no other key rule matches. The key rule defines the sequence in which the key rules are to be executed (Order), the location of the data to be encrypted (Resource), and the encryption key to be applied to the resource set (Key).

When defining a key rule for an LDT policy, you can select a key that is applied to the resource set (Current Key Name) and the key to use to rekey that resource set (Transformation Key Name).

Note

Keys are created and stored on a CipherTrust Manager appliance.

Data Transformation Rules

Data transformation rules define:

-
- Resources to be protected
 - Symmetric encryption key to use for
 - Rekeying the specified resources from one encryption key to a different key or
 - Rekeying resources into a plaintext format (also referred to as clear, unencrypted, or decrypted)

Signature Rules

A signature rule is a type of signature sets that contains container image signatures. Signature rules can only be associated with CTE for Kubernetes policies.

Profiles

A profile contains the CipherTrust Manager logging criteria for CTE clients, Syslog server configuration, default logging level, LDT Quality of Service (QoS) settings, and other settings that can be used for several CTE clients.

A default profile, **DefaultClientProfile**, is created automatically when either of the following happens:

- On successful registration of the first client if no profile is specified during registration.
- On creation of the first client group. A new client group is automatically linked to **DefaultClientProfile**.

When registering a CTE client, the installer prompts to specify a profile for the client. If not specified, **DefaultClientProfile** is automatically linked to the client on successful registration. The linked profile can be modified later.

Tip

It is recommended to not delete or modify **DefaultClientProfile**.

Refer to [Managing Profiles](#).

Learn Mode

Learn Mode permits a policy to be tested without actually denying access to the GuardPoint. In Learn Mode, all actions that would have been denied are instead permitted, but logged. This allows you to test policies by tracking how rules are evaluated, without enforcing the policy. Monitor the log to determine how data is being accessed, then modify the policy accordingly.

In Learn Mode:

- If the policy contains a security rule with the effect permission Permit and the effect option ApplyKey, then a security rule with the permission Deny MUST include the option ApplyKey. If it does not include the option ApplyKey, a user with the Deny permission can overwrite or edit data, which can corrupt the data.
- Effect permission Deny has the same effect as Permit, and Deny ApplyKey has the same effect as Permit

ApplyKey.

This option generates an ERROR log every time an access attempt is made that matches any security rule in the policy. The ERROR log is labeled [LEARN MODE] and can be viewed in the CTE Agent logs or under Records on the CipherTrust Manager GUI (if the log level is configured as ERROR).

Learn Mode is recommended for policies that restrict applications (process sets). Many applications use multiple binaries that may not be known to the creator of the policy at the time of creation. So, Learn Mode should be enabled when creating policies for such applications.

Note

Use Learn Mode to analyze access patterns and make informed decisions about final encryption policies. Do not keep Learn Mode running for long time.

User Roles

CTE has the [CTE Admins](#) and [CTE Clients](#) users with different responsibilities in administering and using the system.

Caution

It is critical that credentials of these users are kept in a secure location. If a credential is compromised, an attacker could gain access to sensitive data.

Note

Additionally, the CipherTrust Manager provides an option to create customized groups for CTE to control permissions on CTE resources. Refer to [Customized Groups for CTE](#) for details.

CTE Admins

Initially, there is a System Defined Group named "CTE Admins". Users within the "CTE Admins" group are CTE Administrators.

A CTE Administrator is responsible for creating and managing the following resources:

- Clients and client groups
- Profiles, policy elements, and policies
- GuardPoints
- Client registration tokens (with additional rights of System Defined Group named "Client Admins")

Note

Only the users of the "CTE Admins" group can delete CTE keys.

CTE Clients

There is a System Defined Group named "CTE Clients". CTE clients registered with the CipherTrust Manager are part of this group.

Cluster Node Preference

A CTE administrator can configure preferred nodes of a CipherTrust Manager cluster for sending status updates from CTE clients. The administrator assigns a priority to every node of the cluster.

The cluster nodes can be categorized into tiers on the CipherTrust Manager GUI, with every tier assigned a priority. For example, Tier 1 is assigned higher priority than Tier 2. All tiers (for example, Tier 1 + Tier 2) can have a total of 20 nodes. This preference is configured through server settings in profiles. If not configured, the CipherTrust Manager continues working with the default settings. Refer to [Communication with CipherTrust Manager](#) for the default behavior.

After the server settings are configured, the CTE clients associated with the profile first try to send status updates to the top tier. If none of the nodes in the tier is reachable, the CTE clients try to send updates to the next tier.

This feature is applicable to the CipherTrust Manager clusters.

Multifactor Authentication

In Multifactor Authentication (MFA), access to the requested data is granted only after the requester satisfies two or more authentication criteria.

CTE adds an extra layer of security before granting access to the protected GuardPoints. If MFA is enabled, the users performing specific tasks on the configured GuardPoints need to perform an additional OpenID Connect (OIDC) based authentication.

MFA can be helpful in scenarios such as when the credentials of a client machine are compromised. As an additional level of authentication is enforced, the data security cannot be breached.

Refer to [Multifactor Authentication](#) for details.

Data Transformation

This section provides an overview of the data transformation process. It covers the following information:

- The Data Transformation Process
- Data Transformation Techniques
- Protection Policies

The Data Transformation Process

Data transformation is the process of transforming GuardPoint data from:

- Plaintext (clear) to encrypted with a key
- Encrypted with a key to plaintext
- Encrypted with one (old) key to encrypted with another (new) key

Tip

Refer to [CTE Agent Data Transformation](#) for detailed instructions on how to use CTE on clients to transform GuardPoint data from clear text to encrypted text or from encrypted text to clear text.

This section covers the following information:

- Uses of Data Transformation
- How CTE Protects Files
- Components of the CTE Solution
- Properties of Data Transformation

Uses of Data Transformation

- **Initial Data transformation:** Encrypting GuardPoint data for the first time.
- **Rekeying:** Changing the encryption key for GuardPoint data, also called key rotation.
- **Reverse Transformation:** Decrypting GuardPoint data to clear text (not a common procedure).
- **Convert:** Non-LDT GuardPoints to LDT GuardPoints.

Note

Data transformation is complex and disruptive to data center operations. It is strongly recommended that you read and understand this section before you proceed to the initial data transformation and rekey.

How CTE Protects Files

The CTE Agent encrypts the data within a file one block at a time. It does not encrypt file metadata such as a file's name or size. This enables administrators to manage files without being able to view or modify their contents. Whether initially encrypting files, rekeying them, or decrypting them, the CTE Agent must therefore:

-
- **Read** each block of file data to be transformed.
 - **Transform** the block by encrypting, decrypting, or rekeying it.
 - **Write** the transformed block, either to its original location, or to an alternate one.

Components of the CTE Solution

CTE protects data either at the file level or at the storage device level. CTE file-level protection consists of two main components:

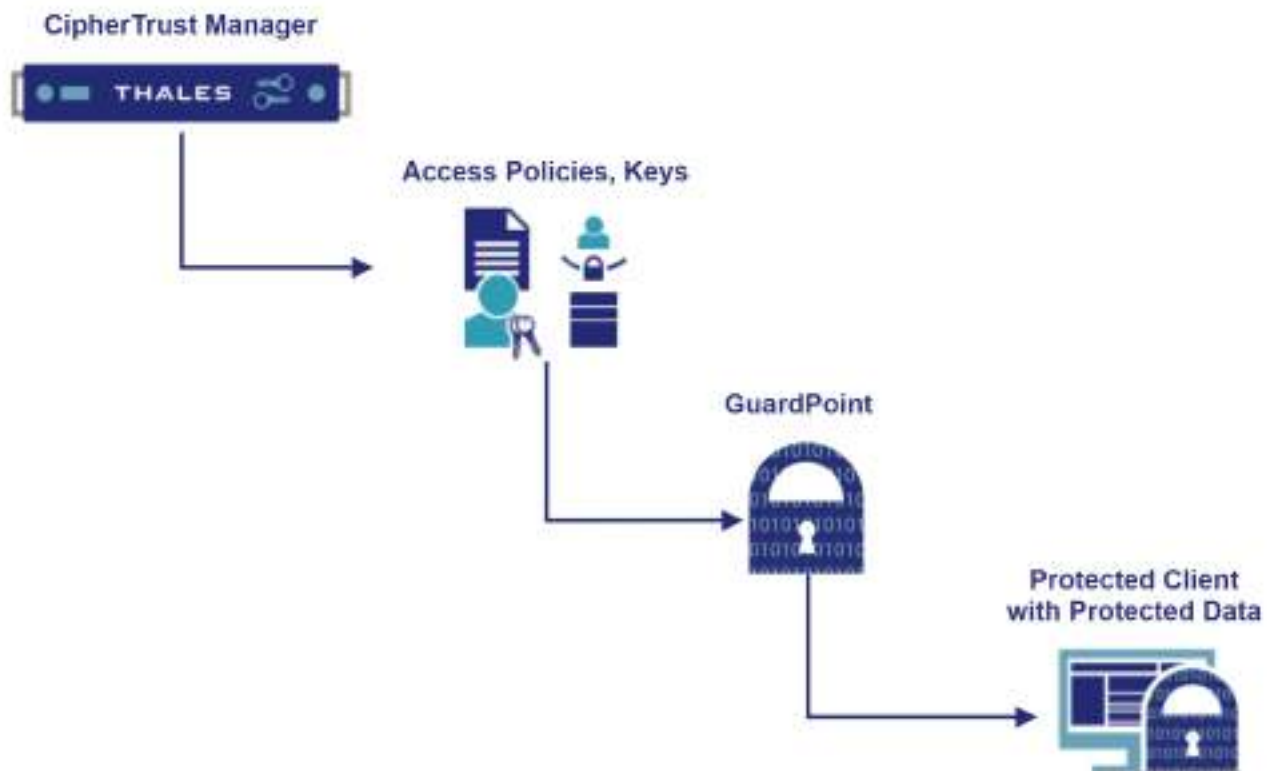
- **CipherTrust Manager**

An appliance that manages a database of the file sets protected by CTE GuardPoints, the encryption keys that protect them, policies that specify access rights and encryption protections that can be applied to GuardPoints. The CipherTrust Manager is also a central point for logging events related to accessing protected files.

- **CTE Agents**

Software components that run on clients with file sets to be protected. A CTE Agent manages the files behind a GuardPoint by enforcing the policy associated with it, and communicates data access events to the CipherTrust Manager for logging.

A GuardPoint is usually associated with a Linux mount point or a Windows volume, but may also be associated with a directory subtree. The CTE Agent sits between applications and the file system that clients files within the GuardPoint. It intercepts every file access request, and enforces the access and encryption rules defined in the GuardPoint's policy.



Properties of Data Transformation

For large file sets (hundreds of GBs or more), bulk transformation is time-consuming. Managing transformation time is important, because file set content must be frozen (inaccessible to applications) throughout the transformation process. Once transformation starts, it must continue until complete. So transformation time determines the window of data unavailability. Two major components contribute to transformation time:

- **Number of Blocks of File Data**

Because CTE must read, transform, and rewrite each block of file data, this component can be estimated by multiplying the number of file blocks to be transformed by the average read, transformation, and write time for a block.

- **Number of Files**

Because the CTE Agent transforms data file by file, each file must be "looked up," opened, and closed during transformation, using underlying file system mechanisms. This typically requires multiple disk accesses. Therefore, file sets that consist of many small files, per file overhead, can actually exceed file block transformation time.

Other factors, such as file system fragmentation, and load from concurrent applications, may also affect transformation time. Mainly, the number of blocks and number of files to be transformed are fundamental because they cannot be reduced or eliminated.

Data Transformation Techniques

Three methods to initially encrypt and rekey files are:

- **The Copy/Restore Method:** Using the operating system file copy utility, the client administrator can copy unprotected files to a location protected by a CTE GuardPoint with a standard/production policy.
- **The CTE Dataxform Utility Method:** Every CTE Agent includes a utility program that can encrypt or transform protected files. The `dataxform` utility encrypts, rekeys, or decrypts data in-place. Refer to the [CTE Agent Data Transformation](#) for details.
- **The Live Data Transformation (LDT):** The CipherTrust Manager Security Administrators can encrypt or rekey GuardPoint data without blocking the user or application access to that data. Refer to the [CTE-Live Data Transformation](#) with CipherTrust Manager for details.

These methods have advantages and limitations that make them suitable in different scenarios. These are discussed in the subsequent sections.

Apart from encrypting data, you can reverse the transformation, that is, decrypt the data to plaintext. To decrypt protected files, copy them to an unprotected location.

Note

CTE can also be configured to protect data at the disk level. For data protected in this way, only the copy transformation technique is available for encryption.

The Copy Method

Properties of the Copy Method

The copy method performs initial encryption, rekeying, and decryption by copying data from one directory, or GuardPoint, to another directory or GuardPoint.

- **Initial Encryption**

The client administrator encrypts a file set by copying it to a directory protected by a CTE GuardPoint with a standard policy. Encryption is transparent to the copy utility.



- **Rekeying Protected Data**

Encrypted files protected by a CTE GuardPoint are rekeyed by copying them to a directory protected by another GuardPoint with a different encryption key. Both decryption and re-encryption are transparent to copy utilities.



- **Decrypting Data by Copying**

Decrypt a protected file set by copying files from their protected location to unprotected directories. The CTE Agent decrypts file blocks before delivery to the copy utility for rewriting.



Caution

If the governing policy does not authorize the copy utility user to access data, CTE delivers encrypted file blocks to it.

Advantages of the Copy Method

- **Simplicity**

After an Agent is installed and GuardPoints are activated on a client, the client's administrator can encrypt, decrypt, or rekey file sets simply by copying them from one location to another. There are no procedures to learn, and no requirements to coordinate with the CipherTrust Manager Security Administrator. Data transformation is simply another routine administrative task.

- **Recoverability**

If a copy-based transformation is interrupted, for example, by a power failure or a system crash, the transformation resumes at or prior to the point of interruption. This is because the source files remain available and can be recopied, overwriting files at the destination that may have been only partially re-encrypted.

Limitations of the Copy Method

- **Storage Resource Consumption**

Copying a file set requires that both source and destination files exist simultaneously. Storage capacity sufficient for both must be available during initial encryption. For very large protected data sets, "extra" temporary storage may be a significant expense. However, a greater concern is likely to be the impact of moving production file sets as they are transformed. File data is unprotected while in the copy utility's buffers.

- **Impact on Operating Procedures**

Original and copied file sets have different path names and/or network addresses. After transformation, either both file sets must be renamed (the old path to a new name, and the new path to the old name), or applications must be adapted to process the transformed data set at the new directory. For a small data center with a few protected file sets, some combination of these options is usually practical. For data centers with hundreds of protected file sets, the administrative complexity and consequent chance of error make copying a complex option.

The Restore Method

A variation of the copy method is to make a backup of the files for transformation and restore the backup to the destination location. This works because:

- Backing up data causes it to be read and decrypted.

- Restoring data causes it to be written (re-encrypting it with an alternative key).
- CTE protection is transparent to backup programs.

This technique also creates a backup of the data set. However, a disadvantage is the time required to copy data twice (once from the source location to backup, and once from backup to destination location).

These considerations suggest that copying data to transform it is more suitable for initial encryption (and final decryption), and less so for rekeying. Additionally, the simplicity of recovering an interrupted transformation makes the copy/restore method useful in situations where the probability of interruption during transformation is significant.

The Datasform Utility Method

The **datasform** utility transforms data-in-place and contains two components:

- User mode that controls the overall operation
- Kernel mode that transforms files block-by-block



Advantages of the Datasform Utility

Transforming data in place has two advantages:

- **Minimal Storage Requirements**

Because the **datasform** utility transforms files in place, where they reside, it does not require temporary file storage. However, the utility does need storage in which to create a list of files for transformation.

▪ Security

The period of time that the data transformed by the **dataxform** utility appears in memory, outside the GuardPoint and therefore, unprotected, is shorter than with copying. This is significant for rekeying (compared to copying), which holds clear file data in memory between reading and rewriting. Moreover, **dataxform** requires coordination between the client and CipherTrust Manager Security Administrators, so that no one individual can subvert security during transformation.

Limitations of the Dataxform Utility

Offsetting the advantages of the **dataxform** utility method is the complexity of recovering from an interrupted **dataxform** run. Because **dataxform** transforms files in-place, data in a file undergoing transformation at the time of a failure may be only partly transformed. There is no way to determine which blocks have been transformed and which have not. These files must be recreated after the **dataxform** utility runs from a backup copy. The client administrator must:

1. Determine (by examining the **dataxform** logs) which files may have been incompletely transformed.
2. Delete them from the transformed file set.
3. Recreate them by selective copying from a backup.

Live Data Transformation

The CipherTrust Manager security administrators can encrypt or rekey the GuardPoint data without blocking the user or application access to that data.

After enabling GuardPoints, LDT performs initial encryption or rekeying in the background, unnoticed by users. The data stays live and available. This accelerates CTE deployments and eliminates the need to block application and user access to data during encryption or rekey operations, which can seriously inconvenience users and affect operational efficiency.

Phases of LDT runtime operation:

1. Initial data transformation starts or key expires

Live Data Transformation begins when an LDT policy is first applied to a GuardPoint, or when a current key version expires. The CipherTrust Manager pushes the new policy, or the notification of a key version change, to the clients that are protected by those policies.

2. New key version triggers a rekey on the affected GuardPoints

On each client, CTE determines which GuardPoints are using the key that has just rotated to a new version. CTE starts an LDT rekey on each of those GuardPoints. (If another rekey is already underway on that GuardPoint, the new rekey is rejected).

3. Scan for files

On each GuardPoint where CTE has started a rekey, LDT determines which files to transform. LDT takes inventory of files encrypted with earlier versions of the rotated key and makes a persistent list of the files for transformation. During this phase, the rekey status of the GuardPoint becomes starting, then scanning.

The scan phase might be interrupted, such as by a client reboot. In this case, when the client reboots and the GuardPoint is enabled again, the scan operation starts over from the beginning.

4. Rekey/Key Rotation

- a. Each file, from the persistent list of files, is decrypted using the old version of the key. The old key is applied to each file and then re-encrypted using the new version of the key. Note that new files created during the LDT process do not need to be rekeyed, as they inherit the new version of the key. Multiple files and multiple regions of files are rekeyed simultaneously.
- b. The LDT extended attribute of each file is updated.
- c. The LDT rekey operation can be suspended and resumed manually, or through the QoS schedule.

This manages the impact LDT has on other applications and processes. During this phase, the rekey status of the GuardPoint is rekeying or suspended.

If system errors occur during rekeying, such as IO errors or crashes, LDT can manage and recover from them after the system error is fixed.

5. Finish

When all of the required files in the GuardPoint have been rekeyed, the system and storage resources used by LDT are released, except for the storage required for the extended attributes. Upon completion of rekey, the rekey status of the GuardPoint is rekeyed.

Summary

The following table summarizes the strengths and weaknesses of the two file set transformation methods.

Factor	Copy Method	The dataxform Utility Method	Live Data Transformation
Temporary storage required	Equal to size of file set.	Sufficient to hold a list of path names of files in file set.	Additional space is required to store LDT metadata only.
Security	File data is unprotected while in copy utility's buffers.	File data is never outside the CTE GuardPoint.	File data is never outside the CTE GuardPoint.
Initial encryption	Files can be copied directly from source directory to a CTE-protected directory.	Files must be in a protected location before transformation.	Files must be in a protected location before transformation.
Operational impact	No access to files during transformation. Path names or operating procedures must be adjusted after transformation.	No access to files during transformation.	No other impact on operating procedures.
Recoverability	Restart copy operation at,	Files undergoing	Transformation process

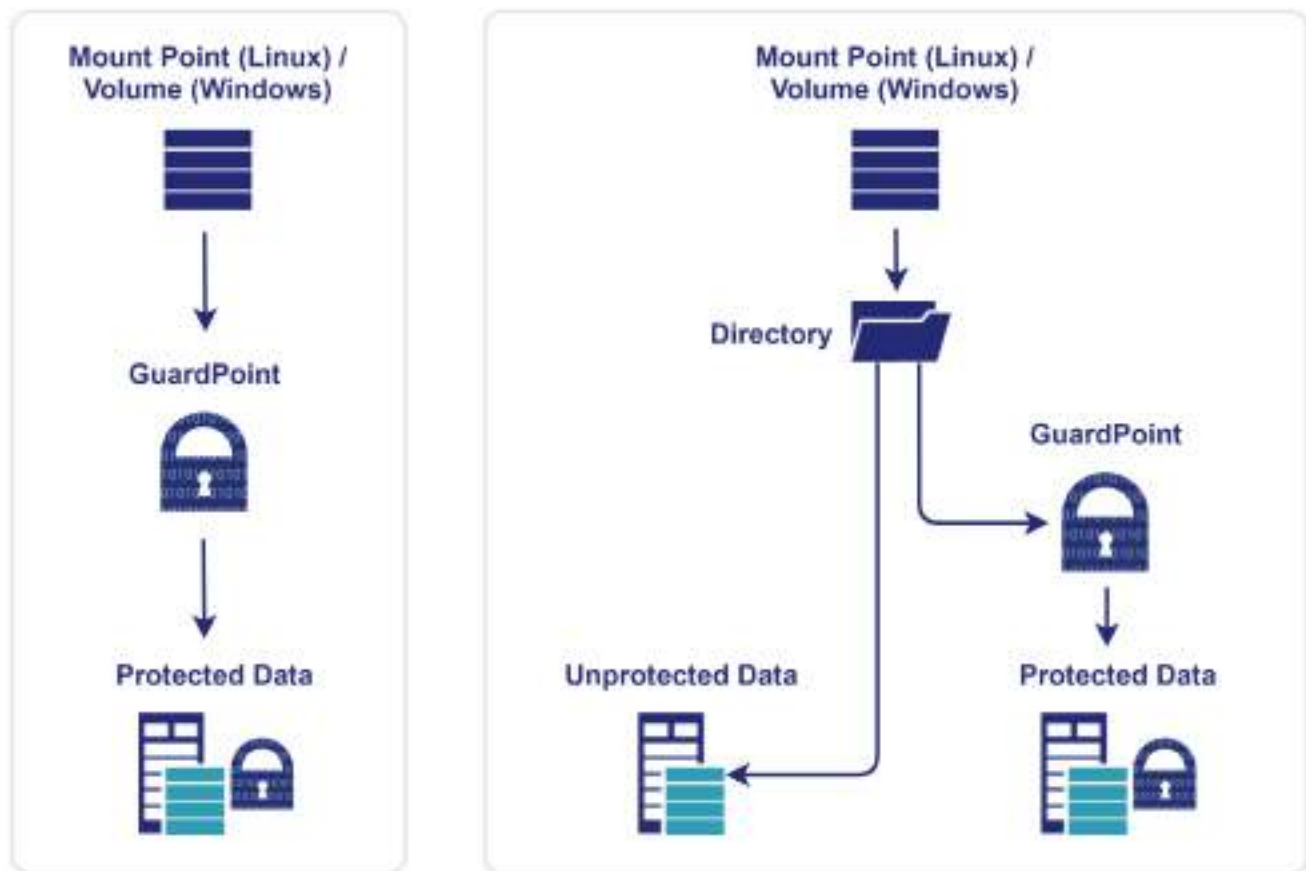
Factor	Copy Method	The dataxform Utility Method	Live Data Transformation
	or prior to, point of failure.	transformation at the point of failure must be discovered from the dataxform logs and restored from backup.	automatically restarts from the point of failure.

Protection Policies

The basic unit of CTE data protection policy application is the GuardPoint. GuardPoints are typically associated with file system mount points, but may also be associated with directory sub-trees.

Note

Nested mount points within a directory, or mount points protected by a GuardPoint, are also protected in Linux environments.



All files in the directory hierarchy, below a GuardPoint, are subject to the GuardPoint's policy, which consists of rules that specify:

-
- **Protected files:** Filenames or filename patterns (example: *.dat) to which the policy applies.
 - **Authorized users:** User(s) group(s), and application(s) permitted to access the protected files.
 - **Permissions:** Actions permitted to users (example: create/delete, read/write, rename, decrypt).

Policies also specify the name of an encryption algorithm and a key for encrypting protected files. For example, a policy might specify that all Excel workbooks protected by a GuardPoint be encrypted using an AES256 key called EXCEL-KEY. Additionally, only users in group 128 have access to the files. All other files that are not encrypted, are freely accessible to all users.

Types of Policies

CTE Agents use two types of policies:

- **Initial Data Transformation**

The data transformation policies contain the elements listed above, plus a data transformation key, used by the `dataxform` utility to rekey file data. Transformation policies contain strict access control rules that prevent application and user access to files during transformation. CTE only uses the data transformation policies for the initial transformation. Afterwards, you replace it with a production policy.

The `dataxform` utility operates on a per-GuardPoint basis. For initial encryption, the data transformation policy specifies a clear production key (meaning that the utility does not decrypt data because the data is unencrypted) and a new data transformation key to encrypt the data.

- **Production/Standard**

Production policies contain the elements listed above. They protect data within GuardPoint(s) during day-to-day IT operations.

For decryption, the policy specifies a clear data transformation key (that is, the utility does not re-encrypt files as it rewrites them) and the current production key.

A rekeying transformation policy specifies both a current production ("old") key and a transformation ("new") key.

Managing Profiles

A profile contains the CipherTrust Manager logging criteria for CTE clients, Syslog server configuration, default logging level, LDT Quality of Service (QoS) settings, server settings, Multifactor Authentication (MFA) settings, Ransomware protection settings, and additional settings that can be used for several CTE clients.

A default profile, `DefaultClientProfile`, is created automatically when either of the following happens:

- On successful registration of the first client if no profile is specified during registration.
- On creation of the first client group. A new client group is automatically linked to `DefaultClientProfile`.

When registering a CTE client, the installer prompts to specify a profile for the client. If not specified, `DefaultClientProfile` is automatically linked to the client on successful registration. The linked profile can be modified later. It is recommended to not delete or modify `DefaultClientProfile`.

Creating a Profile

After you have created a profile, you can define client logging criteria, Syslog configurations, QoS configurations, Ransomware protection settings, MFA configurations, and server settings. These configurations apply to the clients and client groups linked to this profile. Refer to the subsequent sections for details.

Create a profile in WebUI

To create a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Click **Create Profile**.
4. Specify a unique **Name** for the profile. This is a mandatory field.
5. Provide a **Description** for the profile.
6. Click **Create**.

The newly created profile appears in the profiles list.

Profiles

Search			
☐ 0 selected 3 results 3 Profiles  + Create Profile			
	Name	Description	
☐	TestProfile	Test profile	...
☐	DefaultClientProfile		...
☐	abc		...

Create a profile in ksctl CLI

You can create a profile as a CTE Administrator in the ksctl CLI. The only required setting is a profile name, `--cte-profile-name`. Consult the embedded CLI Guide for full description of options.

You can label a client profile dedicated to **FAM**, using the parameter `labels "ncryptify-reserved/dsf-managed": "true"`.

Example command to create a profile dedicated to FAM:

```
ksctl cte profiles create --cte-profile-name FAMprofile --labels "ncryptify-reserved/dsf-managed": "true"
```

Setting Client Log Configuration

Client log configuration includes basic information such as the level of logs to capture, whether to enable the Syslog server, settings to upload logs to the CipherTrust Manager, and settings to store logs on clients.

To define client log configurations for a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile. The edit view of the profile is displayed. Profile settings are divided into three categories, as shown below:

Expand All	
CLIENT LOGGING CONFIGURATION	+
CLIENT SYSLOG CONFIGURATION	+
QUALITY OF SERVICE CONFIGURATION	+
RANSOMWARE PROTECTION CONFIGURATION	+
MULTIFACTOR AUTHENTICATION	+
SERVER SETTINGS	+

4. Click **CLIENT LOGGING CONFIGURATION** to expand it. The client log configuration settings are categorized into basic, log upload to key manager, and log to the file on the clients.

Log Level	ERROR	☐ Log Upload to Key Manager	☒ Log to File
Duplications	SUPPRESS	Upload Log Level	ERROR
Threshold (1-100)	5	Connection Timeout (sec) 1-60	75
Suppress interval (sec) 1-1000	600	☐ Drop if Busy	Max File Size (1-1000 MB)
☐ Enable Concise Logging		Upload Timeout (sec) 1-900	600
☐ Syslog Enabled		Max Interval (sec) 1-1000	20
		Min interval (sec) 1-30	10
		Message Upload Range (100-1000)	1000
		Cache Settings	
		Max Files	100
		Max Space (MB)	100
		☐ Allow Purge	Max Old Files (1-100)
			100

Basic Settings

5. Specify the basic settings:

Field	Description
Log Level	Level of logs to generate. It defines the detail and extent of information to be logged by the linked agents. In sequence, the options are: • DEBUG: Fine-grained informational events that are targeted towards support engineers and developers. • INFO: Informational messages that highlight the progress of the application at coarse- grained level. • WARN: Potentially harmful situations. • ERROR: Error events that might still allow the application to continue running. This is the default log level. • FATAL: Severe error events that will presumably lead the application to abort. Log levels are cumulative. The level that you select not only generates log entries for events that occur at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.
Duplicates	Treatment for duplicate logs. The options are: • SUPPRESS: Messages follow the configured Threshold as to how many times duplicate messages are sent to the CipherTrust Manager during the given

Field	Description
	Interval. • ALLOW : All duplicate messages are captured and displayed in the log.
Threshold (1-100)	(Used when the Duplicates field is set to SUPPRESS .) Maximum number of duplicate messages the CTE Agent can send to the CipherTrust Manager within the time specified by Suppress Interval (see below). The default value is 5 messages.
Suppress Interval (sec) 1-1000	(Used when the Duplicates field is set to SUPPRESS .) Time in which the number of duplicate messages, specified by Threshold, can be uploaded to the CipherTrust Manager. When Suppress Interval exceeds, the count specified by Threshold starts again. The default interval is 600 seconds (10 minutes).
Enable Concise Logging	Whether to enable Concise Logging for the linked clients. Select to enable, clear to disable. By default, Concise Logging is disabled. When enabled, a reduced number of audit log messages are captured. Refer to Concise Logging for details.
Syslog Enabled	Whether the Syslog server is enabled. Select to enable, clear to disable. When you select Syslog Enabled , make sure that client Syslog configurations are defined. Refer to Setting Client Syslog Configuration for details. When the Syslog server is disabled, the logs are sent to the client messages file such as <code>/var/adm/messages</code> . On a Windows client, the messages are sent to the Event Viewer (Application events).

Log Upload Settings

6. Configure settings to upload logs to the CipherTrust Manager:

Field	Description
Log Upload to Key Manager	Whether to enable log upload to the CipherTrust Manager. Select to enable, clear to disable. When this option is selected, you can configure the settings

Field	Description
	listed below. The logs are displayed under the Client Records page of the CipherTrust Manager GUI.
Upload Log Level	Level of logs to upload. In sequence, the options are: • DEBUG: Fine-grained informational events that are targeted towards support engineers and developers. • INFO: Informational messages that highlight the progress of the application at coarse- grained level. • WARN: Potentially harmful situations. • ERROR: Error events that might still allow the application to continue running. This is the default log level. • FATAL: Severe error events that will presumably lead the application to abort. Log levels are cumulative. The level that you select not only generates log entries for events that occur at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.
Connection Timeout (sec) 1-60	Interval after which the connection attempt to the key manager expires. The default value is 59 seconds.
Drop if Busy	Whether to slow log generation and drop log files during periods of extreme logging (that is, when the server is busy). Select to drop, clear to keep trying. This setting is clear by default.
Upload Timeout (sec) 1-900	Interval after which the log upload attempt expires. The default period is 600 seconds (10 minutes).
Max Interval (sec) 1-1000	Maximum interval to wait before the CTE Agent can upload messages to the CipherTrust Manager. Use this option to update the log viewer even when the Message Upload Range has not been reached. Lower the interval if there is little CTE Agent activity. The default maximum interval is 20 seconds.
Min Interval (sec) 1-30	Minimum interval to wait before the CTE Agent can upload messages to the CipherTrust Manager. Increase the interval if there is considerable CTE Agent activity, so the agents do not flood the network with log messages. The minimum interval is 10 seconds.

Field	Description
Message Upload Range (100-1000)	Maximum number of logs to upload at one time. When the specified number of logs is reached, they are uploaded to the CipherTrust Manager. The default number is 1000 .
Cache Settings	Settings to cache logs. The options are: • Max Files: Maximum number of log files to cache. The default number is 200. • Max Space (MB): Maximum log size to cache. The default value is 100 MB.

Log to File Settings

7. Configure settings to gather logs in files on clients:

Field	Description
Log to File	Whether to write logs to files on clients. This option is selected by default. This means that, by default, the logs are written to files on clients. The logs are sent to the <code>/var/log/vormetric/vorvmd_root.log</code> file of a UNIX client, or a Windows equivalent, such as <code>\Documents and Settings\All Users or WINDOWS\Application\ Data\Vormetric\DataSecurityExpert\agent\log\vorvmd.log</code> . When the Log to File option is selected, you can configure the settings listed below.
File Log Level	Level of logs to capture in the log file. In sequence, the options are: • DEBUG: Fine-grained informational events that are targeted towards support engineers and developers. • INFO: Informational messages that highlight the progress of the application at coarse- grained level. • WARN: Potentially harmful situations. • ERROR: Error events that might still allow the application to continue running. This is the default log level. • FATAL: Severe error events that will presumably lead the application to abort. Log levels are cumulative. The level that you select not only generates log entries for events that occur

Field	Description
	at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.
Max File Size (1-1000 MB)	Maximum size of a log file. The CTE Agent starts a new, empty log file when the specified limit is exceeded. The default maximum file size is 1000 MB.
Max Old Files (1-100)	The maximum number of old log files to keep. The default number is 100 .
Allow Purge	Whether to allow purging the old log files. Select to allow purge, clear to disallow. This option works in conjunction with the Max Old Files option (see above). For example, set Max Old Files to 3 and select the Allow Purge check box. After 3 log files are generated, the first log file, log1, is deleted and a new log file, log4, is created. If the Allow Purge check box is clear, log files continue to accumulate in the server database and you have to remove them manually.

8. Click **Update**.

The changes are effective immediately and apply to the clients linked with the profile.

The CTE client logs can be seen on the **Records > Client Records** page of the CipherTrust Manager GUI. Filter the records by **Client Type** and look for the **CTE** records, as shown below.

Client	Client Type	Timestamp	Severity	Event	Details
364859	CTE	Aug 31st 2020 - 13:04:08	ERROR	RedGridPath NotExist	<pre>{ "log": "CGA", "uid": "CGA21345", "pid": 1213, "args": [{ "go": "/Non-Existent-Path" }], "message": "Not guarding path [/Non-Existent-Path] (Reason: Exec not exist)", "version": "7.0.0.50", "filename": "SetFS_upload_3.04.05.0.140", "hostname": "3.04.05.0", "client_id": "79cb51d0-25c2-4fed-8e88-c0720c7f3163" }</pre>

Refer to [Records](#) for details.

Setting Client Syslog Configuration

When you have Syslog servers up and running in your environment, you can redirect your client logs to them. A CipherTrust Manager administrator can configure profiles to redirect client logs to Syslog servers.

To configure Syslog settings in a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **CLIENT SYSLOG CONFIGURATION**.

Log Level
ERROR

☐ Local

Server 1

Hostname or IP:

Port:

Message Format: RFC5424

Protocol: TCP

[Clear](#)

Server 2

Hostname or IP:

Port:

Message Format: RFC5424

Protocol: TCP

[Clear](#)

[Show Additional Servers](#)

5. Specify the following details:

Note

- You can configure up to four servers, labeled as **Server 1**, **Server 2**, **Server 3**, and **Server 4**. By default, **Server 1** and **Server 2** are visible. To view **Server 3** and **Server 4**, click **Show Additional Servers**.
- This document describes steps to configure one server, **Server 1**. Extend the steps to suit your setup requirements.

Field	Description
Log Level	Level of logs to redirect. In sequence, the options are: • DEBUG: Fine-grained informational events that are targeted towards support engineers and developers. • INFO: Informational messages that highlight the progress of the application at coarse- grained level. • WARN: Potentially harmful situations. • ERROR: Error events that might still allow the application to continue running. This is the default log level. • FATAL: Severe error events that will presumably

Field	Description
	lead the application to abort. Log levels are cumulative. The level that you select not only generates log entries for events that occur at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.
Local	Whether logs are sent to the client. If selected, the logs are saved on the client at <code>/var/log/messages</code> . By default, the option is clear.
Server 1	
Hostname or IP	Hostname or IP address of the Syslog server.
Port	Port of the Syslog server.
Message Format	Format in which the log messages are transferred to the Syslog server. The options are: • Plain Message • CEF • RFC5424 • LEEF The default log format is RFC5424. This format adheres to the Syslog Protocol RFC 5424 guidelines.
Protocol	Transport protocol for the Syslog connection. The options are UDP, TCP, and TLS. The default protocol is TCP. When you select TLS, the following fields appear: • CA Certificate: Click Browse to select the CA certificate. • Certificate: Click Browse to select the certificate. • Private Key: Click Browse to select the private key.

6. Click **Update**.

The Syslog server settings are configured.

Setting Quality of Service Configuration

The QoS configuration settings apply to clients that have the LDT feature enabled on them. Administrators use these settings to maintain operational efficiencies in their systems in conjunction with LDT operations. They can specify percentage of CPU usage or a rekey rate and schedules for LDT operations. Refer to the [CTE-Live Data Transformation](#) with CipherTrust Manager for best practices about using LDT and QoS.

A CipherTrust Manager administrator can configure LDT QoS on the CipherTrust Manager.

To configure LDT QoS settings in a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **QUALITY OF SERVICE CONFIGURATION**.

☒ Rekey by Rate
 ☐ Rekey by CPU

LDT QoS Rekey Rate (MB/s)

☐ Cap CPU Allocation

CPU Percentage

LDT Status Check Rate (In minutes) ?

QoS Schedules

LDT QoS Schedule:

ANYTIME
 ▼

Create New QoS Schedule

Name	Time Ranges
ANYTIME	Sunday 12:00 AM - Saturday 11:59 PM

5. Specify the rekey option. The options are:

- **Rekey by Rate:** Select to rekey by rate (in MB/s). This is the default setting. Specify the LDT QoS Rekey Rate. The default value is 0.
- **Rekey by CPU:** Select to rekey by CPU usage. By default, LDT operations use all of the available CPU memory.

Optionally, you can reserve percentage of the clients' CPU for LDT rekey operations. To do so:

- a. Select **Cap CPU Allocation**. The **CPU Percentage** field becomes editable.
- b. Enter the **CPU Percentage**. The value must be greater than 0.

- **LDT Status Check Rate:** Select the frequency to check and update the LDT status on the CipherTrust

Manager. The valid value ranges from 10 to 1440 minutes. The default value is 60 minutes.

6. Specify a QoS schedule to run LDT. Under **QoS Schedules**, select an **LDT QoS Schedule**. The options are:

Name	Time Ranges	Description
ANYTIME	Sunday 12:00 AM - Saturday 11:59 PM	LDT runs any day at any time of the week
WEEKNIGHTS	Monday 12:00 AM - Monday 07:00 AM Monday 09:00 PM - Tuesday 07:00 AM Tuesday 09:00 PM - Wednesday 07:00 AM Wednesday 09:00 PM - Thursday 07:00 AM Thursday 09:00 PM - Friday 07:00 AM Friday 09:00 PM - Friday 11:59 PM	LDT runs between midnight to 7:00 AM from Monday to Friday
WEEKENDS	Sunday 12:00 AM - Monday 07:00 AM Friday 09:00 PM - Saturday 11:59 PM	LDT runs between 9:00 PM Friday to 7:00 AM on Monday
CUSTOM	< Custom Range >	LDT runs at a custom schedule (described below)

Creating a Custom LDT Schedule

To create a custom LDT schedule:

- a. Select **CUSTOM** from the **LDT QoS Schedule** drop-down list. Now, the **Create New QoS Schedule** button is available.

The screenshot shows the 'QoS Schedules' configuration area. Under 'LDT QoS Schedule', the 'CUSTOM' option is selected in a dropdown menu. To the right, a blue button labeled 'Create New QoS Schedule' is visible. Below these, there are two input fields: 'Name' and 'Time Ranges', each with a placeholder text and a small icon.

- b. Click **Create New QoS Schedule**. The Create QoS Schedule dialog box is displayed.

Create QoS Schedule



Starting Day:

Ending Day:

Starting Time: :

Ending Time: :

- Select the **Starting Day**. The LDT process will start on this day of the week. The default starting day is Monday.
 - Specify the **Starting Time** in the **HH:MM AM/PM** format. Use the arrows to select time in hours (1 to 11) and minutes (00 to 59). Select AM or PM from the drop-down list. The default starting time is **1:00 AM**.
 - Select the **Ending Day**. The LDT process will end on this day of the week. The default ending day is Monday.
 - Specify the **Ending Time** in the **HH:MM AM/PM** format. The default ending time is **2:00 AM**.
- Click **Create**. The custom LDT QoS schedule is displayed on the screen. The specified Time Ranges are also displayed.

QoS Schedules

LDT QoS Schedule:

CUSTOM

Create New QoS Schedule

Name

Time Ranges

CUSTOM

Monday 1:00 AM - Friday 3:00 AM

...

- Click **Update**. The configuration is saved successfully.

Note

- To create a new custom schedule, click Create New QoS Schedule.
- To delete a custom schedule, click Delete corresponding to the schedule you want to delete.

Setting Ransomware Protection Configuration

Common Ransomware Protection settings for clients and client groups is configured in profiles. In the profile,

specify the process set to be excluded from monitoring and the action to be taken on all other processes that attempt to access the sensitive data. You can also disable the Ransomware Protection for all GuardPoints on the linked clients from a profile.

To configure Ransomware Protection settings in a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **RANSOMWARE PROTECTION CONFIGURATION**.

RANSOMWARE PROTECTION CONFIGURATION

Trusted Process Set?

Select process set

Select

Operation

Block

Update

5. Specify the Ransomware Protection configuration.
 - a. Next to **Trusted Process Set**, click **Select**. The Select Process Set dialog box shows the list of available process sets.
 - a. Select the process set to be *excluded from monitoring*.
 - b. Click **Select**. The CTE Agent will ignore the processes in the selected process set. All other process sets will be monitored for suspicious behavior.
 - b. Select the **Operation** to be performed on the monitored processes. The available operations are:
 - **Block**: Logs an audit message that a suspicious activity has been detected, and **blocks** its access to the sensitive data. This is the default setting.
 - **Monitor**: Logs an audit message that a suspicious activity has been detected, and **allows** the activity on the sensitive data.
 - **Disable**: Disables Ransomware Protection for all GuardPoints on the clients linked with this profile.

Note

- When you change the operation to **Disable** in a profile, Ransomware Protection for all GuardPoints on the linked clients is disabled.
- When you change the *profile* of a client to another profile with the operation set to **Disable**, Ransomware Protection for all GuardPoints on the client is disabled.

- c. Enable the **Alarm** on clients linked with the profile.

Note

If Ransomware is detected, an [alarm](#) and a [record](#) will be generated on CipherTrust Manager.

- d. Click **Update**.

Setting MFA Configuration

Common MFA configuration for clients and client groups is configured in profiles. When the security configuration for a client is built, the MFA configuration is fetched from the associated profile.

To set up MFA configuration, specify an OIDC connection and the set of exempted users. MFA will not be enforced for users in the exempted user set. By default, MFA is enforced for all users of the associated clients.

To configure MFA settings in a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **MULTIFACTOR AUTHENTICATION**.

MULTIFACTOR AUTHENTICATION



Select OIDC Connection:

Select OIDC Connection



Select MFA Exempted User Set:

Select Userset



i The selected user set will be exempted from MFA enforcement. MFA will not be enforced on the users of this set.

Update

5. Specify the MFA configuration.

- **Select OIDC Connection** from the drop-down list. This is the OIDC connection over which MFA configurations will be enforced. OIDC connections are created on the CipherTrust Manager. Refer to [Connection Manager](#) for details.
- **Select MFA Exempted User Set** from the drop-down list. This user set will be exempted from MFA. MFA will not be enforced on the users of this set.

Note

- A CipherTrust Manager administrator with sufficient privileges can delete an OIDC connection being used by a profile. When an in-use OIDC connection is deleted, the security configuration for the associated clients cannot be built and pushed to the clients. The errors are logged in audit records. The CTE Agent continues working with the current configuration until the connection is restored.
- You can delete the existing OIDC connection and MFA Exempted User set by clicking **Delete (X)**.

6. Click **Update**.

Configuring Server Settings

A CTE administrator can configure preferred nodes of a CipherTrust Manager cluster for sending status updates from CTE clients. The administrator assigns a priority to every node of the cluster.

The cluster nodes can be categorized into tiers on the CipherTrust Manager GUI, with every tier assigned a priority. For example, Tier 1 is assigned higher priority than Tier 2. All tiers (for example, Tier 1 + Tier 2) can have a total of 20 nodes. This preference is configured through server settings in profiles. If not configured, the CipherTrust Manager continues working with the default settings. Refer to [Communication with CipherTrust Manager](#) for the default behavior.

After the server settings are configured, the CTE clients associated with the profile first try to send status updates to the top tier. If none of the nodes in the tier is reachable, the CTE clients try to send updates to the next tier.

To configure the cluster node preference in a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **SERVER SETTINGS**.
5. Click **Configure Settings**.

Before proceeding, make sure the CipherTrust Manager is part of a cluster. Refer to [Clusters and Nodes](#) for information on CipherTrust Manager clusters and nodes.

When the CipherTrust Manager is part of a cluster, the Server Settings section displays cluster nodes grouped into tiers.

6. Add/modify cluster node preference as appropriate.
 - To add/modify the priority of a cluster node, drag it from one tier and drop to another. Alternatively, click the add button () in the target tier and select the node from the displayed list.
 - To remove a node from a tier:
 - a. Click the delete icon () in the node name. A message box appears prompting to confirm the action.
 - b. Click **Yes** to confirm.

The change will be effective only after you click **Update** in the SERVER SETTINGS section of the Profiles page.

- To add a new tier, click **Add Another Tier**. By default, one tier is visible. You can set preference for all nodes of a CipherTrust Manager cluster.

A maximum of 20 tiers can be added.

- To delete a tier, click the delete button (). Tier 1 cannot be deleted.

7. Click **Update**. The server settings are saved successfully.

The Update button is enabled only when the tier list is modified and every tier has at least one node.

Configuring Attestation Settings

After performing the initial attestation to [activate the confidential computing on a CTE client](#), you can perform the reattestation at a certain frequency in a profile.

To configure the Attestation settings in a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **ATTESTATION SETTINGS**.
5. Turn on the **Enable Reattestation** toggle.
6. Set the **FREQUENCY**.
 - a. Enter the **Frequency**. Frequency can be set from 1 to 30 days or 1 to 720 hours.
 - b. Select the unit of frequency, which can be **Hours** or **Days**.
7. Set the **RETRY ON FAIL**.
 - a. Select the **Interval** minutes.
 - b. Select the **Retry Attempts**.
8. Click **Update**.

On successful updating of the attestation settings, a "Profile updated successfully" message will be displayed.

Concise Logging

CTE's standard operational logging sends audit messages for every file system operation. An audit message is sent every time a file is opened, read, updated, or written. Standard logging can generate high volumes of log data. Security administrators might not need most of these logs to monitor file system activities on the protected clients.

A CipherTrust Manager administrator can enable or disable Concise Logging for a profile. After Concise Logging is enabled or disabled, CTE Agent generates a log message to record that event:

```
"[CGA] [INFO] [CGA3201I] [08/07/2020 10:57:18] Concise logging enabled"
"[CGA] [INFO] [CGA3202I] [08/07/2020 10:57:27] Concise logging disabled"
```

Advantages

Concise Logging:

- Helps security administrators to focus on relevant audit messages and important actionable messages such as errors and warnings.
- Can eliminate repetitive and unimportant audit messages generated by read and write activities on a file, read and write directory attributes, and other file system activities.
- Eliminates audit messages:

-
- For each block read by a user or an application. Only one audit message is sent for every read/write activity.
 - That read the attributes, basic information of file set attributes, and other event-based messages.
 - For directory open, read directory attributes, and directory close.

Considerations

Concise Logging:

- Changes the set of messages that are sent to Security Information and Event Management (SIEM) software systems. If this results in loss of data required for customer reports, then disable Concise Logging.
- Applies to all GuardPoints and for all users of the clients linked with a profile. There is no fine-grained control such as per GuardPoint, user, or message type.
- Applies to the existing clients and the new clients to be linked with the profile subsequently.
- Is supported by CTE **secfs** only.
- Should not be used with Learn Mode.

Modifying Profiles

To modify a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.

Alternatively, click the overflow icon () corresponding to the desired profile and click **Edit**.

4. Expand **CLIENT LOGGING CONFIGURATION**.
 - a. Modify the settings, as appropriate. Refer to [Setting Client Log Configuration](#) for details.
 - b. Click **Update**.
5. Expand **CLIENT SYSLOG CONFIGURATION**.
 - a. Modify the settings, as appropriate. Refer to [Setting Client Syslog Configuration](#) for details.
 - b. Click **Update**.
6. Expand **QUALITY OF SERVICE CONFIGURATION**.
 - a. Modify the settings, as appropriate. Refer to [Setting Quality of Service Configuration](#) for details.

-
- b. Click **Update**.
 7. Expand **RANSOMWARE PROTECTION CONFIGURATION**.
 - a. Modify the settings, as appropriate. Refer to [Setting Ransomware Protection Configuration](#) for details.
 - b. Click **Update**.
 8. Expand **MULTIFACTOR AUTHENTICATION**.
 - a. Modify the settings, as appropriate. Refer to [Setting MFA Configuration](#) for details.
 - b. Click **Update**.
 9. Expand **SERVER SETTINGS**.
 - a. Modify the settings, as appropriate. Refer to [Configuring Server Settings](#) for details.
 - b. Click **Update**.

The profile settings are updated.

You can also modify or delete a CUSTOM QoS.

Modifying a CUSTOM LDT QoS Schedule

To modify a CUSTOM schedule:

1. Click the overflow icon () corresponding to the desired custom QoS schedule.
2. Click **Edit**. The Create QoS Schedule dialog box is displayed.
3. Modify the schedule, as appropriate. Refer to [Creating a Custom LDT Schedule](#) for details.
4. Click **Update**.

The CUSTOM LDT QoS schedule is modified.

Deleting a CUSTOM LDT QoS Schedule

To delete a CUSTOM schedule:

1. Click the overflow icon () corresponding to the desired custom QoS schedule.
2. Click **Delete**.
3. Click **Yes** to confirm the deletion.

The CUSTOM LDT QoS schedule is deleted.

Deleting Profiles

Single or multiple profiles can be deleted from the CipherTrust Manager GUI in one go. Before deleting a profile

make sure that no clients or client groups are linked to it.

Deleting Individual Profiles

To delete a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Click the overflow icon () corresponding to the desired profile.

Alternatively, select the desired profile and click the delete icon ().

4. Click **Delete**.

The selected profile is removed from the profiles list.

Deleting Multiple Profiles

To delete multiple profiles:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Select the check boxes corresponding the desired profiles.

To select all profiles visible on the page for deletion, select the top check box to the left of the **Name** heading.

4. Click the delete icon (). A dialog box appears prompting to confirm the action.
5. Click **Delete**.

Managing Clients

A client is a computer system where the data needs to be protected. A compatible CTE Agent software is installed on the client. The CTE Agent can protect data on the client or devices connected to it. A client can be associated with multiple GuardPoints for encryption of various paths (refer to [Managing GuardPoints](#) for details).

The Clients page of the CipherTrust Manager GUI displays all clients protected by encryption Agents.

The K8s Clients page of the CipherTrust Manager GUI displays all the registered [Kubernetes Clients](#).

Registering Clients

Note

Before proceeding, make sure that:

- A compatible CTE Agent is installed on the client.
- The client is registered with the CipherTrust Manager.

Refer to the [CTE Agent Quick Start Guide](#) specific to your platform for information on installing and configuring CTE Agents.

Note

When CTE clients are restored on the CipherTrust Manager from the backup file of another CipherTrust Manager, you must unenroll the client before proceeding with reregistration.

When CTE clients are registered, they are automatically added to the CipherTrust Manager GUI. Refer to the [CTE Agent Quick Start Guide](#) specific to your platform for information on installing and configuring CTE Agents.

Similarly, all the registered [Kubernetes Clients](#) are displayed on the K8s Clients page of the CipherTrust Manager GUI.

Adding Clients Manually

Optionally, the CipherTrust Manager administrator can manually add a client to the CipherTrust Manager GUI - even before the CTE Agent is installed on it.

Note

CTE for Kubernetes clients cannot be added manually. They are automatically added to the CipherTrust Manager on registration.

To add the client manually:

1. Log on to the CipherTrust Manager GUI as administrator.
2. Open the **Transparent Encryption** application. The Clients page is displayed.
3. Click **Create Client**. The General Info screen of the Create Client wizard is displayed.

General Info

1. Specify a unique **Name** for the client.
2. Set the **Password Generation Method**. The options are:
 - **Generate**: A password is generated automatically by CipherTrust Manager. This is the default method.
 - **Manual**: Set the password manually.
 - a. Select **Manual**.
 - b. Enter the new password in the **Password** and **Confirm Password** fields. The password must match in both fields.

Note

The password must contain minimum eight characters including at least:

- One capital letter
- One number
- One of these special characters: ! @ # \$ % ^ & * () { } []

Refer to [Changing Client Password](#) for details.

3. Provide a **Description** for the client.
4. Specify the following, as appropriate:
 - **UserSpace Client**: Ensure that the check box is clear. This check box specifies whether the client will be a CTE UserSpace client.
 - **Registration Allowed**: Whether to allow client's registration with the CipherTrust Manager. Select to allow, clear to deny registration. By default, the registration is not allowed.
 - **Communication Enabled**: Whether to enable the client's communication with the CipherTrust Manager. Select to enable, clear to disable communication. By default, the communication is disabled. This can only be enabled when **Registration Allowed** is enabled.
5. Click **Next**. The Add GuardPoints screen is displayed.

Add GuardPoints (Optional)

Optionally, you can create GuardPoints on the manually added client. CTE supports creation of all types of GuardPoints on such clients.

1. Click **Create GuardPoint**.

2. Select a **Policy**. Refer to **Policy Type** under **Creating Policies > Step 1: Specify General Information** for details.
3. Specify the **Type** of the GuardPoint. Refer to [Automatic and Manual GuardPoints](#) for details on types of GuardPoints.
4. Specify the **Path** (or **Cloud Object Storage URL** for a COS GuardPoint) to be protected. Refer to [Managing GuardPoints](#) for details.
5. Configure **Preserve Sparse Region**, **In-Place Data Transformation**, and/or **Auto Mount** as appropriate. The options vary based on the selected policy, as follows:
 - **Preserve Sparse Region** pre-selected for an LDT policy.
 - **In-Place Data Transformation** pre-selected for an IDT policy.
 - **Auto Mount** for a Standard policy and an LDT policy.

Note

- The Secure Start option cannot be enabled for GuardPoints on manually added clients.
- The Multifactor Authentication option is unavailable for GuardPoints on manually added clients.
- Auto Mount can be enabled only for the Auto Directory GuardPoint.

6. Click **Create**. The newly created GuardPoint appears in the list.
7. Click **Next**. The Confirmation screen is displayed.

Confirmation

1. Verify the client details. The Confirmation screen displays general information about the client and details of the GuardPoints added to the client.

If the details are incorrect or you want to modify them, click **Back** and update the details.

2. Click **Save**.

The newly created client appears in the clients list.

Searching Clients

The Clients page on the CipherTrust Manager GUI shows the list of registered clients.

To search for a registered client:

1. Log on to the CipherTrust Manager GUI as administrator.

2. Open the **Transparent Encryption** application. The Clients page is displayed. This page lists the clients added to this CipherTrust Manager appliance.
3. In the **Search** box, enter the client name. Search is case-insensitive. You can enter all or part of a client name. A partial client name displays every client with a name that contains the specified string.



Viewing Clients

The Clients page shows the total number of clients, clients with errors, clients with warnings, healthy clients, unregistered clients. The Status Bar contains the following tabs:

- **Total Clients:** Shows the total number of registered and unregistered clients with all types of health status.
- **Errors:** Shows the number of clients with errors.
- **Warnings:** Shows the number of clients with warnings.
- **Healthy:** Shows the number of healthy clients.
- **Unregistered:** Shows the number of unregistered clients.
- **Expunged:** Shows the number of expunged clients.

Note

The Unregistered and Expunged states are not applicable to the CTE for Kubernetes clients.

Refer to [Client States](#) for details.



Click each tab to filter the clients. The clients list displays names of clients in the CipherTrust Manager database and details about their configuration.

To view the clients added to the CipherTrust Manager:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The clients list shows the following details:

Status	Client Name ↑	Client Type	Protection Mode	OS Type ↑	FAM State	Agent Version	Description	⚙
▸ ☐  Healthy	P_1	CTE-U	CTE	LINUX	DISABLED	9.5.0.20	TestHost CTE-U	...
▸ ☐  Healthy	P_10	FS	CTE	LINUX	DISABLED	7.2.0.90	TestHost	...
▸ ☐  Healthy	P_11	FS	CTE	LINUX	DISABLED	7.2.0.90	TestHost	...
▸ ☐  Healthy	P_12	FS	CTE	LINUX	DISABLED	7.2.0.90	TestHost	...
▸ ☐  Healthy	P_2	FS	RWP	WINDOWS	DISABLED	7.4.0.0	TestHost	...

Column	Description
Status	Health status of the client: • Healthy • Error • Warning • Unregistered • Expunged The Unregistered and Expunged states are not applicable to the CTE for Kubernetes clients. Refer to Client States for details.
Client Name	Name link of the client on the CipherTrust Manager.
Client Type	The type of the client: • FS (a CTE client) • CTE-U (a CTE UserSpace client)
Protection Mode	The protection mode of the client: • CTE (File system protection, unregistered clients) • RWP (Ransomware protection, Windows clients) • CTE RWP (Both file system and Ransomware protection, Windows clients) When you unenroll (unregister) a client, its Protection Mode does not change. For example, if the Protection Mode of a client before unenrolling is CTE RWP, the mode remains CTE RWP after the client is unenrolled.

Column	Description
OS Type	OS running on the client: • AIX • LINUX • WINDOWS • UNKNOWN • FREEBSD UNKNOWN is displayed for unregistered or manually added clients. FREEBSD is supported by CTE UserSpace.
FAM Status	Whether FAM is ENABLED or DISABLED for the client.
Agent Version	Version of the CTE Agent installed on the client. For unregistered or manually added clients, the field is empty.
Description	Description to identify the client.
Encryption Modes	Encryption mode(s) used to protect GuardPoints on the client, for example, CBC, CBC_CS1, and XTS.
LDT Enabled	Whether LDT is enabled on the client.
Profile	Profile linked to the client.
Domain Sharing Enabled	Whether the client is shared across domains - Yes or No . Refer to Sharing a Client Across Domains for details.
Sharing	Sharing status of the client. • External: The client is external to the current domain. The client is created and shared from another domain. • Shared: The client is shared across other domains. The current domain is the native domain of the client. • -: The client is neither Shared nor External. The field is left blank for clients that were registered with a previous version of the CipherTrust Manager. Such clients can also be shared across domains. Refer to Sharing a Client Across Domains for details.

The **Encryption Modes**, **LDT Enabled**, **Profile**, **Domain Sharing Enabled**, and **Sharing** columns are hidden by default. To show/hide a column, click the custom view icon () , select/clear the desired column, and click **OK**.

Viewing Details of a Client

To view the details of a client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Under **Client Name**, click the desired client. The client details page is displayed.

You can see the details of GuardPoints, FAM, Settings, Membership, and Challenge Response associated with the client.

Warning

If potential ransomware activities are detected, the warning will be displayed at the top of the page.

FAM

Note

You can see the FAM details only if the FAM is enabled for that client.

1. Click the **FAM** tab.
2. Expand **ATTRIBUTE** to view the attribute details such as Destination Name, Duplicates, Threshold, and Suppress Threshold.

Note

After the client has enabled FAM, the attribute can be created. You can create only one attribute for a client.

3. Expand **POLICIES** to view the list of FAM policies linked with the client.

Note

- A client can have multiple FAM policies.
- The FAM policies are reusable. One FAM policy can be linked with multiple clients.

Client States

- **Healthy:** Client is registered with the CipherTrust Manager without any errors, that is, `init` is received from Agent without any issues.
- **Error:** Client's communication is broken with the CipherTrust Manager for more than five minutes.
- **Warning:** Client's communication is broken with the CipherTrust Manager or a GuardPoint is inactive due to any reasons.
- **Unregistered:** Client is unenrolled from the CipherTrust Manager.
- **Expunged:** Client's delete operation is triggered, but its confirmation is not yet received from the Agent.

Note

The Unregistered and Expunged states are not applicable to the CTE for Kubernetes clients. When a CTE for Kubernetes client is deleted or unenrolled (from the client), its entry is automatically removed from the CipherTrust Manager.

Getting Latest Client Status

By default, the status of a registered client is updated on the CipherTrust Manager when the configuration of the client changes. However, if needed, you can manually fetch the latest status of the client at any time.

Note

- The latest status of only a *registered* client can be fetched.
- Request to fetch the latest status can be reattempted after 30 minutes of the previous attempt.
- After registering a new client, wait for 30 minutes to fetch the latest status.

To get the latest status of a client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Click the overflow icon () corresponding to the desired client.
4. Click **Refresh**.

The client status on the Clients page is refreshed.

Unenrolling Clients

A registered CTE client can be unenrolled from the CipherTrust Manager. When the client is unenrolled (unregistered), the communication between the CTE Agent and the CipherTrust Manager is removed. The CTE Agent can no longer communicate with the CipherTrust Manager. However, the CipherTrust Manager still maintains the client configuration to allow re-registration.

Important Notes

- A CTE client with Active LDT GuardPoints cannot be unenrolled (unregistered).
- After unenrolling, the client's GuardPoints will still be displayed on the CipherTrust Manager. However, their status will be displayed as Unknown.
- The status of the client capabilities, for example, LDT, will not change on the CipherTrust Manager. They will be displayed the same as they were before unenrolling the client.
- The associated client under the Client-Management section of the API playground is deleted after unenrolling. If the client is not deleted automatically, you can delete it manually.
- The status of the unenrolled client will be displayed as Unregistered on the CipherTrust Manager.

Note

An unenrolled client requires re-registration to enroll with the CipherTrust Manager again.

Note

When deleting a pod running on a registered CTE for Kubernetes client, you might notice some unwanted error messages. To avoid such messages, it is recommended to unenroll the CTE for Kubernetes client before attempting to delete the pod.

To unenroll a client from the CipherTrust Manager:

1. Open the **Transparent Encryption** application.

-
2. Click **Clients > Clients**.
 3. Click the overflow icon () corresponding to the desired client.
 4. Click **UnEnroll**. A dialog box appears prompting to confirm the action.

An unenrolled client requires re-registration to enroll with the CipherTrust Manager again.

5. Click **UnEnroll**.

The selected client is unenrolled from the CipherTrust Manager. Its status on the CipherTrust Manager becomes Unregistered.

Reregistering Clients

An unenrolled client requires reregistration to enroll with the CipherTrust Manager again.

When you try to reregister a client, you must enable the same set of capabilities that were enabled on the client before reregistration. Also, specify name of at least one client group (if the client was associated with any groups). Refer to [Reregistering CTE Clients](#) for details.

Deleting Clients

A CTE client can be deleted when it is no longer required to be associated with the CipherTrust Manager.

Clients with the Healthy, Unregistered, Warning, and Error states can be deleted from the CipherTrust Manager.

After you initiate the client deletion operation, the operation:

1. Waits for confirmation from the CTE Agent before deleting anything from the CipherTrust Manager.
2. Changes the client status to Expunged on the CipherTrust Manager.
3. After receiving confirmation from the Agent:
 - Deletes all entries, capabilities, and GuardPoints associated with the client.
 - Removes the client record from the CipherTrust Manager.

However, in some cases, due to network issues or any other reasons, the CipherTrust Manager does not receive confirmation from the CTE Agent. In such cases, the client configurations cannot be deleted from the CipherTrust Manager and the client remains stuck at the Expunged state. Such clients need to be deleted manually. Refer to [Deleting Expunged Clients Manually](#) for details.

4. Deletes the associated client from the Client-Management section of the API playground.

Before proceeding with client deletion, read and understand the additional information provided on client deletion, Agent uninstallation, clients with System and Agent locks, and deletion indicators in [Deleting Clients](#).

The CipherTrust Manager provides options to delete individual clients or multiple clients in one go. To delete the client from the CipherTrust Manager GUI.

Note

Before deleting the client, ensure that the Unique to client key is not associated. If the key is associated, decrypt the data. Refer to [Data Transformation](#) for details.

Warning

It is important to decrypt the data. If you don't decrypt it, the data will be lost and cannot be recovered.

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Click the desired tab to view the instructions.

Individual Clients

- a. Under **Client Name**, click the overflow icon () corresponding to the client you want to delete.
- b. Click **Delete**. A dialog box appears prompting to confirm the action.
- c. Click **Delete**.

The selected client is deleted and its entry is removed from the Clients page after the CipherTrust Manager receives confirmation from the CTE Agents.

Multiple Clients

A maximum of 200 clients can be deleted at once.

- a. Select the desired clients.

To select all clients visible on the page, select the top check box to the left of the Status heading.

- b. Click the delete icon (). A dialog box appears prompting to confirm the action.
- c. Click **Delete**.

The selected clients are deleted and their entries are removed from the Clients page after the CipherTrust Manager receives confirmation from the CTE Agents.

Refer to [Deleting Expunged Clients Manually](#) for details on deleting Expunged clients.

Deleting Expunged Clients Manually

If due to any reasons, the CipherTrust Manager does not receive the deletion confirmation from the CTE Agent, the client remains stuck in the Expunged state. The client cannot be deleted automatically from the CipherTrust Manager.

To manually delete an Expunged client and its configurations from the CipherTrust Manager, run the `/v1/transparent-encryption/clients/{id}/delete` API with the force delete option ("force_del_client").

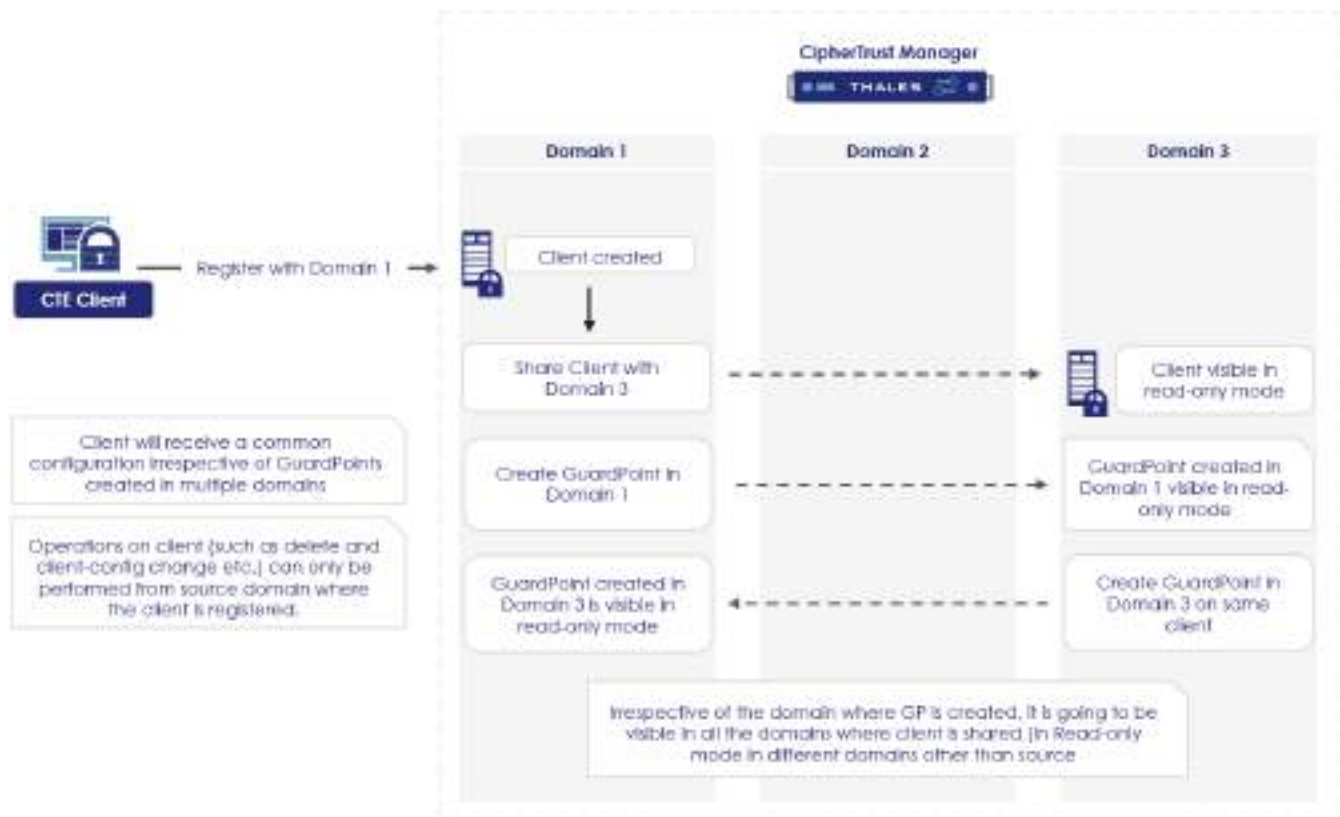
When running the API, set `"force_del_client": true`. Refer to the API playground documentation for details.

Sharing a Client Across Domains

A shared client will be visible in read-only mode in all the domains where it is shared. The GuardPoints can be created on the shared client from any of the linked domains. These GuardPoints will be visible in read-only mode in all the linked domains except their native domains (where the GuardPoints are created). All the valid operations on the GuardPoints will be allowed from the native domains.

This functionality is transparent to the CTE client, that is, the client will receive a single security configuration having GuardPoint details of all the domains.

The following diagram shows the client-sharing workflow:



To share a client across domains:

1. Open the **Transparent Encryption** application.

2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **GENERAL SETTINGS**.
6. Enable **Domain Sharing**.
7. Click **Update**.

Removing Client Sharing from Domains

You can remove client sharing from individual domains or from multiple domains in one go.

1. Open the **Transparent Encryption** application. The Clients page is displayed.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client. The detail view of the Clients page is displayed.
4. Click the **Sharing** tab.
5. Click the desired tab to view the instructions.

From Individual Domains

- a. Under **Domain Name**, select the check box corresponding to the desired domain.
- b. Click **Remove**. A dialog box appears prompting to confirm the action. Deleting this domain is permanent and cannot be undone.

From Multiple Domains

- a. Under **Domain Name**, select the check box corresponding to the desired domains. To select all domains visible on the page, select the top check box to the left of the Domain Name heading.
- b. Click the delete icon (). A dialog box appears stating that deleting the selected domains is permanent and cannot be undone.

6. Click **Delete**.

The client is no longer shared with the selected domain(s).

Enabling Live Data Transformation

The Live Data Transformation (LDT) feature enables the CipherTrust Manager Security Administrators to encrypt or rekey GuardPoint data without blocking the user or application access to that data.

In standard CTE deployments, data access is blocked during the initial encryption or rekeying of the data, and each rekey operation requires guarding your data under separate production and offline data transformation policies. With LDT, encryption and rekeying of the data takes place in the background using one policy, without disrupting user or application access.

Prerequisites

To use LDT, you must have the following:

- CTE Agent license. The feature is called *CTE - TransparentEncryption* on the Licensing page.
- CTE LDT add-on license. The feature is called *CTE - LiveDataTransformation* on the Licensing page.
- CTE Agent installed on a client. Refer to the [CTE Agents Quick Start Guide](#) specific to your platform for information about installing and registering CTE clients.

Refer to the [CTE-Live Data Transformation with CipherTrust Manager](#) and the CipherTrust Manager [Compatibility Matrices](28,186: Refer to the [CTE-Live Data Transformation with CipherTrust Manager](#) and the CipherTrust Manager [Compatibility Matrices](#) for information about implementing LDT and the supported platforms.

Important Notes

- If the CipherTrust Manager fails, all keys that were automatically rotated after the last backup would be lost, making all data encrypted with those keys unusable or unrecoverable. Therefore, it is recommended that the LDT feature is used in a high availability CipherTrust Manager deployment.
- If LDT must be used in a single CipherTrust Manager configuration, it is recommended to:
 - Set "Persistent on Client" to "Yes" for all keys that are created.
 - Set the password creation method to "Manual" for all clients.
 - If the standalone CipherTrust Manager fails or is unavailable, the data on the client can still be accessed by entering the known passphrase. The data is accessible as the encryption keys are cached on the client.

Enable LDT

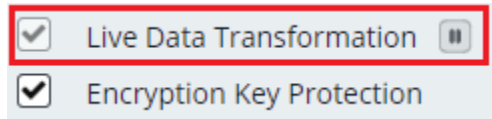
Enable the LDT support for a client either during registration or after registration with the CipherTrust Manager.

- If LDT is enabled during registration, the Live Data Transformation check box appears selected by default on the CipherTrust Manager GUI.
- If LDT is not enabled during registration, you can enable it on the CipherTrust Manager GUI, as described below.

To enable LDT on a client after CTE installation:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.

3. Under **Client Name**, click the desired client.
4. Select **Live Data Transformation**.



By default, LDT performs rekey operations on the LDT protected GuardPoints as soon as GuardPoints are enabled. To pause LDT rekey operations, click the Suspend Live Data Transformation icon (⏸). The icon changes to Resume Live Data Transformation (▶).

5. Click **Apply**. LDT is now enabled on the client.

After LDT has been enabled, it cannot be disabled. To remove the feature, you must migrate existing data protected under LDT policies, unregister the client, and delete the client. Then, you can reregister the client without enabling the feature. This allows you reclaim the license for use on another client.

Refer to [Managing GuardPoints](#) for details on creating LDT GuardPoints. For details about how LDT works, guidelines, and best practices for using the feature, refer to the [CTE-Live Data Transformation with the CipherTrust Manager](#) documentation.

Setting Client Locks

Agent Lock and System Lock are used to protect the CTE Agent and certain system files. CTE Agent protection includes preventing:

- Certain changes to the CTE Agent installation directory.
- Unauthorized termination of the CTE Agent processes.

These locks can be applied to individual clients or client groups. By default, the Agent Lock and System Lock are disabled.

Note

Uninstallation of the Agent software might fail when the Agent Lock and System Lock are enabled. It is recommended to disable the:

- Agent Lock before uninstalling the Agent software on the client system.
- Agent Lock before deleting the client records from the CipherTrust Manager GUI.
- System Lock before updating, deleting, or modifying the protected system files.

Agent Lock

Agent Lock locks the contents of the CTE Agent directories on the client. These directories are `/etc/ciphertrust`

`root>/agent/secfs` and `/<install root>/agent/vmd`.

Files in these directories cannot be modified or removed when Agent Lock is enabled; however, the CipherTrust Manager can still propagate updates to the client system.

Note

The CTE Agent directories `secfs/.sec/conf/` (on Linux) and `secfs\sec\conf\` (on Windows) contain sensitive configuration files. It is highly recommended to enable the Agent Lock to avoid data exposure to unauthorized users.

When Agent Lock is Disabled

- CTE Agent software on the client is not protected

Note

Do not unregister or delete the CTE Agent while locks are applied. The locks stay in effect after the Agent is unregistered, and without Agent credentials, the CipherTrust Manager can neither administer that Agent nor disable the locks. You must boot the client into single-user mode and manually modify the Agent configuration to disable the locks.

When Agent Lock is Enabled

- Certificates are exchanged and the client is bound to the CipherTrust Manager
- CTE Agent installation directory cannot be deleted or overwritten
- CTE Agent services cannot be stopped
- CTE Agent GuardPoints cannot be forcefully unmounted
- On **Linux** systems:
 - All operations are permitted on the following directory:

```
/<install root>/agent/secfs/tmp
```

- Following directories cannot be removed or renamed, and directory and file creation will fail.

```
/<install root>/agent/secfs/bin
/<install root>/agent/vmd
```

- File creations and other operations will work for the following directory, but the directory cannot be removed or renamed.

```
/<install root>/agent/secfs/
```

- On **AIX** systems:

- Contents of the following directories cannot be changed or moved.

```
/<install root>/agent/vmd
```

- Contents of the following files and directories can be modified, but not removed or renamed.

```
/<install root>/agent/secfs/  
/<install root>/agent/secfs/tmp
```

- On **Windows** systems:

- Following folder cannot be moved and its contents cannot be modified.

```
C:\Program Files\Vormetric\DataSecurityExpert\Agent\secfs\sec
```

- CTE Agent entries in the registry cannot be modified or deleted.

System Lock

System Lock applies an internal policy to the client to lock client system directories, such as `/var`, `/bin`, and `/etc`.

Note

System Lock must be disabled before upgrading or installing third-party software, adding new applications, opening SSH sessions remotely, or modifying system directories.

Note

(Windows only) Verify that the volume letter and the path for the Windows system are correct before proceeding. When the CTE Agent is installed, the volume letter defaults to `C:`. The executables on the Client Settings tab may be on a different volume or in a different folder. If the volume or path information is incorrect, the CipherTrust Manager cannot sign the applications and apply Agent Lock and System Lock.

When System Lock is Disabled

- The internal policy is disabled.
- You can install or update system software.

When System Lock is Enabled

- Agent Lock is automatically enabled.
- Operating system directories on the client are protected.
- Microsoft Update cannot be run on Windows systems to protect the client. Microsoft update and other installation-related executables are specifically blocked. Executables like `wuacuc.lt.exe` and `msiexec.exe` cannot be run.
- The installation utility checks if System Lock is enabled on the client system. If it is, the utility aborts installation and displays a message informing you to **unlock system before running install/update program**. Other third-party installation utilities do not check whether System Lock is enabled, and are not prevented from installing software.
- New file or directory creation inside a protected directory is not allowed.

The following files, directories, and subdirectories are, by default, automatically protected when System Lock is enabled. Asterisks (*) indicate pattern matching.

- On **Linux** systems:
 - Following files and the contents of the following directories cannot be changed or moved.
 - `/etc/pam.d`
 - `/etc/rc*`
 - `/etc/security`
 - `/usr/lib/security`
 - Contents of the following files and directories can be modified, but not removed or renamed.
 - `/etc`
 - `/etc/init.d/secfs`
 - `/usr`
 - `/usr/bin/vmd`
 - `/usr/bin/vmsec`
 - `/usr/bin/secfsd`

-
- /usr/bin/dataxform
 - /usr/lib
 - /usr/lib/pam
 - /usr/lib/security
 - /var/log/vormetric
- On **AIX** systems:
 - Following files and the contents of the following directories cannot be changed or moved when System Lock is enabled.
 - /etc/rc.d
 - /etc/security
 - /usr/lib/security
 - /sbin/helpers/mount_secfs
 - Contents of the following files and directories can be modified, but not removed or renamed when System Lock is enabled.
 - /var/log/vormetric
 - On **Windows** systems:
 - Files with the following extensions in the Windows OS installation folder (for instance: `\Windows`, `\WinNT`, and so on) cannot be moved or modified:
 - .exe
 - .dll
 - .sys
 - .cmd
 - .com

When System Lock is applied, a protected file or path cannot be renamed or deleted; however, if it is a directory, other files may be added to it. For example, `/etc` cannot be deleted nor renamed, though you can add files to it. A file that cannot be modified cannot be opened and edited in any way.

Setting Locks

You can apply locks to individual clients or to client groups. To apply the locks:

1. Make sure that no one is currently in or accessing the Agent installation directories; otherwise, the CipherTrust Manager might not lock the Agent software.
2. Open the **Transparent Encryption** application.
3. Click the desired tab to view the instructions.

On an Individual Client

- a. Click **Clients > Clients**. The list of available CTE clients is displayed.
- b. Click the **Name** link of the desired client. The details page of the client is displayed.
- c. Click the **Settings** tab.
- d. Expand **SECURITY SETTINGS**.
- e. On the lock bar, click **Agent Lock**. This protects the CTE Agent files from modification and deletion.



- f. Click **System Lock**. This protects a set of system files from modification and deletion.



Agent Lock is automatically enabled when System Lock is enabled. You can manually enable or disable Agent Lock only when System Lock is disabled.

- g. Click **Update**.

On a Client Group

- a. Click **Clients > Client Groups**.
- b. Under **Client Group Name**, click the desired client group.
- c. On the lock bar, click **Agent Lock**. This protects the CTE Agent files from modification and deletion.



- d. Click **System Lock**. This protects a set of system files from modification and deletion.



Agent Lock is automatically enabled when System Lock is enabled. You can manually enable or disable Agent Lock only when System Lock is disabled.

- e. Click **Apply**.

4. Verify the locks. Refer to [Verifying Locks on Clients](#).

Note

To disable the locks on a client group, select the client, click **Unlock**, and click **Apply**.

Verifying Locks on Clients

A client administrator can verify that the locks are applied to the Agent on the client.

To verify the locks:

1. Log on to the client system.
2. Run the `secfsd` command with the `lockstat` argument:

```
# secfsd -status lockstat
FS Agent Lock: true
System Lock: true
```

Note

Sometimes, the CipherTrust Manager reports the CTE Agent configuration different than the actual configuration. This can be because of the delay between log uploads to the CipherTrust Manager, or because a GuardPoint is in use when the lock is applied.

In some cases, when the locks are enabled, the CipherTrust Manager cannot administer the client. In such cases, after changing authentication credentials or removing the certificate fingerprint, the client administrator must unlock the client manually.

Unlocking Clients Manually

Unlocking Linux Clients

To unlock the client manually:

1. Boot the client into single-user mode.
2. Edit the `secfs/.sec/conf/configuration/secfs_config` file.
3. Set both `coreguard_locked` and `system_locked` to `false`.
4. Save the file.
5. Boot the system into multi-user mode.

You can now administer the client again.

Unlocking Windows Clients

To unlock the client manually:

1. Boot in safe mode.
2. Rename `C:\Windows\system32\drivers\vmgmt.sys` and `.\drivers\vmfiltr.sys` to something else.
3. Boot in regular mode.

You can now administer the client again.

Disabling Locks

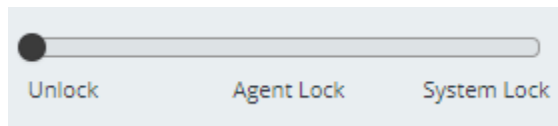
To disable the locks on a client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **SECURITY SETTINGS**.
6. Click **Unlock**. The lock bar should look like the following:



7. Click **Update**.

To disable the locks on a client group, select the client group, click **Unlock**, and click **Apply**. The lock bar should look like the following:



Administering Locking Issues

The client administrator must inform the Security Administrator of changes to the system hierarchy.

- **Example 1:** The client system administrator can request to have the locks temporarily disabled to do administrative functions.
- **Example 2:** The client system administrator can remove directories and files, then, later when the lock is reapplied, the CipherTrust Manager protects non-existent data.
- Another common administrative issue pertains to mounted GuardPoints. The client system administrator can remove or unmount an unlocked, non-automounted GuardPoint. The CipherTrust Manager GUI is not aware of this change and does not issue a warning when you reapply the lock to the now non-existent mounted GuardPoint.
- To recover an unmounted GuardPoint:
 - a. Disable the GuardPoint for the file system on the CipherTrust Manager GUI.
 - b. Mount the file system on the client.
 - c. Enable the GuardPoint for the file system.

Client Settings

Applications such as `su`, `sshd`, and `login` authenticate users' identity by requesting user credentials (user name and password). These are signed applications that identify and authenticate before a child process is executed.

GuardPoints can have an associated policy that restricts access to the data stored in them. For a process to access the data, the user's associated identity must be authorized. This authorization can be done by adding an entry to the Settings field on the Client Settings tab. This entry specifies a program, such as mentioned above, with a keyword that indicates the type of authorization that is applied.

Client settings configured on the CipherTrust Manager are pushed to the clients periodically.

Any changes to the client settings are not automatically signed. Signatures of the newly added processes are compared against the signatures in the existing settings. If they differ, an error message is generated. Refer to [Re-Sign Settings](#) for steps to configure this setting. Refer to the [CTE Agent Advanced Configuration and Integration Guide](#) specific to your platform for details about this feature.

Client settings can also be configured at the client group level, refer to [Inheritance of Client Group Settings](#) for details.

Note

Refer to [CTE Linux Authentication and Client Settings](#) for detailed and additional information on authentication and client settings.

Client Settings for Linux

Specify the authentication mechanisms in place for certain binaries on the client machine.

Default Settings for Linux

```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
|authenticator_euid|/usr/sbin/vsftpd
```

Add, edit, or modify authentication settings as appropriate.

Additional Settings for HDFS (Linux Clients)

Depending on the Hadoop security authentication mode, additional settings are needed for CTE clients in an HDFS cluster. Add the following settings as appropriate.

Note

`/usr/jdk64/jdk1.8.0_40/bin/java` is the Java executable used to launch the HDFS services. Change the Java jdk path to reflect your end-user environment.

- Sample setup when `hadoop.security.authentication` mode is simple.

```
|authenticator+arg+=class=org.apache.hadoop.hdfs.server.namenode.NameNode|/usr/
jdk64/jdk1.8.0_40/bin/java
|authenticator+arg+=class=org.apache.hadoop.hdfs.server.datanode.DataNode|/usr/
jdk64/jdk1.8.0_40/bin/java
```

- Sample setup when `hadoop.security.authentication` mode is Kerberos.

```
|authenticator+arg=+class=org.apache.hadoop.hdfs.server.namenode.NameNode|/usr/
jdk64/jdk1.8.0_40/bin/java
|authenticator+arg=+class=org.apache.hadoop.hdfs.server.datanode.SecureDataNode
Starter|/usr/lib/bigtop-utils/jsvc
```

Authentication Settings for Signature Sets (Linux Clients)

The CipherTrust Manager provides an option to configure authentication of CTE client binaries. If a binary, whose path matches a client setting entry, is executed on the CTE client, the operation is validated using the binary signature stored in a signature set on the CipherTrust Manager. Based on the authenticity of the binary, the operation is validated as "User Authenticated" or "User Not Authenticated" as appropriate.

The format to specify authentication settings for a signature set is:

```
|privilege+sig=<signature-set-name>|/path/to/binary
```

For example, to specify authentication settings for a signature set `test-sign-set` for a binary stored at `/home/test/run-test`, add the entry:

```
|authenticator+sig=test-sign-set|/home/test/run-test
```

The wildcard character asterisk (*) can also be used to specify paths in client settings as:

```
|keyword+sig=<signature-set name>|/path/to/binary/*`
```

For example, to specify authentication settings for all binaries under `/home/test/`, add the entry:

```
|authenticator+sig=test-sign-set|/home/test/*
```

Note

The wildcard character * is supported for Linux clients only.

Specify Authentication Settings

To specify authentication settings for the client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.

4. Click the **Settings** tab.
5. Expand **CLIENT SETTINGS**. The Settings text box contains the authentication settings.

CLIENT SETTINGS

Settings

```

| C:\WINDOWS\system32\winlogon.exe
|lock| C:\WINDOWS\system32\msiexec.exe
|lock| C:\WINDOWS\system32\wuauclt.exe
|lock| C:\WINDOWS\system32\wupdmgr.exe
|lock| C:\Program Files\Wormetric\DataSecurityExpert\Agent\Secfs\sec\bin\wminstall.exe
|exempt| C:\WINDOWS\explorer.exe
|exempt| C:\WINDOWS\regedit.exe
|exempt| C:\WINDOWS\system32\regedt32.exe
|exempt| C:\WINDOWS\system32\svchost.exe
|exempt| C:\WINDOWS\system32\services.exe
|exempt| C:\WINDOWS\system32\smss.exe

```

☐ Re-sign Settings (This toggle resets after a push to the CTE agent.)

Note

- To delete the client settings, delete the content in the Settings box and click Update.
- To edit the client settings, modify the content in the Settings box and click Update. When editing the settings strings, follow the format `|privilege|file name`.

Update

Each line has the format:

```
|privilege|/path/to/binary
```

The format to specify authentication settings for a signature set is:

```
|privilege+sig=<signature-set-name>|/path/to/binary
```

Refer to [Client Settings Keywords](#) for keywords.

6. In the **Settings** box, specify the authentication mechanism.

Note

- To delete the settings, delete the content and click **Update**.

- To edit the settings, modify the content and click **Update**. When editing the setting strings, follow the format `|privilege|binary`.

7. Click **Update**.

Client Settings for Windows

For applications running under **WOW64** that require some form of user authentication, create entries on the Client Settings tab. The **syswow64** paths are created by default when the CTE Agent is installed. **Windows** is for Windows XP and Windows Itanium operating systems.

In **WOW64**, all file access to **C:\Windows\System32** is redirected to **C:\Windows\syswow64**, and is implemented using the File System. Redirected **syswow64** paths are effective only for 64-bit Windows file agents. This is the path where programs compiled for 32-bits are stored to run on a 64-bit system.

Before proceeding, verify that the volume letter and the path for the Windows system are correct. When the CTE Agent is installed, the volume letter defaults to **C:**. It is possible that the executables on the Client Settings tab are on a different volume or in a different folder. If the volume or path information is incorrect, the CipherTrust Manager cannot sign the applications, and it cannot apply Agent Lock and System Lock.

Default Settings for Windows

```
| | C:\WINDOWS\system32\winlogon.exe
| lock| C:\WINDOWS\system32\msiexec.exe
| lock| C:\WINDOWS\system32\wuauclt.exe
| lock| C:\WINDOWS\system32\wupdmgr.exe
| lock| C:\Program Files\Vormetric\DataSecurityExpert\Agent\Secfs\sec\bin\vminstal
l.exe
| exempt| C:\WINDOWS\explorer.exe
| exempt| C:\WINDOWS\regedit.exe
| exempt| C:\WINDOWS\system32\regedt32.exe
| exempt| C:\WINDOWS\system32\svchost.exe
| exempt| C:\WINDOWS\system32\services.exe
| exempt| C:\WINDOWS\system32\smss.exe
```

Add, edit, or modify authentication settings as appropriate.

Specify Authentication Settings

To specify authentication settings for the client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.

- Expand **CLIENT SETTINGS**. The Settings text box contains the authentication settings.

CLIENT SETTINGS

Settings

```

| | C:\WINDOWS\system32\winlogon.exe
| lock | C:\WINDOWS\system32\msiexec.exe
| lock | C:\WINDOWS\system32\wuauclt.exe
| lock | C:\WINDOWS\system32\wupdmgr.exe
| lock | C:\Program Files\Vormetric\DataSecurityExpert\Agent\Secfs\sec\bin\vminstall.exe
| exempt | C:\WINDOWS\explorer.exe
| exempt | C:\WINDOWS\regedit.exe
| exempt | C:\WINDOWS\system32\regedt32.exe
| exempt | C:\WINDOWS\system32\svchost.exe
| exempt | C:\WINDOWS\system32\services.exe
| exempt | C:\WINDOWS\system32\smss.exe

```

☐ Re-sign Settings (This toggle resets after a push to the CTE agent.)

Note

- To delete the client settings, delete the content in the Settings box and click Update.
- To edit the client settings, modify the content in the Settings box and click Update. When editing the settings strings, follow the format |privilege|file name.

Update

Each line has the format:

```
|privilege|/path/to/binary
```

Refer to [Client Settings Keywords](#) for keywords.

- In the **Settings** box, specify the authentication mechanism.

Note

- To delete the settings, delete the content and click **Update**.
- To edit the settings, modify the content and click **Update**. When editing the setting strings, follow the format |privilege|binary.

- Click **Update**.

Oracle Database in a Guarded NFS Mount on AIX

To locate your Oracle database in a guarded NFS mount:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **CLIENT SETTINGS**. The Settings text box contains the authentication settings. Each line has the format:

```
|privilege|/path/to/binary
```

6. In the **Settings** text box, add the following entries:

```
|vfsnumber|<path to>/oracle
|vfsnumber|<path to>/dbca
```

Example:

```
|vfsnumber|/u01/app/oracle/dbhome_1/bin/oracle
|vfsnumber|/u01/app/oracle/dbhome_1/bin/dbca
```

7. Click **Update**.

Client Settings Keywords

The following table lists the keywords that you can enter on the Client Settings tab. These keywords override different authentication requirements:

Keyword	Description
authenticator	(UNIX only) Authenticates based upon the real user ID (ruid) credentials of a process. The indicates that the given binary is trusted to authenticate users. For example, the sshd process on UNIX is a good authenticator . It takes incoming network connections and authenticates the user that attempts to log on to the system. All child processes from this session are trusted as the original user.
authenticator_euid	(UNIX only) Authenticates based upon the effective user ID (euid) credentials of a process. The keyword is used to authenticate the credentials of a setuid

Keyword	Description
	process with the <code>euid</code> value rather than the <code>ruuid</code> value.
<code> vfsnumber </code>	(AIX [all supported]/Oracle 10gR2) Use when Oracle RMAN backups fail on NFS as a result of not receiving underlying file system identifiers. Apply <code> vfsnumber </code> to the Oracle binaries directory.
<code> realfsid </code>	(AIX [All supported]) Use if the <code>cp</code> operation fails while copying files with extent attributes on guarded Veritas file systems. The failure occurs because the underlying file system identifier is not received.
<code> lock </code>	(Windows only) Specifies an application that cannot be executed on the client. An application defined with <code>lock</code> does not go through an internal policy check. The application is not allowed to run at all. A default set of applications is locked on Windows clients to prevent their execution and potential failure during bootup. The same effect can be achieved by configuring the resource and process security rule attributes in a policy. However, certain default applications are automatically locked on the Client Settings tab as a precautionary measure. Those applications must be included in the policy. Sometimes, problems such as installation failure or application lockup occur when installing software on a locked client. In such cases, identify the locked processes, unlock them, and retry installation. The failure goes away. For example: <code> lock c:\winnt\system32\msiexec.exe</code>
<code> exempt </code>	(Windows only) When processes or applications are started, the internal policy and regular policies are checked locally or by the CipherTrust Manager. When a policy check is performed and <code>exempt</code> is applied to the process, a six second timeout is imposed on the check. Without <code>exempt</code> , an application can wait indefinitely for a policy access check to complete, as when the CipherTrust Manager is required but is inaccessible. If the check times out because the CipherTrust Manager is unavailable for any reason, access is denied. <code>Exempt</code> client processes are also "exempt" from popup messages that describe the occurrence of access violations. An example of what causes such popup messages is an application that tries to memory map a file for which it does not have encryption permission (for instance, memory map with no view ability key on Windows). The only reasons to include <code>exempt</code> in the configuration are shorter wait periods and blocked popup messages.
<code> su_root_no_auth </code>	(UNIX only) Assigned only to the <code>su</code> process for tracking root users issuing unauthenticated <code>su</code> logins. The <code> su_root_no_auth /usr/bin/su</code> host setting in conjunction with <code> authenticator /usr/</code>

Keyword	Description
	<code>lib/ssh/sshd</code> prevents root from being authorized as another user. Non-root users using <code>su</code> to log on as another user after authentication, that is, after providing a password are not affected.
<code> path_no_trust </code>	(UNIX only) Any executable path that is marked with a <code> path_no_trust </code> client setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies. CTE prevents overrides from other client settings authenticators, using the <code> path_no_trust </code> status. If a user runs the <code>su</code> command from a non-trusted shell, that new shell is still marked as <code> path_no_trust </code> , even if <code> authenticator /usr/bin/su</code> is specified in the client settings. The <code> path_no_trust </code> feature overrides any and all authenticators under client settings.
<code> protect </code>	When a file is marked as protected in the client host settings, that file is protected from being modified or deleted, (even from a root process). It is not guarded and the file can be external to a GuardPoint. If the file marked as <code> protect </code> does not exist, then CipherTrust Transparent Encryption creates a 0-length file in its place. This provides an efficient means to identify and implement file protection. When the agent is stopped or uninstalled, these 0-length files are deleted and then re-created if the agent is restarted. Additionally, an audit record is generated when a file operation is denied. The <code> protect </code> status is displayed using the command <code>secfsd -status auth.</code>

The following table shows different results you get when using `authenticator` or `authenticator_euid` to verify user identities.

Product	Application	Client Setting	User
Oracle	oracle	<code>authenticator_euid</code>	"oracle"
Oracle	oracle	<code>authenticator</code>	*

* indicates the real uid of the user who starts the application. This means that if the policy is configured to check the user ID, a security rule must be generated for every possible user.

Note

Apply the `|authenticator_euid|` keyword to the oracle binary on the Client Settings tab to authenticate the `oracle` user because regardless of who starts the oracle process, the `EUID` is always `oracle`.

Configuring Application Authentication Credentials

To configure application authentication credentials:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **CLIENT SETTINGS**. The Settings box displays the default set of system applications that may require authentication entries.
6. In the **Settings** box, add, modify, or delete entries to control their access permissions. When you add more processes, you must include the entire path.

Note

A keyword such as `|authenticator|` must be used in front of a process, otherwise, the entry is ignored by the CipherTrust Manager GUI.

7. Click **Update**.

Client users currently logged on to the client must log off and log on again to refresh their user authentication credentials. They can verify the change by logging on to the client, accessing a GuardPoint, and checking the user information in the message logs.

Inheriting Client Settings from a Client Group

To inherit client settings from a client group:

1. Open the **Transparent Encryption** application.
2. Under **Client Name**, click the desired client.
3. Click the **Client Settings** tab.
4. Select the desired client group from the **Inherit Client Setting From** drop-down list. This drop-down shows the list of client groups the client is a member of. The drop-down is not available for standalone clients.
5. Click **Apply**.

The client now inherits client settings from the selected client group. Refer to [Inheritance of Client Group Settings](#) for details on inheritance.

Note

An unregistered client cannot inherit client settings from its client groups.

Re-Sign Settings

If you add another process to the set of trusted applications on the Client Settings tab, enable the Re-sign Settings toggle. This ensures that the new process is signed and authenticated by the client.

Subsequently, when the client settings are pushed to the CTE Agent, the updated settings are re-signed. The Re-sign Settings toggle is turned off (or reset).

To ensure that new processes are signed and authenticated by the client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **CLIENT SETTINGS**. The Settings text box contains the authentication settings.

CLIENT SETTINGS

Settings

| C:\WINDOWS\system32\winlogon.exe
| lock | C:\WINDOWS\system32\msiexec.exe
| lock | C:\WINDOWS\system32\wuauclt.exe
| lock | C:\WINDOWS\system32\wupdmgr.exe
| lock | C:\Program Files\Wormetric\DataSecurityExpert\Agent\Secfs\sec\bin\wminstall.exe
| exempt | C:\WINDOWS\explorer.exe
| exempt | C:\WINDOWS\regedit.exe
| exempt | C:\WINDOWS\system32\regedt32.exe
| exempt | C:\WINDOWS\system32\svchost.exe
| exempt | C:\WINDOWS\system32\services.exe
| exempt | C:\WINDOWS\system32\smss.exe

☐ Re-sign Settings (This toggle resets after a push to the CTE agent.)

Note

1 To delete the client settings, delete the content in the Settings box and click Update.
2 To edit the client settings, modify the content in the Settings box and click Update. When editing the settings strings, follow the format | privilege | file name.

Update

6. In the **Settings** box, update settings as appropriate.
7. Turn on the **Re-sign Settings** toggle.

☒ **Re-sign Settings** (This toggle resets after a push to the CTE agent.)

8. Click **Update**.

Enabling the Re-sign Settings toggle forces a signature update. On subsequent push of the client settings to the CTE Agent, the updated settings are re-signed and the Re-sign Settings toggle is turned off (or reset). If you do not turn on this toggle after adding a new process, the client ignores the newly added process.

Modifying Client Configuration

To modify the client configuration:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.

Note

Any data protection related fields such as Live Data Transformation and LDT Access Only and Multifactor Authentication are unavailable for Windows clients with the RWP protection mode.

1. Modify the following, as appropriate:
 - **Live Data Transformation:** Enabled or disabled based on the feature selection during registration. By default, LDT performs rekey operations on the LDT protected GuardPoints as soon as GuardPoints are enabled. To pause LDT rekey operations, expand the **ADVANCE SETTINGS** and enable **Live Data Transformation**.

After LDT has been enabled, it cannot be disabled. To remove the feature, you must migrate existing data protected under LDT policies, unregister the client, and delete the client. Then, you can reregister the client without enabling the feature. This allows you reclaim the license for use on another client.
 - **LDT Passive Mode:** By default, LDT Passive Mode is disabled. To enable LDT Passive Mode, expand **ADVANCE SETTINGS** and enable **LDT Passive Mode**. After you enable it, you can't disable it.

Note

- If the client supports LDT_P, this field appears.
- If Live Data Transformation is enabled, this field is hidden.

- **LDT Access Only:** (Windows only) Whether the client can be added to an LDT communication group.
 - If the check box is clear, the client can be added to or removed from an LDT communication group.
 - If the check box is selected, the client cannot be added to an LDT communication group.
- **Encryption Key Protection:** Enable or disable protection of encryption keys stored in the cache memory on the CTE client. The field is available to registered clients only.

When enabled, keys are removed from the cache after three minutes of inactivity and memory is overwritten with random data any time after a key is used.

When keys are cached in memory, they are encrypted in the cache and only decrypted when used. This adds a small overhead but extra security. The in-memory key cache is held in the operating system kernel and is not accessible to any user-space applications. Furthermore, Thales recommends that CTE only be run on operating systems that have been patched to prevent Meltdown and Spectre attacks. Subsequent releases will prevent the CTE agent from running if patches are not in place.

If a kernel crash dump is initiated, any clear-text key information (used to derive keys from encrypted cached key counterparts) is erased from memory before the crash dump is taken.

- **Cloud Object Storage:** (Non-editable, Linux only) Enabled or disabled based on the feature selection during registration. From the GUI, you can neither disable nor enable the Cloud Object Storage feature. To enable or disable it, register the client again and opt or opt out of the Cloud Object Storage feature. Refer to the [CTE Agent for Linux Quick Start Guide](#) for details.
- **File Header Supported (FHS):** (Non-editable, Windows only) Enabled or disabled based on the feature selection during Agent installation. When this feature is enabled, you can apply GuardPoints to SMB shares.

After FHS has been enabled, it cannot be disabled from the CipherTrust Manager. To turn off the feature, you must migrate existing data protected under LDT policies, unregister the client, and delete the client. Then, you can reinstall the client with the *LDT on CIFS* (File Header Support, FHS) capability *turned off*, and register with the CipherTrust Manager.

- **Secure Start:** (Non-editable, Windows only) Enabled or disabled based on the installed Agent capability. If the Agent supports the Secure Start feature, then this option is enabled, otherwise, the option is disabled.

To enable Secure Start, expand **ADVANCE SETTINGS** and enable **Secure Start**.

-
- **Multifactor Authentication (MFA):** Available based on the installed Agent capability.
 - If the Agent supports MFA, you can enable or disable the feature. By default, the feature is disabled. To enable MFA on the client, expand **ADVANCE SETTINGS** and enable **Multifactor Authentication**. To disable, clear the check box.

When enabled, access to the requested data is granted only after the requester satisfies configured authentication criteria. Refer to [Multifactor Authentication](#) for details.

 - If the Agent does not support MFA, the option is disabled and cannot be modified.
- **In-place Data Transformation - Device:** (Non-editable, Linux only) Enabled or disabled based on the installed Agent capability. If the Agent supports the feature, then this option is enabled, otherwise, the option is disabled.
 - **Domain Sharing:** Allow or deny sharing the client resources across domains. Refer to [Sharing Resources Across Domains](#) for details.
 - **Unlock:** Unlock Agent Lock and System Lock.
 - **Agent Lock:** Lock the contents of the CTE Agent directories on the client.
 - **System Lock:** Apply an internal policy to the client to lock client system directories, like `/var`, `/bin`, `/etc`. Enabling System Lock automatically enables Agent Lock.
 - **Communication Enabled:** Whether to enable the client's communication with the CipherTrust Manager. Expand **GENERAL SETTINGS**, select to enable and clear to disable communication. By default, the communication is enabled. For manually added unregistered clients, this option is editable if **Registration Allowed** is selected.
 - **Registration Allowed:** (Manually added unregistered clients) Whether to allow client's registration with the CipherTrust Manager. Expand **GENERAL SETTINGS**, select to allow and clear to deny registration. By default, the registration is not allowed.
 - **Password Creation Method:** Set the password creation method—Manual or Generate. Refer to [Changing Client Password](#) for details.
 - **Protection Mode:** (Editable for Windows clients) Set the protection mode for the Windows client.

To change the protection mode:

- a. Expand **ADVANCE SETTINGS**.
- b. Select the desired **Protection Mode**.

Note that changing the protection mode from RWP (Ransomware Protection) to CTE RWP is irreversible. Review your decision before proceeding with this change.

- c. Click **Update**.
-

Note

For non-Windows CTE clients and unregistered clients, the Protection Mode is **CTE**.

- **Supports Unique to Client keys:** Enable to generate the key-salt. To enable Unique to Client keys, expand **ADVANCE SETTINGS** and enable **Supports Unique to Client keys**.

The default state of this field depends on the CipherTrust Manager version used to create/register the client:

- Version 2.13 or later: The field is enabled by default.
- Version 2.12 or earlier: If the client uses [unique to client keys](#), this field is disabled. Follow the steps below to enable it.
 - a. Ensure that the client is ready to enable the **Supports Unique to Client keys** field.

Warning

The client functions correctly without the "Supports Unique to Client keys" enabled. Enable this field only when the client status is healthy and ready, that is, the client has no GuardPoints using the unique to client keys. Applying it to a client in another state may cause configuration conflicts or unexpected behavior.

- b. Identify the GuardPoints that are using a unique to client key.
 - If no GuardPoints are found, skip to the next step to enable the **Supports Unique to Client keys** field.
 - If the GuardPoints are found, unguard the GuardPoints using the unique to client keys.

Warning

It is important to decrypt the data. If you don't decrypt it, the data will be lost. After all the GuardPoints are unguarded, proceed to the next step.

- c. Enable the **Supports Unique to Client keys** field. Once this field is enabled, you cannot disable it.
- d. Guard the GuardPoints that you've unguarded above.

e. Perform the above steps for all the clients.

- **Client Profile:** Select a profile for the client. The default profile is DefaultClientProfile. If you did not specify a profile during registration, the client is linked with default profile. To change the client profile, refer to [Changing the Profile](#) for details.
- **Advanced Security Configuration:** View or edit the client's security configuration parameters. Refer to [Changing Security Configuration Parameters](#) for details.
- **Details (Read-only):** Shows the versions of the platform and kernel installed on the client, for example, RHEL7.8 - 3.10.0-1127.el7.x86_64. For unregistered or manually added clients, a hyphen (-) is displayed. For Windows clients, the field is empty.
- **Upgrade On Reboot (Read-only):** Displays when the next upgrade of the CTE Agent is scheduled. None is displayed if the upgrade is not scheduled. For unregistered clients, the field remains blank.
- **Agent Information:** Collect and download the Agent information (**agentinfo**) from the CTE Agent.
 - **Collect:** Informs the CTE client to collect the Agent information and send it back to the CipherTrust Manager. This is the default link.

After the Agent information is successfully received, the link changes to **Recollect** and **Download**.

- **Recollect:** Collects the latest Agent information from the CTE Agent.
- **Download:** Downloads the Agent information from the CipherTrust Manager in a tar file. After the download, the Agent information is removed from the CipherTrust Manager. In a CipherTrust Manager cluster, the information will be downloaded from the node where the Agent information is requested.

Refer to [Collecting Agent Information](#) for details.

- **Confidential Computing:** Enabled or disabled based on the feature selection during registration. If enabled, the all the data executions takes place within a trusted environment, safeguarding user's data from software attacks. For more information, see [Confidential Computing](#).
 - **ATTESTED:** Indicates that Confidential Computing is enabled and attestation is successful.
 - **NOT ATTESTED:** Indicates that Confidential Computing is enabled but attestation has failed.

After confidential computing has been enabled, it cannot be disabled. To remove the feature, you must unregister and delete the client. Then, you can re-register the client without enabling the feature. This allows you to reclaim the license for using on another client.

Note

If Confidential Computing feature is not opted during client registration, the **Confidential Computing**

field will display '-' as status.

- **FAM:** Whether FAM is enabled on the client. For more information, see [File Activity Monitoring \(FAM\)](#).

2. Click **Update**.

Changing the Profile

To change the client profile:

1. Open the **Transparent Encryption** application.
2. Click **Clients** > **Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **GENERAL SETTINGS**. The Client Profile section shows the current client profile and Rekey Option, Rekey Rate, and Schedule of the selected profile.

The screenshot shows the 'Client Profile' section with a dropdown menu currently set to 'DefaultClientProfile'. Below the dropdown, there are four status indicators: 'Log Level: ERROR', 'Rekey Option: RekeyRate', 'Rekey Rate: 0', and 'Schedule: ANY_TIME'. A blue link 'Go to the Selected Profile' is located to the right of these indicators.

6. From the **Profile** drop-down list, select the desired profile.
7. Click **Update**. The selected profile is linked successfully.

Changing Security Configuration Parameters

The CipherTrust Manager provides options to modify certain security configuration parameters configured on the CTE client. The list of editable configuration parameters can vary based on the capabilities supported by the CTE Agent installed on the client. Refer to the [CTE Agent documentation](#) for compatible versions and dynamic parameters.

To view or change the security configuration parameters:

1. Open the **Transparent Encryption** application.
2. Under **Client Name**, click the desired client.
3. Next to **Advanced Security Configuration**, click the **View/Edit Settings** link. The Advanced Security

Configuration dialog box lists the security configuration parameters that can be updated after the CTE client is registered with the CipherTrust Manager. Every parameter has the fixed set of values.

Note

The `PTRACE_PROTECTION` feature is not applicable to CTE for Windows Agents.

4. Change the security configuration, as appropriate.
5. Click **Save**. The security configuration is changed successfully.

CTE Linux Authentication and Client Settings

CTE Linux client (also known as host) settings, which ensure CTE user access controls and systems protection, is a CipherTrust encryption feature that is often difficult to understand and configure. This section provides an updated description of CTE Linux 7.1.1 client settings, authentication, and different authenticators.

The intended audience of this information are CTE and CipherTrust Manager administrators. It is assumed that they are knowledgeable on Linux/Unix concepts, techniques, and security features. Additionally, it is assumed that they have read the CTE and CipherTrust Manager administration documents and are familiar with the CipherTrust Manager security policies and capabilities.

Root Privileges

Users with root privileges on Linux systems have unrestrained capabilities to override all file access and execution permissions imposed by the system. `setuid` programs running with root permissions and privileges can create, remove, or modify any files in the system. By exploiting the ability to escalate privileges, adversaries can subvert system controls and access and steal confidential data.

CTE Access Controls

Use CTE access controls to:

- Curtail privileges of root users and `setuid` programs.
- Specify policies to restrict "who, *the client system users or groups*" and "what, *the application processes or binaries*" access to protected data within CTE GuardPoints.

Individual users (including root) accessing the CTE GuardPoint data can therefore be granted or denied access.

The CipherTrust Manager policies track and prevent privileged users (including `setuid` root programs) from reading, modifying, or executing files and directories residing in the GuardPoints owned by normal/unprivileged users.

For every running operating system process, CTE maintains a separate trusted ID distinct from each process' real and effective UIDs. This trusted ID is used for making decisions based on user-related policy evaluations. One such example is CTE differentiating between:

-
- A user who logs in, and is therefore explicitly authorized, as root.

AND

- A user who logs in, is authorized as a normal/unprivileged user, and subsequently runs a potentially malicious `setuid` program like `su` to gain root privileges.

System (and in some cases, certain classes of users) applications on the CTE client such as `sshd`, `login`, and `su` etc. authenticate a user's identity by requesting user credentials, authorizing the user, and spawning child processes.

Therefore, for a process to access protected data, the user's identity must be established as authenticated and authorized by these special authenticator binaries. Processes (including their descendants) spawned by authenticators like `sshd` and `login` are treated as authorized and therefore trusted. The real (or in some cases, effective) UID of the progeny is recorded for granting access. Processes continue to be tracked and identified with the original trusted ID even though its operating system UID and effective user ID (EUID) may change without proper authorization. Invocation of a `setuid` root program to acquire root privileges or a root user issuing `su` to become another user are some examples of unauthorized (and possibly malicious) transitions.

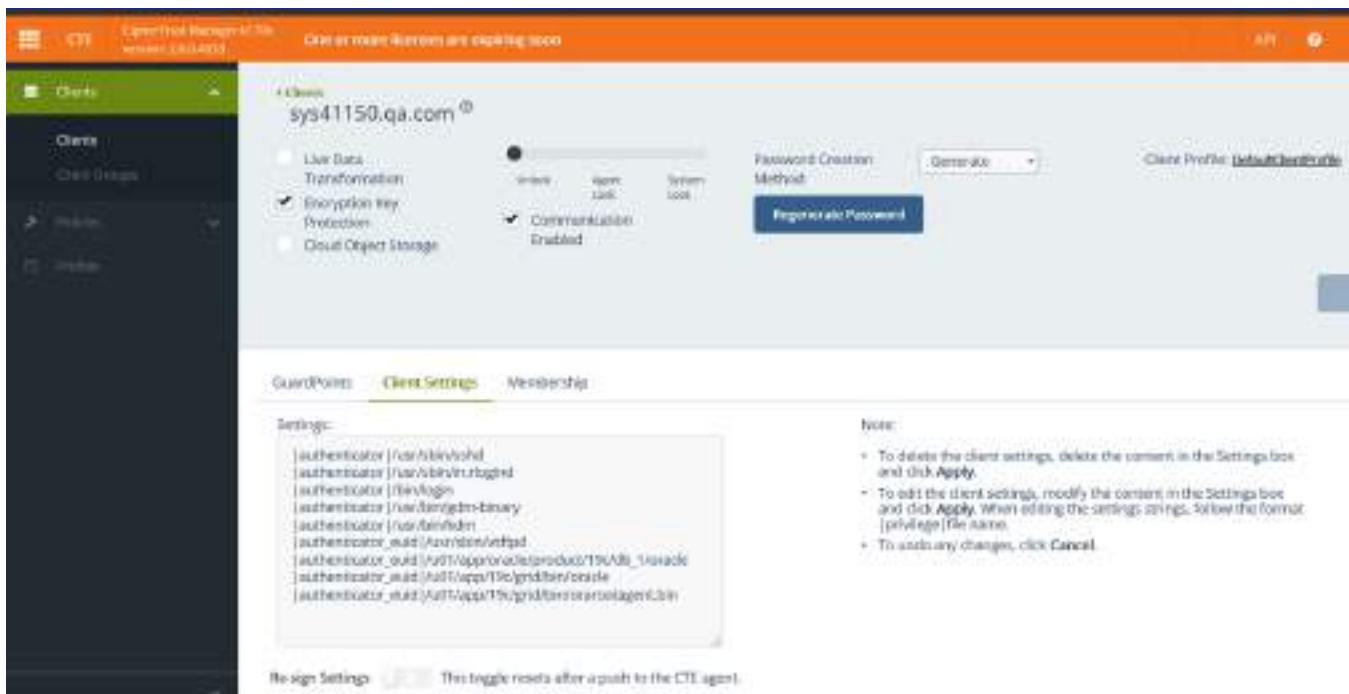
For example, `sshd` runs as user root. When a user logs into a system using `sshd`, it forks off a child process, changes the UID of that process to the logged in user (say, `alice`), and then executes a process like `bash`. Because `sshd` is tagged with `|authenticator|`, CTE records the trusted user ID of the new process and of every process that it spawns with `alice`'s real UID. If `alice` tries to change its UID to root by running a `setuid` root program, it changes according to the operating system, but not according to CTE. From a policy evaluation standpoint, CTE still treats the `setuid`-escalated root process with user ID `alice`. If the GuardPoint policy prevents root accesses, CTE denies this root-escalated process from accessing the GuardPoint as an unauthorized operation. In this case, CTE terms the root user as a fake user and logs it as such.

By default, the CTE Agent does NOT trust any process as authenticated. Any attempt to access a resource by any process is therefore flagged with a `User Not Authenticated` notification. Therefore, the CTE Agent is to be instructed to trust the authenticator process progeny. For example, `/usr/sbin/sshd` is a process that can be trusted to authenticate the user to the system and to CTE.

CTE client settings are the means by which an administrator configures user authorization. Client settings are tags or keywords with pipe (|) delimiters specifying full-system binary paths to trusted programs (referred to as authenticators) on the CTE client. The subsequent sections describe the client settings tags, their properties and behavior, and the equivalent binaries and best practices.

Enabling CTE Client Settings for Authenticator Programs on the CipherTrust Manager

Client settings can be enabled for individual clients or client groups with the CipherTrust Manager GUI or REST API. On the CipherTrust Manager GUI, the Client Settings tab of clients is used to configure client settings.



Refer to [Client Settings](#) for details.

The client settings provided by the default installation are examples. It is recommended to *remove* all unnecessary client settings, as these may pose *security risks*.

Adding, Removing, or Modifying Client Settings

When client settings are modified, it is recommended to verify the updated settings after some time (a few minutes later). This can be done by running `secfsd -status auth`. Also, before applying the new client settings, the dependent applications, if any, should be *stopped*.

Description of Authenticators

authenticator

The `authenticator` keyword is used to specify the full path of the authenticator program authorizing the real UID of the process progeny. The real UID of the process and its descendants are used to set CTE's trusted UID. Therefore, CTE follows and authorizes the real UID of the user authenticator process and its descendants. In general, programs that use user name and password pairs (for example, `sshd` and `login`) are candidates for being authenticators.

Example of client settings:

```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
```

Programs that do not authenticate users should not be tagged as authenticators. Examples of such programs include `su` invoking `setuid/seteuid` or `setgid/setegid` system calls. Tagging `/usr/bin/su` with the

authenticator keyword authorizes a root user to become a non-privileged user even without authentication. Therefore, `/usr/bin/su` should not be set as an authenticator.

`/usr/bin/su` can be set as an authenticator in cases where a root administrator legitimately uses `su` to temporarily switch privileges. This mode should be used *sparingly*.

authenticator_euid

The **authenticator_euid** keyword works similar to **authenticator**, but instead of the real UID, the CTE access control uses EUID for granting access. Specifically for Oracle, the database process (**oracle**) is started by the root process and then a **setuid** system call forces the service account user ID of either **oracle** or **orauser**. For such processes, CTE should rely on the EUID of the process for authentication.

The `|authenticator_euid|` keyword is applied as follows:

```
|authenticator_euid|/u01/app/oracle/dbhome_1/bin/oracle
|authenticator_euid|/u01/app/grid/bin/grid
```

Similarly, DB2's **db2start** application binary should have the **authenticator_euid** tag.

su_root_no_auth

The **su_root_no_auth** keyword is applicable only to the `/usr/bin/su` binary and should be deployed with the **sshd** authenticator:

```
|authenticator| /usr/bin/sshd
|su_root_no_auth| /usr/bin/su
```

With **su_root_no_auth**, a non-root user is permitted to log in as another user through `su`. The new user is authorized after authentication, that is, after providing the new user's password. However, root is prevented from being authorized as another user.

path_no_trust

The **path_no_trust** keyword instructs CTE to not trust, that is, not authorize a binary's process and its progeny. Therefore, users associated with these processes are unauthorized and flagged as such when accessing CTE GuardPoint data.

For example, `/usr/bin/ksh` is tagged as **path_no_trust** while `/usr/bin/su` is tagged as **authenticator**. A user who runs `/usr/bin/su` from this non-trusted `ksh` is unauthorized even though `/usr/bin/su` is a valid authenticator.

The **path_no_trust** keyword can be used to disallow selected executables from a large pool, for example, to trust all client binaries except three specific ones. This is achieved as follows:

```
|trust|*
|path_no_trust| /usr/bin/su
|path_no_trust| /usr/bin/ksh
|path_no_trust| /usr/bin/login
```

These client settings allow all client binaries to be trusted except `/usr/bin/su`, `/usr/bin/ksh`, and `/usr/`

`bin/login`.

It is important to note the `path_no_trust` authenticator overrides any previous authenticator tags placed on the same binary. For example, when tagging the `/usr/bin/su` binary, `path_no_trust` overrides any authenticator tags already set on `/usr/bin/su`.

The behavior described above is applicable to CTE 7.1.1 and higher versions. For older CTE versions, `|trust|*` overrides all other authenticator tags.

trust

The `trust` keyword is a carryover from older CTE versions and retained for legacy/backwards compatibility. The `|trust|*` authenticator allows users to be trusted regardless of the authentication method.

This mode, however, weakens against attacks by root users (that is, system administrators). Its use is *strongly discouraged*.

Conclusion

CTE access controls require correct specification of client setting authenticators for proper authorization. This document highlights various authenticators supported by CTE 7.1.1 and their use cases. Future releases of CTE will continue to expand access controls and authenticator capabilities.

References

1. Using Host Settings for Linux with VTE. Thales white paper. March 2017
2. [CTE and CipherTrust Manager Documentation](#)
3. Advanced Programming in Linux and Unix Environments. Stevens & Rago 3rd Edition
4. Linux man pages including `su(1)`, `login(1)`, `sshd(8)`, `setuid(2)`, the `setuid(4)`, and `seteuid(4)` APIs etc.

Appendix 1: Deploying the Correct Authenticator

Here are the basic questions for determining what client setting authenticators to apply to the process.

- Does the process authenticate users, having them supplied credentials?

YES:

```
|authenticator|<path-to-binary>/<binary-name>
```

- Is the process started and run as a service account, specifically by the root account?

YES:

```
|authenticator_euid|<path-to-binary>/<binary-name>
```

- Does the process run with a specific user ID, and whether no other user IDs should be allowed?
-

YES:

```
|authenticator_euid|<path-to-binary>/<binary-name>
```

- Should root be prevented from becoming any other user to access data?

YES:

```
|authenticator|/usr/bin/sshd
|su_root_no_auth|/bin/su
```

- How do I use authenticator keywords with Java applications?

Java runtime binary file can be set as follows:

```
|authenticator_euid|<path-to-binary>/java
```

Contact [Thales Customer Support](#) for specifying arguments to Java programs.

Appendix 2: Related Non Authenticator Client Settings

protect

The `|protect|` keyword protects the system credential files from tracking and preventing malicious updates. Refer to the [CTE Agent Advanced Configuration and Integration](#) documentation for additional details on these client settings.

Appendix 3: Description of Common Audit Messages

User Not Authenticated

This message indicates CTE is unable to establish the user's authorization status due to incomplete information from authenticator application processes.

```
2021-04-07 03:46:06.728 [CGP] [ERROR] [5206] [CGP2602E] [ALARM] Policy[host-sett
ings-policy] User[root,uid=0,euid=0 (User Not Authenticated) (bash[pid=5058,ui
d=0,euid=0] : sshd[pid=5035,uid=0,euid=0]:sshd[pid=4991,uid=0,euid=0] : systemd[p
id=1,uid=0,euid=0]]) Process[/usr/bin/cat]Action[read_file]Res[/home/bob/gp/testf
ile]Key[None] Effect[PERMITTED Code (1A,2U,3M)]
```

Possible reasons include:

- The user logging in even before CTE started.
- A misconfigured authenticator client setting (possibly due to incorrect paths).

Therefore, a policy restricting specific user accesses to GuardPoints fails evaluation.

User Impersonation

```
2021-04-07 04:10:24.714 [CGP] [ERROR] [7865] [CGP2602E] [ALARM] Policy[host-sett
ings policy] User[root,uid=0,euid=1004,gid=0\\root\\ (faked as(bob,1004)) (bash[p
id=7819,uid=1004,euid=1004] : su[pid=7818,uid=0,euid=0] : bash[pid=7736,uid=0,eui
d=0] : sshd[pid=7724,uid=0,euid=0] : sshd[pid=7697,uid=0,euid=0]]) Process[/usr/b
in/cat] Action[read_file] Res[/home/bob/gp/testfile] Key[None] Effect[FAKED USE
R!! DENIED Code (1A,2U,3M)]
```

A user (in this case, root) logs in and is authorized by an authenticator application. A descendant process subsequently runs an unauthorized (non-client setting authenticator) `setuid` binary to change to another user named bob without authentication. Therefore, the process is still authorized as root and not bob. Therefore, bob is termed a fake user.

Cron

Cron is started by the `init` process during system boot. It runs as a root process, processes the `crontab` jobs, and runs the requests as the designated user. A root user could cause a cron entry to be run as any other user without that user being authenticated or authorized. Cron-based authentication is not supported.

Changing Client Password

Offline Password

CTE supports the offline password feature. This feature is designed to enable retrieval of the keys being used to protect data in a GuardPoint. When communication between the CipherTrust Manager and the CTE Agent are lost, the GuardPoint continues to encrypt/decrypt data with the current last known key and policy. However, if the communication is lost and the protected client is rebooted, the CTE Agent attempts to validate it using the latest keys and policies, but fails. Therefore, a password can be used by the isolated CTE Agent to retrieve the last known key and policy to enable the GuardPoint to continue with encryption/decryption operations. After the communication is re-established, any policy or key changes can be applied.

The offline password feature enables access to encryption keys that are stored locally on a client. This keeps the data secure when the CipherTrust Manager is inaccessible. To access the data, provide the offline password. Then, the CTE Agent encrypts/decrypts the guarded data according to the applied policy.

Password Types

The client password is initially set when the client is added to the CipherTrust Manager. Passwords can be set on a client-by-client or client group basis. The CipherTrust Manager supports two types of offline passwords:

- **Manual** (Static): A password is specified manually.
- **Generate** (Dynamic): A password is generated automatically by the CipherTrust Manager.

Changing the Password

You can change the password manually or dynamically. To change the password:

1. Open the **Transparent Encryption** application.

2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **SECURITY SETTINGS**.
6. Click the desired tab to view the instructions.

Change Password Manually

- a. In the **Password Creation Method** section, select **Manual**. The **Regenerate Password** button is replaced by **Change Password**.



- b. Click **Change Password**.
- c. Enter the new password in the **Password** and **Confirm Password** fields. The password must match in both the fields.

Note

The password must contain minimum eight characters including at least:

- One capital letter
- One number
- One of these special characters: ! @ # \$ % ^ & * () { } []

- d. Click **Update**.

When changing a static password or modifying a client to use a static password instead of a dynamic password, provide the new static password to the client users. Without the password, they cannot access encrypted data when there is no network connection between the client and the CipherTrust Manager.

The users can access the data stored in GuardPoints on the client by either running the `vmsec password` command or using the [challenge-response](#) method.

Change Password Dynamically

- a. In the **Password Creation Method** section, select **Generate**. This is the default method.
- b. Click **Regenerate Password**.

A new generated password is downloaded to the client.

Note

When modifying a client to use a dynamic password instead of a static password, inform the client users that challenge-response authentication is enabled and they need to run `vmsec challenge` on UNIX/Linux clients or select **Password...** on the Windows etray when the client cannot connect to the CipherTrust Manager.

Accessing GuardPoints in Offline Mode

This section is applicable to the CTE client administrators. This information is given here to show the end-to-end flow of the challenge-response process.

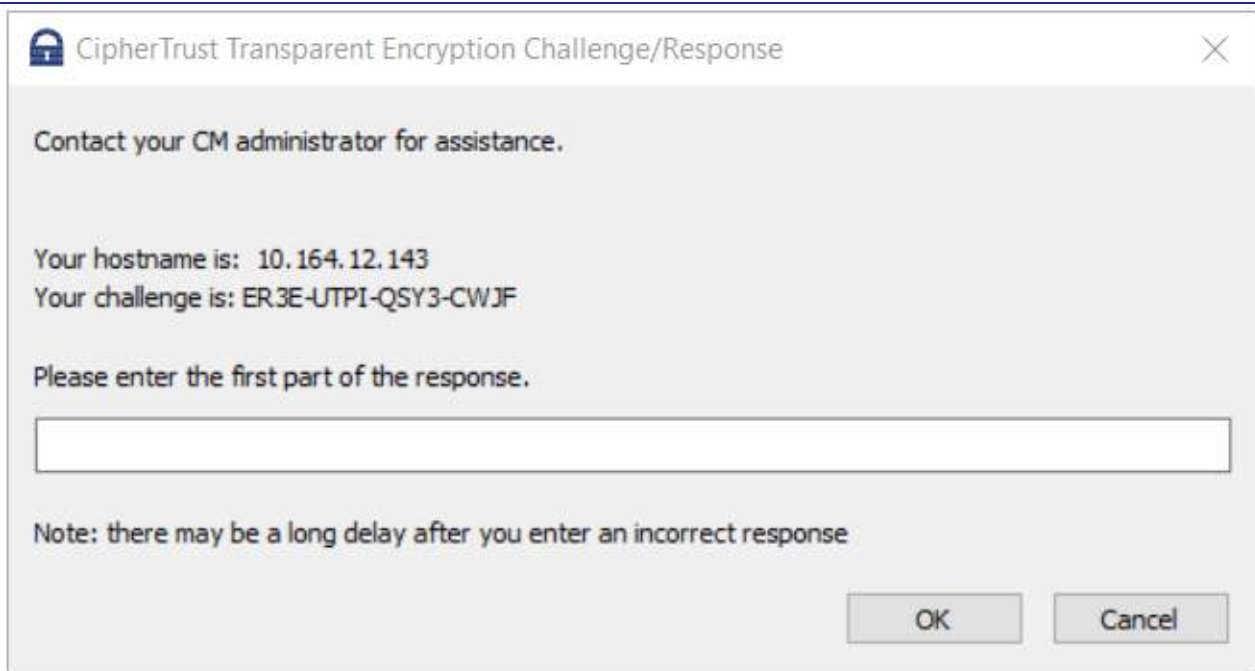
When the CipherTrust Manager is unreachable from a protected client, the data stored in GuardPoints on the client cannot be accessed without the challenge-response.

To access the GuardPoints in offline mode:

1. Log on to the offline CTE client.
2. Depending on your platform, do the following:
 - On UNIX/Linux, run the command, `vmsec challenge`.

```
vmsec challenge
Contact your CM administrator for assistance.
Your hostname is 10.164.14.207
Your challenge is: FHEH-ICPL-2MCZ-2AHI
Response (part 1) ->
```

- On Windows, select **Password...** on the Windows etray, then select **Challenge... > Response...**. The CipherTrust Transparent Encryption Challenge/Response dialog box is displayed, as shown below.



Your CipherTrust Manager administrator will need the hostname of your client and the challenge shown above in the command output (for Linux/AIX) and in the screenshot (for Windows).

3. Contact your CipherTrust Manager administrator.
4. Provide the challenge (for example, **FHEH-ICPL-2MCZ-2AHI**) to the administrator.

The CipherTrust Manager administrator generates responses in four parts on the CipherTrust Manager. Refer to [Generating Response for a Challenge](#) for details. Contact the CipherTrust Manager administrator for the response codes.

5. Enter the response (part 1 through 4) on the `vmsec challenge` command prompt (on Linux/AIX) or on the CipherTrust Transparent Encryption Challenge/Response dialog box (on Windows). The responses must be entered in the given order. For example:

```
Response (part 1) -> STYB-JAZE-C2PB-6FLU
Response (part 2) -> F7ME-R3MG-BQB5-5MXB
Response (part 3) -> QN26-0A6F-5ZKA-T5LG
Response (part 4) -> BI4Y-53AI-30XZ-N2EC
Success!
```

The client users can now access protected GuardPoints on the client.

Generating Response for a Challenge

To generate a response for a challenge:

1. Log on to the **CipherTrust Manager** GUI.

-
2. Open the **Transparent Encryption** application.
 3. Click **Clients > Clients**.
 4. Click the desired client.
 5. Click the **Challenge Response** tab.
 6. In the **Challenge From the Client** box, enter the challenge provided by the client administrator.
 7. Click **Submit**.

A set of four responses (part 1 through 4) for the provided challenge is shown on the GUI. Provide those to the client administrator.

Managing Membership

View and manage the client group memberships of a client on the Membership tab. The Membership tab is divided into CLIENT GROUPS and LDT COMMUNICATION GROUP sections. The CLIENT GROUPS section provides an option to remove the client from individual or multiple client groups. The LDT COMMUNICATION GROUP section provides an option to add or change the LDT communication group membership for the client.

Viewing Group Membership of a Client

To view the client groups of a client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **Membership** tab.
5. Expand the **CLIENT GROUPS** section. The section shows the client groups the client is a member of.

GuardPoints Client Settings **Membership** Sharing Challenge Response

CLIENT GROUPS

Search

☐ 0 Selected 1 Result | 1 Client Group

Client Group Name	
☐	A1

Removing a Client

As part of the CipherTrust Manager maintenance, you occasionally need to remove a client from its client groups. The CipherTrust Manager provides options to remove a client from individual client groups or from multiple client groups in one go.

To remove the client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **Membership** tab.
5. Expand the **CLIENT GROUPS** section, if needed.

GuardPoints

Client Settings

Membership

Sharing

Challenge Response

CLIENT GROUPS

Search

☐ 0 Selected 1 Result | 1 Client Group

Client Group Name		
☐	A1	...

6. Click the desired tab to view instructions.

From a Single Client Group

- Under **Client Group Name**, select the group from which you want to remove the client.
- Click the delete icon ().

Alternatively, click the overflow icon () corresponding to the desired client group, and click **Remove**. A dialog box appears prompting to confirm the action. Click **Remove** to remove the client.

- Click **Delete**.

The client is removed from the selected client group. Also, the client group is removed from the CLIENT GROUPS section of the client's Membership tab.

From Multiple Client Groups

- Under **Client Group Name**, select the groups from which you want to remove the client.

To select all client groups visible on the page, select the top check box to the left of the Client Group Name heading.

- Click the delete icon ().

A dialog box appears prompting to confirm the action.

- Click **Delete**.

The client is removed from the selected client groups. Also, the client groups are removed from the CLIENT

GROUPS section of the client's Membership tab.

Viewing LDT Communication Group Membership of a Client

To view the LDT communication group of a client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **Membership** tab.
5. Expand the **LDT COMMUNICATION GROUP** section. The LDT Communication Group drop-down list shows the LDT communication group the client is a member of.

GuardPoints Client Settings **Membership** Sharing Challenge Response

[Expand All](#)

CLIENT GROUPS +

LDT COMMUNICATION GROUP -

LDT Communication Group

ldt-gp1

Update

Adding or Changing LDT Communication Group Membership of a Client

Clients can be added to an LDT communication group when creating or updating the group. You can also add or change the LDT membership of a client on the Membership tab. A client can be added to only one LDT communication group at a time.

The Windows clients that have the **LDT Access Only** check box selected cannot be added to the LDT communication group.

To add or change the LDT communication group of a client:

1. Open the **Transparent Encryption** application.

-
2. Click **Clients > Clients**.
 3. Under **Client Name**, click the desired client.
 4. Click the **Membership** tab.
 5. Expand the **LDT COMMUNICATION GROUP** section, if needed.
 6. Select the desired **LDT Communication Group** from the drop-down list.
 7. Click **Update**.

The selected LDT communication group is linked with the client.

Removing LDT Communication Group Membership of a Client

To remove the LDT communication group membership of a client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **Membership** tab.
5. Expand the **LDT COMMUNICATION GROUP** section, if needed.
6. Click the remove icon () next to the LDT Communication Group drop-down list.

The LDT communication group membership is removed from the client.

Deleting Clients

Only CipherTrust Manager administrators can delete clients. When a client is deleted from the CipherTrust Manager, the client moves to the [Expunged state](#) and the CTE Agent is notified to drop client configuration. The CTE Agent installations on the client continue to run, complete with the applied policies. To completely remove a CTE Agent from the client, uninstall the Agent from the client system.

When Agent uninstallation is initiated, the client record is deleted from the CipherTrust Manager. The CipherTrust Manager pushes the configuration change to the CTE Agent running on that client. As a result, the following occur on the client:

- CTE Agent certificates are deleted.
- The URL line is removed from the `agent.conf` file.
- The GuardPoints are removed.
- The client is no longer recognized by the CipherTrust Manager. If the CTE Agent tries to communicate with the CipherTrust Manager, the connection is refused.

Deleting Clients with System Lock or Agent Lock

Do not unregister or delete the CTE client while locks are applied. The locks remain effective after the client is unregistered. Without client credentials, the CipherTrust Manager cannot administer that CTE Agent and cannot disable the locks. You must boot the client in single-user mode and manually modify the Agent configuration to disable the locks.

To remove everything associated with a client (including the CTE Agent):

1. Apply a rekey policy and run `dataxform` on the client to decrypt encrypted files.
2. Disable the locks on the client. Refer to [Disabling Locks](#).
3. Remove all the GuardPoints from the client.
4. Click **Clients > Clients**.
5. Under **Client Name**, click the overflow icon () corresponding to the desired client.
6. Click **Delete**. A dialog box appears prompting to confirm the action.
7. Click **Delete**.

The client administrator with root permissions must log on to the client system and uninstall the CTE Agent.

Refer to [Deleting Clients](#) for more information on deleting clients from the CipherTrust Manager.

Deleted Client Indicators

A client is successfully deleted from the CipherTrust Manager GUI if:

- CipherTrust Manager URL is deleted from the CTE Agent `agent.conf` file.
- Certificates are removed from the `./agent/pem` directory.

However, if the client is deleted and its identity is changed while it is *offline*:

- The GuardPoints are not removed
- The certificates remain intact in the `./agent/pem` directory
- The `agent.conf` file remains unchanged
- But the Agent and CipherTrust Manager still cannot communicate with each other.

Logging for the CTE Agent on the CipherTrust Manager is also affected if an offline client is deleted. When the client comes online, log messages about the denied connection can be viewed only by CipherTrust Manager administrators of type System or All (when not in a domain). This is because the CipherTrust Manager:

- No longer has the client's record.
- Does not know which domain and the group the client belongs to.

- Cannot send messages to the appropriate log service.

Kernel Compatibility Matrix

A registered CTE Linux client should be running a compatible kernel. Refer to the latest [Compatibility Matrix](#) for the list of supported kernels.

You can also upload the latest Compatibility Matrix (a .tgz file) to the CipherTrust Manager so it automatically matches the kernels running on the registered clients. If a client is running an incompatible kernel, its status becomes Warning on the GUI.

Note

After upgrading CipherTrust Manager to version 2.21 or later, the **Uploaded File Creation Date (Local Timezone)** label incorrectly displays the upload time of the previously uploaded compatibility matrix, instead of its creation time.

When you reupload the old or new compatibility matrix, the original creation time is shown.

Uploading Compatibility Matrix

To upload the Compatibility Matrix:

1. Download the latest [Compatibility Matrix](#) file.
2. Open the **Transparent Encryption** application.
3. Click **Clients > Clients**.
4. Click **Compatibility Matrix**. The Compatibility Matrix dialog box is displayed.

Compatibility Matrix

The CipherTrust Manager uses the compatibility matrix to display warning for the clients running unsupported kernels.

Upload Compatibility Matrix

Browse

5. Click **Browse** to locate and select the Compatibility Matrix file.
6. Click **Save**.

After the matrix is uploaded, the CipherTrust Manager starts matching the kernels running on the registered

clients. Depending on the number of registered clients, the Status may take some time to update.

Note

When you upload a compatibility matrix to a domain, it will automatically be inherited by any subdomains that don't have their matrix. This inheritance continues down the hierarchy from domain to subdomain to sub-subdomain, and so on until a domain with its matrix is found.

If a domain doesn't have a compatibility matrix, it will inherit the compatibility matrix of its nearest ancestor. For example, if a domain is a sub-subdomain, it will inherit the compatibility matrix of the subdomain, not the domain.

Replacing the Compatibility Matrix

Whenever a new version of the Compatibility Matrix is available, you can replace the existing matrix with the new one. The Compatibility Matrix dialog box shows details of the currently uploaded matrix, with the uploaded file creation date (local timezone).

To replace the matrix:

1. Download the latest [Compatibility Matrix](#) file.
2. Open the **Transparent Encryption** application.
3. Click **Clients > Clients**.
4. Click **Compatibility Matrix**. The Compatibility Matrix dialog box is displayed.
5. Under REPLACE/UPLOAD NEW FILE, click **Browse** to locate the latest Compatibility Matrix file.
6. Click **Save**.

The old Compatibility Matrix is now replaced with the latest version. The CipherTrust Manager now starts matching the kernels running on the registered clients with those in the new matrix. Depending on the number of registered clients, the Status may take some time to update.

Downloading the Compatibility Matrix

Whenever needed, you can download the Compatibility Matrix uploaded to the CipherTrust Manager.

To download the matrix from the CipherTrust Manager:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Click **Compatibility Matrix**. The Compatibility Matrix dialog box is displayed.
4. Under EXISTING FILE DETAILS, click the Overflow Icon (), and click **Download**.

The uploaded Compatibility Matrix is now downloaded to your local machine.

Removing the Compatibility Matrix

Whenever needed, you can remove the Compatibility Matrix uploaded to the CipherTrust Manager.

To remove the matrix from the CipherTrust Manager:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Click **Compatibility Matrix**. The Compatibility Matrix dialog box is displayed.
4. Under EXISTING FILE DETAILS, click the Overflow Icon (), and click **Remove**.

The Compatibility Matrix is now removed. The CipherTrust Manager no longer matches the kernels running on the registered clients.

Collecting Agent Information

A CTE Agent provides the **agentinfo** utility to collect system and CTE configuration data. The **agentinfo** utility takes a configuration snapshot of the system that you can send to Thales Customer Support to debug an issue.

The latest information about individual CTE Agents can also be collected and downloaded on the CipherTrust Manager GUI. The collected information about all the CTE Agents is stored in a dedicated volume on the CipherTrust Manager. An option is provided to clean the Agent information about all the CTE Agents from the volume.

Collecting the CTE Agent Information

To collect the latest CTE Agent information:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **GENERAL SETTINGS**.
6. Click **Collect Agent Information**. A request is sent to the CTE Agent to send the latest Agent information to the CipherTrust Manager.

Note

If the connection between CM and Agent is not established, the agent information will not be available for the client.

Fetching the latest Agent information from the CTE Agent might take some time. You need to *refresh* the page to download the latest Agent information. As soon as the information is available, the **Collect Agent Information** link is replaced with the **Recollect Agent Information** and **Download Agent Information** links.

Recollecting the CTE Agent Information

After you have fetched the CTE Agent information from the CTE client, a CTE Client Administrator might make some confirmation changes. To get the updated CTE Agent configuration on the CipherTrust Manager, use the Recollect option.

To recollect the updated CTE Agent information:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **GENERAL SETTINGS**.
6. Click **Recollect Agent Information**. A request is sent to the CTE Agent to send the updated Agent information to the CipherTrust Manager.

Fetching the latest Agent information from the CTE Agent might take some time. The **Recollect Agent Information** and **Download Agent Information** links are replaced with **Collect Agent Information**. You need to *refresh* the page to download the latest Agent information. As soon as the information is available, the **Collect Agent Information** link is replaced with the **Recollect Agent Information** and **Download Agent Information** links.

Downloading the CTE Agent Information

After you have fetched the Agent information from a CTE client, you can download this information from the CipherTrust Manager GUI. The information is downloaded in a tar file.

After the download, the Agent information is removed from the CipherTrust Manager.

In a CipherTrust Manager cluster, the information will be downloaded from the node where the Agent information is requested.

To download the CTE Agent information:

1. Open the **Transparent Encryption** application.

2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. Click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **GENERAL SETTINGS**.
6. Click **Download Agent Information**.

The CTE Agent information currently available on the CipherTrust Manager is downloaded in a tar file, and removed from the CipherTrust Manager. The **Recollect Agent Information** and **Download Agent Information** links are again replaced with **Collect Agent Information**.

Cleaning the CTE Agent Information Volume

When you fetch the CTE Agent information from a CTE Agent, this information is stored in a file in a dedicated volume on the CipherTrust Manager. This volume contains information about all the CTE Agents from which you have collected the information.

The CipherTrust Manager provides an option to [clean the Agent information volume any time](#) to remove all the files containing the Agent information from the CipherTrust Manager. Also, when the [volume is 80% full](#), you are prompted to clean it while collecting the latest Agent information from clients.

Clean the Volume Any Time

To clean the volume containing the CTE Agent information:

1. Log on to the **CipherTrust Manager** GUI.
2. Open the **Transparent Encryption** application.
3. Navigate to **Settings > Client Information and Capabilities**.
4. Under **Empty CTE Agent Information Log Volume**, click **Remove Agent Information**. A warning message is displayed.

Warning

The Agent information currently available on the CipherTrust Manager will be removed. You will have to regenerate the Agent information.

5. Select **Yes, clean up the entire volume containing the Agent information**.
6. Click **Clean**.

Clean the Volume When 80% Full

When the volume containing the Agent information is 80% full, a warning message is displayed while collecting the Agent information from a client. You need to clean the volume to collect the latest information.

To clean the volume, click **Clear Volume**. All the files containing the Agent information are removed from the volume. You can now retry collecting the latest Agent information.

Fetching Latest Capabilities from Clients

Note

This feature will be available from CTE 7.5.0.

CipherTrust Manager 2.14 and Lower

When a CTE Agent supports a capability but the CipherTrust Manager with which the Agent is registered doesn't, the CipherTrust Manager ignores the unsupported capability. After the CipherTrust Manager is upgraded to 2.14 or a lower version, the CipherTrust Manager requires the CTE Agent restart to fetch the latest capabilities from the client.

CipherTrust Manager 2.15 and Higher

When a CTE Agent supports a capability but the CipherTrust Manager with which the Agent is registered doesn't, the CipherTrust Manager ignores the unsupported capability. After the CipherTrust Manager is upgraded, the CipherTrust Manager administrator can fetch the latest capabilities from all the active clients present in the current domain without requiring the Agent restart.

Note

When a CipherTrust Manager that doesn't support the CTE Confidential Computing (CC) capability is upgraded to a version that supports the capability, you must unenroll and re-register any CC-capable CTE Agents already registered with the CipherTrust Manager to use CC.

To fetch the latest capabilities from active clients of the current domain:

1. Log on to the **CipherTrust Manager** GUI.
2. Switch to the desired domain.
3. Open the **Transparent Encryption** application.
4. Navigate to **Settings > Client Information and Capabilities**.
5. Under **Request Capabilities from All Clients**, click **Get Capability**.

A confirmation message appears stating that this is a time intensive operation and would run in the

background. This process may take a few minutes to complete depending on the number of active clients in the current domain. The active CTE clients will continue working with no impact. Do you want to continue?

6. Click **Get Capability**.

The latest capabilities are fetched from all the active CTE clients present in the current domain. Update Client Capability audit records are generated on the CipherTrust Manager. Review the records on the Server Records tab of the Loki Audit Records page (**Records > Loki Audit Records**).

Note

When a request to fetch the latest client capabilities is in progress, triggering the operation again will lead to an error message.

Managing LDT Communication Groups

An LDT communication group contains a group of LDT-enabled CTE clients that can communicate with each other. An LDT communication group is mandatory when using a multi-node solution for LDT over NFS/CIFS. The CipherTrust Manager pushes the LDT communication group details to all clients in the group.

Note

- The LDT communication groups are applicable to the LDT-enabled CTE clients.
- A client can be added to only one LDT communication group at a time.
- For successful communication among clients in an LDT communication group, make sure that clients are registered with the CipherTrust Manager using their hostnames or IP addresses.

Warning

All the clients guarding a common share must be part of the same LDT communication group, otherwise, data may be corrupted. If you need to change the LDT communication group of a client, ensure that the client no longer guards the common share.

For example, if 10 clients will be guarding a common share, add all of them to the same LDT communication group only. To change the LDT communication group of one of these clients, ensure that the client no longer guards the share. However, to change the LDT communication group of all 10 clients, it is recommended to take the GuardPoint offline, change the LDT communication group, and reapply the GuardPoint.

Creating an LDT Communication Group

To create an LDT communication group:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > LDT Communication Groups**.
3. Click **Create LDT Communication Group**. The Create LDT Communication Group wizard is displayed.
4. On the General Info screen:
 - a. Specify a **Name** for the LDT communication group. The name must start with a letter or number and can only have alphanumeric characters, periods (.), underscores (_), pipes (|), and hyphens (-).
 - b. Provide a **Description** for the LDT communication group.
 - c. Click **Next**.
5. On the Add Clients screen:
 - a. Select the clients to be added to the LDT communication group. Use the Client Name filter to search for the desired clients. Only the clients that are not part of an LDT communication group are displayed. Also, the Windows clients that have the **LDT Access Only** check box selected cannot be added to the LDT communication group.

To select all clients visible on the page, select the top check box to the left of the Client Name heading.
 - b. Click **Next**. The Confirmation screen is displayed.
6. Verify the group details.

If the details are incorrect or you want to modify them, click Back and update the details.
7. Click **Create**. The LDT communication group is created and displayed in the LDT communication groups list.

An association is created between the CTE clients that you selected for the group and the LDT communication group. The LDT communication group is listed under the LDT COMMUNICATION GROUP section on the Membership tab of the client.

Viewing LDT Communication Groups

To view an LDT communication group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > LDT Communication Groups**. A list of existing LDT communication groups appears. The LDT Communication Groups page displays the following details:

Field	Description
Status	Status of the LDT communication group. Can be Healthy or Unhealthy.
Name	Alias of the LDT communication group. A unique, user-friendly name that helps in searching for specific LDT communication groups.
Created At	The time when the LDT communication group was created.
Updated At	The time when the LDT communication group was last updated.
Description	A brief explanation of the LDT communication group.

Editing an LDT Communication Group

After an LDT communication group is created, you can modify its description. The name of the group cannot be modified.

To edit an existing LDT communication group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > LDT Communication Groups**. The list of existing LDT communication groups is displayed.
3. Under **Name**, click the overflow icon () corresponding to the desired LDT communication group.
4. Click **Edit**.
5. Change the **Description** of the group.
6. Click **Update**.

The LDT communication group description is updated.

Viewing Group Status Reports

To view a group status report:

1. Open the **Transparent Encryption** application.
2. Click **Clients > LDT Communication Groups**. A list of existing LDT communication groups appears.
3. Under **Name**, click the overflow icon () for the desired LDT communication group.
4. Select **View Group Status Report**. The Group Status Report wizard opens.

The report shows the status of the LDT communication service on the master and replica nodes.

Adding Clients to an LDT Communication Group

You can add clients to an LDT communication group during or after the group creation. A client can be added to only one LDT communication group at a time.

To add clients to an existing LDT communication group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > LDT Communication Groups**. The list of existing LDT communication groups is displayed.
3. Under **Name**, click the desired LDT communication group. The Member Clients list shows the list of clients in the group.
4. Click **Add Clients**. The Add Clients dialog box is displayed.
5. Select the clients to be added to the LDT communication group. Use the Client Name filter to search for the desired clients. Only the clients that are not part of an LDT communication group are displayed. Also, the Windows clients that have the **LDT Access Only** check box selected cannot be added to the LDT communication group.

If no client exists, you can create one by clicking **Create Client**. Refer to [Adding Clients Manually](#) for details.

To select all clients visible on the page, select the top check box to the left of the Client Name heading.

6. Click **Save**.

The selected clients are added to the LDT communication group and are displayed in the Member Clients list.

Note

Client association with the LDT communication group is restricted based on the operating system of the clients. An LDT communication group can associate with only a single type of operating system, it can be Windows or Linux.

If an existing LDT communication group has clients running different operating systems, move clients running different operating systems to different LDT groups. For example, if the existing group has two clients, WinClient and LinxClient, running Windows and Linux respectively, then, it is recommended to move WinClient to an LDT communication group of Windows clients. Similarly, move the LinxClient to an LDT communication group of Linux clients.

Removing Clients from an LDT Communication Group

If needed, you can remove LDT clients from an LDT communication group. However, if a client associated with an LDT communication group contains an active LDT over NFS/SMB GuardPoint, **do not** remove the client from the LDT communication group directly.

Note

To remove a client from an LDT communication group gracefully:

1. Disable or unguard the LDT over NFS/SMB GuardPoint on the client. Refer to [Disabling GuardPoints](#) and [Removing GuardPoints](#) for details.
2. Remove the client from the LDT communication group, as described below.

To remove clients from an existing LDT communication group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > LDT Communication Groups**. The list of existing LDT communication groups is displayed.
3. Under **Name**, click the desired LDT communication group. The Member Clients list shows the list of clients in the group.
4. Click the overflow icon () corresponding to the client you want to remove from the group.
5. Click **Remove**. Removal of a client is permanent and cannot be undone.
6. Click **Remove** to confirm the action.

The client is removed from the LDT communication group.

Deleting an LDT Communication Group

To delete an LDT communication group:

1. Open the **CipherTrust Transparent Encryption** application.
2. In the left pane, click **Clients > LDT Communication Groups**. The list of existing LDT communication groups is displayed.
3. Under **Name**, click the overflow icon () corresponding to the desired LDT communication group.
4. Click **Delete**. Deletion of an LDT communication group is permanent and cannot be undone.
5. Click **Delete** to confirm the action.

The LDT communication group is deleted.

Managing Client Groups

A client group is used to group one or more clients to simplify configuration and administration. GuardPoints created on a client group are applied to all members of the group. Additionally, you can apply client group configuration settings to all clients in a client group. A client can be a member of multiple client groups.

CTE supports two types of client groups, clustered and non-clustered. A clustered client group contains clients that are members of a cluster with a cluster file system. A non-clustered client group contains members that are not members of a cluster. A client can be a member of multiple client groups. However, membership in a cluster group is exclusive, so a client that belongs to a cluster, cannot join another cluster group or client group.

If you have created a group of one type of clients, then you should only add similar clients to the group. Same configuration settings can only be applied to clients of the type with which the client group is created. If a different type of client is added, configuration settings cannot be applied to that client.

Creating a Client Group

To create a client group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Click **Create Client Group**. The General Info screen of the Create Client Group wizard is displayed.

Add General Info

On the **General Info** screen:

1. Specify a unique **Name** for the client group.
2. Select the **Cluster Type**. The options are:
 - **NON CLUSTER**: Create a non-clustered client group.
 - **HDFS**: Create a clustered client group. An HDFS client group is required to apply GuardPoints on CTE clients in an HDFS cluster.
3. Set the **Password Generation Method**. The options are:
 - **Generate**: A password is generated automatically by CipherTrust Manager. This is the default method.
 - **Manual**: Set the password manually.
 - a. Select **Manual**.
 - b. Enter the new password in the **Password** and **Confirm Password** fields. The password must match in both fields.

Note

The password must contain minimum eight characters including at least:

- One capital letter

- One number
- One of these special characters: ! @ # \$ % ^ & * () { } []

Refer to [Changing Client Group Password](#) for details.

4. Select **NON CLUSTER** as the **Cluster Type**. CTE UserSpace does not support HDFS client groups.
5. (Optional, if a profile already exists) From the **Client Profile** drop-down list, select the desired client profile. The default profile is **DefaultClientProfile**.

If the **DefaultClientProfile** does not exist, it is created as soon as the first client group is created.

6. (Optional) Provide **Description** to identify the client group. The maximum length can be 256 characters.

Name: *

Password Creation Method: *

Cluster Type: *

Client Profile:

Description:

Communication Enabled: ☒

7. (Optional) Specify whether to enable the client's communication with the CipherTrust Manager. Select **Communication Enabled** to enable, clear to disable communication. By default, the communication is disabled.
8. Click **Next**. The Add Clients screen is displayed.

Add Clients (Optional)

Optionally, you can add clients to the group. The Add Clients screen shows the list of clients added to the CipherTrust Manager.

On the **Add Clients** screen:

1. Select the clients to be added to the group. Filter the clients by using the Client Name text box.

If no client exists, you can add one by clicking **Create Client**. Refer to the [Adding Clients Manually](#). The newly created client is added to the clients list.

2. Click **Next**. A dialog box is displayed asking you to confirm inheritance settings.
3. Confirm whether the selected clients should inherit settings from the client group. The options are:
 - **Inherit Client Group Settings:** This is the default and recommended option. Clients inherit the following properties of the group except the password:
 - Client Settings
 - Agent Lock
 - System Lock
 - Communication Enabled
 - Profile Settings
 - QoS Settings
 - GuardPoints

Refer to [Inheritance of Client Group Settings](#) for details.

- **Do not Inherit Client Group Settings:** Clients retain their individual settings. Selecting this option can introduce configuration conflicts. *This is not the recommended option.* Read the instructions carefully before selecting this option.

Note

When a client is added to a client group, the password generation method of the client remains unchanged. However, when the client group's password or password generation method is updated in the future, this change is applied to all the clients in the client group. This is true irrespective of whether the clients inherit settings from the client group or not.

4. Click **OK**. The Add GuardPoint screen is displayed.

Add GuardPoints (Optional)

Optionally, you can create GuardPoints on the manually added client. CTE supports creation of all types of supported GuardPoints on such clients.

On the **Add GuardPoint** screen:

1. Click **Create GuardPoint**. The Add GuardPoints > Create GuardPoints screen is displayed.
2. Select a **Policy**. The Select Policy dialog box displays the available policies.
3. Select the desired policy.

If no policy exists, you can create one by clicking **Create Policy**. Refer to **Creating Policies > Creating Policies** for details.

4. Click **Select**. The selected policy appears in the Policy field.
5. Specify the **Type** of the GuardPoint. Refer to **Automatic and Manual GuardPoints** for details on types of GuardPoints.
6. (COS GuardPoints only) Select the **Cloud Storage Type**. CTE UserSpace does not support COS GuardPoints.
7. Specify the **Path** (or **URL** for a COS GuardPoint) to be protected. Refer to **Managing GuardPoints** for details.
8. Configure **Preserve Sparse Region**, **Secure Start**, and/or **Auto Mount** as appropriate. The options vary based on the selected policy.

The Multifactor Authentication option is unavailable for manually added clients.

9. Click **Create**. The newly created GuardPoint appears in the list.

To remove a GuardPoint, click **Remove** corresponding to it.

10. Click **Next**. The Confirmation screen is displayed.

Confirmation

On the **Confirmation** screen:

1. Verify the client group details. The Confirmation screen displays general information about the client group, the list of clients in it, and details of the GuardPoints added to the group.

If the details are incorrect or you want to modify them, click **Back** and update the details.

2. Click **Create**.

The newly created client group appears in the client groups list.

Adding Clients to a Client Group

Clients can be added to a client group either manually or by specifying the group when registering clients with the CipherTrust Manager. If you specify a client group during client registration, the client automatically appears under the client group on the CipherTrust Manager GUI. Refer to the [CTE Agent Clients Guide](#) for information on the registration process.

When protecting an HDFS cluster, the CTE clients with the HDFS configuration must be added to an HDFS client group on the CipherTrust Manager.

To manually add clients to a client group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the expand icon () to the left of the desired client group.

Note

Select an HDFS client group if the CTE client to be added is in an HDFS cluster.

Alternatively, click the desired client group and click the **Membership** tab.

4. Click **Add Client**. The Add Client to Client Group <ClientGroupName> dialog box is displayed with the list of available clients, if any. At least, one client must already exist.

Add Client to Client Group A1

Search					
☐ 1 Selected 7 Results 7 Clients					
	Status	Name	Client Type	OS Type	Description
☐	 Healthy	P_1	CTE-U	LINUX	TestHost
☒	 Healthy	P_10	FS	LINUX	TestHost
☐	 Healthy	P_11	FS	LINUX	TestHost

5. Select the desired clients.
6. Click **Add**. A dialog box is displayed asking you to confirm settings inheritance.

7. Confirm whether the selected clients should inherit settings from the client group. The options are:

- **Inherit Client Group Settings:** This is the default and recommended option. Clients inherit the following properties of the group except the password:
 - Client Settings
 - Agent Lock
 - System Lock
 - Communication Enabled
 - Profile Settings
 - QoS Settings
 - GuardPoints

Refer to [Inheritance of Client Group Settings](#) for details.

- **Do not Inherit Client Group Settings:** Clients retain their individual settings. Selecting this option can introduce configuration conflicts. *This is not the recommended option.* Read the instructions carefully before selecting this option.

Note

When a client is added to a client group, the password generation method of the client remains unchanged. However, when the client group's password or password generation method is updated in the future, this change is applied to all the clients in the client group. This is true irrespective of whether the clients inherit settings from the client group or not.

8. Click **OK**.

The selected clients are added to the group. They are displayed in the mini view and on the Membership tab of the client.

Displaying Client Groups

To view the list of client groups:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**. The list of available client groups is displayed.

Client Group Name	Created At	Cluster Type	Description	Sharing	Native Domain
☐ A1	09 Sep 2021, 16:20	NON-CLUSTER	A test client group	-	root
☐ A10	09 Sep 2021, 16:21	HDFS	A test client group	-	root
☐ A11	09 Sep 2021, 16:22	NON-CLUSTER	A test client group	-	root

The client groups list shows the following details:

Column	Description
Client Group Name	Name link of the client group on CipherTrust Manager. Click the link to open client group details in edit mode. The edit mode shows additional details and configuration settings. In the edit mode, you can also view and add clients, GuardPoints, and Client Group Settings.
Created At	When the client group is created.
Cluster Type	Cluster type of the client group. • NON CLUSTER: A non-clustered client group. • HDFS: A clustered client group.
Description	(Optional) Description to identify the client group.
Sharing	Sharing status of the client group. • External: The client group is external to the current domain. The client group is created and shared from another domain. • Shared: The client group is shared across other domains. The current domain is the native domain of the client group. • -: The client group is neither Shared nor External. The field is left blank for client groups that were created on a previous version of the CipherTrust Manager. Such client groups can also be shared across domains. Refer to Sharing a Client Group Across Domains for details.
Native Domain	Name of the native domain of the client group. If the

Column	Description
	client group is not external, the current domain is the native domain of the client group.

Modifying Client Groups

After you have created a client group, you can update group details and configuration settings. You can make the following changes:

- Enable or disable Agent communication for the clients in the group
- Lock or unlock the CTE Agent files on the clients in the group
- Change the CTE Agent password for the clients in the group
- Change the linked profile
- Add new clients to the group
- Remove clients from the group
- Enable the LDT Passive Mode
- Share the group across domains
- Remove the group sharing from a domain

The cluster type of a client group cannot be modified after it is created.

To modify a client group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the expand icon () to the left of the desired client group.



4. Modify the required details:
 - **Unlock:** Unlock Agent Lock and System Lock.
 - **Agent Lock:** Lock the contents of the CTE Agent directories on the clients.
 - **System Lock:** Apply an internal policy to the clients to lock system directories like `/var`, `/bin`, and `/etc`. Enabling System Lock automatically enables Agent Lock.

- **Communication Enabled:** Whether to enable clients' communication with the CipherTrust Manager. Select to enable, clear to disable communication.
- **Live Data Transformation:** Initiates the suspend/resume rekey operation on LDT protected GuardPoints on LDT clients in the group. By default, the rekey operation is initiated. However, to get the actual state of the rekey operation, check the status on individual clients.
 - To suspend the LDT rekey operations, click the **Suspend Live Data Transformation** icon (⏸). The icon changes to **Resume Live Data Transformation** (▶).
 - To resume the LDT rekey operations, click the **Resume Live Data Transformation** (▶) icon. The icon changes to **Suspend Live Data Transformation** icon (⏸).

Note

When ⏸ or ▶ is clicked, an error is generated on non-LDT clients in the client group. To view the error details, go to **Records > Server Records** on the CipherTrust Manager GUI.

- **LDT Passive Mode:** By default, LDT Passive Mode is disabled. After you enable it, you can't disable it.
- **Password Creation Method:** Set the password creation method — **Generate** or **Manual**. Refer to [Changing Client Group Password](#) for details.
- **Client Profile:** Select a profile for the client group. The default profile is **DefaultClientProfile**. To change the client profile, refer to [Changing the Profile](#) for details.

5. Click **Apply**.

Additionally, you can define GuardPoints for the clients in the group. Refer to [Managing GuardPoints](#).

Managing Designated Primary Set

A Designated Primary Set (DPS) is used to create a group of clients from which you can select a primary client to perform key rotation and versioning.

Adding Designated Primary Set to a Client Group

Before creating a Designated Primary Set:

- Ensure that a CIFS connection is configured.
- Ensure that clients that you want to add are part of the LDT Communication Group and Client Group. See [Managing LDT Communication Groups](#) to create an LDT Communication Group clients.

Note

- Modifications made to the Designated Primary Set list will not be updated to the clients that are associated with a Client Group for which inheritance is disabled. See [Inheritance of Client Group Settings](#) for more details on Client Group inheritance.
- The clients associated with the Designated Primary Set must inherit properties from the client group. This ensures that any changes made to the Designated Primary Set are pushed to the associated clients.
- A Designated Primary Set (DPS) is fully enforced when all members of the client group are DPS-capable (that is, running CTE Agent 7.7.0 or higher). If a client group with DPS enabled has non-DPS capable members, the GuardPoints will not be pushed to those members.

To create a Designated Primary Set:

1. Click **Clients > Client Groups**.
2. Click the desired client group name.
3. Select the **Designated Primary Set** tab.

It shows the list of Designated Primary Sets. Expand the desired Designated Primary Set to see its details.

4. Click **Create Designated Primary Set**.
5. In the **General Info** screen, provide a name for the Designated Primary Set and select an LDT Communication Group.
6. Click **Next**.
7. In the **Add Clients** screen, select the clients for the primary set.

Use the search box to search for a particular client.

Note

- A Designated Primary Set should contain at least one client.
- Add two or more clients to the Designated Primary Set to prevent issues during LDT primary failover.

8. In the **Confirmation** screen, review the details of Designated Primary Set.
9. Click **Create**.

The screen will display a message indicating whether the Designated Primary Set was created successfully.

10. Click **Close** to close the screen.

The Designated Primary Set will appear in the **Designated Primary Set** tab.

After you have created a Designated Primary Set for a client group, you can create a corresponding LDT guard point for it. See [Creating LDT GuardPoints on SMB/NFS Paths](#) for details.

Removing Designated Primary Set

To remove a Designated Primary Set:

1. Click the **Remove** icon next to the desired Designated Primary Set name.
2. In the confirmation dialog box, click **Remove**.

Adding New Clients to a Designated Primary Set

To add new clients to an existing Designated Primary Set:

1. Under **Clients > Client Groups**, click the desired client group name.
2. Select the **Designated Primary Set** tab.
3. Expand the desired Designated Primary Set.

It displays the list of clients.

4. Click **Add Clients**.
5. Select the checkboxes for the desired client names.
6. Click **Add**.

Removing Clients from a Designated Primary Set

To remove a client from a designated primary set:

1. Under **Clients > Client Groups**, click the desired client group name.
2. Select the **Designated Primary Set** tab.
3. Expand the desired Designated Primary Set.

It displays the list of clients.

4. Click the **Remove** icon next to the client name.
5. In the confirmation dialog box, click **Remove**.

Removing Multiple Clients from a Client Group

As part of the CipherTrust Manager maintenance, you occasionally need to remove clients from their client groups.

To remove clients from a client group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the expand icon () to the left of the desired client group.

Alternatively, click the desired client group and click the **Membership** tab.

4. Select the clients that you want to remove from the group.

To select all clients visible on the page, select the top check box to the left of the Status heading.

5. Click the delete icon ().

A warning message appears stating that deleting the selected clients is permanent and cannot be undone.

6. Click **Delete**.

The selected clients are removed from the client group. Also, the client group is removed from the Membership tab of the linked clients.

Removing a Client from a Client Group

As part of the CipherTrust Manager maintenance, you occasionally need to remove a client from its client group.

To remove an individual client from a client group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the expand icon () to the left of the desired client group.

Alternatively, click the desired client group and click the **Membership** tab.

4. Select the client that you want to remove from the group.

5. Click the delete icon ().

Alternatively, click the overflow icon (), and click **Remove**. When prompted, click **Remove**.

A warning message appears stating that deleting the selected clients is permanent and cannot be undone.

6. Click **Delete**.

The selected client is removed from the client group. Also, the client group is removed from the Membership tab of the client.

Changing the Profile

To change the profile:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the expand icon () to the left of the desired client group.
4. Next to **Client Profile**, click the profile link (for example, **DefaultClientProfile**). The Select Profile dialog box shows the current client profile, Log Level, Rekey Option, Rekey Rate, and Schedule of the selected profile.



5. From the **Profile** drop-down list, select the desired profile.
6. Click **OK**. The selected profile is linked successfully.

Changing Client Group Password

The CipherTrust Manager allows for client password management using client groups. For large scale deployments where the CipherTrust Manager must manage several hundreds or thousands of agents, administering passwords on a per-client basis becomes untenable and burdensome. Using a common password across all the clients in a client group mitigates the administrative burden.

This feature is also useful for offline agent recovery. If a remote agent reboots (planned or unplanned) and cannot communicate with the CipherTrust Manager in the central office, it prompts the administrator at the remote site to enter the client password. The remote site administrator typically calls the corporate help desk for the password. Using the password provided by the help desk personnel, the remote site administrator enables offline agent recovery and the resumption of services. As the password is now known to the remote site administrator and the help desk personnel, it may result in a breach of security and/or render the IT operations non-compliant with respect to guaranteeing data privacy.

To remedy the compromised situation, the security administrators should change the password (rotate the password) according to existing security practices. The client group password management feature allows changing the password on all the clients in the client group when the password is compromised.

The use cases for client group password feature can be summarized as follows:

1. Set a common password for all clients in a client group.

- Reset the common password for all clients in a client group (if the password is provided to a remote CTE Agent administrator for offline agent recovery).

This feature is best suited for large scale deployments when many agents are under the management of a CipherTrust Manager cluster.

Note

When a client group's password or password generation method is updated, this change is applied to all the clients in the client group. This is true irrespective of whether the clients inherit settings from the client group or not.

Changing the Password Manually

Note

The manual password creation method is recommended for disaster recovery scenarios.

To change the password:

- Open the **Transparent Encryption** application.
- Click **Clients > Client Groups**.
- Under **Client Group Name**, click the expand icon () to the left of the desired client group.



- From the **Password Creation Method** drop-down list, select **Manual**. The **Regenerate Password** button is replaced by **Change Password**.



- Click **Change Password**.
- Enter the new password in the **Password** and **Confirm Password** fields. The password must match in both the fields.

The password must contain minimum eight characters including at least:

- One capital letter
- One number
- One of these special characters: ! @ # \$ % ^ & * () { } []

To cancel the password change, click **Cancel Change Password**.

7. Click **Apply**.

When the new password is applied, the server pushes the password to all clients in the client group. Clients that are removed from the client group retain the password set for the group. Clients added to the group later do not receive the new password.

Changing the Password Dynamically

To change the password:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the expand icon (▸) to the left of the desired client group.



4. From the **Password Creation Method** drop-down list, select **Generate**. This is the default method.
5. Click **Regenerate Password**.
6. Click **Apply**.

A new generated password is downloaded to the client.

Inheritance of Client Group Settings

Instead of specifying settings for applications running on multiple clients individually, configure them at the client group level. Those settings can be automatically applied to all clients in the group. Refer to [Client Settings](#) for details on client settings.

Caution

Take care when defining client settings at the client group level. If a group contains clients running different operating systems (for example, Linux and Windows) that inherit client settings from the group, conflicts and issues may be observed with file and user access permissions.

-
- A client that joins a client group can opt to inherit client group configuration including the client settings.
 - If the client settings are not defined at the group level, the client retains its own settings.
 - If the client settings at the group level are modified later, the updated settings apply to all group members that inherit configuration from the group.
 - Individual clients in the group have client settings overwritten by the group's client settings.

For example:

- a. `clientA` has client settings defined, joins `clientGroup1` and inherits its group configuration. `clientB` also joins `clientGroup1` but does not inherit its group configuration. `clientGroup1`, however, does not have any client settings defined. In this case, both `clientA` and `clientB` retain their own client settings.
 - b. Now, client settings of `clientGroup1` are modified. This overwrites the client settings of all clients that inherit group configuration from `clientGroup1`. So `clientA` inherits the modified group configuration but `clientB` does not, as it does not inherit client group configuration.
 - c. `clientB` is modified to inherit settings from `clientGroup1`. The next time `clientGroup1` updates its client settings, the changes apply to both `clientA` and `clientB`.
- A client can be a member of more than one client groups. If the client inherits client group configuration from the first client group it joins, and the next groups it joins subsequently, the client inherits the client settings from the last group that it joins.

For example:

- a. `clientC` joins `clientGroup2` and inherits the client group configuration. `clientC` now has `clientGroup2` client settings.
 - b. `clientC` is added to `clientGroup1` and set to inherit client group configuration. So, `clientC` gets `clientGroup1` client settings.
- If client settings of a client group are emptied, member clients that inherit settings from the group retain the last defined client settings.

For example:

- a. `clientGroup1` deletes its client settings. All member clients (`clientA`, `clientB`, and `clientC`) retain the last client settings defined for `clientGroup1`— blank client settings are not passed to members of the group.
 - b. `clientB` leaves `clientGroup1`. Now, `clientB` retains the client settings it last inherited from `clientGroup1`.
- If the client settings of a member of a client group are modified, that client no longer inherits client settings from
-

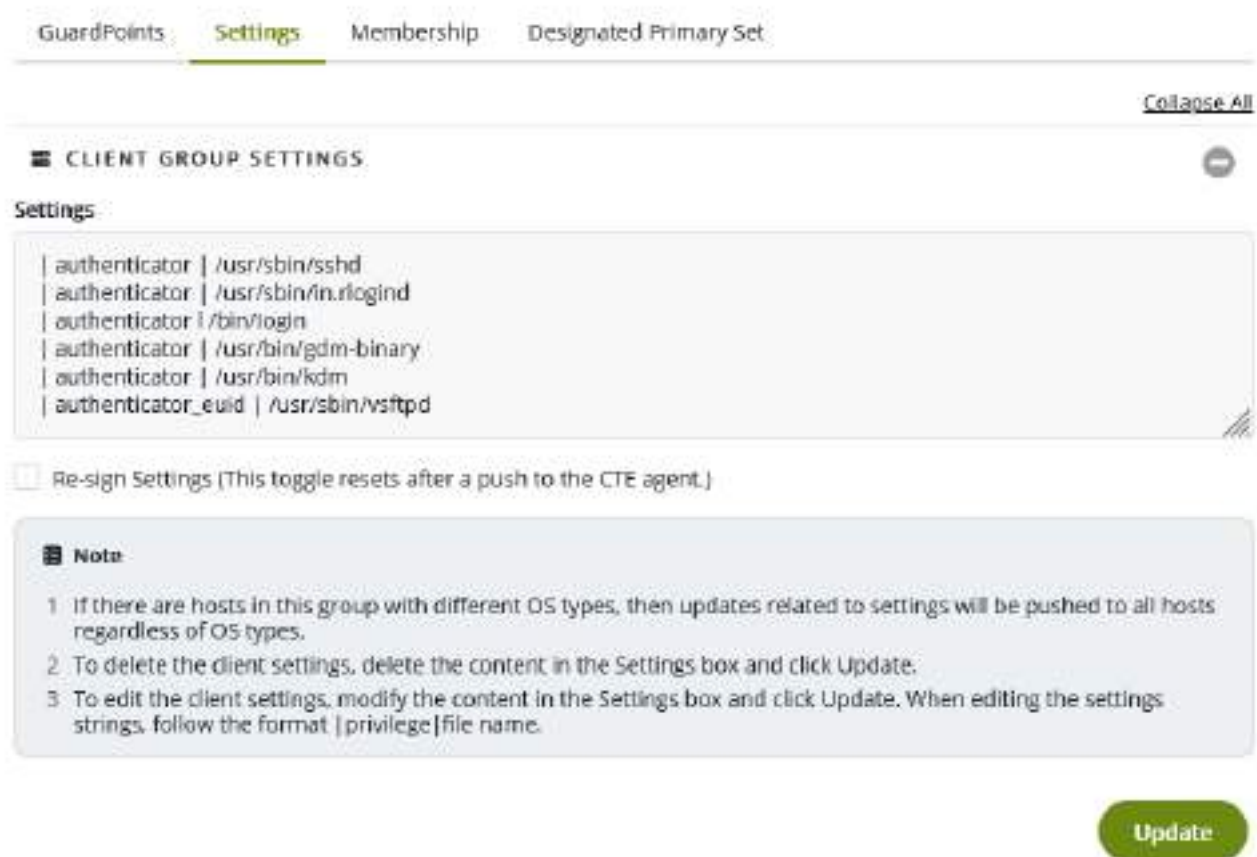
the client group.

For example, client settings on `clientB` are modified. Then, the client settings for `clientGroup1` are modified, all members except `clientB` inherit the changes made to the client settings for `clientGroup1`.

Configuring Client Group Settings

To configure client settings at group level:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group.
4. Click the **Settings** tab.
5. Expand **CLIENT GROUP SETTINGS**. The Settings text box contains the authentication settings.



6. In the **Settings** text box, add `|authenticator|` before the path of the binary. For example, `|authenticator|/bin/su` to allow `su` to be a trusted method of authentication. For further consideration of authentication options, refer to [Client Settings](#).
7. (Optional, if you add another process to the set of trusted applications) Enable **Re-sign Settings** to ensure

that the new process is signed and authenticated by the client. The next time the client settings are pushed to the CTE Agent, the updated client settings are re-signed and the **Re-sign Settings** toggle is disabled (or reset).

If, after adding a new process, you do not enable **Re-sign Settings**, the client ignores the newly added process. See [Re-Sign Settings](#) for more information.

8. Click **Update**.

Deleting Client Groups

As part of the CipherTrust Manager maintenance, you occasionally should remove client groups from the CipherTrust Manager.

- When you delete a client group, only the group is removed from the CipherTrust Manager GUI. Individual clients that are members of the group remain intact.
- If you configured a client group password, the individual clients retain the group password.

Deleting a Client Group

To remove a client group:

1. Make sure that no GuardPoints is applied on the group.
2. Open the **Transparent Encryption** application.
3. Click **Clients > Client Groups**.
4. Under **Client Group Name**, click the overflow icon () corresponding to the desired group.

Alternatively, select the check box corresponding to the desired group, click the delete icon (), and click **Delete**.

5. Click **Delete**. A dialog box appears prompting to confirm the action.
6. Click **Delete**.

The client group is removed from the client groups list. Also, the client group is removed from the Membership tab of the linked clients.

Deleting Multiple Client Groups

The CipherTrust Manager provides an option to delete multiple client groups.

To remove multiple client groups:

1. Make sure that no GuardPoints is applied on the group to be deleted.
 2. Open the **Transparent Encryption** application.
-

3. Click **Clients > Client Groups**.
4. Under **Client Group Name**, select the check boxes corresponding to the desired groups.

To select all client groups visible on the page, select the top check box to the left of the Client Group Name heading.

5. Click the delete icon ().

A warning message appears stating that deleting the selected client groups is permanent and cannot be undone.

6. Click **Delete**.

The client groups are removed from the client groups list. Also, the client groups are removed from the Membership tab of the linked clients.

Sharing a Client Group Across Domains

A shared client group will be visible in read-only mode in all the domains where it is shared. The GuardPoints can be created on the shared client group from any of the linked domains. These GuardPoints will be visible in read-only mode in all the linked domains except their native domains (where the GuardPoints are created). All the valid operations on the GuardPoints will be allowed from the native domains.

Clients can be added to the shared client group from all the linked domains (including the native domain). All the GuardPoints added to the client group (from all the domains) will be propagated to the clients in the group.

Propagation of client settings and other configuration (like LDT suspend/resume) is passed on to all the clients in the group irrespective of the domain.

To share a client group across domains:

1. Open the **Transparent Encryption** application. The Clients page is displayed. This page lists the clients added to this CipherTrust Manager appliance.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group.
4. In the mini detail view, select **Domain Sharing**.

Alternatively, to enable domain sharing on a client group, click the expand icon () corresponding to the desired group, select **Domain Sharing** in the mini detail view, and click **Apply**.

5. Click **Apply**. Now, the **Sharing** tab is displayed.
6. On the **Sharing** tab, click **Share With Other Domains**. The Share With Other Domains dialog box is displayed.
7. Under **Domain Name**, select the domains with which you want to share the client group. The dialog box also provides an option to select all the domains, if required.

-
8. Click **Share**.

The client group is shared across selected domains of the CipherTrust Manager.

Note

If a client group is shared across domains, then deleting its native domain member clients returns the "resource not found" error.

Removing Group Sharing from Domains

Removing Individual Domains

To remove group sharing from a domain:

1. Open the **Transparent Encryption** application. The Clients page is displayed.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group. The detail view of the Client Groups page is displayed.
4. Click the **Sharing** tab.
5. Under **Domain Name**, select the check box corresponding to the desired domain.
6. Click **Remove**. A dialog box appears stating that deleting the selected domain is permanent and cannot be undone.
7. Click **Delete**.

The client group is no longer shared with the selected domain.

Removing Multiple Domains

To remove group sharing from multiple domains:

1. Open the **Transparent Encryption** application. The Clients page is displayed.
 2. Click **Clients > Client Groups**.
 3. Under **Client Group Name**, click the desired client group. The detail view of the Client Groups page is displayed.
 4. Click the **Sharing** tab.
 5. Under **Domain Name**, select the check box corresponding to the desired domains. To select all domains visible on the page, select the top check box to the left of the Domain Name heading.
-

-
6. Click the delete icon (). A dialog box appears stating that deleting the selected domains is permanent and cannot be undone.
 7. Click **Delete**.

The client group is no longer shared with the selected domains.

Managing Signature Sets

File signing checks the authenticity and integrity of executables and applications before they are allowed to access GuardPoint data. When you initiate file signing on the CipherTrust Manager, the CTE Agent calculates the cryptographic signatures of the executables that are eligible to access GuardPoint data. Files are individually signed as part of a set and the set is configured in a policy that defines the processes to allow.

When an executable tries to access a GuardPoint, the **secfs** service checks the fingerprint, a SHA-2 (Secure Hashing Algorithm) message digest, of the executable against the fingerprint stored in the CTE database. If they match, the executable's authenticity is verified and it can be allowed to access protected data. A hostile or compromised executable, such as a Trojan application, malicious code, or rogue process, with a missing or mismatched signature, is denied access.

Once a set of files to be signed is created, the executables are signed on a selected client and a copy of each signature is stored on the CTE. This is done as a background process on the selected client. The time it takes to complete signing depends upon the number of files to be signed, the response time of the client system, and other load factors. The completion status is indicated in the Signature Sets window.

Completed signature sets are configured in a (CTE Agent) policy so that not only are the executables attempting GuardPoint access identified, but their signatures are checked to ensure that they had not been compromised.

The Signing Process

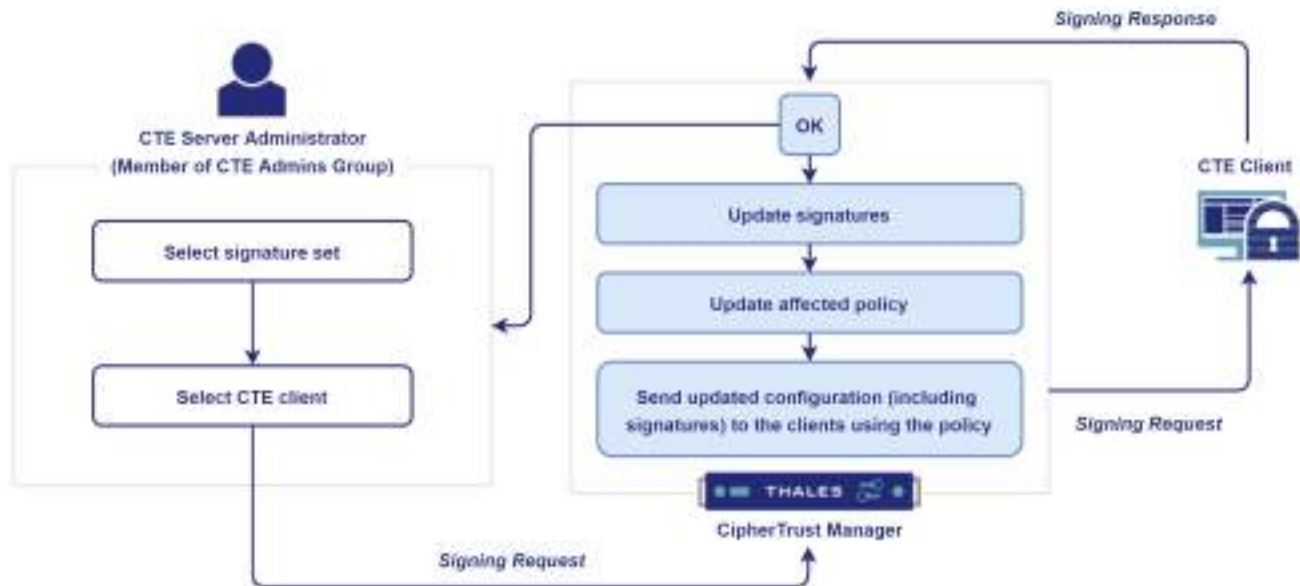
The basic steps involved in the signature signing process are:

1. The CTE Server Administrator creates signature sets. Refer to [Creating Signature Sets](#) for details.
2. The CTE Server Administrator initiates the signature signing request. The administrator selects the signature set to be signed and the CTE client that will sign the set. Refer to [Signing Files in a Signature Set](#) for details.
3. The CipherTrust Manager forwards the request to the selected CTE client.
4. The CTE client signs the set and sends it to the CipherTrust Manager.
5. The CipherTrust Manager:
 - a. Updates the signatures in the set.
 - b. Updates the affected policies.
 - c. Sends the updated configuration files including the signatures to the clients that are using the affected policies.

In future, if any processes in the signature set are updated, the signature set should be signed again. The CTE Server Administrator can initiate the signature signing process again. This is referred to as the signature re-

signing process.

The following diagram shows the high level signature signing process:



The Signing Process for CTE for Kubernetes

The CTE for Kubernetes clients cannot sign files. So, the signing process is different for CTE for Kubernetes clients. The CTE Server Administrator needs to manually upload the files signed by a Kubernetes image.

The basic steps involved in the signature signing process are:

1. The CTE Server Administrator creates signature sets for Kubernetes clients. Refer to [Creating Signature Sets for Kubernetes Clients](#) for details.
2. The CTE Server Administrator manually adds the signatures to the signature set on the CipherTrust Manager.
3. The CipherTrust Manager:
 - a. Updates the affected policies.
 - b. Sends the updated configuration files to the CTE for Kubernetes clients that are using the affected policies.

In future, if any processes in the signature set are updated, the CTE Server Administrator needs to reupload the latest signatures to the signature set. This is referred to as the signature re-signing process.

Using Signature Sets in a Policy

Policies can be configured to identify the executables trying to access GuardPoint data and to verify that the executables themselves are unchanged since they were signed. You must, however, anticipate the effect of encryption on file signatures.

When a file inside a GuardPoint is copied to a location outside the GuardPoint, the two files have different

signatures. The file in the GuardPoint is encrypted, but the file outside the GuardPoint is not.

- Encryption makes the two files different. The VMD process does not decrypt guarded files before checking their signatures. So, when you rekey guarded files, their signatures also change. Re-sign the files that use the signatures of those files in process sets.
- If both files must access the GuardPoint data, add both files to the signature set and sign them. If encryption is not applied, both files have the same signature; a signature mismatch should not occur.

Creating Signature Sets

A signature set is a collection of hashes of processes and executables that you want to grant or deny access to GuardPoints. You can enter the full path of files and directories manually or use the browser to locate and select them. Specify a directory to sign all the files in that directory and all the subdirectories that it may contain.

Signing many files can take a while. To shorten processing time, verify that the files and directories in the signature set exist. It takes longer to process non-existent files. If they do not exist, it is recommended that you delete them as sources from the signature set. Refer to [Deleting Source from Signature Sets](#) for details.

To create a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click **Create Signature Set**. The General Info screen of the Create Signature Set wizard is displayed.

General Info

1. Enter a unique **Name** for the set.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
2. Select **Application** as the **Type**. The signature set will have signatures of the running applications.
3. (Optional) Provide a **Description** for the set.
4. Enable or disable the **Add Signatures** toggle. If you enable this option, an **3 - Add Signatures** screen becomes available.
5. Click **Next**. The Add Sources screen is displayed. On this screen, you can add files to be signed, as described below.

Add Sources

Specify path of the directory or file to be signed. If a directory is specified, all files in the directory and its subdirectories are signed.

The CipherTrust Manager provides an option to add multiple sources. A maximum of 200 sources can be added at once.

1. Click **Add Source**.
2. Click **Select Client**. The list of registered clients is displayed.
3. Select the desired client.

Status	Name	OS Type	Description
☒ Healthy	10.164.13.209	LINUX	ABLinux
☐ Healthy	ABWin	WINDOWS	AB Windows Client

4. Click **Select**. The selected client appears next to the Change Client button (previously Select Client).

If needed, change the client by clicking **Change Client**.

5. Specify the path to be signed by either typing manually or using the browser.

Client

Change Client

10.164.13.209

Enter Source:

/usr/bin/

Start Directory

Apply

Select Source:

tmp

tools

usr

bin

To jump to a specific directory, enter the directory path in the **Start Directory** field and click **Apply**. The browser shows the subdirectories and files, as shown below.

Client

Change Client

10.164.13.209

Enter Source:

/usr/bin

Start Directory

/usr/bin

Apply

Select Source:



You cannot browse above the Start Directory. Enter a start point that is higher in the directory hierarchy than all the directories and files that you want to select, or you will have to re-enter start points to locate and select the desired files. The default is the top-level, either slash (Linux) or backslash (Windows).

Alternatively, if you know the directory path, you can enter it manually in the **Path** field.

- Click **Add Source**. The selected source is displayed in the SELECTED SOURCES list.

Client

Change Client

10.164.13.209

Enter Source:

Start Directory

/usr/bin

Apply

Select Source:



SELECTED SOURCES

/usr/bin

Remove

Optionally, you can add a new source by clicking **Add Source**. To remove a source, click **Remove** to the right of the source. A signature set must contain at least one source.

- Click **Add**. The selected source is displayed in the Source Directory list.

Optionally, you can add a new source by clicking **Add Source**. To remove a source, click the overflow icon () corresponding to the source and click **Remove**.

- Click **Next**. The Add Signatures screen is displayed. On this screen, you can manually add signatures or upload a CSV file containing signatures.
-

Add Signatures

If you enabled **Add Signatures** on the **General Info** screen, CipherTrust Manager provides options to add signatures to a signature set manually, and to upload the signatures to a signature set through CSV.

Click the desired tab to view the instructions.

Adding Signatures to a Signature Set Manually

1. Click **Create Signature**. The Create Manually tab is displayed.
2. Under **Signature 1**, enter the following details:
 - **Program**: Full path of the file.
 - **Signature**: Signature of the file.

To add multiple signatures, click **+ Add More Signatures**. To remove a signature, click **X**.

3. Click **Add**. The signatures are added to the signature set. The list of programs and their signatures are displayed.

Optionally, you can add more signature(s) by clicking **Create Signature**, and repeating step 2 and 3. To remove a signature, click the overflow icon () corresponding to the signature and click **Remove**.

4. Click **Next**. The Confirmation screen is displayed. The screen shows the General Info, Sources and Signatures details of the signature set.

Uploading Signatures to a Signature Set through CSV

1. Click **Create Signature**. The Create Manually tab is displayed.
2. Click the **Upload** tab.
 - a. Next to **Upload CSV**, click **Browse**.
 - b. Select and upload the CSV file. The Upload CSV field shows the uploaded file.
3. Click **Add**. The signatures from the CSV file are added. The name of the file is displayed.

Optionally, you can change the file by clicking **Create Signature**, and repeating step 2 and 3. To remove the file, click the overflow icon () corresponding to the uploaded CSV file and click **Remove**.

4. Click **Next**. The Confirmation screen is displayed. The screen shows the General Info, Sources and Signatures details of the signature set.

Confirmation

1. Verify the set details. If the details are incorrect or you want to modify them, click **Back** and update the details.
2. Click **Save**.

The newly created set appears on the Signature Sets tab. By default, the signature set has the status **UNSIGNED**.

Name	Type	Signing Status	Updated At ↓	Description	
☐ testsigset	Application	Unsigned	24 Nov 2022, 14:14	Test signature set	...
☐ test	Container Image	Unsigned	24 Nov 2022, 14:12		...

It is recommended that the signature set is signed before you apply policies to processes. This ensures that a tampered with or compromised process executable is not granted permissions to access protected GuardPoints. Refer to [Signing Files in a Signature Set](#) for details.

Creating Signature Sets for Container Images

A signature set is a collection of file names and their signatures. A signature is a hash of a process or an executable file. Through signature sets, a signature can be used to verify the integrity of the process before it is allowed access to the guarded data.

You can enter the full path of files and their signatures manually or use the browser to upload YAML files containing the list of files and their signatures.

To create a signature set for CTE for Container Images:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click **Create Signature Set**. The General Info screen of the Create Signature Set wizard is displayed.

General Info

1. Enter a unique **Name** for the set.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
2. Select **Container Image** as the **Type**. The signature set will have the signatures of containers.
3. (Optional) Provide a **Description** for the set.
4. Enable or disable **Add Signatures**.
5. Click **Next**. The Add Sources screen is displayed. On this screen, you can add source paths or upload the YAML file containing the source paths, as described below.

Add Sources

Specify path of the directory or file to be signed. If a directory is specified, all files in the directory and its subdirectories are signed.

The CipherTrust Manager provides an option to add multiple sources. A maximum of 200 sources can be added at once.

Click the desired tab to view the instructions.

Adding Sources Manually

1. Click **Add Source**. The Create Manually tab is displayed.
2. In the **Enter Source** field, add source for the container images to be trusted.
3. Click **Add**. The sources are added to the signature set. The list of Source Directory is displayed.

Optionally, you can add more sources by clicking **Add Source**, and repeating step 2 and 3. To remove a source, click the overflow icon () corresponding to the source and click **Remove**.

4. Click **Next**. The Add Signatures screen is displayed. On this screen, you can manually add signatures or upload the list of signatures.

Uploading Sources through YAML

1. Click **Add Source**. The Create Manually tab is displayed.
2. Click the **Browse** tab.
 - a. Next to **Upload YAML**, click **Browse**.
 - b. Select and upload the YAML file that contains the source for the container images to be trusted. The Upload YAML field shows the uploaded file.
3. Click **Add**. The sources from the YAML file are added. The name of the file is displayed.

Optionally, you can change the file by clicking **Add Source**, and repeating step 2 and 3. To remove a signature, click the overflow icon () corresponding to the source and click **Remove**.

4. Click **Next**. The Add Signatures screen is displayed. On this screen, you can manually add signatures or upload the list of signatures.

Note

The Add Signatures tabs is displayed if you selected **Add Signatures** on the General Info screen.

Add Signatures

If you enabled **Add Signatures** on the **General Info** screen, CipherTrust Manager provides options to add

signatures to a signature set manually, and to upload the signatures to a signature set through CSV.

Click the desired tab to view the instructions.

Adding Signatures to a Signature Set Manually

1. Click **Create Signature**. The Create Manually tab is displayed.
2. Under **Signature 1**, enter the following details:

- **Program**: Full path of the file.
- **Signature**: Signature of the file.

To add multiple signatures, click **+ Add More Signatures**. To remove a signature, click **X**.

3. Click **Add**. The signatures are added to the signature set. The list of programs and their signatures are displayed.

Optionally, you can add more signature(s) by clicking **Create Signature**, and repeating step 2 and 3. To remove a signature, click the overflow icon () corresponding to the signature and click **Remove**.

4. Click **Next**. The Confirmation screen is displayed. The screen shows the General Info, Sources and Signatures details of the signature set.

Uploading Signatures to a Signature Set through CSV

1. Click **Create Signature**. The Create Manually tab is displayed.
2. Click the **Upload** tab.
 - a. Next to **Upload CSV**, click **Browse**.
 - b. Select and upload the CSV file. The Upload CSV field shows the uploaded file.
3. Click **Add**. The signatures from the CSV file are added. The name of the file is displayed.

Optionally, you can change the file by clicking **Create Signature**, and repeating step 2 and 3. To remove the file, click the overflow icon () corresponding to the uploaded CSV file and click **Remove**.

4. Click **Next**. The Confirmation screen is displayed. The screen shows the General Info, Sources and Signatures details of the signature set.

Confirmation

1. Verify the set details. If the details are incorrect or you want to modify them, click **Back** and update the details.
2. Click **Save**.

The newly created set appears on the Signature Sets tab. By default, the signature set has the status **UNSIGNED**.

Signing Files in a Signature Set

This section is applicable to CTE clients only. CTE for Kubernetes clients do not support signing files.

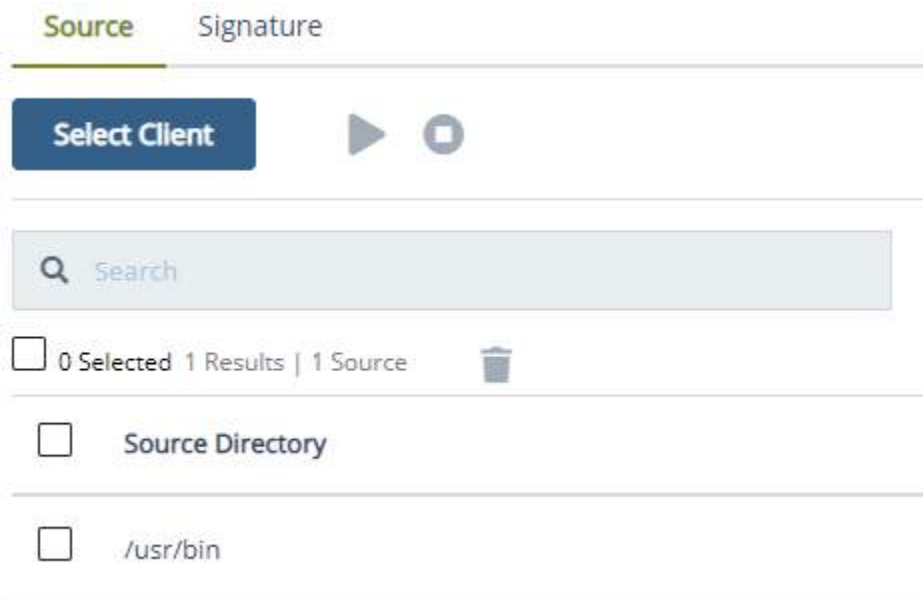
Signing involves calculating a hash value for a file and storing the value on the CipherTrust Manager. Later, when a policy checks signatures, the signature of the process or executable accessing the GuardPoint is calculated and compared against the value in the CipherTrust Manager. If the two values match, the process or executable satisfies the Process requirement of a policy and may be granted access to the guarded data.

Note

If the executable itself is volatile, or subject to frequent change, it may not be worthwhile to use a file signature as a criteria in a policy because you have to re-sign the executable after each change. If the volatile executables are members of a large signature set, it can take a while to re-sign the files because the signature of every file in the signature set is recalculated. If the volatile files are few, it might be quicker to add the volatile files to a different signature set and sign that set, rather than re-sign all the files in the original signature set.

To sign the files in a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Click the desired signature set.



5. Select a client to sign the signature set. A signing client is required to start the signing process.
 - a. On the **Source** tab, click **Select Client**. Based on the type of the signature set, the list of registered clients

or sign-capable container images is displayed. Select any client or image to sign the signature set.

b. Select the client.

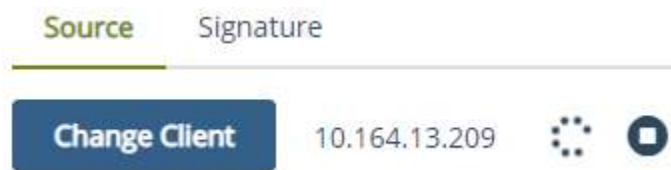
c. Click **Select**. The selected client appears next to the Select Client button. The Sign icon () is now enabled.



Note

Do not select check boxes when signing a signature set. They are used to select source directories to be deleted from the set.

6. Click the Sign icon (). The signing process starts.



The signing status of the signature set becomes **InProgress**.

- To view the percent completion of the signing process, hover over the Spinner () progress bar.
- To stop the signing process before it completes, click the Stop Signing icon (). Refer to [Stopping the Signing Process](#) for details.

The time for the signing process to complete depends on the number of files being processed. Signing occurs as a background process. So, you can use the CipherTrust Manager GUI for other administrative functions during this process.

When the signing completes, the signing status of the signature set becomes **Finished**. Refer to [Checking Signing Completion Status](#) for details about the signing status.

The resulting signatures are available on the Signature tab of the signature set.

Checking Signing Completion Status

To view the signing completion status of a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.

	Name	Signing Status	Updated At ↓	Description	
☐	testsigset	Finished	18 Aug 2020, 08:04	Test signature set	...
☐	test	Unsigned	18 Aug 2020, 00:55		...

4. View the **Signing Status** for the signature set. The Signing Status can be:

Status	Description
Manual	(Applicable to CTE for Kubernetes clients) Signature set signed manually.
Unsigned	Signature set is unsigned. Either no files exist in the set or no attempt is made to sign them yet.
InProgress	The CipherTrust Manager is actively signing the files in the set. This can take some time depending on the system load, accessibility, and the number of files being signed at one time.
Finished	All the files in the set are signed successfully. The set is ready for use.
FinishedWithWarning	All the files in the set are processed, but one or more files in the set could not be signed. Possible causes are missing files or inadequate access permissions. Check the VMD logs for details: • On Unix, <code>vorvmd_root.log</code>. • On Windows, <code>vorvmd.log</code>. Alternatively, view the logs in Event Viewer > CipherTrust Encryption Expert. Refer to Checking Agent Logs if Signing Fails for details.
Aborted	Signing was started but stopped before completion.

Stopping the Signing Process

This section is applicable to CTE clients only. CTE for Kubernetes clients do not support signing files.

Interrupt the signing process at any time before it completes. Click the Stop Signing () icon on the Source tab of the Signature Sets tab. The CipherTrust Manager does prompt you to verify your choice.

It takes a while for the signing process to stop. After the process is stopped, the Signing Status displayed on the Signature Sets tab is set to abort. All the files that were signed until you stopped the process remain intact and can be viewed on the Signature tab of the signature set.

Displaying Signatures of Files in a Signature Set

CipherTrust Manager provides options to display signatures of all or specific files in a signature set.

Displaying Signatures of All Files in the Signature Set

To display the signatures of all files in a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Under **Name**, click the desired signature set.
5. Click the **Signature** tab.



Source		Signature
Search		
☐ 0 Selected 10 Results 1758 Signatures		
Program	Signature	
☐ /usr/bin/crash	8849AA3A71BD1D2C3C0A347932E93F7A17F6635380699540975B855E28E1CA62 ***	
☐ /usr/bin/wrwc	56FE294800C9B9895589D1983A556807DA1E06E227E63D611325F81803A9123D ***	
☐ /usr/bin/woradmin	7BB14D0AAAFFD0ED8FCD55D445AEAF4C2418FB830CA3EA00844A013906E3029 ***	

The list of all files (programs) in the signature set with their signatures is displayed. By default, 10 records per page are displayed. Adjust the pagination to view more records.

Displaying Specific Signed Files in the Signature Set

To display specific signed files in a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Under **Name**, click the desired signature set.
5. Click the **Signature** tab. By default, all signed files in the set are displayed in alphanumeric order.
6. In the **Search** box, enter the string that matches the partial or full name of the program whose signature you are searching for.



The search is case-insensitive. All files that contain the string in their names are displayed.

Detecting Duplicate Files

Unless the content of a file is modified, its signature remains the same regardless of the file name and location. Also, the signature of all copies of a file remains the same. So, to determine the duplicates of a file, display the files based on their signature. If you search using a signature, it is recommended to enter the complete signature.

To detect the duplicates of a file:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Under **Name**, click the signature set in which you want to detect duplicate files.
5. Click the **Signature** tab. The signatures of the files in the set are displayed.
6. Copy the signature of a file from the **Signature** column.
7. Paste the signature in the **Search** box. Remove any extra space, if inserted when pasting.

8. Notice the search result.

If multiple records are displayed, duplicates of the file exist. If a single record is displayed, duplicates of the file do not exist. For example, the following figure shows two files with different names and locations, but with identical content based on their signature.

Source	Signature
Q: 7724722A749E444883B8ACE63C20E688D09C4905EE34D039E	
Selected 2 results (2 Signatures)	
Program	Signature
☐ /dir2/men_o	7724722A749E444883B8ACE63C20E688D09C4905EE34D039E5B734A90E900062
☐ /dir1/o	7724722A749E444883B8ACE63C20E688D09C4905EE34D039E5B734A90E900062

2 Signatures 10 per page

Deleting Signatures from Signature Sets

Delete either individual signatures from a set or the complete signature sets. Refer to [Deleting Signature Sets](#) for information on deleting complete signature sets.

Delete signatures from a signature set when you want to continue to use the signature set to authenticate processes, but you no longer want to authenticate the files that you are deleting from the set.

You can delete signatures individually or one page at a time.

Deleting Single Signatures

To delete a single signature from a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click the desired signature set.
5. Click the **Signature** tab. The list of signatures in the signature set is displayed.
6. Click the overflow icon (**...**) corresponding to the desired signature.

Program	Signature
☐ /usr/bin/crash	8849AA3A71BD1D2C3C0A347932E93F7A17F6635380699540975B855E28E1CA02
☐ /usr/bin/vortc	56FE2948D0C9B98905589D1983A5568D7DA1E06E227E63D611325F81803A0723D

Delete

7. Click **Delete**. A dialog box appears prompting you to confirm the action.
8. Click **Delete**.

The selected signature is removed from the list and the CipherTrust Manager database.

Deleting Multiple Signatures

To delete single or multiple signatures from a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click the desired signature set.
5. Click the **Signature** tab.
6. Select the check boxes corresponding to the signatures you want to delete.

2 Selected 10 Results 1759 Signatures	
Program	Signature
☒ /usr/bin/crash	8849AA3A71BD1D2C3C0A3
☒ /usr/bin/vortc	56FE294800C9B9895589D1

To select all signatures for deletion, select the top check box to the left of the Signature heading.

7. Click the delete icon (). A dialog box appears prompting you to confirm the action.
8. Click **Delete**.

The selected signatures are removed from the list and the CipherTrust Manager database.

Deleting Source from Signature Sets

This section is applicable to CTE clients only. CTE for Kubernetes clients do not support signing files.

Signing many files can take a while. To shorten processing time, verify that the files and directories in the signature set exist. It takes longer to process non-existent files. If they do not exist, it is recommended that you delete them as sources from the signature set.

Deleting Single Sources

To delete a single source from a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click the desired signature set. The Source tab shows the list of source directories.
5. Click the overflow icon () corresponding to the desired source directory.



6. Click **Delete**. A dialog box appears prompting you to confirm the action.
7. Click **Delete**.

The selected source is removed from the list and the CipherTrust Manager database.

Deleting Multiple Sources

To delete single or multiple sources from a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click the desired signature set. The Source tab shows the list of source directories.
5. Select the check boxes corresponding to the desired source directories.



To select all sources for deletion, select the top check box to the left of the Source Directory heading.

6. Click the delete icon (). A dialog box appears prompting you to confirm the action.
7. Click **Delete**.

The selected sources are removed from the list and the CipherTrust Manager database.

Deleting Signature Sets

Delete either individual signatures from a set or the complete signature sets. Refer to [Deleting Signatures from Signature Sets](#) for information on deleting individual signatures.

An active (in use) signature set cannot be deleted. Before deleting a signature set from the CipherTrust Manager, make sure that no policies are using it.

CipherTrust Manager provides options to delete single or multiple signature sets.

Deleting Single Signature Sets

To delete a single signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Click the overflow icon () corresponding to the desired signature set.

	Name	Signing Status	Updated At ↓	Description	
☐	testsigset	Finished	18 Aug 2020, 08:12	Test signature set	
☐	test	Unsigned	18 Aug 2020, 00:55		Edit Delete

5. Click **Delete**. A dialog box appears prompting you to confirm the action.
6. Click **Delete**.

The selected signature set is removed from the list.

Deleting Multiple Signature Sets

To delete single or multiple signature sets:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.

3. Click the **Signature Sets** tab. The list of configured signature sets is displayed.
4. Select the check boxes corresponding to the desired signature sets.

☒ 2 Selected 2 Results 2 Signature Sets	
Name	Signing Status
☒ testsigset	Finished
☒ test	Unsigned

To select all sets for deletion, select the top check box to the left of the Name column.

5. Click the delete icon (). A dialog box appears prompting you to confirm the action.
6. Click **Delete**.

The selected signature sets are removed from the list.

Re-Signing Files in a Signature Set

Signatures are computed values. Unless the files in a signature set are compromised or modified, the signature always remains the same for a given file. If the files are modified, they must be re-signed to ensure that their signatures match the signatures on the CipherTrust Manager.

To re-sign the files, you can:

- Create and sign a new signature set with the files and directories to be signed. Use this option if the set contains only a few files and directories.
- Create and sign a new signature set with the paths of the directories that contain the files to be signed. Use this option if the directories contain only a few files or most files in the directories need re-signing.
- Open and re-sign the existing signature set that is originally used to sign the files. Use this option if you have the time or the signature set is small.

Computing the signature of every file in a large signature set takes a long time.

Re-signing the files in a set takes longer than signing the files the first time. It requires additional handling to update information on the CipherTrust Manager. If you plan to re-sign a large number of files (say hundreds of thousands), it can be quicker to:

1. Delete the existing signature set. Refer to [Deleting Signature Sets](#) for details.
2. Create the signature set again, from scratch. Refer to [Creating Signature Sets](#) for details.

3. Sign the files of the signature set again. Refer to [Signing Files in a Signature Set](#) for details.

Tip

CTE for Kubernetes clients do not support signing of files. To re-sign files, you need to [delete the signature set](#) and [create the signature set](#) of manually signed files again.

Checking Agent Logs if Signing Fails

If signing fails, or you want more information about the signing process such as which files were skipped, check the CTE Agent logs captured on the client.

Messages are logged to:

- (UNIX) `/var/log/vormetric/vorvmd_root.log` with Log to File enabled and to a Syslog server with Syslog enabled.
- (Windows) `\Documents and Settings\...\agent\log\vorvmd.log` with Log to File enabled.

In the `vorvmd_root.log`/`vorvmd.log` file on the client, look for messages like:

```
[VMD] [WARN ] [3732] [VMD3824W] Failed to create the signature for
E:\apps\lib\dx1\aa_dir\dataxform_auto_config for the signature
request 9, error code 3
```

The following table lists error codes with their description:

Code	Description
0	System is okay.
1	Does not exist.
2	DO NOT USE.
3	Invalid argument.
4	Operation not supported.
5	Out of memory.
6	No space left on device.
7	Timeout reached.
8	I/O error.
9	Interrupted.
10	Permission denied.
11	Too many keys in key group.
12	Error in soap rpc layer.

Code	Description
13	Returned buffer is partially full.
14	Given target buffer is too small.
15	Unable to compress buffer.
16	Internal test failed.
17	Overflow.
18	Error setting up logging.
19	Overloaded error.
20	Server responded to a file upload with "bad request".
21	Unknown user name or bad password.
22	The directory service is not available.

Managing Policies

The primary job of a CipherTrust Manager Security Administrator is to create policies that protect data. Policies govern access to, and encryption of, the files in GuardPoints.

Overview

A policy is a collection of rules that govern data access and encryption. Think of a policy as an if-then statement. Policy rules are processed sequentially. If the criteria of rule one are not met, the policy enforcement engine moves on to the second rule and so on.

Policies specify:

- **Actors:** Users, groups, and processes that are permitted/denied access to protected data.
- **Actions:** What actions authorized actors are allowed to perform. For example create/delete, read/write, decrypt, modify permissions, and so on.
- **Files acted upon:** Policy rules may apply to entire directories and mount points, or only to files named in a specific way (for example, .docx files may be encrypted and restricted to read-only access by designated users, while other files may be stored clear and read and written by anyone).

Additionally, each CTE policy specifies one or more encryption keys used to encrypt blocks of file data when applications write them, and decrypt them when they are read.

CTE encryption is transparent to applications. This means that the CTE Agent encrypts blocks of data as they are written, and decrypts data when they are read by authorized users and applications. This architecture separates administration of files from access to the data in them. Backup programs, for example, may be authorized to read files, but not view the data in them. Therefore, data can be backed up and taken offsite while remaining encrypted so that security is not breached.

The following criteria are processed by the policy enforcement engine:

Criteria	Description
Order	Security rule enforcement sequence.
Resource	Files and/or directories to which the policy will apply, plus key rules that govern those files and directories.
User	Users and user groups authorized to access the resources.
Process	Executables which will access the files.
Action	Type of user access being made (read, write, copy, move etc.). Before you can define Data Transformation Rules, you must select an Action type of Key_op.
Effect	When all the other rules match, this describes the type of access granted or denied per the rule.
Browsing	Allow browsing is enabled by default, while the Enable Communication check box is enabled on the client. This allows the server to browse the client's file system. This option can be deselected even if client communication is still enabled.

A policy comprises [Security Rules](#), [Key Rules](#), [Data Transformation Rules](#), and [Signature Rules](#).

Policy Rule Criteria and Effects

Policy Rules consist of five criteria, which specify the attributes of an access attempt, and effects, which define whether that access is permitted or denied, and whether encryption/decryption is required.

Policy Rule Criteria

Criteria	Action
Resource	Files and/or directories in a GuardPoint to be blocked. Example: <code>/secure_dir/financials</code> .
User	Users or groups of users that can access the files.
Process	Executables that can operate on the files.
Action	Allowed file action. Example: read, write, remove, rename, and make directory.

Policy Rule Effects

Effect	Action
Permit	Allows access to the data.
Deny	Disallows access to the data.
Apply Key	Encrypts data written to a GuardPoint with the specified key. Decrypts data that is accessed using the same key.

Effect	Action
Audit	Creates an entry in the Message Log that describes what is being accessed, when it is being accessed, and the security rule being applied.

Every time a user's application tries to access a GuardPoint file, the security policy tests that access attempt against the criteria of each rule. For example, suppose a user, Harry, wants to access and modify a file called secret, using the command cp. For Harry to be successful, there must be a rule that allows access to the secret (resource), by the user Harry (user), using the command cp (process), and includes the permission write (action).

A blank criteria field specifies a value of All. If User is blank, the rule applies to all users; if Process is blank, the rule applies to all executables, and so on. Effect can never be blank. It must have at least a permit (allow access) or deny (disallow access).

A policy can have multiple rules. Rules are evaluated much like firewall rules. They are evaluated in order, from first to last, and evaluation stops when a rule is found for which all the criteria are met. The effect for that rule is then enforced. So, carefully order a policy's rules to achieve the desired result.

Creating Policy Elements

Policy rule criteria consist of resource sets, user sets, signature sets, process sets, action, and effect, and are called policy elements. These elements should exist on the CipherTrust Manager before you can use them in security policies.

Although you can add policy elements when creating policies, it may be a better approach to have them created in advance. This document describes creation of policy elements separately, before creating policies.

A CipherTrust Manager administrator can create, modify, and delete resource sets, user sets, process sets, and signature sets on the CipherTrust Manager. Actions and effects are preconfigured on the CipherTrust Manager.

After you have created policy elements, you can use them in creating and configuring policies. Refer to [Creating Policies](#) for details.

Note

You can only label a profile for [File Activity Monitoring \(FAM\)](#) in the ksctl CLI.

Creating Resource Sets

A resource is a combination of a directory, a file, and patterns or special variables. A resource set is a named collection of directories, files, or both, that a user or process will be permitted or denied access to.

Use the Create Resource Set wizard to create resource sets.

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. On the **Resource Sets** tab, click **Create Resource Set**. The Create Resource Set wizard is displayed.

4. On the **General Info** screen:

- a. Enter a unique **Name** for the set.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
- b. Make sure that **Directory** is selected as the **Resource Set Type**.
- c. Provide a **Description** for the set.
- d. Click **Next**. The Add Resources screens is displayed.

5. Specify the resource **Directory**.

Note

- Resource sets must be relative to the guard path. Resource sets created using the absolute paths are not supported.
- The path must end with a slash. For example, a Windows path must end with a `\` (backward slash). A Linux path must end with a `/` (forward slash).

6. Specify a **File** or enter the asterisk (`*`). The asterisk acts as a wild card character.

Note

An asterisk can be used to include all files of a specific extension in the resource set. For example, to include all text files under a resource directory, specify `*.txt`.

Later, a policy with desired permissions can be applied to the resource set. That policy will apply to all files of the specified extension under the specified resource directory.

7. (Optional) Specify whether to include subfolders in the set. Turn on **Include Sub Folders**. By default, the subfolders are not included.

Directory

/cte-test/

File

*

Include Sub Folders: ☒HDFS File System: ☐

8. (Optional, Linux only) Turn on the **HDFS File System** toggle for an HDFS resource. When you turn on this toggle, ensure that **Directory** and **File** contain HDFS paths.

HDFS is applicable to Linux clients. By default, the **HDFS File System** toggle is turned off. Keep it turned off for a non-HDFS resource.

Note

To protect an HDFS resource, the CTE clients (NameNode and DataNodes in the HDFS cluster) must be configured for HDFS. Refer to the "Installing CTE on Hadoop" section in the [CTE Agent for Linux Advanced Configuration](#) document for details.

Note

For the list of supported HDFS systems, refer to the [Compatibility Matrix for CTE Agent with Data Security Manager](#). The matrix also applies to the CTE clients registered with the CipherTrust Manager.

9. Click **Next**. The Confirmation screen is displayed.

The screen shows general information about the set and the selected sources.

Directory	File	Include Sub Folders	File System Type	
/cte-test/	*	Yes	Local FileSystem	...

10. Verify the resource set details.

If the details are incorrect or you want to modify them, click **Back** and update the details. To add another resource, click **Add Another Resource**, and specify the details, as described above.

11. Click **Save**. The resource set is created.

The newly created resource set appears on the Resource Sets tab.

	Name	Type	Updated At ↓	Description	
☐	resourceset	Directory	18 Aug 2020, 11:47	Resource set	...
☐	5G-ResourceSet	Directory	18 Aug 2020, 11:38		...

Creating User Sets

A user set is a collection of users and user groups that you want to grant or deny access to GuardPoints. User sets are configured in policies. Policies can be applied to user sets, not to individual users.

Use the Create User Set wizard to create user sets. The wizard provides two options to add user sets. Specify a user set either by querying the registered client or by manually entering the members (individual members, groups, or group members). If needed, you can manually add AD users to a user set.

Creating User Sets by Browsing the Client

To create a user set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **User Sets** tab.
4. Click **Create User Set**. The Create User Set wizard is displayed.
5. On the **General Info** screen:
 - a. Enter a unique **Name** for the set.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
 - b. (Optional) Provide a **Description** for the set.
 - c. Click **Next**. The Add Users screen is displayed.
6. On the **Add Users** screen:
 - a. Click **Create User**. By default, the **Manually Add Users** tab is active.

-
- b. Click the **Browse to Add Users** tab.

This tab allows you to browse the client for members. To add members manually, refer to [Creating User Sets by Adding Members Manually](#).

- c. Select a **Connection Type**. You can select either Agent or LDAP. Click the desired tab to view the instructions.

Agent

- a. Click **Select**. The list of registered clients is displayed.
- b. Select the desired client. Members, groups, or group members of this client will be added to the set.
- c. Click **Select**. The IP address or hostname of the selected client is displayed next to the Select button. The **User Type** and **Member Choice** fields are also displayed.

Agent *

Select 10.164.13.209

User Type *

Member Choice *

Select Option

- d. Select the desired **User Type**. The options are:
- **System**: Select to add system users to the user set.
 - From the **Member Choice** drop-down list, select members. The options are:
 - **Users**: Users of the client.
 - **Groups**: User groups of the client.
 - **Group Members**: Group members of the client. When you select this option, the Select Groups field appears. This is a mandatory field. Select a group from the drop-down list. Search will retrieve members of the selected group.
 - Click **Apply**. The search result based on the specified criteria is displayed on the right. A set of sample system users/groups is displayed below.

The screenshot shows a configuration window with the following elements:

- User Type:** A dropdown menu set to "System".
- Member Choice:** A dropdown menu set to "Group Members".
- Select Groups:** A dropdown menu set to "Administrators".
- Apply:** A blue button.
- Search Results:** A table with columns "uname" and "gname". Above the table, it says "0 Selected" and "Administrator" with an unchecked checkbox.

The search can display only the first 100 results. Refine your search by entering the exact name.

- Select the desired members from the list.

The screenshot shows the same configuration window as before, but with the following changes:

- Search Results:** The table now shows one row with a checked checkbox, "Administrator", and empty "uname" and "gname" fields. Above the table, it says "1 Selected".

- **LDAP:** Select to add LDAP users to the user set.
 - From the **Member Choice** drop-down list, select members. The options are:
 - **Users:** Users of the client.
 - **Groups:** User groups of the client.
 - **Group Members:** Group members of the client. When you select this option, the Select Groups field appears. This is a mandatory field. Select a group from the drop-down list. Search will retrieve members of the selected group.
 - Click **Apply**. The LDAP Credentials dialog box is displayed.
 - Specify LDAP credentials to browse LDAP users and groups.
 - **Domain:** User-friendly network address that can be resolved through the Domain Name System (DNS).
 - **Username:** Name of the LDAP user for LDAP authentication.
 - **Password:** Password of the LDAP user for LDAP authentication.
 - Click **Submit**. The search result based on the specified criteria is displayed on the right. A set of sample LDAP users/groups is displayed below.

The search can display only the first 100 results. Refine your search by entering the exact name.

If the specified LDAP credentials are incorrect or you want to change them, click **Edit Credentials** and specify the updated details.

- Select the desired members from the list.

- Click **Create**.

LDAP

- Select LDAP Connection** from the drop-down list.
- Max Number of Entries to Return:** Number of Users, Groups, and Group Mmembers and their records to return in the search results. By default, a maximum of 300 records will be returned. Enter a number from 1 to 10000. For example, if you enter 100:
 - A maximum of 100 users/groups will be displayed when Member Choice is *Users* or *Groups*.
 - A maximum of 100 groups will be displayed in the Select Groups drop-down box when Member Choice is *Group Members*.
 - A maximum of 100 search results based on the specified criteria above is displayed on the right.
- From the **Member Choice** drop-down list, select members. The options are:
 - **Users:** Users of the client.
 - **Groups:** User groups of the client.

- **Group Members:** Group members of the client. When you select this option, the Select Groups field appears, which lists the Common Name (CN) of the groups. This is a mandatory field. Select a group from the drop-down list.

d. (Optional) Enter an **LDAP Query** to filter members meeting specific criteria.

For example, if you select Users in the Member Choice drop-down list, enter `(&(objectClass=posixAccount)(uidNumber=2001))` in the LDAP Query field, and click **Apply**, the search results will only display users with the UID number 2001.

e. Click **Apply**. Search will retrieve members based on the specified search criteria.

f. Select the desired users/groups.

7. Click **Create**.

uname	UID	gname	GID	OS domain
		WseManagedGroups		 Remove
		Administrators		 Remove
		Administrator		 Remove

To add more users, click **Create User**.

You can add System and LDAP users and groups simultaneously.

If you want to remove users from the set, identify the user and click **Remove**.

8. Click **Next**. The Confirmation screen shows general information about the set and the selected members.

9. Verify the set details.

If the details are incorrect or you want to modify them, click **Back** and update the details.

10. Click **Save**. The user set is created.

The newly created set appears on the User Sets tab.

	Name	Updated At ↓	Description	
☐	userset	14 Sep 2022, 12:34	A test user set	...
☐	testuserset	14 Sep 2022, 15:05	Test user set	...

Creating User Sets by Adding Members Manually

This method is useful when you already know the names of users and groups that should be added to a user set. Also, use this method to add AD users and groups to the user set.

Using Variables

You can also use the variables `|uname|` (user name) and `|gname|` (group name) when adding members manually. On the UNIX systems, `|uid|` and `|gid|` can also be used.

When the security rule is applied, the variable is replaced by the actual user name or user group name. For example, if **Directory** is set to `/opt/local/|gname|`, when you later make `/opt/local` the GuardPoint, only the members of the group **engineering** in **Users** are allowed access to `/opt/local/engineering`. `|uname|` and `|gname|` act like macros.

Similarly, if you want to define a policy to protect all of the user directories under `/home`, you don't need to enumerate `/home/user1`, `/home/user2`, `/home/user3`, and so on. You only need to define `/home/|uname|`. When the agent evaluates the policy, it replaces `|uname|` with the actual user. So, when **user1** logs on, the agent evaluates the policy with `/home/user1`. They can't access `/home/user2`.

To create a user set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **User Sets** tab.
4. Click **Create User Set**. The Create User Set wizard is displayed.
5. On the **General Info** screen:
 - a. Enter a unique Name for the set.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
 - b. (Optional) Provide a **Description** for the set.
 - c. Click **Next**. The Add Users screen is displayed.
 - d. Click **Create User**.

To browse the client for adding members manually, click the **Browse to Add Users** tab. This tab allows you to browse the client for members. Refer to [Creating User Sets by Browsing the Client](#) for details.

6. On the **Manually Add Users** tab, specify the following details, as appropriate:

Element	Description
uname	Login name of the user.
UID	(AIX/Linux only) ID of the user.
gname	Comma-separated list of group names.
GID	(AIX/Linux only) Group ID of the user. Specify only the primary group ID.
OS domain	(Windows only) Network domain of the user. Multiple domain names, separated by commas, can be entered. Specify the string <code>localhost</code> to configure a generic domain.

7. Click **Create**.

To add more users, click **Create User**. You can add different types of users and groups simultaneously.

If you want to remove users from the set, identify the user and click **Remove** next to the user.

8. Click **Next**. The Confirmation screen shows general information about the set and the selected members.

9. Verify the set details.

If the details are incorrect or you want to modify them, click **Back** and update the details.

10. Click **Save**. The user set is created.

The newly created set appears on the User Sets tab.

Creating Signature Sets

A signature set is a collection of hashes of processes and executables that you want to grant or deny access to GuardPoints. A signature set can be configured in a policy as part of a process set to verify the integrity of a process before it is allowed access to guarded data. Policies are applied to signature sets, not to individual signatures.

To create a signature set:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click **Create Signature Set**. The General Info screen of the Create Signature Set wizard is displayed.

General Info

1. Enter a unique **Name** for the set.

- The name must start with a character. The maximum length can be 64 characters.
- The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
- The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`

2. Select **Application** as the **Type**. The signature set will have signatures of the running applications.
3. (Optional) Provide a **Description** for the set.
4. Enable or disable the **Add Signatures** toggle. If you enable this option, an **3 - Add Signatures** screen becomes available.
5. Click **Next**. The Add Sources screen is displayed. On this screen, you can add files to be signed, as described below.

Add Sources

Specify path of the directory or file to be signed. If a directory is specified, all files in the directory and its subdirectories are signed.

The CipherTrust Manager provides an option to add multiple sources. A maximum of 200 sources can be added at once.

1. Click **Add Source**.
2. Click **Select Client**. The list of registered clients is displayed.
3. Select the desired client.

Status	Name	OS Type	Description
☒ Healthy	10.164.13.209	LINUX	ABLinux
☐ Healthy	ABWin	WINDOWS	AB Windows Client

4. Click **Select**. The selected client appears next to the Change Client button (previously Select Client).

If needed, change the client by clicking **Change Client**.

5. Specify the path to be signed by either typing manually or using the browser.

Client

Change Client

10.164.13.209

Enter Source:

/usr/bin/

Start Directory

Apply

Select Source:

tmp

tools

usr

bin

To jump to a specific directory, enter the directory path in the **Start Directory** field and click **Apply**. The browser shows the subdirectories and files, as shown below.

Client

Change Client

10.164.13.209

Enter Source:

/usr/bin

Start Directory

/usr/bin

Apply

Select Source:

usr

bin

You cannot browse above the Start Directory. Enter a start point that is higher in the directory hierarchy than all the directories and files that you want to select, or you will have to re-enter start points to locate and select the desired files. The default is the top-level, either slash (Linux) or backslash (Windows).

Alternatively, if you know the directory path, you can enter it manually in the **Path** field.

- Click **Add Source**. The selected source is displayed in the **SELECTED SOURCES** list.

Client

Change Client 10.164.13.209

Start Directory

/usr/bin

Apply

SELECTED SOURCES

/usr/bin **Remove**

Enter Source:

Select Source:

usr bin

Optionally, you can add a new source by clicking **Add Source**. To remove a source, click **Remove** to the right of the source. A signature set must contain at least one source.

- Click **Add**. The selected source is displayed in the Source Directory list.

Optionally, you can add a new source by clicking **Add Source**. To remove a source, click the overflow icon () corresponding to the source and click **Remove**.

- Click **Next**. The Add Signatures screen is displayed. On this screen, you can manually add signatures or upload a CSV file containing signatures.

Add Signatures

If you enabled **Add Signatures** on the **General Info** screen, CipherTrust Manager provides options to add signatures to a signature set manually, and to upload the signatures to a signature set through CSV.

Click the desired tab to view the instructions.

Adding Signatures to a Signature Set Manually

- Click **Create Signature**. The Create Manually tab is displayed.
- Under **Signature 1**, enter the following details:
 - Program**: Full path of the file.
 - Signature**: Signature of the file.

To add multiple signatures, click **+ Add More Signatures**. To remove a signature, click **X**.

- Click **Add**. The signatures are added to the signature set. The list of programs and their signatures are displayed.

Optionally, you can add more signature(s) by clicking **Create Signature**, and repeating step 2 and 3. To remove a signature, click the overflow icon () corresponding to the signature and click **Remove**.

- Click **Next**. The Confirmation screen is displayed. The screen shows the General Info, Sources and Signatures details of the signature set.

Uploading Signatures to a Signature Set through CSV

- Click **Create Signature**. The Create Manually tab is displayed.
- Click the **Upload** tab.
 - Next to **Upload CSV**, click **Browse**.
 - Select and upload the CSV file. The Upload CSV field shows the uploaded file.
- Click **Add**. The signatures from the CSV file are added. The name of the file is displayed.

Optionally, you can change the file by clicking **Create Signature**, and repeating step 2 and 3. To remove the file, click the overflow icon () corresponding to the uploaded CSV file and click **Remove**.

- Click **Next**. The Confirmation screen is displayed. The screen shows the General Info, Sources and Signatures details of the signature set.

Confirmation

- Verify the set details. If the details are incorrect or you want to modify them, click **Back** and update the details.
- Click **Save**.

The newly created set appears on the Signature Sets tab. By default, the signature set has the status **UNSIGNED**.

	Name	Type	Signing Status	Updated At ↓	Description	
☐	testsigset	Application	Unsigned	24 Nov 2022, 14:14	Test signature set	
☐	test	Container Image	Unsigned	24 Nov 2022, 14:12		

It is recommended that the signature set is signed before you apply policies to processes. This ensures that a tampered with or compromised process executable is not granted permissions to access protected GuardPoints. Refer to [Signing Files in a Signature Set](#) for details.

Creating Signature Sets for Container Images

A signature set is a collection of file names and their signatures. A signature is a hash of a process or an executable file. Through signature sets, a signature can be used to verify the integrity of the process before it is allowed access to the guarded data.

You can enter the full path of files and their signatures manually or use the browser to upload YAML files containing the list of files and their signatures.

To create a signature set for CTE for Container Images:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**.
3. Click the **Signature Sets** tab.
4. Click **Create Signature Set**. The General Info screen of the Create Signature Set wizard is displayed.

General Info

1. Enter a unique **Name** for the set.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
2. Select **Container Image** as the **Type**. The signature set will have the signatures of containers.
3. (Optional) Provide a **Description** for the set.
4. Enable or disable **Add Signatures**.
5. Click **Next**. The Add Sources screen is displayed. On this screen, you can add source paths or upload the YAML file containing the source paths, as described below.

Add Sources

Specify path of the directory or file to be signed. If a directory is specified, all files in the directory and its subdirectories are signed.

The CipherTrust Manager provides an option to add multiple sources. A maximum of 200 sources can be added at once.

Click the desired tab to view the instructions.

Adding Sources Manually

1. Click **Add Source**. The Create Manually tab is displayed.
2. In the **Enter Source** field, add source for the container images to be trusted.
3. Click **Add**. The sources are added to the signature set. The list of Source Directory is displayed.

Optionally, you can add more sources by clicking **Add Source**, and repeating step 2 and 3. To remove a source, click the overflow icon () corresponding to the source and click **Remove**.

4. Click **Next**. The Add Signatures screen is displayed. On this screen, you can manually add signatures or upload the list of signatures.
-

Uploading Sources through YAML

1. Click **Add Source**. The Create Manually tab is displayed.
2. Click the **Browse** tab.
 - a. Next to **Upload YAML**, click **Browse**.
 - b. Select and upload the YAML file that contains the source for the container images to be trusted. The Upload YAML field shows the uploaded file.
3. Click **Add**. The sources from the YAML file are added. The name of the file is displayed.

Optionally, you can change the file by clicking **Add Source**, and repeating step 2 and 3. To remove a signature, click the overflow icon () corresponding to the source and click **Remove**.

4. Click **Next**. The Add Signatures screen is displayed. On this screen, you can manually add signatures or upload the list of signatures.

Note

The Add Signatures tabs is displayed if you selected **Add Signatures** on the General Info screen.

Add Signatures

If you enabled **Add Signatures** on the **General Info** screen, CipherTrust Manager provides options to add signatures to a signature set manually, and to upload the signatures to a signature set through CSV.

Click the desired tab to view the instructions.

Adding Signatures to a Signature Set Manually

1. Click **Create Signature**. The Create Manually tab is displayed.
2. Under **Signature 1**, enter the following details:
 - **Program**: Full path of the file.
 - **Signature**: Signature of the file.

To add multiple signatures, click **+ Add More Signatures**. To remove a signature, click **X**.

3. Click **Add**. The signatures are added to the signature set. The list of programs and their signatures are displayed.

Optionally, you can add more signature(s) by clicking **Create Signature**, and repeating step 2 and 3. To remove a signature, click the overflow icon () corresponding to the signature and click **Remove**.

4. Click **Next**. The Confirmation screen is displayed. The screen shows the General Info, Sources and

Signatures details of the signature set.

Uploading Signatures to a Signature Set through CSV

1. Click **Create Signature**. The Create Manually tab is displayed.
2. Click the **Upload** tab.
 - a. Next to **Upload CSV**, click **Browse**.
 - b. Select and upload the CSV file. The Upload CSV field shows the uploaded file.
3. Click **Add**. The signatures from the CSV file are added. The name of the file is displayed.

Optionally, you can change the file by clicking **Create Signature**, and repeating step 2 and 3. To remove the file, click the overflow icon () corresponding to the uploaded CSV file and click **Remove**.

4. Click **Next**. The Confirmation screen is displayed. The screen shows the General Info, Sources and Signatures details of the signature set.

Confirmation

1. Verify the set details. If the details are incorrect or you want to modify them, click **Back** and update the details.
2. Click **Save**.

The newly created set appears on the Signature Sets tab. By default, the signature set has the status **UNSIGNED**.

Creating Process Sets

A process set is a collection of processes (executables) that you want to grant/deny access to GuardPoints or exempt from RWP monitoring. Like user sets, process sets can be configured in policies. Policies can be applied to process sets, not to individual processes.

In a process set, you can also specify processes with and without signatures and directories to be exempted from RWP monitoring. This process set can be used as a Trusted Process Set in the [Ransomware Protection Configuration](#).

Optionally, file signing can be configured to check the authenticity and integrity of executables and applications before they are allowed to access GuardPoint data. A signature set must already exist before you can configure file signing in a policy for a process set.

Use the Create Process Set wizard to create process sets.

To create a process set:

1. Open the **Transparent Encryption** application.
 2. Click **Policies > Policy Elements**.
 3. Click the **Process Sets** tab.
 4. Click **Create Process Set**. The Create Process Set wizard is displayed.
-

5. On the **General Info** screen:

- a. Enter a unique **Name** for the set.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
- b. Provide a **Description** for the set.
- c. Click **Next**. The Add Processes screen is displayed.

6. On the **Add Processes** screen:

- a. Click **Create Process**.
- b. Click **Select** next to the Directory field. The Browse Path dialog box is displayed.
 - a. Click **Select Client**. The list of registered clients is displayed.
 - b. Select the desired client and click **Add**. The selected client appears next to the **Change Client** button. Click this button to change the client. The dialog box shows the filesystem of the selected client.
- c. Select the directory and file(s). The selected path automatically appears in the Search Local Path field.

Alternatively, specify the process name (with its path) in the **Search Local Path** field. Use `/` (forward slashes) to specify the path. A directory path must end with `/`.

You can also **Add Full Directory** or select multiple files of a single directory individually. Select a file and click **Add Path**.

The selected directory and process appear in the **Selected Directory** and **Selected Files** fields. If a process is not selected, the **Selected Files** field shows an (`*`) asterisk. The asterisk acts as a wild card character.

- d. Click **Add**.

Alternatively, you can update or specify the directory and process in the **Directory** and **File** fields. Use `/` (forward slashes) to specify the path. A directory path must end with `/`.

- c. Link the desired signature set to the process set.
 - a. Click **Select** next to the Signature field. The list of Application type signature sets is displayed.

The signature sets of the Container Image type are not displayed. They are used by the CTE for Kubernetes policies.

Optionally, you can create a new signature set by clicking **Create Signature Set**, and link it with the process set. Refer to [Creating Signature Sets](#) for details.

b. Select the desired signature set.

c. Click **Add**.

The selected signature set appears in the Signature field.

d. Link the desired RWP Exempted Resource to the process set.

Note

It is recommended to add the resource set if the process set is used as the Trusted Process Set in the [Ransomware Protection Configuration](#).

a. Click **Select** next to the RWP Exempted Resource. The list of Application type resource sets is displayed.

b. Select the desired **Resource Set** from the list.

c. Click **Add**.

7. Click **Add**. The Confirmation screen shows general information about the set.

Directory	File	Signature	
/usr/bin/	*	testsigset	...

8. Verify the set details.

If the details are incorrect or you want to modify them, click **Back** and update the details. To add another process, click **Create Process**, and specify the details, as described above.

To remove a process, click the overflow icon () corresponding to the desired process and click **Remove**.

9. Click **Next**.

10. Review the process set details.

11. Click **Save**. The process set is created.

The newly created set appears on the Process Sets tab.

	Name	Updated At ↓	Description	
☐	testprocessset	18-Aug-2020, 12:34	Test process set	...
☐	aprocesstest	18-Aug-2020, 12:34	A process set	...

After you have created policy elements, you can use them in creating and configuring policies. Refer to [Creating Policies](#) for details.

Viewing Policy Elements

The Policy Elements page shows the list of configured policy elements.

Note

Any updates to the policy elements will be applied without confirmation if the linked policy is not in use by any Enabled/Active GuardPoints.

To view the policy elements:

1. Open the **Transparent Encryption** application.
2. Click **Policies > Policy Elements**. The Policy Elements page contains the following tabs:

Column	Description
Resource Sets	Displays the list of configured resource sets. This is the default tab.
User Sets	Displays the list of configured user sets.
Process Sets	Displays the list of configured process sets.
Signature Sets	Displays the list of configured signature sets.

3. Click the **Resource Sets** tab. This tab displays the following details:

	Name	Type	Updated At ↓	Description	
☐	resourceset	Directory	18-Aug-2020, 11:47	Resource set	...
☐	5G-ResourceSet	Directory	18-Aug-2020, 11:38		...

Column	Description
Name	Name of the resource set.
Updated At	Time when the set is created or updated.
Description	Optional description of the resource set.

By default, the records are displayed in descending order by Updated At. To add a new resource set, refer to [Creating Resource Sets](#).

To modify an existing resource set, click the desired set, modify the **Description**, and click **Apply**.

The edit view also provides the **Add Resource** button to add new resources to the set. While saving the new resource details, specify the applicable OS for the resource - Windows or Non Windows.

- Click the **User Sets** tab. This tab displays the following details:

Name	Updated At ↓	Description	
☐ userset	14 Sep 2022, 12:34	A test user set	...
☐ testuserset	14 Sep 2022, 15:05	Test user set	...

Column	Description
Name	Name of the user set.
Updated At	Time when the set is created or updated.
Description	Optional description of the user set.

By default, the records are displayed in descending order by Updated At. To add a new user set, refer to [Creating User Sets](#).

To modify an existing user set, click the desired set, modify the **Description**, and click **Apply**. The edit view also provides the **Browse users** and **Manually add user** buttons to add new users to the set.

- Click the **Process Sets** tab. This tab displays the following details:

Name	Updated At ↓	Description	
☐ testprocessset	18 Aug 2020, 12:34	Test process set	...
☐ aprocessset	18 Aug 2020, 12:34	A process set	...

Column	Description
Name	Name of the process set.
Updated At	Time when the set is created or updated.
Description	Optional description of the process set.

By default, the records are displayed in descending order by Updated At. To add a new process set, refer to [Creating Process Sets](#).

To modify an existing process set, click the desired set, modify the **Description**, and click **Apply**. The edit view also provides the **Add Process** button to add new processes to the set.

6. Click the **Signature Sets** tab. This tab displays the following details:

Name	Type	Signing Status	Updated At ↓	Description	
☐ testsigset	Application	Unsigned	24 Nov 2022, 14:14	Test signature set	...
☐ test	Container Image	Unsigned	24 Nov 2022, 14:12		...

Column	Description
Name	Name of the signature set.
Type	Type of the signature set. The type can be: • Application: The signature set will have signatures of the running applications. • Container Image: The signature set will have the signatures of containers.
Signing Status	Signing status of the signature set. Refer to Checking Signing Completion Status) for details.
Updated At	Time when the set is created or updated.
Description	Optional description of the signature set.

By default, the records are displayed in descending order by Updated At. To add a new signature set, click **Create Signature Set** (refer to [Creating Signature Sets](#)).

To add a new source to an existing signature set, click the desired set, and click **Add Source**. Refer to [Creating Signature Sets](#) for details.

To add a new signature to an existing signature set, click the desired set, click the **Signature** tab, and click **Create Signature**. Refer to [Creating Signature Sets](#) for details.

Creating Policies

A policy is a collection of rules that govern data access and encryption. Think of a policy as an if-then statement. Policy rules are processed sequentially. If the criteria of rule one are not met, the policy enforcement engine moves on to the second rule and so on.

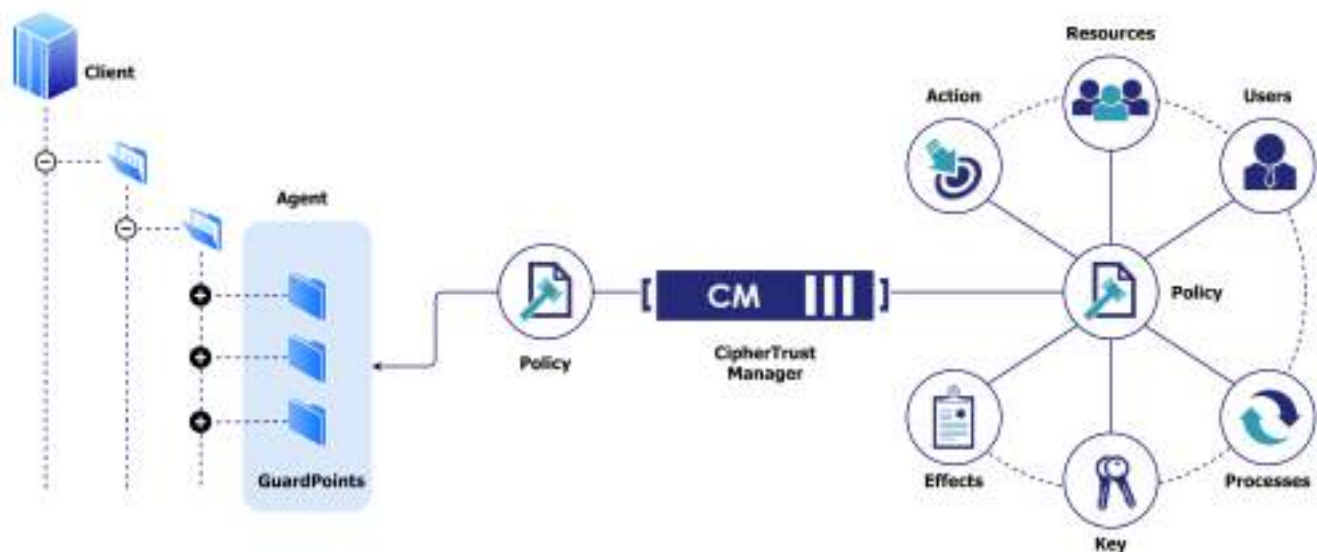
Policies specify:

- **Actors:** Users, groups, and processes that are permitted/denied access to protected data.
- **Actions:** What actions authorized actors are allowed to perform. For example create/delete, read/write, decrypt, modify permissions, and so on.
- **Files acted upon:** Policy rules may apply to entire directories and mount points, or only to files named in a specific way (for example, `.docx` files may be encrypted and restricted to read-only access by designated users, while other files may be stored clear and read and written by anyone).

Additionally, every CTE policy specifies one or more encryption keys used to encrypt blocks of file data when applications write them, and decrypt them when they are read.

CTE encryption is transparent to applications. This means that the CTE Agent encrypts blocks of data as they are written, and decrypts data when they are read by authorized users and applications. This architecture separates administration of files from access to the data in them. Backup programs, for example, may be authorized to read files, but not view the data in them. Therefore, data can be backed up and taken offsite while remaining encrypted so that security is not breached.

The following diagram shows policies and how they relate to the GuardPoints, clients, and the CipherTrust Manager.



Before you can create a policy, policy elements should exist on the CipherTrust Manager. This section assumes that you have already created policy elements, as described in [Creating Policy Elements](#).

When creating a policy, you can specify security rules, key rules, and data transformation rules that apply to the policy. At least one key or security rule must be added to a policy. Use the Create Policy wizard to create a policy.

Step 1: Specify General Information

To specify general information about policy:

1. Open the **Transparent Encryption** application.
2. Click **Policies**. The Policies page shows the list of available policies.
3. Click **Create Policy**.
4. Specify a unique **Name** for the policy. For example, basic-access-policy or ldt-policy.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
5. Select a **Policy Type**. The options are:
 - **Standard**: Access to data is blocked during initial encryption or rekeying of data. This is the default policy type. Refer to [Creating Standard GuardPoints](#) for details.
 - **Live Data Transformation**: Encryption and rekeying of data takes place in the background, without disrupting user or application access to that data. The LDT policy is available if you have a valid LDT license.

 If you select an LDT policy type, then the first security rule for the policy is created by default. This rule permits key operations on all resources for that policy, without denying user or application access to resources. This allows a rekey operation whenever the encryption key is versioned. This rule is always the first rule in an LDT policy and cannot be edited.
 - Refer to [Enabling Live Data Transformation](#) for more information about LDT.
 - An LDT policy is needed for creating LDT GuardPoints. Refer to [Creating LDT GuardPoints on Clients](#) for details.
 - **Cloud Object Storage (COS)**: Access to data is blocked during initial encryption or rekeying of data. This policy type is needed for creating GuardPoints for cloud storages. Refer to [Creating Cloud Object Storage GuardPoints on Clients](#) for details.
 - **In-place Data Transformation (IDT)**: Access to data is blocked during encryption or rekeying of data. This policy type is needed for creating GuardPoints for Teradata clusters. Refer to [Creating IDT GuardPoints](#) for details.
 - **CTE for Kubernetes**: Applicable to GuardPolicies for CTE for Kubernetes (K8s) clients. Access to data is blocked during initial encryption or rekeying of data. The CTE for Kubernetes policies are used to protect K8s clients. Refer to [Protecting Kubernetes Clients](#) for details.

6. Provide a basic **Description** for the policy.
7. (Optional) Turn on the **Learn Mode** toggle. A warning message is displayed indicating that the policy is in Learn Mode.

Learn Mode:



Warning: This Policy is in Learn Mode [Click here for more details](#)

Refer to [Learn Mode](#) for details. By default, the toggle is turned off.

Note

Learn Mode is not applicable to *In-place Data Transformation* policies.

8. (Optional) Turn on the **Restrict Update** toggle. This option is used to restrict or allow any changes to the policy. By default, the toggle is turned off. This setting can be changed any time after the policy is created. Refer to [Controlling Updates to Policies](#).
9. (Optional, applicable to *Standard* policies) Turn on the **Data Transformation** toggle. This option is used to create a *data transformation* policy. By default, the toggle is turned off.

Note

The Data Transformation option is not applicable to *LDT*, *Cloud Object Storage*, and *In-place Data Transformation* policies. For a data transformation policy, the Create Policy wizard shows five steps including the Data Transformation step, as shown below.

Create Policy [?]

1 General Info 2 Security Rules 3 Key Rules 4 Data Transformation 5 Confirmation

10. Click **Next**. The Security Rules screen is displayed.

For a *standard data transformation* policy, a security rule with the Action **key_op**, the Effect **permit**, **applykey**, and Browsing set to Yes is added automatically. Edit or delete the rule, as appropriate. Click the overflow icon (**⋮**) for options.

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit,applykey	Yes

For an *LDT policy*, the default security rule with the Action **key_op**, the Effect **permit, applykey**, and Browsing set to No is added automatically. The rule is *read only*.

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit,applykey	No

Step 2: Add Security Rules

1. Click **Add Security Rule**. The Create Security Rule dialog box is displayed. This dialog box contains the following fields:

Field	Description
Resource Set	(Not applicable to <i>COS</i> policies) Resource set for the rule.
User Set	User set for the rule.
Process Set	Process set for the rule.
Action	Actions for the rule. Refer to Actions for the complete list of supported actions.
Effect	Effect permission and options for the rule. This is a mandatory field.
Allow Browsing	(Not applicable to <i>COS</i> and <i>CTE for Kubernetes</i> policies) Whether browsing of directories under the GuardPoint down to the resources in the rule is allowed.

2. (Optional, not applicable to *COS* policies) Select a **Resource Set**.
 - a. Click **Select** next to the Resource Set field. The list of available resource sets is displayed.

Optionally, you can add a new resource set by clicking **Create Resource Set**. Walk through the Create Resource Set wizard, as described in [Creating Resource Sets](#). The newly created resource set appears in the resource sets list.
 - b. Select a resource set.
 - c. (Optional) Select **Exclude Rule** to exclude the resource set from the policy. The security rule does not apply to this resource set.

d. Click **Select**. The selected resource set appears in the Resource Set field.

3. (Optional) Select a **User Set**.

a. Click **Select** next to the User Set field. The list of available user sets is displayed.

Optionally, you can add a new user set by clicking **Create User Set**. Walk through the Create User Set wizard, as described in [Creating User Sets](#). The newly created user set appears in the user sets list.

b. Select a user set.

c. Click **Select**. The selected user set appears in the User Set field.

4. (Optional) Select a **Process Set**.

a. Click **Select** next to the Process Set field. The list of available process sets is displayed.

Optionally, you can add a new process set by clicking **Create Process Set**. Walk through the Create Process Set wizard, as described in [Creating Process Sets](#). The newly created process set appears in the process sets list.

b. Select a process set.

c. (Optional) Select **Exclude Rule** to exclude the process set from the policy. The security rule does not apply to this process set.

d. Click **Select**. The selected process set appears in the Process Set field.

5. (Optional) Select an **Action**. Specify the type of file and directory action allowed on a GuardPoint. To specify *all* actions, leave the **Action** field blank.

a. Click **Select** next to the Action field. By default, the Select Action(s) dialog box displays basic actions.

To view advanced actions, expand **Advanced Options** by clicking **+**. The Select Action(s) dialog box provides the names and brief description of actions. Refer to [Actions](#) for the complete list of supported actions.

b. Select the desired actions.

Note

- For a data transformation policy, the action **key_op** is selected automatically. If you select **key_op**, then you must add a data transformation rule.
- For an IDT policy, the allowed actions are **read**, **write**, and **all_ops**.

c. Click **Select**. The selected actions appear in the Action field.

6. Select an **Effect**. Effect is the action that occurs when the attempted access matches all the criteria in the rule. This is a mandatory field. The default action is Deny.
 - a. Click **Select** next to the Effect field. The Select Effect dialog box displays the available Effect Permissions and Effect Options.
 - b. From the **Effect Permissions** list, select a permission. An effect must have a permission. The available options are:
 - **Deny**: Denies the access attempts to a resource. For example, you can specify an effect that denies any attempts to access a resource.
 - **Permit**: Allows the access attempt to a resource. For example, you can specify an effect that allows writing to a resource.
 - c. From the **Effect Options** list, select appropriate options. The available options are:
 - **ApplyKey**: Applies an encryption key to data in a GuardPoint. When applied, data copied to the GuardPoint is encrypted with the key specified on the Create Key Rule screen and data that is accessed in the GuardPoint is decrypted using the same key. It allows the access attempt to the resource. For example, you can specify an effect that allows writing to a directory.

Note

If you select ApplyKey, you must also specify the key rules to apply for encrypting and decrypting the resources. Refer to [Step 3: Add Key Rules](#) for details.

- **Audit**: Creates a message log entry for each qualifying event. It records what, when, and who is accessing the information.
- d. Click **Select**. The selected effects appear in the Effect field.
7. (Optional, not applicable to *COS* and *CTE for Kubernetes* policies) Specify whether to **Allow Browsing** the directories under the GuardPoint down to the resources in the rule.

By default, the **Allow Browsing** toggle is on. Users that match the criteria set by the security rule can access the directories between the GuardPoint and the resource. If you define a resource, then that resource should exist in the GuardPoint. The files in these directories can be listed like any file in a browser, but they cannot be modified, copied, or deleted.

To prevent users from browsing the directories under the GuardPoint, turn off the **Allow Browsing** toggle.

8. Click **Add**. The newly created security rule appears in the list of security rules.

Similarly, you can add multiple security rules to the policy by clicking **Create Security Rule**. To delete a security rule, click **Delete** next to the rule.

Note

A security rule with the **ApplyKey** Effect must be supported by at least one key rule. Refer to [Step 3: Add Key Rules](#).

9. Click **Next**. The Key Rules screen is displayed.

Step 3: Add Key Rules

If you added a security rule with the Effect **ApplyKey** on the Security Rules screen, then you must add at least one key rule.

Note

For the **IDT** policies, only *one* key rule can be specified. So, you only need to specify the **Current Key** and **Transformation Key**. You can add a `clear_key`, `XTS`, `CBC`, or `CBC_CS1` key as the **Current Key**. After adding the key, click **Next**. Verify the policy details on the Confirmation screen. Refer to [Step 5: Confirm Details](#).

To add a key rule:

1. Click **Create Key Rule**. The Create Key Rule dialog box is displayed.
2. (Optional, not applicable to *COS* policies) Select a **Resource Set**.
 - a. Click **Select** next to the Resource Set field. The list of available resource sets is displayed.

Optionally, you can add a new resource set by clicking **Create Resource Set**. The newly created resource set will appear in the resource sets list.
 - b. Select a resource set.
 - c. Click **Select**. The selected resource set appears in the Resource Set field.
3. Select a **Key Name**. This is a mandatory field. For *LDT* and Data Transformation policies, the field name is **Current Key Name** instead of Key Name.
 - a. Click **Select** next to the field. The Select Key dialog box shows the list of available keys. Optionally, you can create a new `CBC`, `CBC-CS1`, or `XTS` key on this dialog box.

To create a new key

- a. Click **Create a New Key**. The **Key created will be AES 256** section is displayed on the dialog box below.

- b. Specify an optional **Name** for the key.
- c. Select the **Encryption Mode**. The encryption mode can be CBC, CBC-CS1, or XTS. The default mode is CBC.
- d. (Optional, not applicable to COS and CTE for Kubernetes policies) Select **Unique to Client** to make the key a unique to client key.
- e. Click **Create**. The newly created key appears in the keys list.

If you selected the **Unique to Client** check box when creating the key, you will see a check mark for the key under the Unique to Client column. This indicates the key is a unique to client key. Refer to [Unique to Client Keys](#) for details.

Alternatively, encryption keys for CTE can be created on the **Keys** page of the CipherTrust Manager GUI. Refer to [Creating a New Key](#) for details.

Note

When creating the XTS keys using the CipherTrust Manager CLI or the API:

- Set the `xts` flag to `true`.
- Set the key as exportable, that is, set `unexportable` to `false`.
- Share the key with the CTE Users group with the `read_key` and `export_key` permissions.

Refer to the following sample for creating an XTS key:

```
{
  "name": "CTE-XTS-Key",
  "algorithm": "aes",
  "size": 256,
  "undeletable": true,
  "unexportable": false,
  "meta": {
    "ownerId": "local|59ba6797-e5a6-4427-b11c-a5534b5a975e",
    "permissions": {
      "ExportKey": [
        "CTE Clients"
      ],
      "ReadKey": [
        "CTE Clients"
      ]
    }
  }
}
```

```

    },
    "cte": {
      "persistent_on_client": true,
      "encryption_mode": "XTS",
      "cte_versioned": false
    }
  },
  "xts": true,
  "id": "95cc7868-89bf-492b-b868-bbb884a9b379"
}

```

Note

When an XTS key is created, an additional tweak key (<key-name>_xts) is generated with the original key. Make sure that both the original and the tweak keys are part of the CTE Users group with the read key (read_key) and export key (export_key) permissions.

- b. Select the desired key.

Note

For CTE for Kubernetes policies, select a CBC-CS1 key. These policies do not support XTS keys.

- c. Click **Select**. The selected key appears in the Key Name / Current Key Name field.

The next two steps are specific to *LDT* policies.

4. (Applicable to LDT policies) Select a **Transformation Key Name**. This is a mandatory field.

- a. Click **Select** next to the field. The list of available keys is displayed.

Optionally, you can create a new key by clicking **Create a New Key**. Optionally, specify a **Name** for the key and click **Create**. The newly created key will appear in the keys list.

Alternatively, encryption keys for CTE can be created on the **Keys** page of the CipherTrust Manager GUI. Refer to [Creating a New Key](#) for details.

- b. Select the desired key.
- c. Click **Select**. The selected key appears in the Transformation Key Name field.

-
- Click **Add**. The newly created key rule appears in the list of key rules.

Similarly, you can add multiple key rules to the policy by clicking **Create Key Rule**. To delete a key rule, click **Delete** next to the rule.

- Click **Next**.

For *Live Data Transformation*, *Cloud Object Storage*, and *In-place Data Transformation* policies, the Confirmation screen is displayed. Verify policy details, as described in [Step 6: Confirm Details](#).

For *Standard* policies, the following screen is displayed:

- **Data Transformation:** If you selected the **Data Transformation** check box on the **General Info** screen of the Create Policy wizard. Add data transformation rules, as described in [Step 4: Add Data Transformation Rules](#).
- **Confirmation:** If you cleared the **Data Transformation** check box. Verify policy details, as described in [Step 6: Confirm Details](#).

For *CTE for Kubernetes* policies, the following screen is displayed:

- **Data Transformation:** If you selected the **Data Transformation** check box on the **General Info** screen of the Create Policy wizard. Add data transformation rules, as described in [Step 4: Add Data Transformation Rules](#).
- **Signature Rules:** If you cleared the **Data Transformation** check box. Add signature rules, as described in [Step 5: Add Signature Rules](#).

Step 4: Add Data Transformation Rules

This step is applicable to *Standard* and *CTE for Kubernetes* policies if you selected the Data Transformation check box on the General Info screen of the Create Policy wizard.

- Click **Create Data Transformation Rule**. The Create Data Transformation Rule dialog box is displayed.
- (Optional) Select a **Resource Set**.

- Click **Select** next to the Resource Set field. The list of available resource sets is displayed.

Optionally, you can add a new resource set by clicking **Create Resource Set**. The newly created resource set will appear in the resource sets list.

- Select a resource set.
- Click **Select**. The selected resource set appears in the Resource Set field.

- Select the **Transformation Key Name**. This is a mandatory field.

- Click **Select** next to the Transformation Key Name field. The Select Key dialog box shows the list of available keys. Optionally, you can create a new CBC, CBC-CS1, or XTS key on this dialog box.

To create a new key

- a. Click **Create a New Key**. The **Key created will be AES 256** section is displayed on the dialog box below.
- b. Specify an optional **Name** for the key.
- c. Select the **Encryption Mode**. The encryption mode can be CBC, CBC-CS1, or XTS. The default mode is CBC.
- d. (Optional, not applicable to COS and CTE for Kubernetes policies) Select **Unique to Client** to make the key a unique to client key.
- e. Click **Create**. The newly created key appears in the keys list.

If you selected the **Unique to Client** check box when creating the key, you will see a check mark for the key under the Unique to Client column. This indicates the key is a unique to client key. Refer to [Unique to Client Keys](#) for details.

Alternatively, encryption keys for CTE can be created on the **Keys** page of the CipherTrust Manager GUI. Refer to [Creating a New Key](#) for details.

Note

When creating the XTS keys using the CipherTrust Manager CLI or the API:

- Set the `xts` flag to `true`.
- Set the key as exportable, that is, set `unexportable` to `false`.
- Share the key with the CTE Users group with the `read_key` and `export_key` permissions.

Refer to the following sample for creating an XTS key:

```
{
  "name": "CTE-XTS-Key",
  "algorithm": "aes",
  "size": 256,
  "undeletable": true,
  "unexportable": false,
  "meta": {
    "ownerId": "local|59ba6797-e5a6-4427-b11c-a5534b5a975e",
    "permissions": {
      "ExportKey": [
        "CTE Clients"
      ],
    },
  },
}
```

```

    "ReadKey": [
      "CTE Clients"
    ],
  },
  "cte": {
    "persistent_on_client": true,
    "encryption_mode": "XTS",
    "cte_versioned": false
  },
  "xts": true,
  "id": "95cc7868-89bf-492b-b868-bbb884a9b379"
}

```

Note

When an XTS key is created, an additional tweak key (<key-name>_xts) is generated with the original key. Make sure that both the original and the tweak keys are part of the CTE Users group with the read key (read_key) and export key (export_key) permissions.

- b. Select the desired key.
- c. Click **Select**. The selected key appears in the Transformation Key field.
4. Click **Add**. The newly created data transformation rule appears in the list of rules.

Similarly, you can add multiple rules to the policy by clicking **Create Data Transformation Rule**. To delete a rule, click **Delete** next to the rule.

5. Click **Next**. The Confirmation screen is displayed.

Step 5: Add Signature Rules

This step is applicable to *CTE for Kubernetes* policies.

A signature rule is a type of signature sets that contains container image signatures. Signature rules can only be associated with CTE for Kubernetes policies.

1. Click **Add Signature Rule**. The Add Signature Rule dialog box is displayed. The list of available signature rules is displayed.
2. Select the desired signature rules.

Note

Ensure that you have already created a [signature set for container images](#).

- Click **Add**. The newly added rule appears in the list of signature sets on the Signature Rules tab.

Similarly, you can add more rules to the policy by clicking **Add Signature Rule**. To delete a rule, click **Remove** next to the rule.

- Click **Next**. The Confirmation screen is displayed.

Step 6: Confirm Details

- Verify the policy details. The Confirmation screen displays general information about the policy and details of the rules added to the policy.

If the details are incorrect or you want to modify them, click **Back** and update the details.

- Click **Save**.

The newly created policy appears in the policies list on the Policies page. Similarly, add as many policies as required. A sample list of policies is shown below:

	Name	Type		Version	Updated At ↓	Description	Learn Mode	
☐	test-k8s-plc	CTE for Kubernetes		0	20 Jun 2022, 10:17	Test K8s policy		...
☐	test-idt-plc	In-place Data Transformation		1	14 Mar 2022, 12:02	Test IDT policy	N/A	...
☐	testpolicy	Standard		1	14 Mar 2022, 12:02	Test standard...		...
☐	ldtplc	Live Data Transformation		1	14 Mar 2022, 12:01	Test LDT policy		...
☐	testcosplc	Cloud Object Storage		1	14 Mar 2022, 12:01	Test COS policy		...

Creating a New Key

When creating a key rule for a policy, you can either select an existing key or create a new key. The list of available keys is displayed on the Select Key dialog box. The new keys that you create on this dialog box appear under the keys list.

Alternatively, encryption keys for CTE can be created on the **Keys** page of the CipherTrust Manager GUI, as described below. However, XTS keys must be created on the Select Key dialog box only.

Note

The CTE keys must be:

- AES-128, AES-256, ARIA-128, or ARIA-256
- Shared with the CTE Clients group
- Set as exportable

Only the clients that support the CBC CS1 encryption mode can have GuardPoints that use a policy with a CBC CS1 key.

To create a new key:

1. In the top left corner, click the App Switcher icon. The Products page is displayed.
2. In the left pane, click **Keys**. The Keys page is displayed.
3. Click **Add Key**.
4. Specify the **Key Name**.
5. Select the **Algorithm** from the drop-down list. The default algorithm is **AES**. CTE supports **AES** and **ARIA** algorithms.
6. Select the key **Size** from the drop-down list. The default size is **256**.
7. (Optional) Under **Key Properties**, select **XTS/CBC CS1** if you want to create a key for enhanced encryption mode.
8. (Optional) Under **CTE Property**, select **Unique to Client** if you want to create a unique to client key. Refer to [Unique to Client Keys](#) for details on these keys.
9. Click **Add Key** to create the key. The edit view of the key is displayed.

For an enhanced encryption key, a set of two keys is created with names **<key - name>** and **<key - name>_xts**.

10. In the mini detail view, turn on the **Exportable** toggle. This makes sure the key is displayed in the keys list when you add the key rule to the policy.
11. Specify whether the key can be deleted. To make the key deletable, turn on the **Deletable** toggle. By default, the **Deletable** toggle is turned off, that is, the key cannot be deleted.

Owner	local admin	Object Type	Symmetric Key
Created	06 Mar 2021, 22:39	Algorithm	AES
Last Modified	06 Mar 2021, 23:03	Size	256
Exportable	☒	Deletable	☒

12. Expand the **KEY ACCESS** section.

13. On the General tab:

- Make sure that the **Show All Groups** toggle is enabled. It displays the list of available groups.
- In the **Search groups** box, type **CTE Clients** to filter the groups. The **CTE Clients** group is displayed.
- Select the **All** check box. All the available permissions are selected.

KEY ACCESS

General NAE

Key Owner

Search groups: CTE Clients

1 Result | 1 group

Group	Read	Use	Decrypt	Encrypt	Sign	Verify	Export	All
CTE Clients	☒	☒	☒	☒	☒	☒	☒	☒

Show All Groups ☒

1 group 5 per page

d. Click **Update**.

14. Click the **CTE** tab. You need to scroll down the page.

15. Specify the CTE key properties (metadata):

Note

You must be a member of **both** the **CTE Admins** and **Key Admins** groups to update the CTE key

properties.

Refer to [create users](#) and [assign groups](#) to them.

- **CTE Versioned:** Specify whether the key is versioned.
 - For Standard, COS, and IDT policies, clear the **CTE Versioned** check box. This makes sure that the key is displayed in the keys list when you add the key rule to the policy.
 - For LDT policies, make sure that the **CTE Versioned** check box is selected.
- **Unique to Client:** (Read only) Specifies whether the key is a unique to client key. This field is non-editable and its state (selected or clear) depends on how you configured the **Unique to Client** check box under **CTE Property** when creating the key.
- **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.
 - When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client. This can be used in the event that a connection to the CipherTrust Manager is unreliable.

Note

For a unique to client key, the **Persistent on Client** check box is selected automatically and is non-editable.

- When the check box is left clear, the key is only stored on disk inside the CipherTrust Manager. When required, the key is downloaded to the CTE client but only cached in memory. Every time the key is needed, the client retrieves it from the CipherTrust Manager.
- **Encryption Mode:** Encryption mode of the key. The options are:
 - **CBC CS1**
 - **XTS**
 - **CBC**

Note

- For ARIA-128 and ARIA-256 keys, select **CBC** as the encryption mode. These keys don't support the **CBC CS1** encryption mode.
- For CTE for Kubernetes policies, select **CBC CS1**. These policies do not support XTS keys.
- If you selected the **XTS/CBC CS1** check box when creating the key, you must select either **CBC CS1** or XTS as the encryption mode. Encryption using the XTS and **CBC CS1** keys is known as *enhanced encryption*. Refer to [Enhanced Encryption Mode](#) for details.

If you left the **XTS/CBC CS1** check box clear when creating the key, **CBC** is the available encryption mode.

Properties of a sample CTE key are shown below:

KMIP
NAE
CTE
Meta

 **CTE PROPERTIES**

☒ CTE Versioned
☐ Unique to Client
☒ Persistent on Client

Encryption Mode

CBC CS1 ▼

Note

To set Group Permissions for accessing this key, specify the settings on the General tab under the KEY ACCESS section.

16. Click **Update**.

The key is updated for use with CTE.

Note

- Only CTE Administrators (users of the **CTE Admins** group) can delete the CTE keys.
- An in-use CTE key cannot be deleted. Before you delete a CTE key, make sure that no key rule is using the key.

Modifying Policies and Rules

On the Policies page, you can view details of policies, update their description, and delete that policies that are no longer needed. Additionally, you can modify the key and security rules linked to the policy.

Note

Any updates to a policy will be applied without confirmation if the policy is not in use by any Enabled/Active GuardPoints.

Displaying Policies

The Policies page shows the list of configured policies with their details such as names, types, and versions. You can view the version history of policies from the Policies page. Additionally, you can delete policies from this page. In the detail view, you can view types of rules linked with the policies.

Additionally, the Policies page shows a warning banner at the top with the number of policies that have Learn Mode enabled for more than 3 days.

	Name	Type		Version	Updated At ↓	Description	Learn Mode	⚙
☐	test-k8s-plc	CTE for Kubernetes		0	20 Jun 2022, 10:17	Test K8s policy	☐	...
☐	test-idt-plc	In-place Data Transformation		1	14 Mar 2022, 12:02	Test IDT policy	N/A	...
☐	testpolicy	Standard		1	14 Mar 2022, 12:02	Test standard...	☐	...
☐	ldt-plc	Live Data Transformation		1	14 Mar 2022, 12:01	Test LDT policy	☐	...
☐	testcos-plc	Cloud Object Storage		1	14 Mar 2022, 12:01	Test COS policy	☐	...

This section covers the following information:

- Viewing Policies

- Viewing Details of Policies
- Viewing Policy Version History
- Controlling Updates to Policies
- Updating Policy Description
- Cloning a Policy
- Adding New Security Rules
- Adding New Key Rules
- Adding New Data Transformation Rules
- Adding New Signature Rules
- Modifying Security Rules
- Modifying Key Rules
- Modifying Data Transformation Rules
- Modifying Signature Rules
- Automatic Addition/Removal of ApplyKey Effect for All Security Rules
- Exporting Policies
- Deleting Policies

Viewing Policies

To view the complete list of configured policies:

1. Open the **Transparent Encryption** application.
2. Click **Policies**. The Policies page shows the following details:

Column	Description
Name	Unique name of the policy.
Type	Type of the policy can be: • Standard • Live Data Transformation • Cloud Object Storage • In-place Data Transformation • CTE for Kubernetes

Column	Description
Version	Version of the policy. Click to view the version history of the policy. Refer to Viewing Policy Version History for details.
Updated At	Time when the policy is created or updated.
Description	Optional description of the policy.
Learn Mode	Whether Learn Mode is turned on for the policy. Use the toggle to turn on/off Learn Mode for the policy. Turning Learn Mode on/off automatically inserts/removes the ApplyKey effect for all security rules having the Deny effect. Refer to Automatic Insertion/Removal of ApplyKey Effect for All Security Rules for details. Turn off Learn Mode for the policy for which you have analyzed the valid processes and users.
Restrict Update	Whether the updates to the policy are restricted. Use the toggle to restrict or allow updates to the policy. Turning on the toggle restricts updates to the policy, which can be useful when the policy is in use by GuardPoints. However, turning off the toggle allows updates to the policy. Refer to Controlling Updates to Policies .

The **Restrict Update** column is hidden by default. To show/hide a column, click the custom view icon (⚙️), select/clear the desired column, and click **OK**.

By default, the policies are displayed in descending order by Updated At. By default, 10 records per page are displayed. Adjust pagination and/or the number of records to display per page to view more records.

To add a new policy, click Create Policy. Refer to [Creating Policies](#) for details.

Viewing Details of Policies

The detail view of a policy shows the security rules, key rules, and data transformation rules, as appropriate. The Restrict Update and Learn Mode toggles are also provided. Use these toggles to turn on or off learn mode and updates to the policy.

To view the details of a policy:

1. Open the **Transparent Encryption** application.
2. Click **Policies**. The list of configured policies is displayed.
3. Under **Name**, click the desired policy. The edit view of the policy is displayed. The rules linked with the policy are displayed on the following tabs:

- Security Rules
- Key Rules
- Data Transformation Rules (Applicable to policies that contain data transformation rules)
- Signature Rules (Applicable to CTE for Kubernetes policies)

Note

If a policy is in Learn Mode, a warning banner stating the following is displayed at the top of the page:

Warning: This Policy is in Learn Mode

To disable Learn Mode, turn off the **Learn Mode** toggle on the right.

If the Restrict Update toggle is turned on, updates to a policy that is in use by active GuardPoints are restricted. Security rules and key rules linked with the policy cannot be changed.

4. Click the **Security Rules** tab. This tab displays the following details:

Column	Description
Order	Sequence to enforce security rules. Rules higher in the order take higher priority. Click to edit the rule.
Resource Set	(Not applicable to Cloud Object Storage policies) Resource set linked with the rule. Click the link to edit the resource set.
User Set	User set linked with the rule. To modify an existing user set, click the desired user set link, modify the Description , and click Apply . The edit view also provides the Browse users and Manually add user buttons to add new users to the set.
Process Set	Process set linked with the rule. To modify an existing process set, click the desired process set link, modify the Description , and click Apply . The edit view also provides the Add Process button to add new processes to the set.
Action	Action applied to the rule. Refer to Actions for the complete list of supported actions.
Effect	Effect applied to the rule.

Column	Description
Browsing	Whether browsing of directories under the GuardPoint down to the resources in the rule is allowed. For Cloud Object Storage policies, No is displayed.

To add a new security rule, refer to [Step 2: Add Security Rules](#) for details.

- Click the **Key Rules** tab. This tab displays the following details:

Standard Policies

Column	Description
Order	Sequence to enforce key rules. Rules higher in the order take higher priority. Click to edit the rule.
Resource Set	Resource set linked with the key rule.
Key Name / Current Key Name	Encryption key currently applied to the resource. For Data Transformation policies, the name is Current Key Name .

Live Data Transformation Policies

Column	Description
Order	Sequence to enforce key rules. Rules higher in the order take higher priority. Click to edit the rule.
Resource Set	Resource set linked with the key rule. Click the link to edit the resource set.
Current Key Name	Encryption key currently applied to the resource.
Transformation Key Name	Encryption key to perform data transformation for LDT policies.
Exclusion Rule	Whether to exclude the resource set from the policy.

Cloud Object Storage Policies

Column	Description
Key Name	Name of the key.

In-place Data Transformation Policies

Column	Description
Current Key	Name of the current encryption key.
Transformation Key	Encryption key to perform data transformation for IDT policies.

CTE for Kubernetes Policies

Column	Description
Order	Sequence to enforce key rules. Rules higher in the order take higher priority. Click to edit the rule.
Resource Set	Resource set linked with the key rule. Click the link to edit the resource set.
Key Name	Encryption key currently applied to the resource.

To add a new key rule, refer to [Step 3: Add Key Rules](#) for details.

- Click the **Data Transformation Rules** tab. This tab is displayed if the policy contains data transformation rules. This tab displays the following details:

Column	Description
Order	Sequence to enforce key rules. Rules higher in the order take higher priority. Click to edit the rule.
Resource Set	Resource linked with the key rule. Click the link to edit the resource set.
Transformation Key Name	Transformation key to use for rekeying.

To add a new data transformation rule, refer to [Step 4: Add Data Transformation Rules](#) for details.

- Click the **Signature Rules** tab. This tab is displayed for CTE for Kubernetes policies. This tab displays the following details:

Column	Description
Signature Set Name	Name of the linked signature set (signature rule).
Created At	Time when the signature rule is created.

To add a new signature rule, refer to [Step 5: Add Signature Rules](#) for details.

Viewing Policy Version History

Viewing Policy Version History

The policy version defines the number of times a policy has been changed. This number indicates the current revision only. It cannot be used to roll back to a previous version. Restore a backup to revert to a previous online policy version. The version count starts at zero when the policy is initially created and increments by one each time it is saved thereafter.

Policy Version History

Version	Date	Author	Comment
4	01/05/21	admin	Delete LDT Key Rule
2	01/04/21	admin	LDT Key Rule Created
2	01/04/21	admin	DataXform Rule Created
1	01/04/21	admin	Key Rule Created
0	01/04/21	admin	Policy Created
0	01/04/21	admin	LDT Key Rule Created
0	01/04/21	admin	DataXform Rule Created
0	01/04/21	admin	Key Rule Created
0	01/04/21	admin	Security Rule Created

9 Policy Audit Records 10 per page ▾

To view the version history of a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the version number of the policy. The Policy Version History popup displays the following details:

Field	Description
Version	Version of the policy.
Date	Date when the version is created.
Author	User who changed the policy.
Comment	Description of change.

4. Click **OK**.

Controlling Updates to Policies

CTE provides options to restrict or allow changes to a policy that is in use by active GuardPoints. When updates are restricted, security rules and key rules linked with the policy cannot be changed.

To restrict or allow changes to a policy:

1. Open the **Transparent Encryption** application.
2. Click **Policies**. The list of configured policies is displayed.
3. Under **Name**, click the desired policy. The edit view of the policy is displayed.
4. Turn on/off the **Restrict Update** toggle.

Note

Before turning on the Restrict Update, ensure that the active GuardPoints are disabled.

Turning on the toggle restricts updates to the policy. Any attempts to change the policy will result in an error. Turning off the Restrict Update toggle allows updates to the policy.

Updating Policy Description

To update the description of a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the overflow icon () corresponding to the desired policy.
4. Click **Edit**.
5. Add or modify the **Description**. The policy **Name** and **Type** cannot be modified.
6. Click **Update**.

The updated description appears in the policies list.

Cloning a Policy

Cloning is an efficient and simple method to create a copy of an existing policy. The clone is a separate policy and contains all the configurations of its parent policy. When cloning a policy, specify a new unique name for the clone. Also, enable or disable Learn Mode and Restrict Update for the clone, if required.

To duplicate a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the overflow icon (**⋮**) corresponding to the desired policy.

Name	Type	Version	Updated At	Description	Learn Mode	
☐ Idtplc	Live Data Transformation	0	10 Nov 2021, 12:11		☐	⋮

1 Policy

Edit
 Clone
 Delete

4. Click **Clone**.
5. Enter a unique **Name** for the clone.
6. (Optional) Provide a **Description** for the clone.
7. (Optional) Turn on/off the **Learn Mode** toggle. Refer to [Learn Mode](#) for details.

Cloning policy Idtplc

Name *

clone-plc

Description

A copy of Idtplc

Learn Mode:



Restrict update:



8. (Optional) Turn on/off the **Restrict Update** toggle. Refer to [Controlling Updates to Policies](#) for details.

The clone with the specified name appears at the top of the policies list.

Name	Type	Version	Updated At	Description	Learn Mode	
☐ clone-plc	Live Data Transformation	0	10 Nov 2021, 15:39	A copy of Idtplc	☐	⋮

Adding New Security Rules

To add a new security rule to a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. On the **Security Rules** tab, click **Add Security Rule**. The Add Security Rule dialog box is displayed.
5. Specify the required details. The fields on the Add Security Rule dialog box are same as the fields on the Create Security Rule dialog box. Refer to [Step 2: Add Security Rules](#) for details.
6. Click **Add**.

The newly added security rule appears in the security rules list. Similarly, you can add more security rules to the policy.

Adding New Key Rules

To add a new key rule to a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Key Rules** tab.
5. Click **Add Key Rule**.

An IDT policy can have only one key rule. So, the **Add Key Rule** button is not available for IDT key rules.

6. Specify the required details. The fields on the Add Key Rule dialog box are same as the fields on the Create Key Rule dialog box. Refer to [Step 3: Add Key Rules](#) for details.
7. Click **Add**.

The newly added key rule appears in the key rules list. Similarly, you can add more key rules to the policy.

Adding New Data Transformation Rules

This section is applicable to policies that contain data transformation rules.

To add a new data transformation rule to a policy:

1. Open the **Transparent Encryption** application.

-
2. In the left pane, click **Policies**.
 3. Click the desired policy.
 4. Click the **Data Transformation Rules** tab.
 5. Click **Add Data Transformation Rule**. The Add Data Transformation Rule dialog box is displayed.
 6. Specify the required details. The fields on the Add Data Transformation Rule dialog box are same as the fields on the Create Data Transformation Rule dialog box. Refer to [Step 4: Add Data Transformation Rules](#) for details.
 7. Click **Add**.

The newly added data transformation rule appears in the data transformation rules list. Similarly, you can add more rules to the policy.

Adding New Signature Rules

This section is applicable to CTE for Kubernetes policies.

A signature rule is a type of signature sets that contains container-image signatures. Signature rules can only be associated with CTE for Kubernetes policies.

To add a new signature rule to a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired CTE for Kubernetes policy.
4. Click the **Signature Rules** tab.
5. Click **Add Signature Rules**. The Add Signature Rules dialog box is displayed.
6. Select the desired signature rules.

The fields on the Add Signature Rules dialog box are same as the fields on the Add Signature Rules dialog box that appears when creating a CTE for Kubernetes policy. Refer to [Step 5: Add Signature Rules](#) for details.

The signature rules already in use by a policy are read-only, and cannot be selected.

7. Click **Add**.

The newly added signature rule appears in the signature rules list. Similarly, you can add more rules to the policy.

Modifying Security Rules

- [Editing Security Rules](#)

- Changing Order of Security Rules
- Deleting Security Rules

Editing Security Rules

To edit a security rule in a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Security Rules** tab.
5. Click the overflow icon () corresponding to the desired rule.
6. Click **Edit**. The Edit Security Rule dialog box is displayed.
7. Change the required fields. The fields on the Edit Security Rule dialog box are the same the fields on the Create Security Rule dialog box. Refer to [Step 2: Add Security Rules](#) for details.
8. Click **Update**.

The updated details appear in the security rules list.

Changing Order of Security Rules

To change the order of a security key rule in a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Security Rules** tab.
5. Select the desired rule. Depending on the current order, the following ordering icons are activated.

Icon	Description
Bottom ()	Move the rule to the bottom. Unavailable for the rule at the bottom.
Down ()	Move the rule one place lower. Unavailable for the rule at the bottom.
Up ()	Move the rule one place higher. Unavailable for the rule at the top.

Icon	Description
Top ()	Move the rule to the top. Unavailable for the rule at the top.

6. Click the desired icon.

The rules list shows the updated order.

Deleting Security Rules

To delete security rules from a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Security Rules** tab.
5. Select the check boxes corresponding to the desired rules.

To select all rules visible on the page for deletion, select the top check box to the left of the Order heading.

6. Click the delete icon ().

The selected rules are removed from the security rules list.

Modifying Key Rules

Modifying key rules linked with a policy involves:

- [Editing Key Rules](#)
- [Changing Order of Key Rules](#)
- [Deleting Key Rules](#)

Editing Key Rules

To edit a key rule in a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Key Rules** tab.

5. Click the overflow icon () corresponding to the desired rule.
6. Click **Edit**. The Edit Key Rule dialog box is displayed.
7. Change the required fields. The fields on the Edit Key Rule dialog box are the same the fields on the Create Key Rule dialog box. Refer to [Step 3: Add Key Rules](#) for details.
8. Click **Update**.

The updated details appear in the key rules list.

Changing Order of Key Rules

To change the order of a key rule in a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Key Rules** tab.
5. Select the desired rule. Depending on the current order, the following ordering icons are activated.

Icon	Description
Bottom ()	Move the rule to the bottom. Unavailable for the rule at the bottom.
Down ()	Move the rule one place lower. Unavailable for the rule at the bottom.
Up ()	Move the rule one place higher. Unavailable for the rule at the top.
Top ()	Move the rule to the top. Unavailable for the rule at the top.

6. Click the desired icon.

The key rules list shows the updated order.

Deleting Key Rules

To delete key rules from a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.

- Click the desired policy.

Note

The key rule linked with an IDT policy cannot be deleted from the CipherTrust Manager. However, you can update the key rule when required (refer to [Editing Key Rules](#)).

- Click the **Key Rules** tab.
- Select the check boxes corresponding to the desired rules.

To select all rules visible on the page for deletion, select the top check box to the left of the Order heading.

- Click the delete icon ().

The selected rules are removed from the key rules list.

Modifying Data Transformation Rules

Modifying data transformation rules linked with a policy involves:

- Editing Data Transformation Rules
- Changing Order of Data Transformation Rules
- Deleting Data Transformation Rules

Editing Data Transformation Rules

To edit a data transformation rule in a policy:

- Open the **Transparent Encryption** application.
- In the left pane, click **Policies**.
- Click the desired policy.
- Click the **Data Transformation Rules** tab.
- Click the overflow icon () corresponding to the desired rule.
- Click **Edit**. The Edit Data Transformation Rule dialog box is displayed.
- Change the required fields. The fields on the Edit Data Transformation Rule dialog box are the same the fields on the Create Data Transformation Rule dialog box. Refer to [Step 4: Add Data Transformation Rules](#) for details.

8. Click **Update**.

The updated details appear in the data transformation rules list.

Changing Order of Data Transformation Rules

To change the order of a data transformation rule in a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Data Transformation Rules** tab.
5. Select the desired rule. Depending on the current order, the following ordering icons are activated.

Icon	Description
Bottom ()	Move the rule to the bottom. Unavailable for the rule at the bottom.
Down ()	Move the rule one place lower. Unavailable for the rule at the bottom.
Up ()	Move the rule one place higher. Unavailable for the rule at the top.
Top ()	Move the rule to the top. Unavailable for the rule at the top.

6. Click the desired icon.

The rules list shows the updated order.

Deleting Data Transformation Rules

To delete data transformation rules from a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired policy.
4. Click the **Data Transformation Rules** tab.
5. Select the check boxes corresponding to the desired rules.

To select all rules visible on the page for deletion, select the top check box to the left of the Order heading.

-
6. Click the delete icon ().

The selected rules are removed from the data transformation rules list.

Modifying Signature Rules

Modifying signature rules linked with a policy involves:

- [Editing Signature Rules](#)
- [Deleting Signature Rules](#)

Editing Signature Rules

To edit a signature rule in a policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.
3. Click the desired CTE for Kubernetes policy.
4. Click the **Signature Rules** tab.
5. Click the overflow icon () corresponding to the desired rule.
6. Click **Edit**. The Edit Signature Rule dialog box is displayed.
7. Select the required signature set.

The signature sets already in use by a policy are read-only.

8. Click **Update**.

The updated details appear in the signature rules list.

Deleting Signature Rules

To delete a signature rule from a policy:

1. Open the **Transparent Encryption** application.
 2. In the left pane, click **Policies**.
 3. Click the desired policy.
 4. Click the **Signature Rules** tab.
 5. Click the overflow icon () corresponding to the desired rule.
 6. Click **Delete**. The *<signature-rule> will be deleted* dialog box is displayed.
-

7. Click **Delete**.

The rule is removed from the signature rules list.

Automatic Addition/Removal of ApplyKey Effect for All Security Rules

If you enable Learn Mode on an existing policy, the ApplyKey effect is **added** to *all* the security rules having the Deny effect in the policy. Similarly, if you disable Learn Mode on an existing policy, the ApplyKey effect is **removed** from *all* the security rules having the Deny and ApplyKey effects in the policy.

To automatic add or remove the ApplyKey effect from all security rules of a policy in one go:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies > Policies**.
3. Turn on/off the **Learn Mode** toggle corresponding to the desired policy that contains the security rules having the Deny effect.

Alternatively, click the **Name** link corresponding to the desired policy and turn on/off the **Learn Mode** toggle in the mini details view.

Note

When you enable Learn Mode for a policy, the ApplyKey effect will only be inserted if the policy contains at least one key rule.

Refer to [Learn Mode](#) for details.

Exporting Policies

CipherTrust Manager provides options to back up CTE policies and restore them to other CipherTrust Manager appliances. Refer to [Backup and Restore](#) for details.

Deleting Policies

CipherTrust Manager provides options to delete single or multiple policies.

Deleting Single Policy

To delete a single policy:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Policies**.

- Click the overflow icon () corresponding to the desired policy.
- Click **Delete**.

The selected policy is removed from the policies list.

Deleting Multiple Policies

To delete single or multiple policies:

- Open the **Transparent Encryption** application.
- In the left pane, click **Policies**.
- Select the check boxes corresponding to the desired policies.

To select all policies visible on the page for deletion, select the top check box corresponding to the left of the Name heading.

- Click the delete icon ().

The selected policies are removed from the policies list.

Managing FAM Policies and Rules

The primary job of a DSF Hub user is to create policies that protect data. Policies govern access to the files in GuardPoints. FAM policies allow you to manage the FAM audit rules.

Viewing FAM Policies

The FAM Policies page shows the list of configured FAM policies with their details such as names, versions, and descriptions.

To view the complete list of configured FAM policies:

- Open the **Transparent Encryption** application.
- Click **Policies**. The Policies page is displayed
- Click the **FAM Policies** tab. The FAM Policies tab provides the list of added FAM policies. The tab displays the following details:

Column	Description
Name	Unique name of the FAM policy.
Version	Version of the FAM policy. Click to view the version history of the FAM policy.
Created At	The time when the FAM policy is created.

Column	Description
Updated At	The time when the FAM policy is updated.
Description (Optional)	Description of the FAM policy.

By default, the FAM policies are displayed in descending order by Updated At. By default, 10 records per page are displayed. Adjust pagination and/or the number of records to display per page to view more records.

Managing GuardPoints

A GuardPoint specifies the list of folders that contain paths to be protected. Access to files and encryption of files under the GuardPoint is controlled by security policies.

Before you apply GuardPoints:

- A CTE Agent must be installed on the client system and registered with CipherTrust Manager. Refer to the [CTE Agent Quick Start Guide](#) specific to your platform for details.
- A client must be added to the CipherTrust Manager. The client is automatically added to the CipherTrust Manager on successful registration with the CipherTrust Manager.
- Policies must be created using the encryption keys on the CipherTrust Manager. This involves creation of policy elements and encryption keys. Refer to [Managing Policies](#) for details.
- A GuardPoint must be created. No one must be using the directory to be guarded before making it a GuardPoint.

If users are working on the directory when it is made a GuardPoint, they can continue to use data in memory rather than use the actual data in the GuardPoint. Inform users to:

- Save their work
- Close applications that are running on the directory
- Exit the directory before applying the GuardPoint

When the users re-enter the directory, they will use protected data and the CTE Agent will work appropriately.

Related Topics

- [Secure Start GuardPoints](#)
- [Considerations Before Creating GuardPoints](#)
- [Creating GuardPoints](#)
- [Enabling Secure Start for GuardPoints](#)
- [Protecting Teradata Appliances](#)

-
- Automatic and Manual GuardPoints
 - Viewing GuardPoints
 - Viewing GuardPoint Status
 - Changing SMB Connection
 - Removing GuardPoints
 - Disabling GuardPoints
 - Enabling GuardPoints
 - Enabling and Disabling MFA on GuardPoints

Secure Start GuardPoints

Note

The Secure Start feature is supported on Windows clients.

Secure Start offers a new type of GuardPoint that offers data protection for applications that start earlier in the boot sequence than VMD (CTE Agent daemon). For example, an AD (Active Directory) or a SQL Server service starts very early. A Secure Start GuardPoint starts before the AD and SQL services, and can, therefore, encrypt those services.

For more information on protecting such applications using Secure Start, refer to the [CTE Agent for Windows Advanced Configuration and Integration Guide](#). To determine whether other applications qualify for Secure Start, contact Thales Customer Support.

Considerations Before Creating GuardPoints

Before creating GuardPoints, consider the following:

- If a client is to be added to a client group, do not apply a GuardPoint at the client level. Rather, apply the GuardPoint at the client group level. You can do both, but it is harder to keep track of GuardPoints applied at the client group level and custom GuardPoints applied at the client level.
- Certain directories are protected against guarding. So plan your GuardPoints accordingly:

Linux Platforms

- The following directories cannot be guarded:
 - `<secfs install root>/agent/secfs/`
 - `<install root>/agent/secfs/bin` and everything under it

-
- `<secfs install root>/agent/vmd` and everything under it
 - `/etc/vormetric` and everything under it
 - `/etc`
 - `/etc/pam.d` and everything under it
 - `/etc/security` and everything under it
 - `/usr`
 - `/usr/lib`
 - `/usr/lib/pam`
 - `/usr/lib/security` and everything under it
 - `/etc/rc*` and everything under it
 - `/var/log/vormetric`
 - You cannot apply CTE Agent protection to already mounted and guarded directories, nor can you nest GuardPoints.
 - The `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec` directory is automatically mounted and guarded by `secfs` when the CTE Agent process starts on the client.
 - You cannot apply a GuardPoint to `/opt` because it contains the existing GuardPoint, `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec`; however, you can guard a directory like `/opt/myapps` because it is in a different hierarchy and has no impact on `/opt/vormetric`.
 - Mounted and guarded directories can be displayed using the `df` command.

Windows Platforms

- Be careful when specifying paths for Windows agents. Cross-guarding the same folder with different policies and encryption keys returns unexpected results and corrupts the files in that folder.
- GuardPoint paths must use standard Windows path notation and delimiters.
 - Incorrect notation and delimiters are ignored and discarded by the Windows agent. Therefore, it is possible to enter two paths that resolve to the same Windows folder and successfully guard both of them. The CipherTrust Manager reports that it is guarding two unique folders when, in fact, it is guarding the same folder twice.
 - Do not use any of the following characters as path delimiters: `| ? < > : * " / ,`

For example, both `C:\gp\` and `C:\gp/` are allowed by the CipherTrust Manager. When the second

GuardPoint is applied, the extraneous / is discarded by the Windows CTE Agent and the Windows CTE Agent applies a GuardPoint to C:\gp\ a second time.

- Both CipherTrust Manager and CTE support a new enhanced encryption mode (CBC-CS1). If your client groups contain clients with older versions of CTE, you cannot apply policies containing keys that use this new encryption mode. The action fails with an error message informing you that all clients in the client group do not support the key's encryption mode. Refer to the [CTE Agent Advanced Configuration and Integration Guide](#) specific to your platform for details.

When Changing a Policy or Rekeying a GuardPoint

- To change a policy or rekey a GuardPoint, be prepared to temporarily stop access to the GuardPoint. Changing policies for a GuardPoint requires an interruption of service because the transition process entails disabling one policy and then enabling another policy. The GuardPoint must be inactive during the transition period to ensure GuardPoint integrity. The same rule applies to moving a client between client groups when it includes a change in policies. Coordinate policy changes during a maintenance outage window.
- If LDT is enabled on your clients, encryption and rekeying of GuardPoint data is done without blocking user or application access to the data. LDT is a separately licensed feature, refer to [Enabling Live Data Transformation](#).

Creating GuardPoints

A GuardPoint is created to enforce protection on a GuardPath according to linked security policy. This is also called guarding a path. For a Ransomware protection GuardPoint, a policy is not required.

Refer to the following sections for information on creating different types of GuardPoints:

- [Creating Standard GuardPoints](#)
- [Creating LDT GuardPoints](#)
- [Creating Cloud Object Storage GuardPoints](#)
- [Creating IDT GuardPoints](#)
- [Creating Ransomware GuardPoints](#)

Creating Standard GuardPoints

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

Creating Standard GuardPoints on Local Paths

To create a GuardPoint:

1. Open the **Transparent Encryption** application.
-

2. Select the client or client group on which you want to create a GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click **Create GuardPoint**.
4. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field.
 - b. Select a *Standard* policy. If no policy exists, create one, as described in [Creating Policies](#).

Name	Type	Version
☐ testcosplc	Cloud Object Storage	0
☒ testpolicy	Standard	1
☐ idtvlc	Live Data Transformation	0
☐ test-jdt-plc	In-place Data Transformation	0

- c. Click **Select**.
5. Select the **Type** of device to protect. This is a mandatory field. Depending on the platform, the options for a *Standard* policy are:

Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system directories to be guarded manually.
Auto Raw or Block Device	Yes	Yes	Select for standard policies for raw (block) devices.
Manual Raw or Block Device	No	Yes	Select for standard policies for raw (block) devices to be guarded manually.

Note

Manual Directory and Manual Raw or Block Device are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd -unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

Note**Access Rules to Apply for Raw/Block Devices**

When creating a GuardPoint on a raw/block device, ensure that the policy contains a signature set for the following system processes that require access to the guarded devices:

```
/usr/lib/systemd/systemd-udev
/sbin/dmsetup
```

Adjust the above paths as per their location on the file server. On newer systems (for example, RHEL 9.4, SLES 15SP6, and Ubuntu 22.04), include the following paths.

```
/usr/bin/udevadm
/usr/sbin/dmsetup
```

Failure to include the above two processes in the policy might cause the GuardPoint creation to fail with the error `Does not exist`.

6. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:

- **Enter/Browse Path:** Select this option, and enter the GuardPoint paths by either typing or clicking the **Browse** button.

Note

A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

Browse Method

- a. Click **Browse** to select a path by browsing the client file system. This method prevents typographical

errors and verifies client availability. This is the recommended method to specify individual paths.

File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

- b. In the **Search Local Path** field, specify a starting path and click **Refresh** or select from the on-screen file system browser.
- c. Click **Add**.

Note

If the paths are already guarded, you'll see an active GuardPoint icon before them.

Manual Method

Alternatively, if you know the path, manually enter full paths of one or more directories in the given text box. Enter one path per line.

- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more directories. This is the recommended method to specify a large number of paths in one step.

Note

- If a manually entered path does not yet exist, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.
- See [Considerations Before Creating GuardPoints](#) for what to be aware of before creating a GuardPoint.
- If multiple paths are specified, they will all be protected by the same policy.
- A maximum of 1000 GuardPaths per CSV file can be uploaded.
- The following paths are restricted.

Linux: /proc, /usr/bin, /usr/sbin, /sbin, /bin, /opt/vormetric or install directory, /usr, /opt, /tmp, /var/log/vormetric, /lib64, /lib, /proc/*, /usr/bin/*, /usr/lib, /usr/lib/pam, /usr/lib/security, /usr/lib/security/*, /usr/sbin/*, /etc/, /sbin/*, /bin/*, /opt/vormetric/*, /etc/init.d/secfs, /etc/pam.d, /etc/pam.d/*, /etc/rc, /etc/security, /etc/security/*, /etc/ssh/ssh_config, /etc/ssh/sshr, /etc/systemd, /lib/systemd, and /usr/lib/systemd.

Windows: A few folders are restricted in the boot drive. If C:\ is the boot drive, the restricted folders are C:\Windows, C:\Program Files, C:\ProgramData, C:\User, C:\Users, C:\Program Files (x86), and C:\Documents And Settings.

7. (Optional, Linux only) Select **Auto Mount** to specify an automount path. For a regular (non-auto) mount path, make sure that the check box is clear.

Create GuardPoint



Policy: *

testpolicy

Select

Type: *

Auto Directory

Path: *

☒ Enter/Browse Path ☐ Upload CSV

/opt/cte-test/

Browse

i To apply the same GuardPoint settings to multiple paths, type paths in the Path field or specify them using the Browse button. A maximum of 200 GuardPaths can be specified.

Auto Mount: ☒

8. (Optional, Windows only) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in [Enabling Secure Start for GuardPoints](#).

9. (Optional) Select **Multifactor Authentication**. Refer to [Multifactor Authentication](#) for details.

10. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to [GuardPoint Status Information](#) for details.

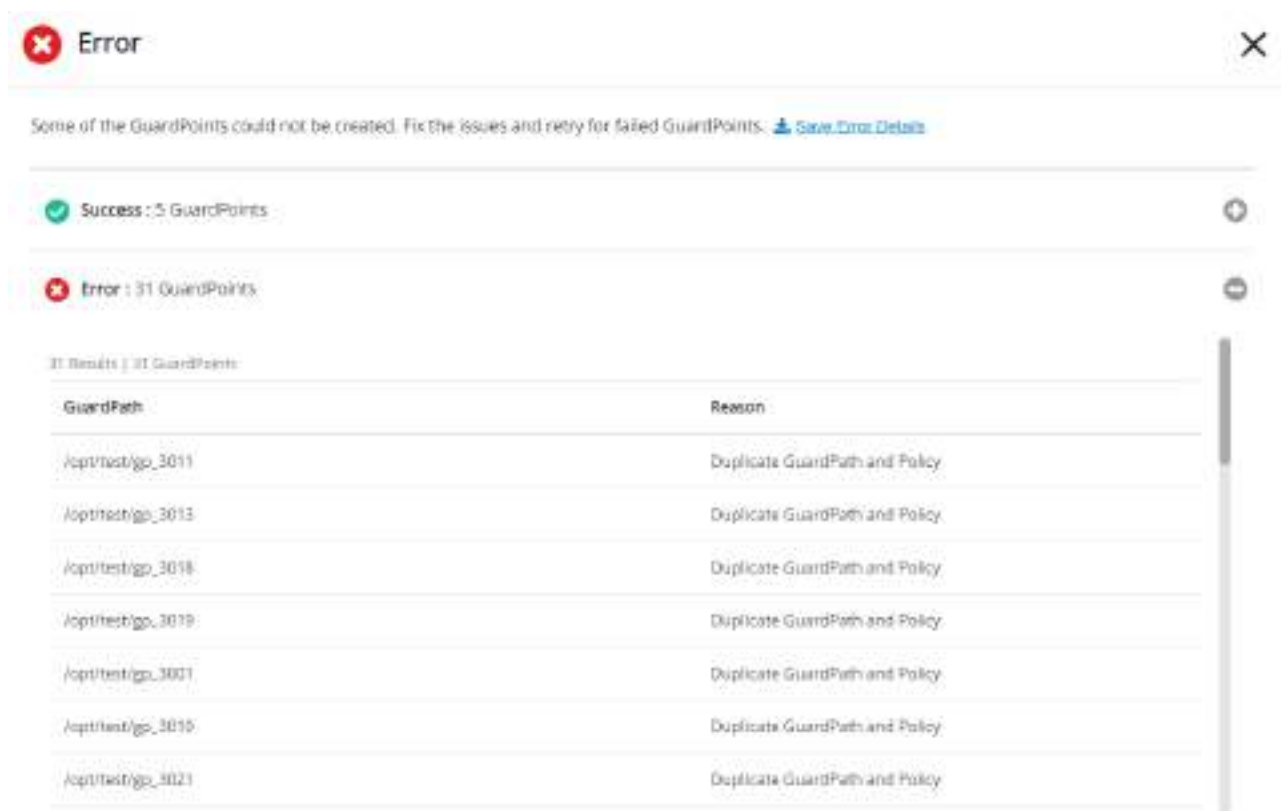
The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon () to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to [Viewing GuardPoint Status](#) for details.

GuardPoint Status Information

- When you add multiple paths to a GuardPoint:
 - If the GuardPoint is created successfully for all paths, a message is displayed at the top right corner of the screen.
 - If the GuardPoint creation failed for all paths, an error message is displayed stating that none of the GuardPoints could be created. Fix the issues and retry for failed GuardPoints.
 - If the GuardPoint is disabled or failed for at least one of the paths (for example, when a path is already guarded), an error message is displayed stating that some of the GuardPoints could not be created. Fix the issues and retry for failed GuardPoints.

The message shows the number of created and failed GuardPoints. The list of failed GuardPaths with their respective failure reasons is also displayed.



Error

Some of the GuardPoints could not be created. Fix the issues and retry for failed GuardPoints. [Save Error Details](#)

Success : 5 GuardPoints

Error : 31 GuardPoints

31 Results | 31 GuardPoints

GuardPath	Reason
/opt/test/gp_3011	Duplicate GuardPath and Policy
/opt/test/gp_3013	Duplicate GuardPath and Policy
/opt/test/gp_3018	Duplicate GuardPath and Policy
/opt/test/gp_3019	Duplicate GuardPath and Policy
/opt/test/gp_3021	Duplicate GuardPath and Policy
/opt/test/gp_3025	Duplicate GuardPath and Policy
/opt/test/gp_3027	Duplicate GuardPath and Policy

To download the CSV file with the list of failed GuardPoints, click the **Save Error Details** link at the top of the error message.

- When you add only one path, and the GuardPoint for that path fails, then an error message is displayed stating the reason of failure.

Refer to [Creating Standard GuardPoints on Network Paths](#) for information on creating Standard GuardPoints on network paths.

Creating Standard GuardPoints on Network Paths

To create a GuardPoint:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of registered clients is displayed.
3. Under **Client Name**, click the client on which you want to create a GuardPoint.
4. On the **GuardPoints** tab, click **Create GuardPoint**.
5. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field.
 - b. Select a *Standard* policy. If no policy exists, create one, as described in [Creating Policies](#).

	Name	Type	Version
☐	testcospic	Cloud Object Storage	0
☒	testpolicy	Standard	1
☐	ldtpic	Live Data Transformation	0
☐	test-jdt-pic	In-place Data Transformation	0

- c. Click **Select**.
6. Select the **Type** of device to protect. This is a mandatory field. Depending on the platform, the options for a *Standard* policy are:

Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system

Type	Windows	Linux	Description
			directories to be guarded manually.
Auto Raw or Block Device	Yes	Yes	Select for standard policies for raw (block) devices.
Manual Raw or Block Device	No	Yes	Select for standard policies for raw (block) devices to be guarded manually.

Note

Manual Directory and Manual Raw or Block Device are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd -unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

7. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:

- **Enter/Browse Path:** Select this option, and enter the GuardPoint paths by either typing or clicking the **Browse** button.

Note

A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

Browse Method

- In the text box, type the Windows network share (in the format, `\\nas-machine-hostname\share` or `\\nas-machine-ip\share`).
- Click **Browse** if you want to specify a lower-level network path. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths.

File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

- Select **Network Path** as the **Path Type**.
- Specify the **User Name** and **Password** to access the desired network path on the NAS machine.

-
- e. (Optional) Specify the **Domain** where the NAS machine exists.
 - f. In the **Search Network Path** field, specify a starting path and click **Refresh** or select from the on-screen network path browser.
 - g. Click **Add**.

Manual Method

Alternatively, if you know the network path, manually enter full network paths in the given text box. Enter one path per line.

- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more directories. This is the recommended method to specify a large number of paths in one step.

Note

- If a manually entered path does not yet exist, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.
- See [Considerations Before Creating GuardPoints](#) for what to be aware of before creating a GuardPoint.
- If multiple paths are specified, they will all be protected by the same policy.
- A maximum of 1000 GuardPaths per CSV file can be uploaded.

8. (Optional, Linux only) Select **Auto Mount** to specify an automount path. For a regular (non-auto) mount path, make sure that the check box is clear.

Create GuardPoint



Policy: *

testpolicy

Select

Type: *

Auto Directory

Path: *

☒ Enter/Browse Path ☐ Upload CSV

/opt/cte-test/

Browse

i To apply the same GuardPoint settings to multiple paths, type paths in the Path field or specify them using the Browse button. A maximum of 200 GuardPaths can be specified.

Auto Mount: ☒

9. (Optional, Windows only) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in [Enabling Secure Start for GuardPoints](#).

10. (Optional, Windows only). Select **Multifactor Authentication** Refer to [Multifactor Authentication](#) for details.
11. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to [GuardPoint Status Information](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon (🔄) to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to [Viewing GuardPoint Status](#) for details.

Refer to [Creating Standard GuardPoints on Local Paths](#) for information on creating Standard GuardPoints on

local filesystem paths.

Creating LDT GuardPoints

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

Creating LDT GuardPoints on Local Paths

To create an LDT GuardPoint on a client:

1. Open the **Transparent Encryption** application.
2. Select the client or client group on which you want to create a GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click **Create GuardPoint**.
4. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field.
 - b. Select a *Live Data Transformation* policy. If no policy exists, create one, as described in [Creating Policies](#).

Name	Type	Version
☐ testcospic	Cloud Object Storage	0
☐ testpolicy	Standard	1
☒ ldtpic	Live Data Transformation	0
☐ test-jdt-plc	In-place Data Transformation	0

- c. Click **Select**.
5. Select the **Type** of device to protect. This is a mandatory field. Depending on the platform, the options for an *LDT* policy are:

Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system

Type	Windows	Linux	Description
			directories to be guarded manually.

Note

Manual Directory is guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd -unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

6. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:

- **Enter/Browse Path:** Select this option, and enter the GuardPoint paths by either typing or clicking the **Browse** button.

Note

A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

Browse Method

- Click **Browse** to select a path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths.

File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

- In the **Search Local Path** field, specify a starting path and click **Refresh** or select from the on-screen file system browser.
- Click **Add**.

Note

If the paths are already guarded, you'll see an active GuardPoint icon before them.

Manual Method

Alternatively, if you know the path, manually enter full paths of one or more directories in the given text box. Enter one path per line.

- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more directories. This is the recommended method to specify a large number of paths in one step.

Note

- If a manually entered path does not yet exist, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.
- See [Considerations Before Creating GuardPoints](#) for what to be aware of before creating a GuardPoint.
- If multiple paths are specified, they will all be protected by the same policy.
- A maximum of 1000 GuardPaths per CSV file can be uploaded.
- The following paths are restricted.

Linux: /proc, /usr/bin, /usr/sbin, /sbin, /bin, /opt/vormetric or install directory, /usr, /opt, /tmp, /var/log/vormetric, /lib64, /lib, /proc/*, /usr/bin/*, /usr/lib, /usr/lib/pam, /usr/lib/security, /usr/lib/security/*, /usr/sbin/*, /etc/, /sbin/*, /bin/*, /opt/vormetric/*, /etc/init.d/secfs, /etc/pam.d, /etc/pam.d/*, /etc/rc, /etc/security, /etc/security/*, /etc/ssh/sshd_config, /etc/ssh/sshr, /etc/systemd, /lib/systemd, and /usr/lib/systemd.

Windows: A few folders are restricted in the boot drive. If C:\ is the boot drive, the restricted folders are C:\Windows, C:\Program Files, C:\ProgramData, C:\User, C:\Users, C:\Program Files (x86), and C:\Documents And Settings.

7. Configure the **Preserve Sparse Region** toggle. The toggle is turned on by default.

Caution

If you turn off the **Preserve Sparse Region** toggle, you are prompted to confirm the action. This is an irreversible action.

Create GuardPoint



Policy: *

ldtplc

Select

Type: *

Auto Directory

Path: *

☒ Enter/Browse Path ☐ Upload CSV

/opt/cte-test/

Browse

i To apply the same GuardPoint settings to multiple paths, type paths in the Path field or specify them using the Browse button. A maximum of 200 GuardPaths can be specified.

Preserve Sparse Region: ☒

8. (Optional, Windows only) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in [Enabling Secure Start for GuardPoints](#).

9. (Optional, Windows only). Select **Multifactor Authentication** Refer to [Multifactor Authentication](#) for details.

10. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to [GuardPoint Status Information](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon (🔄) to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to [Viewing GuardPoint Status](#) for details.

An LDT GuardPoint is applied automatically according to the QoS settings configured in the linked profile. Refer

to [Creating a Profile and Setting Quality of Service Configuration](#).

Creating LDT GuardPoints on SMB/NFS Paths

You can apply LDT GuardPoints on:

- CIFS/SMB paths, for CTE Windows clients
- NFS paths, for Linux clients

Before applying LDT GuardPoints:

- Ensure that the LDT capability is enabled for the client. LDT capability can be enabled during the CTE Agent installation or later through the CipherTrust Manager console.
- Ensure that the File Header Support (FHS) capability is enabled on the Windows clients. By default, this capability is turned on when installing a compatible CTE Agent on a Windows client. Refer to the [CTE Agent Quick Start Guide](#) for details.

Note

- FHS on Windows paths and their browsing are supported CTE Agent 7.1.0.84 onward.
- A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.
- A maximum of 1000 GuardPaths per CSV file can be uploaded.

GuardPoint on a Client

To create an LDT over SMB/NFS GuardPoint on a client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the LDT client on which you want to create a GuardPoint.
4. In the **GuardPoints** tab, click **Create GuardPoint**.
5. Select a **Policy**. This is a mandatory field.
 - a. Click **Select**.
 - b. Select a *Live Data Transformation* policy. If no policy exists, create one, as described in [Creating Policies](#).

Name	Type	Version
☐ testcospic	Cloud Object Storage	0
☐ testpolicy	Standard	1
☒ idtpic	Live Data Transformation	0
☐ test-jdt-pic	In-place Data Transformation	0

c. Click **Select**.

6. Select **Auto Directory** as the **Type** of device to protect. This is a mandatory field.

7. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:

- **Enter/Browse Path:** Select this option, and enter GuardPoint paths (network paths) manually or click the **Browse** button.

Note

- Paths of only one type can be specified at once - either local or network, not a mix of both.

Browse Method

- a. In the text box, type the Windows SMB share (in the format, `\\nas-machine-hostname\share` or `\\nas-machine-ip\share`) or Linux NFS path (in the format, `/opt/nfs_shared_path1/`).

Note

Mount the Linux NFS path on the agent machine before applying guard point.

- b. Click **Browse** if you want to specify a lower-level network path. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths.

File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

- c. (Applicable only for Client Groups) Click **Select Client** to select the Windows or Linux client.
- d. Select **Network Path** as the **Path Type**.
- e. Specify the **User Name** and **Password** to access the desired network path on the NAS machine.

- f. (Optional) Specify the **Domain** where the NAS machine exists.
- g. In the **Search Network Path** field, specify a starting path and click **Refresh** or select from the on-screen network path browser.
- h. Click **Add**. The selected paths appear on the right.

Manual Method

Alternatively, if you know the network path, manually enter full network paths in the given text box. Enter one path per line.

- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more directories. This is the recommended method to specify a large number of paths in one step.

Note

- If a manually entered path doesn't exist, be sure to enter the path correctly. The CipherTrust Manager doesn't parse manually entered paths for correct syntax.
- See [Considerations Before Creating GuardPoints](#) for what to be aware of before creating a GuardPoint.
- If multiple paths are specified, they will all be protected by the same policy.

8. (Windows only) Select the desired **SMB/CIFS Connection** if the GuardPaths are on an SMB/CIFS share.

This drop-down list is displayed when you specify a Windows SMB/CIFS share in the **Path** field.

Note

An SMB/CIFS connection must already exist on the CipherTrust Manager before you can apply GuardPoints to an SMB/CIFS share. Creating an SMB/CIFS connection requires credentials to access the share. Refer to [Connection Manager](#) for details.

9. (*Applicable only for Client Groups*) Select a **Designated Primary Set** from the dropdown options. See [Adding Designated Primary Set to a Client Group](#) for creating Designated Primary Set.
10. Configure the **Preserve Sparse Region** toggle. The toggle is turned on by default.

Caution

If you turn off the **Preserve Sparse Region** toggle, you are prompted to confirm the action. This is an irreversible action.

11. (Optional) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in [Enabling Secure Start for GuardPoints](#).

12. (Optional, Windows only). Select **Multifactor Authentication** Refer to [Multifactor Authentication](#) for details.

13. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to [GuardPoint Status Information](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon () to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to [Viewing GuardPoint Status](#) for details.

An LDT GuardPoint is applied automatically according to the QoS settings configured in the linked profile. Refer to [Creating a Profile](#) and [Setting Quality of Service Configuration](#).

Refer to [Creating LDT GuardPoints on Local Paths](#) for information on creating LDT GuardPoints on local filesystem paths.

GuardPoint on a Client Group

Note

- All clients in the Client Group should be part of LDT Communication Group. See [Managing LDT Communication Groups](#) for more details.
- Clients within a Client Group should either be all Windows clients or all Linux clients.

To create an LDT over SMB/NFS GuardPoint on a client group:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Client Groups**.
3. Click the LDT client group name on which you want to create a GuardPoint.

4. In the **GuardPoints** tab, click **Create GuardPoint**.
5. Select a **Policy**. This is a mandatory field.
 - a. Click **Select**.
 - b. Select a *Live Data Transformation* policy. If no policy exists, create one, as described in [Creating Policies](#).

	Name	Type	Version
☐	testcospic	Cloud Object Storage	0
☐	testpolicy	Standard	1
☒	ldtpic	Live Data Transformation	0
☐	test-ldt-pic	In-place Data Transformation	0

- c. Click **Select**.
6. Select **Auto Directory** as the **Type** of device to protect. This is a mandatory field.
7. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:
 - **Enter/Browse Path:** Select this option, and enter GuardPoint paths (network paths) manually or click the **Browse** button.

Note

- Paths of only one type can be specified at once - either local or network, not a mix of both.

Browse Method

- a. In the text box, type the Windows SMB share (in the format, `\\nas-machine-hostname\share` or `\\nas-machine-ip\share`) or Linux NFS path (in the format, `/opt/nfs_shared_path1/`).

Note

Mount the Linux NFS path on the agent machine before applying guard point.

- b. Click **Browse** if you want to specify a lower-level network path. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths.

File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

- c. (Applicable only for Client Groups) Click **Select Client** to select the Windows or Linux client.
- d. Select **Network Path** as the **Path Type**.
- e. Specify the **User Name** and **Password** to access the desired network path on the NAS machine.
- f. (Optional) Specify the **Domain** where the NAS machine exists.
- g. In the **Search Network Path** field, specify a starting path and click **Refresh** or select from the on-screen network path browser.
- h. Click **Add**. The selected paths appear on the right.

Manual Method

Alternatively, if you know the network path, manually enter full network paths in the given text box. Enter one path per line.

- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more directories. This is the recommended method to specify a large number of paths in one step.

Note

- If a manually entered path doesn't exist, be sure to enter the path correctly. The CipherTrust Manager doesn't parse manually entered paths for correct syntax.
- See [Considerations Before Creating GuardPoints](#) for what to be aware of before creating a GuardPoint.
- If multiple paths are specified, they will all be protected by the same policy.

8. (Windows only) Select the desired **SMB/CIFS Connection** if the GuardPaths are on an SMB/CIFS share.

This drop-down list is displayed when you specify a Windows SMB/CIFS share in the **Path** field.

Note

An SMB/CIFS connection must already exist on the CipherTrust Manager before you can apply GuardPoints to an SMB/CIFS share. Creating an SMB/CIFS connection requires credentials to access the share. Refer to [Connection Manager](#) for details.

9. (Applicable only for Client Groups) Select a **Designated Primary Set** from the dropdown options. See [Adding Designated Primary Set to a Client Group](#) for creating Designated Primary Set.
10. Configure the **Preserve Sparse Region** toggle. The toggle is turned on by default.

Caution

If you turn off the **Preserve Sparse Region** toggle, you are prompted to confirm the action. This is an irreversible action.

11. (Optional) Select **Secure Start** to enable the Secure Start feature. By default, the check box is clear.

If you plan not to enable the Secure Start now, you can do that later, as described in [Enabling Secure Start for GuardPoints](#).

12. (Optional, Windows only). Select **Multifactor Authentication** Refer to [Multifactor Authentication](#) for details.
13. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to [GuardPoint Status Information](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon () to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to [Viewing GuardPoint Status](#) for details.

An LDT GuardPoint is applied automatically according to the QoS settings configured in the linked profile. Refer to [Creating a Profile and Setting Quality of Service Configuration](#).

Refer to [Creating LDT GuardPoints on Local Paths](#) for information on creating LDT GuardPoints on local filesystem paths.

Creating Cloud Object Storage GuardPoints

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

CTE supports protection of Amazon S3 and Wasabi cloud storages. Before proceeding, review the "CTE COS for Amazon S3" section of the [CTE Agent for Linux Advanced Configuration](#) document. Make sure to fulfill the COS requirements.

To create a Cloud Object Storage GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group on which you want to create a GuardPoint.

- Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click **Create GuardPoint**.
 4. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field.
 - b. Select a *Cloud Object Storage* policy. If no policy exists, create one, as described in [Creating Policies](#).

Name	Type	Version
☒ testcospic	Cloud Object Storage	0
☐ testpolicy	Standard	1
☐ idtpic	Live Data Transformation	0
☐ test-jdt-plc	In-place Data Transformation	0

- c. Click **Select**.
5. Select the **Type** of device to protect. This is a mandatory field. The options are:
 - **Auto Cloud Storage**: Select for Cloud Storage policies.
 - **Manual Cloud Storage**: Select for Cloud Storage policies to be guarded manually.

Note

Manual Cloud Storage are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd -unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

6. Specify the **Cloud Object Storage URL** of the storage to be protected. The URL format must be valid. For example, the URL format for an S3 bucket is `https://s3.amazonaws.com/[bucket_name]`.

Options to specify the URLs are:

- **URL**: Select this option, and enter the URL in the box. Only one URL can be specified in the box.
- **Upload CSV**: Select this option and click **Browse** to upload the CSV file containing the list of one or more URLs. This is the recommended method to specify a large number of paths in one step.

Note

- When specifying the URLs using the Upload CSV option, be sure the URLs in the file are correct. The CipherTrust Manager does not parse manually specified URLs for correct syntax.
- See [Considerations Before Creating GuardPoints](#) for what to be aware of before creating a GuardPoint.
- If multiple URLs are specified, they will all be protected by the same policy.
- A maximum of 1000 URLs per CSV file can be uploaded.

Create GuardPoint **Policy:** *

testcosplc

Select**Type:** *

Auto Cloud Storage

Cloud Object Storage URL: *☒ URL ☐ Upload CSV

https://s3.amazonaws.com/testbucket

7. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to [GuardPoint Status Information](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon () to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to [Viewing GuardPoint Status](#) for details.

Creating IDT GuardPoints

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the

GuardPoints tab of individual clients and client groups.

Before proceeding, review the "CipherTrust InPlace Data Transformation for Linux" section of the [CTE Agent for Linux Advanced Configuration](#) document. Make sure to fulfill the IDT requirements.

To create an IDT GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group on which you want to create a GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click **Create GuardPoint**.
4. Select a **Policy**. This is a mandatory field.
 - a. Click **Select** next to the Policy field.
 - b. Select an *In-place Data Transformation* policy. If no policy exists, create one, as described in [Creating Policies](#).

	Name	Type	Version
☐	testcospic	Cloud Object Storage	0
☐	testpolicy	Standard	1
☐	idtpic	Live Data Transformation	0
☒	test-idt-pic	In-place Data Transformation	0

- c. Click **Select**.

Note

When an IDT policy is selected, the read-only **In-place Data Transformation** toggle is displayed on the Create GuardPoint dialog box.

5. Select the **Type** of device to protect. This is a mandatory field. The options for a **In-place Data Transformation** policy are:

Type	Description
Auto Raw or Block Device	Select for IDT policies for raw (block) devices.
Manual Raw or Block Device	Select for IDT policies for raw (block) devices to be guarded manually.

Note

Manual Raw or Block Device are guarded and unguarded (for example, mounted and unmounted) by running the `secfsd -guard` and `secfsd -unguard` commands. Do not run the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

6. Specify the **Path** to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:

- **Enter/Browse Path:** Select this option, and enter the GuardPoint paths by either typing or clicking the **Browse** button.

Note

A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

If the paths are already guarded, you'll see an active GuardPoint icon before them.

- Click **Browse** to select a path by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths.

File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

- Alternatively, if you know the path, manually enter full paths of one or more directories in the given text box. Enter one path per line.
- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more directories. This is the recommended method to specify a large number of paths in one step.

Note

- If a manually entered path does not yet exist, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.

- See [Considerations Before Creating GuardPoints](#) for what to be aware of before creating a GuardPoint.
- If multiple paths are specified, they will all be protected by the same policy.
- A maximum of 1000 GuardPaths per CSV file can be uploaded.
- If the paths are already guarded, you'll see an active GuardPoint icon before them.

Create GuardPoint



Policy: *

test-idt-plc

Select

Type: *

Auto Raw or Block Device

Path: *

☒ Enter/Browse Path ☐ Upload CSV

/dev/sdb/

Browse

i To apply the same GuardPoint settings to multiple paths, type paths in the Path field or specify them using the Browse button. A maximum of 200 GuardPaths can be specified.

In-place Data Transformation: ☒

Efficient Storage: ☐

7. (Optional, Windows only). Select **Multifactor Authentication** Refer to [Multifactor Authentication](#) for details.

8. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to [GuardPoint Status Information](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon () to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to [Viewing GuardPoint Status](#) for details.

A use case of IDT GuardPoints is protection of Teradata appliances. Refer to [Protecting Teradata Appliances](#) for details.

Creating Ransomware Protection GuardPoints

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

Note

- Using Ransomware Protection GuardPoints to protect Network Shares in CTE for **Windows** is compatible with CipherTrust Manager v2.14 and subsequent versions.
- Using Ransomware Protection GuardPoints to protect Network Shares in CTE for Linux is compatible with CipherTrust Manager v2.17 and subsequent versions.

To create an RWP GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group on which you want to create a GuardPoint.
 - Click an RWP-enabled client under the **Client Name** column (**Clients > Clients**). These are the clients with RWP or CTE RWP as Protection Mode.
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click **Create GuardPoint**.

When creating an **RWP** GuardPoint, you do not need to specify a CTE policy when Guardpoint Type is "Ransomware Protection Only". For clients with the RWP protection mode, the **Policy** field is unavailable.

On clients with the **CTE RWP** protection mode, you can create RWP GuardPoints as well as other types of GuardPoints with policies. The **Policy** field is available for such clients. Although the field is available, do not select any policy when creating an RWP GuardPoint.

Refer to [Protection Modes](#) for information on CTE protection modes.

4. (For clients with the **CTE RWP** protection mode) Select **Ransomware Protection Only** as the **Type** of device to protect. This is a mandatory field.

For clients with the **RWP** protection mode, **Ransomware Protection Only** is the default **Type** and cannot be modified.

Note

A process set and the default operation that you want CTE to perform on Ransomware protected GuardPoint can be configured in the profile linked with the client. Refer to [Setting Ransomware Protection Configuration](#) for details.

5. Specify the **Path** (volume or network share) to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:
 - **Enter/Browse Path:** Select this option, and enter the path (for example, C:\, D:\, shared volume, or network share) by either typing or clicking the **Browse** button.

Note

- For CTE for Windows, Ransomware Protection GuardPoints are applied at the volume level. Even if you specify the path of a folder or a file, the GuardPoint will be applied at the volume level.
- For CTE for Linux, Ransomware Protection is applied at GuardPoint level.
- If you specify a network share, *all the network shares to be mounted subsequently* will be protected.
- A CTE client administrator can configure protection of all existing volumes and mount points, and those to be added to the client subsequently. Refer to the [CTE Agent for Windows Advanced Configuration Guide](#) for details.

Note

A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

Browse Method

- a. Click **Browse** to select the volume by browsing the client file system. This method prevents

typographical errors and verifies client availability. This is the recommended method to specify individual paths.

File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

- b. In the **Enter Path** field, specify the volume path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.
- c. Click **Add**.

Note

If the paths are already guarded, you'll see an active GuardPoint icon before them.

Manual Method

Alternatively, if you know the volume, manually enter volume in the given text box. Enter one volume per line.

- **Upload CSV:** Select this option and click **Browse** to upload the CSV file containing the list of one or more paths. This is the recommended method to specify a large number of paths in one step.

Note

- If a manually entered path does not yet exist, be sure to enter the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.
- See [Considerations Before Creating GuardPoints](#) for what to be aware of before creating a GuardPoint.
- A maximum of 1000 paths per CSV file can be uploaded.
- The following paths are restricted on Linux: `/proc`, `/usr/bin`, `/usr/sbin`, `/sbin`, `/bin`, `/opt/vormetric` or `install` directory, `/usr`, `/opt`, `/tmp`, `/var/log/vormetric`, `/lib64`, `/lib`, `/proc/*`, `/usr/bin/*`, `/usr/lib`, `/usr/lib/pam`, `/usr/lib/security`, `/usr/lib/security/*`, `/usr/sbin/*`, `/etc/`, `/sbin/*`, `/bin/*`, `/opt/vormetric/*`, `/etc/init.d/secfs`, `/etc/pam.d`, `/etc/pam.d/*`, `/etc/rc`, `/etc/security`, `/etc/security/*`, `/etc/ssh/sshd_config`, `/etc/ssh/sshr`, `/etc/systemd`, `/lib/systemd`, and `/usr/lib/systemd`.

6. Click **Create**.

Depending on the number of paths you add to a GuardPoint, a status information message may appear. Refer to [GuardPoint Status Information](#) for details.

The newly created GuardPoint appears on the GuardPoints tab. The status remains **Unknown** until the client sends the response after processing the GuardPoint request. Click the **Refresh GuardPoints** icon () to view the updated status.

Status of a GuardPoint can be checked at any time on the GuardPoints tab. Refer to [Viewing GuardPoint Status](#) for details.

Enabling Secure Start for GuardPoints

Note

Information in this section is applicable to Windows clients.

Access to a Secure Start GuardPoint is permitted only during the boot sequence and for a short period. After the VMD is up and running, it performs normal agent initialization and communicates with the CipherTrust Manager to access files within a GuardPoint location.

A CipherTrust Manager administrator can enable Secure Start either when creating a GuardPoint or later by modifying the GuardPoint.

To enable Secure Start for a GuardPoint:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired Windows client.
4. Click the **GuardPoints** tab.
5. Click the overflow icon () corresponding to the desired GuardPoint.
6. Click **View/Edit**. The Edit GuardPoint dialog box is displayed. In the edit mode, you can enable or disable the Secure Start and Preserve Sparse Region toggles.
7. Turn on the **Secure Start** toggle. By default, the toggle is off.

Preserve Sparse Region: 

Secure Start: 

8. Click **Save**.

Refer to the [CTE Agent for Windows Advanced Configuration and Integration Guide](#) for details about using the Secure Start feature.

Note

To disable Secure Start for a GuardPoint, turn off the **Secure Start** toggle in the Edit GuardPoint dialog box.

Protecting Teradata Appliances

Data on a Teradata appliance can be protected using IDT GuardPoints. In a Teradata appliance, the disks used by the database cannot be resized. So, when they are guarded as an IDT capable device, the metadata for those disks is stored externally in a directory on the local file system.

Fulfill the IDT requirements before proceeding. Refer to the CipherTrust InPlace Data Transformation for Linux section of the [CTE Agent for Linux Advanced Configuration](#) document.

To protect a Teradata appliance:

1. Register the Teradata node with the CipherTrust Manager. Refer to the [CTE Agent Quick Start Guide](#) for details.

After registration, you can apply GuardPoints to the data stored on the device, for example, `/dev/sdb`.

2. Make sure the path `/opt/vte/vte-metadata-dir` exists. Create, if it does not.
3. Apply a Standard GuardPoint to `/opt/vte/vte-metadata-dir`. Refer to [Creating Standard GuardPoints](#) for details.
4. Configure the device as IDT capable. Run the command:

```
voradmin idt config -external xform /dev/sdb
```

5. Apply an IDT GuardPoint to the device, as appropriate. Refer to [Creating IDT GuardPoints](#) for details.

Automatic and Manual GuardPoints

The following table lists the type of GuardPoints depending on the platform and type of the policy type:

Type	Windows	Linux	Description
Auto Directory	Yes	Yes	Select for file system directories.
Manual Directory	No	Yes	Select for file system directories to be guarded manually.
Auto Raw or Block Device	Yes	Yes	Select for standard policies for raw (block) devices.

Type	Windows	Linux	Description
Manual Raw or Block Device	No	Yes	Select for standard policies for raw (block) devices to be guarded manually.
Auto Cloud Storage	No	Yes	Select for Cloud Storage policies.
Manual Cloud Storage	No	Yes	Select for Cloud Storage policies to be guarded manually.

A GuardPoint is usually applied immediately after it is configured on the CipherTrust Manager GUI; however, it can be applied later on the client system.

When would you want to apply the GuardPoint later? Consider the case of a 2-node cluster configured as active/passive in a cluster environment, such as VCS, HACMP, or MSCS. There are two nodes, one which is currently active and the other that is currently inactive. Both nodes are locked.

Apply GuardPoint protection to active nodes only. You should never apply a GuardPoint to a passive node. If the active node develops a problem and tries to switch over to the inactive node, the cluster process fails to switch over because the mirror directory on the inactive node is currently mounted on the active node.

The solution is, for the cluster process to unmount (for example, unguard) the currently active node:

1. Place it in an inactive state.
2. Place the old inactive node in an active state.
3. Mount (for example, guard) the mirror directory on the newly active node.

Generally, when you get error messages, check that only active nodes are properly guarded.

When an auto GuardPoint is applied, regardless of whether it is a file system directory or a raw device, the change is pushed to the client system, and the GuardPoint is applied immediately.

Use the `df` command to display `secfs` mounts (for example, GuardPoints) or `secfsd` to display the GuardPoints themselves. The `secfsd` output shows a guard type of local for directories configured with Directory (Auto Guard).

Run:

```
df
```

Output:

```
Filesystem 1K-blocks  Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
40123784  11352236  26733380   30% /
/dev/sda1  101086  14590   81277   16% /boot
none      254492    0   254492    0% /dev/shm
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec
40123784  11352236  26733380   30%
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec
```

```
/opt/apps/apps1/tmp 40123784 11352236 26733380 30% /opt/apps/apps1/tmp
/opt/apps/apps1/lib 40123784 11352236 26733380 30% /opt/apps/apps1/lib
/opt/apps/apps1/doc 40123784 11352236 26733380 30% /opt/apps/apps1/doc
```

Run:

```
secfsd -status guard
```

Output:

```
GuardPoint  Policy  Type    ConfigState  Status  Reason
-----
/opt/apps/apps1/tmp allowAllOps_fs local    guarded    guarded  N/A
/opt/apps/apps1/lib allowAllRootUsers_fs local    guarded    guarded  N/A
/opt/apps/apps1/doc allowAllOps-winusers1_fs local    guarded    guarded  N/A
```

When a manual GuardPoint is applied, regardless if it is a file system directory or a raw device, the change is pushed to the client system only. The client is aware of the GuardPoint but the client does not mount it. This is indicated in the **Type** column of the `secfsd -status guard` command output.

For example, the GuardPoint `/opt/apps/apps2/bin` has been configured with Manual Directory, so the guard type is set to `manual`.

```
secfsd -status guard
```

Output:

```
GuardPoint  Policy  Type    ConfigState  Status  Reason
-----
/opt/apps/apps1/tmp allowAllOps_fs local    guarded    guarded  N/A
/opt/apps/apps1/lib allowAllRootUsers_fs local    guarded    guarded  N/A
/opt/apps/apps1/doc allowAllOps-winusers1_fs local    guarded    guarded  N/A
/opt/apps/apps2/bin HR_policy01 manual    unguarded    not guarded  Inactive
```

Note the **Type** value. A **Type** of `manual` indicates a manual GuardPoint. A **Type** of `local` indicates an automatic GuardPoint.

A manually applied GuardPoint remains Inactive until the GuardPoint is applied on the client. After the GuardPoint is applied on the client, and the client communicates the change to the server, the status changes to Active. It returns to the Inactive state when the GuardPoint is manually unguarded.

Use the `secfsd` command to guard and unguard Manual GuardPoints. The `secfsd` command syntax is:

To guard, run:

```
secfsd -guard path
```

To unguard, run:

```
secfsd -unguard path
```

Example

To manually guard and unguard a file system directory:

1. As CipherTrust Manager administrator, configure a GuardPoint with the type Manual Directory.
2. Log on to the client as an administrator with root permissions.
3. Wait until the configuration change is downloaded to the Agent system.
4. Run the status command until the manual GuardPoint is displayed.

Run:

```
secfsd -status guard
```

Output:

GuardPoint	Policy	Type	ConfigState	Status	Reason
/opt/apps/etc	allowAllOps_fs	manual	unguarded	not guarded	N/A
/opt/apps/lib/dx3	allowAllOps_fs	local	guarded	guarded	N/A

5. Enable the GuardPoint.

Run:

```
secfsd -guard /opt/apps/apps2/bin
```

Output:

```
secfsd: Guard initiated
```

The manual GuardPoint is active and the policy is enforced.

6. Disable the GuardPoint.

Run:

```
secfsd -unguard /opt/apps/apps2/bin
```

Output:

```
secfsd: Unguard initiated
```

Viewing GuardPoints

The Status Bar on the GuardPoints tab of a client shows the total number of GuardPoints on the client, and inactive, disabled, active, and unknown GuardPoints. The Status Bar contains the following tabs:

- **Total GuardPoints:** Shows the total number of GuardPoints with all types of health status.
- **Inactive:** Shows the number of inactive GuardPoints. An inactive GuardPoint is enabled but not yet applied.
- **Disabled:** Shows the number of disabled GuardPoints. The CTE client does not enforce protection on disabled GuardPoints. However, references to the GuardPoints exist in the CipherTrust Manager configuration.
- **Active:** Shows the number of active GuardPoints. An active GuardPoint is deployed successfully and connection to the CTE Agent is healthy. The CTE client enforces protection on active GuardPoints.
- **Unknown:** Shows the number of GuardPoints whose status is unclear.

Click each tab to filter the GuardPoints. The GuardPoints list displays details of the GuardPoints on the client.

To view the GuardPoints created on a client:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client. The GuardPoints tab shows the GuardPoints configured on the client.

Status	Policy Name	Protected Path	Type	LGS Primary	SMB Connection	Efficient Storage	Client Group	Rekey Status	Enabled	LDT Progress	Native Domain
Active	Default	C:\ProgramData	directory_auto	N/A	N/A	No	-	Rekeyed	Yes	Rekeyed	root

The GuardPoints list shows the following details:

Column	Description
Status	Status of the GuardPoint. The status can be: • Inactive • Disabled • Active • Unknown A status Processing is displayed for a brief period until an operation on the GuardPoint completes.
Policy Name	Policy applied to the GuardPoint.
Protected Path	Path of the protected directory.
Type	Type of the GuardPoint. • Auto Directory

Column	Description
	• Manual Directory • Auto Raw or Block Device • Manual Raw or Block Device • Auto Cloud Storage • Manual Cloud Storage • Ransomware Protection Only
LDT Group Role	Whether the client is the primary or secondary node for this GuardPoint in the linked LDT communication group. The values can be: • Primary • Secondary • N/A: Displayed for clients that are not associated with an LDT communication group. N/A is also displayed for clients that do not share an NFS/CIFS path in an LDT communication group. When the primary node is down, another client is automatically assigned the primary role. Refer to Managing LDT Communication Groups for details on LDT communication groups.
SMB Connection	(Applicable to LDT over SMB GuardPoints, Windows clients) Name of the linked SMB connection.
Client Group	Origin of the GuardPoint. The origin can be the client itself or its client group. Filter the results by: • Client: GuardPoint is created on the client. A hyphen (-) indicates the GuardPoint is applied to the client itself. • Client Group: GuardPoint is applied through the client's client group. Name of the linked client group is displayed.
Rekey Status	Rekey status of the GuardPoint.
Enabled	Whether the GuardPoint is enabled.
LDT Progress	(Applicable to LDT GuardPoints) Progress of LDT. Rekeyed is displayed when LDT is complete. N/A is displayed for non-LDT GuardPoints.
Native Domain	Domain where the GuardPoint is created on the shared client.

Viewing GuardPoint Status

Status of GuardPoints can be seen on the CipherTrust Manager and on the client running the CTE Agent. The CipherTrust Manager GUI shows the GuardPoint status as it is configured on the CipherTrust Manager. It is not a real-time indication of the actual status.

Viewing GuardPoint Status on the Client

To view the actual status:

1. Log on to the CTE client as root/administrator.
2. Run the CTE Agent utilities.
3. Compare the GuardPoint status on the client with the status on the CipherTrust Manager GUI. If they do not match, go with the status on the CTE client.

Viewing GuardPoint Status on the GUI

The GuardPoints tab of the Clients page shows the total number of configured GuardPoints with their status. Similarly, status of GuardPoints on a client group can viewed on its GuardPoints tab.

To view the status on the GUI:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. Click the **GuardPoints** tab. This tab shows the list of configured GuardPoints.
5. View the **Status** of the GuardPoint. The status can be:
 - **Active:** GuardPoint is deployed successfully and connection to the CTE Agent is healthy. The CTE client enforces protection on active GuardPoints.
 - **Inactive:** GuardPoint is enabled but not yet applied. Possible reasons are:
 - The GuardPoint is manual and is not mounted on the client. To apply manual GuardPoints, the client administrator needs to run the `secfsd -guard` command on the client.
 - A communication error has occurred between the CipherTrust Manager and CTE client.
 - **Disabled:** GuardPoint is disabled. The CTE client does not enforce protection on disabled GuardPoints. However, references to the GuardPoints exist in the CipherTrust Manager configuration.
 - **Unknown:** GuardPoint is created. Awaiting response from the CTE Agent on the GuardPoint request.

To view more details about an **Active** or **Inactive** GuardPoint, click the corresponding status link.

A status **Processing** is displayed for a brief period until an operation on the GuardPoint completes.

Changing Designated Primary Set Connection

If a GuardPoint is associated with a Designated Primary Set, the Designated Primary Set can be modified after the GuardPoint is created.

To change the Designated Primary Set associated with a GuardPoint:

1. Open the **Transparent Encryption** application.
2. Click the client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click the overflow icon () corresponding to the desired GuardPoint.
4. Click **View/Edit**. The Edit GuardPoint dialog box is displayed.
5. Select the desired **Designated Primary Set** from the drop-down list.
6. Click **Save**.

The GuardPoint is updated successfully with the new Designated Primary Set.

Changing SMB Connection

If the GuardPaths are on an SMB share, the SMB connection can be modified after a GuardPoint is created.

To change the SMB connection:

1. Open the **Transparent Encryption** application.
2. Select the desired client or client group.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click the overflow icon () corresponding to the desired GuardPoint.
4. Click **View/Edit**. The Edit GuardPoint dialog box is displayed.
5. Select the desired **SMB Connection** from the drop-down list.
6. Click **Save**.

The GuardPoint is updated successfully with the new SMB connection.

Removing GuardPoints

GuardPoints can be unguarded (removed) from entire client groups or individual clients. When a GuardPoint is removed from a client group, the GuardPoint is automatically removed from all clients in the group.

When unguarded, all references to the GuardPoint are removed from the CipherTrust Manager, the mount point is removed from the client, and the client stops enforcing protection on the GuardPoint.

Before Removing GuardPoints

The following preliminary steps need to be taken before removing a GuardPoint:

- Encrypted data in a GuardPoint will still be encrypted when the GuardPoint is removed. If you are not going to reuse the GuardPoint for any reason, such as uninstalling the CTE Agent software from a client, do either of the following:
 - Copy the encrypted files out of the GuardPoint so that they are saved as unencrypted files. The GuardPoint must be enabled while copying encrypted files out. Also, ensure that the user or process copying files out of the GuardPoint is not restricted to ciphertext read access under any security rule in the policy applied to the GuardPoint.
 - Rekey the encrypted files while the GuardPoint is still applied under an offline transformation policy.

Note

For LDT GuardPoints, refer to [Migrating a GuardPoint Out of CTE-LDT](#) in the CTE-Live Data Transformation with CipherTrust Manager to ensure that the data in those GuardPoints remains available.

- Take the GuardPoint out of service so that no user or application is accessing the directories and files in the GuardPoint. A GuardPoint is a mounted file system. Removing a GuardPoint involves unmounting the file system. File systems cannot be unmounted when in use.
- Remove all the GuardPoints and disable the locks for a client before deleting the client from the CipherTrust Manager. This ensures that there are no residual GuardPoints in effect on the client.
- For LDT GuardPoints, refer to procedures described in the [CTE-Live Data Transformation](#) with CipherTrust Manager to ensure that the data in those GuardPoints remains available.

Removing a GuardPoint

To remove a GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group from which you want to remove the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).

3. On the **GuardPoints** tab, select the GuardPoint to be removed.

4. Click the delete icon ().

Alternatively, click the overflow icon () corresponding to the desired GuardPoint, and click **Unguard**.

A warning message appears stating that unguarding a GuardPoint is permanent and cannot be undone.

5. Click **Unguard** to confirm the action.

The GuardPoint status becomes **Processing**. While processing the GuardPoint removal:

- a. CipherTrust Manager notifies the CTE Agent that the GuardPoint is removed from the CipherTrust Manager.
- b. CTE Agent removes the mount point from the client.
- c. CTE Agent notifies the CipherTrust Manager about the GuardPoint removal.
- d. CipherTrust Manager removes the GuardPoint from the GuardPoints tab.

6. Click the **Refresh GuardPoints** icon () to update the tab.

7. Verify the mount points on the CTE client.

- On UNIX, run the command `df` or `secfsd -status guard`.
- On Windows, click the **Vormetric** icon and **View > File System > GuardPoints**.

Removing Multiple GuardPoints

The CipherTrust Manager provides an option to remove/unguard multiple GuardPoints. A maximum of 200 GuardPoints can be removed at once.

To remove multiple GuardPoints:

1. Open the **Transparent Encryption** application.
2. Select the client or client group from which you want to remove the GuardPoints.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, select the GuardPoints to be removed.

To select all GuardPoints visible on the page, select the top check box to the left of the Status heading.

4. Click the delete icon ().

A warning message appears stating that unguarding GuardPoints is permanent and cannot be undone.

- Click **Unguard** to confirm the action.

The GuardPoint status becomes **Processing**. While processing the GuardPoint removal:

- CipherTrust Manager notifies the CTE Agent that the GuardPoint is removed from the CipherTrust Manager.
- CTE Agent removes the mount point from the client.
- CTE Agent notifies the CipherTrust Manager about the GuardPoint removal.
- CipherTrust Manager removes the GuardPoint from the GuardPoints tab.

- Click the **Refresh GuardPoints** icon () to update the tab.
- Verify the mount points on the CTE Agent client.
 - On UNIX, run the command `df` or `secfsd -status guard`.
 - On Windows, click the **Vormetric** icon and **View > File System > GuardPoints**.

Disabling GuardPoints

If you have protected a GuardPath with a GuardPoint, and you want to protect the path with a different policy, then you need to remove or disable the existing GuardPoint first.

When a GuardPoint is disabled, the client stops enforcing protection on the GuardPoint. However, references to the GuardPoint exist in the CipherTrust Manager configuration.

Disable individual GuardPoints

To disable a GuardPoint:

- Open the **Transparent Encryption** application.
- Select the client or client group from which you want to disable the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
- On the **GuardPoints** tab, select the GuardPoint to be disabled.
- Click the overflow icon () corresponding to the desired GuardPoint, and click **Disable**.

The GuardPoint status becomes **Disabled**.

Disable multiple GuardPoints

To disable multiple GuardPoints at once:

1. Open the **Transparent Encryption** application.
2. Select the client or client group from which you want to enable the GuardPoints.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. In the the **GuardPoints** tab, select the checkboxes corresponding to the GuardPoints that you want to disable.
4. Select the **Disable** option from the top.

A confirmation dialog box with a message will appear.

5. Click **Disable**.

After the process is complete, a screen will be displayed showing the details of the successfully disabled GuardPoints. The status of these GuardPoints becomes **Disabled**.

This screen also provides information on any GuardPoints that could not be disabled, along with the corresponding troubleshooting error messages. After addressing the issues, you may attempt the disable operation again.

Enabling GuardPoints

A CTE client does not enforce protection on disabled GuardPoints. References to those GuardPoints exist in the CipherTrust Manager configuration. To resume protection of such GuardPoints, you need to enable them.

Enable individual GuardPoints

To enable a disabled GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group from which you want to enable the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, select the GuardPoint to be enabled.
4. Click the overflow icon () corresponding to the desired GuardPoint, and click **Enable**.

The GuardPoint status becomes **Active**. It might take some time to update the status. When the GuardPoint is enabled, the CTE client starts enforcing protection on the GuardPoint.

Enable multiple GuardPoints

To enable a disabled GuardPoints at once:

1. Open the **Transparent Encryption** application.
2. Select the client or client group from which you want to enable the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. In the the **GuardPoints** tab, select the checkboxes corresponding to the GuardPoints that you want to enable.
4. Select the **Enable** option from the top.

A confirmation dialog box with a message will appear.

5. Click **Enable**.

After the process is complete, a screen will be displayed showing the details of the successfully enabled GuardPoints. The status of these GuardPoints becomes **Active**. This screen also provides information on any GuardPoints that could not be enabled, along with the corresponding troubleshooting error messages. After addressing the issues, you may attempt the enable operation again.

It might take some time to update the status. When the GuardPoints are enabled, the CTE client starts enforcing protection on the GuardPoint.

Enabling and Disabling MFA on GuardPoints

In Multifactor Authentication (MFA), access to the requested data is granted only after the requester satisfies two or more authentication criteria.

After you have configured MFA, you can enable it for individual clients and GuardPoints at the client and client group levels.

GuardPoint-level MFA can be enabled at the time of GuardPoint creation. Also, you can enable or disable it later.

- **GuardPoints on Clients**

When MFA is disabled at the client level, you can enable MFA for individual GuardPoints on clients. In this case, the CTE Agent processes the MFA configuration of individual GuardPoints. However, if client-level MFA is enabled, the MFA configuration of the client takes priority.

- **GuardPoints on Client Groups**

MFA cannot be enabled at the client group level. However, you can enable MFA for individual GuardPoints on client groups.

While propagating the MFA-enabled GuardPoints to the member clients, the CTE service on the CipherTrust Manager checks the MFA capability on the member clients. If a client is MFA-capable, the GuardPoints are added to the client. If a client is not MFA-capable, the GuardPoints are skipped.

Note

After GuardPoints are propagated to the member clients, the MFA configuration specified in the profiles associated with the member clients is used to send the security configuration to the CTE Agent.

Therefore, if the profiles of a client group and its member clients are different, the profiles of the member clients are used.

Enabling MFA on GuardPoints

MFA for individual GuardPoints can only be enabled when the client-level MFA is disabled.

To enable MFA on a GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group on which you want to enable the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, turn ON the **Multifactor Authentication** toggle corresponding to the desired GuardPoint.

MFA is enabled on the selected GuardPoint.

Disabling MFA on GuardPoints

MFA can't be disabled on individual GuardPoints of a *client* if MFA is enabled at the client level. Before proceeding with disabling MFA for individual GuardPoints, make sure that MFA is *disabled* on the client. Refer to [Enabling or Disabling MFA on Client Level](#) for details.

MFA enabled on the GuardPoints created on client groups can be disabled directly.

To disable MFA at GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group on which you want to disable the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click the expand icon (▶) corresponding to the desired GuardPoint.
4. Clear **Multifactor Authentication**.

5. Click **Apply**.

MFA is disabled at the GuardPoint level.

Managing Kubernetes Storage Groups and Clients

This section describes how to manage Kubernetes (K8s) storage groups, manage K8s clients, apply GuardPolicies to storage groups, and protect K8s clients.

This section covers the following information:

- [Managing Kubernetes Storage Groups](#)
- [Managing Kubernetes Clients](#)
- [Protecting Kubernetes Clients](#)
- [Collecting Kubernetes Agent Information](#)

Managing Kubernetes Storage Groups

Create, view, edit, and delete Kubernetes (K8s) storage groups on the K8s Storage Groups page of the CipherTrust Manager GUI.

Note

The terms storage group, CSI storage group, Kubernetes storage group, and K8s storage group refer to the same resource and can be used interchangeably.

Creating Kubernetes Storage Groups

Note

All the K8s clients that you want to attach to a storage group must have the same K8s Namespace and K8s StorageClass.

To create a storage group:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Storage Groups**. The K8s Storage Groups page is displayed.
3. Click **Create K8s Storage Group**. The General Info screen of the Create K8s Storage Group wizard is displayed.

4. Specify a unique **Name** for the group.
5. Enter the **K8s Namespace**.
6. Enter the **K8s StorageClass**.
7. (Optional) Select a **Client Profile** for the storage group. The default profile is **DefaultClientProfile**.
8. (Optional) Provide a **Description** for the storage group.
9. Click **Next**. The Review screen is displayed.
10. Review the provided details. The Review screen displays general information about the storage group you specified. If the details are incorrect or you want to modify them, click **Back** and update the details.
11. Click **Save**.

The newly created storage group appears in the K8s Storage Groups list.

You can change the client profile linked to the storage group later. Refer to [Changing the Client Profile](#) for details.

Viewing Details of Kubernetes Storage Groups

To view the details K8s storage groups:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Storage Groups**. The list of K8s storage groups is displayed. The following details are displayed:

Column	Description
Name	Name of the K8s storage group.
StorageClass	K8s StorageClass linked to the storage group.
Namespace	K8s Namespace linked to the storage group.
Created At	Date and time when the storage group is created.
Updated At	Date and time when the storage group is updated the last.
Description	Description of the storage group.

The K8s Storage Groups page also provides options to view the client profile and K8s clients linked to the storage groups. To view these details, click the expand icon  corresponding to the desired storage group.

The K8s clients attached to a storage group are also visible on the Membership tab of the storage group. Refer to [Viewing Attached K8s Clients](#) for details.

Changing the Client Profile

To change the linked client profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Storage Groups**.
3. Click the expand icon  corresponding to the desired storage group.

Alternatively, click the **Name** link corresponding to the desired storage group.

4. Next to **Client Profile**, click the profile link (for example, **DefaultClientProfile**). The Select Profile dialog box shows the current client profile and Rekey Option, Rekey Rate, and Schedule of the selected profile.
5. From the **Profile** drop-down list, select the desired profile.
6. Click **OK**. The selected profile is linked successfully.

Updating Description of a Kubernetes Storage Group

To add or edit the description of a K8s storage group:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Storage Groups**. The list of K8s storage groups is displayed.
3. Click the overflow icon () corresponding to the desired K8s storage group.
4. Click **Edit**.
5. Add or update the **Description** field.
6. Click **Update**.

The storage group description is updated.

Viewing GuardPolicies Applied to a Storage Group

To view GuardPolicies applied to a storage group:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Storage Groups**. The list of K8s storage groups is displayed.
3. Under **Name**, click the desired storage group. The **GuardPolicies** tab shows the following details:

Column	Description
Policy Name	Name of the applied policy.
Type	Type of the GuardPolicy - csi_manual.
Enabled	Whether the GuardPolicy is enabled - Yes or No.

To remove/disable a GuardPolicy, click the overflow icon () corresponding to the GuardPolicy and click **Remove/Disable**.

Note

If a GuardPolicy is **active** on a K8s client, the policy cannot be removed or disabled from the storage group associated with that client.

Viewing Attached Kubernetes Clients

The Membership tab of a storage group displays the attached K8s clients.

To view the K8s clients attached to a storage group:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Storage Groups**. The list of K8s storage groups is displayed.
3. Under **Name**, click the desired storage group.
4. Click the **Membership** tab. The tab displays the K8s clients attached to the storage group. The following details are displayed:

Column	Description
Status	Health status of the K8s client.
Name	Name of the K8s client. The name is a combination of: • The node on which the K8s client is running • The linked StorageClass • The namespace where the K8s client pod runs • A random string
Description	Description of the K8s client.

Deleting a Kubernetes Storage Group

A storage group can only be deleted if no K8s clients are attached to it. As K8s clients are automatically attached

to a storage group, they cannot be detached explicitly. K8s clients are detached from the linked storage groups only when the clients crash.

When a storage group is deleted, any attached GuardPolicies are removed automatically.

To delete a K8s storage group:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Storage Groups**. The list of K8s storage groups is displayed.
3. Click the overflow icon () corresponding to the K8s storage group you want to delete.
4. Click **Delete**. A dialog box appears prompting to confirm the action.
5. Click **Delete**.

The K8s storage group is deleted.

Managing Kubernetes Clients

Register and view Kubernetes (K8s) clients on the K8s Clients page of the CipherTrust Manager GUI.

Every node of a Kubernetes cluster consumes one CTE for Kubernetes license. The license applies to worker nodes where CSI is attached to the application pod. Refer to [CTE Licensing Model](#) for details.

Registering Kubernetes Clients

Registration is the process of configuring a Kubernetes (K8s) client with a CipherTrust Manager.

This process creates SSL certificates for further communication between the CipherTrust Manager and the K8s client. Refer to [Preparing a CTE for Kubernetes Volume for Deployment](#) for details.

After registration, the K8s client can communicate with the CipherTrust Manager. All the GuardPolicies applied to the K8s storage group are automatically added to the K8s client. The client configuration is then built for K8s client (exactly like a CTE client) and sent to the client.

After successful registration, the K8s client appears on the K8s Clients page of the CipherTrust Manager GUI. The client status becomes Healthy.

Note

- All the K8s clients that you want to attach to a storage group must have the same K8s Namespace and K8s StorageClass.
- To automatically delete a node from CipherTrust Manager, you must be running both CipherTrust Manager 2.20 or later and CTE Agent 1.6 or later. If either component is older than these versions, the node will not be automatically deleted.

Viewing Details of Kubernetes Clients

The K8s Clients page shows the total number of K8s clients, clients with errors, clients with warnings, and healthy clients. The Status Bar contains the following tabs:

- **Total Clients:** Shows the total number of registered clients with all types of health status.
- **Errors:** Shows the number of clients with errors.
- **Warnings:** Shows the number of clients with warnings.
- **Healthy:** Shows the number of healthy clients.

Refer to [Client States](#) for details.



Click each tab to filter the K8s clients. The clients list displays names of clients in the CipherTrust Manager database and details about their configuration.

To view the details of a K8s client:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Clients**. The list of K8s clients registered with the CipherTrust Manager is displayed. The following details are displayed:

Column	Description
Status	Health status of the K8s client.
Client Name	Name of the K8s client registered with the CipherTrust Manager. The name is a combination of: • The node on which the K8s client is running • The linked StorageClass • The namespace where the K8s client pod runs • A random string
Agent Version	Version of the CTE for Kubernetes Agent installed on the K8s client.
Description	Description of the K8s client.

Reregistration and Reenrollment

Unlike a CTE client, when a K8s client crashes or stops, it does not persist any information about its previous interaction with the CipherTrust Manager.

If you try to reregister the K8s client with same name (`<node-name>_<csi-storage-class>_<csi-namespace>`), the client is registered as a new client (with a new random string `_<random-string>` appended to its name).

After registration:

1. K8s client sends the enrollment request to the CipherTrust Manager.
2. CipherTrust Manager checks the request for the node name, namespace, and StorageClass.
3. CipherTrust Manager removes the existing registration entry of the client (with the old random string).

Viewing GuardPolicies Applied to Kubernetes Clients

To view the GuardPolicies applied to a K8s client:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Clients**. The list of K8s clients registered with the CipherTrust Manager is displayed.
3. Under **Client Name**, click the desired client link. The detail view of the K8s client is displayed. The **GuardPolicies** tab shows the list GuardPolicies applied to the K8s client.
4. Under **Policy**, click the expand icon () to the left of the desired policy. The following policy details are displayed:

Column	Description
Pod	Name of the K8s pod.
CTE PVC Name	Name of the CTE PVC.
K8s PVC Name	Name of the K8s PVC.
K8s PVC Phase	Name of the K8s PVC phase.
StorageClass	Name of the K8s StorageClass.
CTE Guard Name	Name of the CTE GuardPolicy.

Deleting Kubernetes Clients with Error Status

The Kubernetes clients with the Error status can be deleted from the CipherTrust Manager GUI. Kubernetes clients with other status cannot be deleted.

To delete such a Kubernetes client:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Clients**. The list of K8s clients registered with the CipherTrust Manager is displayed.

3. Click the **Delete** button corresponding to the erroneous Kubernetes client (with the status "Error") that you want to delete. A dialog box appears prompting to confirm the action.

Deleting a client is permanent and cannot be undone.

4. Click **Delete**.

A request to delete the client is submitted successfully to the CTE Agent. After the CipherTrust Manager receives confirmation from the CTE Agent, the Kubernetes client is deleted and its entry is removed from the K8s Clients page.

Note

You can force delete the Kubernetes clients from the CipherTrust Manager. Run the delete API, and set `"force_del_client": true`.

Protecting Kubernetes Clients

This section describes how to protect Kubernetes (K8s) clients attached to storage groups.

To protect a K8s client:

1. [Create a Kubernetes Storage Group](#)
2. [Apply a GuardPolicy to the Storage Group](#)
3. [Register the Kubernetes Client](#)

These steps are described below.

Create a Kubernetes Storage Group

First of all, you need to create a K8s storage group on the CipherTrust Manager. A storage group refers to a combination of a K8s StorageClass and a K8s Namespace. It is used to group together different K8s pods running on different nodes with the same K8s StorageClass and K8s Namespace. Different storage groups can exist for the same combination of K8s StorageClass and K8s Namespace.

While creating a K8s storage group, the Namespace and StorageClass of the K8s cluster are required. Contact your K8s administrator for these details.

Refer to [Creating Kubernetes Storage Groups](#) for details.

Apply a GuardPolicy to the Storage Group

After you have created a K8s storage group, you need to apply a GuardPolicy to it. Until a GuardPolicy is applied, a K8s client attached to the storage group cannot be registered successfully with the CipherTrust Manager.

To add a GuardPolicy to the storage group:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Clients > K8s Storage Groups**. The list of K8s storage groups is displayed.
3. Under **Name**, click the storage group to which you want to apply a GuardPolicy. The detail view of the K8s storage group is displayed.
4. On the **GuardPolicies** tab, click **Create GuardPolicy**. The General Info tab of the Create GuardPolicy screen is displayed.

The Create GuardPolicy screen shows the list of available GuardPolicies. If no policies exist, you can create a new one. You can either select an available GuardPolicy or create a new one. This section describes how to create a new GuardPolicy to a storage group.

Step 1: General Info

- a. Click **Create Policy**. The Create Policy wizard is displayed.
- b. Specify a unique **Name** for the policy. For example, `csi-policy`.
 - The name must start with a character. The maximum length can be 64 characters.
 - The name can contain alphanumeric characters, underscores (`_`), and dashes (`-`).
 - The name cannot contain the following special characters:
`? : ; | ! @ # $ % ^ & * < = > + ( ) { } ~ , \ / [ ] ' "`
- c. Select **CTE for Kubernetes** as the **Policy Type**. This policy is required to protect K8s clients.
- d. (Optional) Turn on the **Learn Mode** toggle. A warning message is displayed indicating that the policy is in Learn Mode.

Learn Mode:



 **Warning: This Policy is in Learn Mode** [Click here for more details](#)

Refer to [Learn Mode](#) for details. By default, the toggle is turned off.

- e. (Optional) Turn on the **Restrict Update** toggle. This option is used to restrict or allow any changes to the policy. By default, the toggle is turned off. This setting can be changed any time after the policy is created. Refer to [Controlling Updates to Policies](#).
- f. Click **Next**. The Security Rules screen is displayed.

Step 2: Security Rules

- a. Click **Create Security Rule**. The Create Security Rule dialog box is displayed.

- b. Specify the following details:

Field	Description
User Set	User set for the rule.
Process Set	Process set for the rule.
Resource Set	Resource set for the rule.
Action	Actions for the rule. Refer to Actions for the complete list of supported actions.
Effect	Effect permission and options for the rule. This is a mandatory field. By default, deny , audit is added.

Refer to [Step 2: Add Security Rules](#) for details on the fields.

- c. Click **Add**. The newly created security rule appears in the list of security rules.
- d. Click **Next**. The Key Rules screen is displayed.

Step 3: Add Key Rules

If you added a security rule with the Effect **ApplyKey** on the Security Rules screen, then you must add at least one key rule.

To add a key rule:

- a. Click **Create Key Rule**. The Create Key Rule dialog box is displayed.
- b. Select a **Key Name**. This is a mandatory field.
 - a. Click **Select** next to the field. The Select Key dialog box shows the list of available keys.

Optionally, you can create a new CBC-CS1 key on this dialog box by clicking **Create a New Key**. Refer to [Step 3: Add Key Rules](#) for details on the fields.
 - b. Select the desired **CBC-CS1** key. CTE for Kubernetes policies do not support XTS keys.
 - c. Click **Select**. The selected key appears in the Key Name field.
- c. Click **Add**. The newly created key rule appears in the list of key rules.
- d. Click **Next**. The Signature Rules screen is displayed.

Step 4: Add Signature Rules

- a. Click **Add Signature Rules**. The Add Signature Rules dialog box is displayed.

- b. Select a **Signature Rule** from the list.

Note

Ensure that you have already created a [signature set for container images](#).

- c. Click **Add**. The newly added signature rule appears in the list of signature rules.
- d. Click **Next**. The Confirmation screen is displayed.

Step 5: Confirmation

- a. Verify the policy details. The Confirmation screen displays general information about the policy and details of the security and key rules added to the policy.

If the details are incorrect or you want to modify them, click **Back** and update the details.

- b. Click **Save**.

The newly created CTE for Kubernetes policy appears on the Create GuardPolicy dialog box. Similarly, add as many policies as required.

5. Select the desired policy.
6. Click **Save**.

The newly created GuardPolicy is displayed on the GuardPolicies tab.

Register the Kubernetes Client

Registration is the process of configuring a Kubernetes (K8s) client with a CipherTrust Manager.

This process creates SSL certificates for further communication between the CipherTrust Manager and the K8s client. Refer to [Preparing a CTE for Kubernetes Volume for Deployment](#) for details.

After registration, the K8s client can communicate with the CipherTrust Manager. All the GuardPolicies applied to the K8s storage group are automatically added to the K8s client. The client configuration is then built for K8s client (exactly like a CTE client) and sent to the client.

After successful registration, the K8s client appears on the K8s Clients page of the CipherTrust Manager GUI. The client status becomes Healthy.

Collecting Kubernetes Agent Information

A Kubernetes Agent provides the `agentinfo` utility to collect system and CTE configuration data. The `agentinfo` utility takes a configuration snapshot of the system that you can send to Thales Customer Support to debug an issue.

The latest information about individual Kubernetes Agents can also be collected and downloaded on the CipherTrust Manager GUI. The collected information about all the Kubernetes Agents is stored in a dedicated volume on the CipherTrust Manager. An option is provided to clean the Agent information about all the Kubernetes Agents from the volume.

Collecting the Kubernetes Agent Information

To collect the latest Kubernetes Agent information:

1. Open the **Transparent Encryption** application.
2. Click **Clients > K8s Clients**.
3. Under **Client Name**, click the desired client.

Alternatively, click the expand icon () to the left of the desired client in the clients list.

4. Next to the **Agent Information** label, click **Collect**. A request is sent to the Kubernetes Agent to send the latest Agent information to the CipherTrust Manager.

Fetching the latest Agent information from the Kubernetes Agent might take some time. You need to *refresh* the page to download the latest Agent information. As soon as the information is available, the **Collect** link is replaced with the **Recollect** and **Download** links.

Recollecting the Kubernetes Agent Information

After you have fetched the Kubernetes Agent information from the Kubernetes client, a CTE Client Administrator might make some confirmation changes. To get the updated Kubernetes Agent configuration on the CipherTrust Manager, use the Recollect option.

To recollect the updated Kubernetes Agent information:

1. Open the **Transparent Encryption** application.
2. Click **Clients > K8s Clients**.
3. Under **Client Name**, click the desired client.

Alternatively, click the expand icon () to the left of the desired client in the clients list.

4. Next to the **Agent Information** label, click **Recollect**. A request is sent to the Kubernetes Agent to send the updated Agent information to the CipherTrust Manager. The **Recollect** and **Download** links are replaced with **Collect**.

Fetching the latest Agent information from the Kubernetes Agent might take some time. You need to *refresh* the page to download the latest Agent information. As soon as the information is available, the **Collect** link is replaced with the **Recollect** and **Download** links.

Downloading the Kubernetes Agent Information

After you have fetched the Agent information from a Kubernetes client, you can download this information from the CipherTrust Manager GUI. The information is downloaded in a tar file.

After the download, the Agent information is removed from the CipherTrust Manager. In a CipherTrust Manager cluster, the information will be downloaded from the node where the Agent information is requested.

To download the Kubernetes Agent information:

1. Open the **Transparent Encryption** application.
2. Click **Clients > K8s Clients**.
3. Under **Client Name**, click the desired client.

Alternatively, click the expand icon () to the left of the desired client in the clients list.

4. Next to the **Agent Information** label, click **Download**.

The Kubernetes Agent information currently available on the CipherTrust Manager is downloaded in a tar file, and removed from the CipherTrust Manager.

Cleaning the Kubernetes Agent Information Volume

When you fetch the Agent information from a Kubernetes Agent, this information is stored in a file in a dedicated volume on the CipherTrust Manager. This volume contains information about all the Kubernetes Agents from which you have collected the information.

The CipherTrust Manager provides an option to [clean the Agent information volume any time](#) to remove all the files containing the Agent information from the CipherTrust Manager. Also, when the [volume is 80% full](#), you are prompted to clean it while collecting the latest Agent information from clients.

Clean the Volume Any Time

To clean the volume containing the Kubernetes Agent information:

1. Log on to the **CipherTrust Manager** GUI.
2. Open the **Transparent Encryption** application.
3. Navigate to **Settings > Client Information and Capabilities**.
4. Under **Empty CTE Agent Information Log Volume**, click **Remove Agent Information**. A warning message is displayed.

Warning

The Agent information currently available on the CipherTrust Manager will be removed. You will have to regenerate the Agent information.

5. Select **Yes, clean up the entire volume containing the Agent information**.
6. Click **Clean**.

Clean the Volume When 80% Full

When the volume containing the Agent information is 80% full, a warning message is displayed while collecting the Agent information from a client. You need to clean the volume to collect the latest information.

To clean the volume, click **Clear Volume**. All the files containing the Agent information are removed from the volume. You can now retry collecting the latest Agent information.

Sharing Resources Across Domains

CTE clients having sensitive data can be shared across multiple departments and teams. Every department manages their data security requirements through different domains on the CipherTrust Manager. So, such a machine having sensitive data at multiple locations needs to be protected by different security administrators with different kinds of policies.

CipherTrust Manager supports sharing of CTE clients and client groups across multiple domains. Different domain administrators can apply different GuardPoints on the same client from their domains. On the client, there will be a single security configuration with all types of protection policies applied to multiple paths irrespective of the domains they are created in.

Note

If multiple domains with the same name exist in the domain hierarchy, clients and client groups are shared with the first domain found with that name.

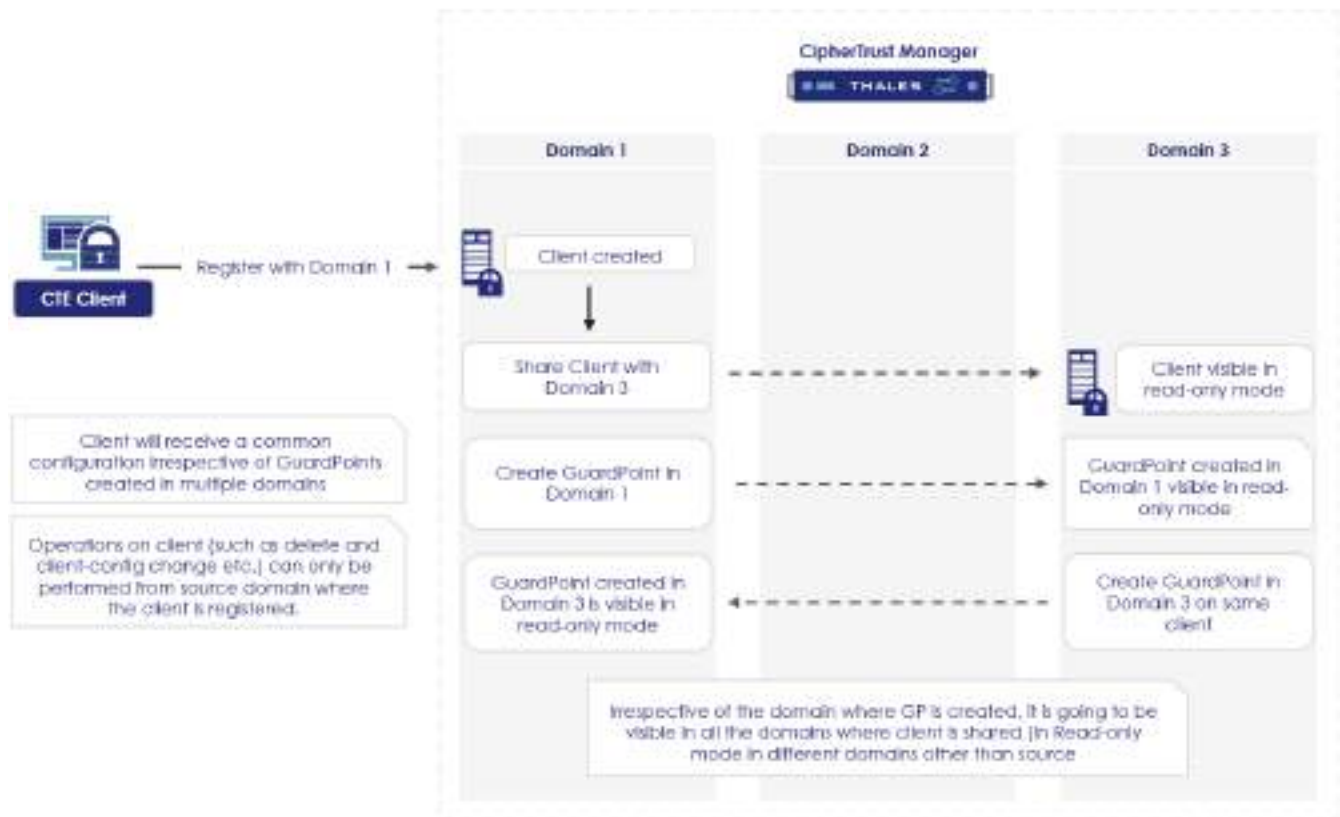
The GuardPoints created on the clients and client groups in one domain (called native domain) will also be visible in other (nonnative) domains but in read-only mode.

Sharing a Client Across Domains

A shared client will be visible in read-only mode in all the domains where it is shared. The GuardPoints can be created on the shared client from any of the linked domains. These GuardPoints will be visible in read-only mode in all the linked domains except their native domains (where the GuardPoints are created). All the valid operations on the GuardPoints will be allowed from the native domains.

This functionality is transparent to the CTE client, that is, the client will receive a single security configuration having GuardPoint details of all the domains.

The following diagram shows the client-sharing workflow:



To share a client across domains:

1. Open the **Transparent Encryption** application.
2. Click **Clients > Clients**. The list of available CTE clients is displayed.
3. click the **Name** link of the desired client. The details page of the client is displayed.
4. Click the **Settings** tab.
5. Expand **GENERAL SETTINGS**.
6. Enable **Domain Sharing**.
7. Click **Update**.

Removing Client Sharing from Domains

You can remove client sharing from individual domains or from multiple domains in one go.

1. Open the **Transparent Encryption** application. The Clients page is displayed.
2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client. The detail view of the Clients page is displayed.

4. Click the **Sharing** tab.
5. Click the desired tab to view the instructions.

From Individual Domains

- a. Under **Domain Name**, select the check box corresponding to the desired domain.
- b. Click **Remove**. A dialog box appears prompting to confirm the action. Deleting this domain is permanent and cannot be undone.

From Multiple Domains

- a. Under **Domain Name**, select the check box corresponding to the desired domains. To select all domains visible on the page, select the top check box to the left of the Domain Name heading.
- b. Click the delete icon (). A dialog box appears stating that deleting the selected domains is permanent and cannot be undone.

6. Click **Delete**.

The client is no longer shared with the selected domain(s).

Sharing a Client Group Across Domains

A shared client group will be visible in read-only mode in all the domains where it is shared. The GuardPoints can be created on the shared client group from any of the linked domains. These GuardPoints will be visible in read-only mode in all the linked domains except their native domains (where the GuardPoints are created). All the valid operations on the GuardPoints will be allowed from the native domains.

Clients can be added to the shared client group from all the linked domains (including the native domain). All the GuardPoints added to the client group (from all the domains) will be propagated to the clients in the group.

Propagation of client settings and other configuration (like LDT suspend/resume) is passed on to all the clients in the group irrespective of the domain.

To share a client group across domains:

1. Open the **Transparent Encryption** application. The Clients page is displayed. This page lists the clients added to this CipherTrust Manager appliance.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group.
4. In the mini detail view, select **Domain Sharing**.

Alternatively, to enable domain sharing on a client group, click the expand icon () corresponding to the desired group, select **Domain Sharing** in the mini detail view, and click **Apply**.

5. Click **Apply**. Now, the **Sharing** tab is displayed.

6. On the **Sharing** tab, click **Share With Other Domains**. The Share With Other Domains dialog box is displayed.
7. Under **Domain Name**, select the domains with which you want to share the client group. The dialog box also provides an option to select all the domains, if required.
8. Click **Share**.

The client group is shared across selected domains of the CipherTrust Manager.

Note

If a client group is shared across domains, then deleting its native domain member clients returns the "resource not found" error.

Removing Group Sharing from Domains

Removing Individual Domains

To remove group sharing from a domain:

1. Open the **Transparent Encryption** application. The Clients page is displayed.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group. The detail view of the Client Groups page is displayed.
4. Click the **Sharing** tab.
5. Under **Domain Name**, select the check box corresponding to the desired domain.
6. Click **Remove**. A dialog box appears stating that deleting the selected domain is permanent and cannot be undone.
7. Click **Delete**.

The client group is no longer shared with the selected domain.

Removing Multiple Domains

To remove group sharing from multiple domains:

1. Open the **Transparent Encryption** application. The Clients page is displayed.
2. Click **Clients > Client Groups**.
3. Under **Client Group Name**, click the desired client group. The detail view of the Client Groups page is

displayed.

4. Click the **Sharing** tab.
5. Under **Domain Name**, select the check box corresponding to the desired domains. To select all domains visible on the page, select the top check box to the left of the Domain Name heading.
6. Click the delete icon (). A dialog box appears stating that deleting the selected domains is permanent and cannot be undone.
7. Click **Delete**.

The client group is no longer shared with the selected domains.

Multifactor Authentication

In Multifactor Authentication (MFA), access to the requested data is granted only after the requester satisfies two or more authentication criteria.

CTE adds an extra layer of security before granting access to the protected GuardPoints. If MFA is enabled, the users performing specific tasks on the configured GuardPoints need to perform an additional OpenID Connect (OIDC) based authentication.

MFA can be helpful in scenarios such as when the credentials of a client machine are compromised. As an additional level of authentication is enforced, the data security cannot be breached.

Prerequisites

Before configuring MFA, make sure that:

- A valid OIDC connection exists on the CipherTrust Manager. Refer to [Connection Manager](#) for details. Use this connection to configure MFA in CTE profiles.
- MFA is configured in profiles, which can be associated with the clients and client groups. Refer to [Setting MFA Configuration](#) for details.

After you have configured MFA, you can enable it for individual clients and GuardPoints at the client and client group levels.

MFA at Client Level

You can enable or disable MFA for all of the GuardPoints on a client. When MFA is enabled at the client level, the CTE Agent enforces MFA configuration for all GuardPoints configured on the client. It overrides any MFA configuration set for individual GuardPoints.

Enabling or Disabling MFA on Client Level

To enable MFA at client level (that is, for all GuardPoints on a client):

1. Open the **Transparent Encryption** application.
-

2. Click **Clients > Clients**.
3. Under **Client Name**, click the desired client.
4. In the mini details view, select **Multifactor Authentication**.
5. Select **Apply**.

On the GuardPoints tab, the **Multifactor Authentication** toggles for all the GuardPoints will be turned ON.

The GUI may take some time to reflect the changes. You can click the Refresh GuardPoints icon () to refresh the status. At this point, you can't disable MFA for individual GuardPoints.

Note

To disable MFA for all GuardPoints on the client, clear the **Multifactor Authentication** check box in the mini details view and click **Apply**. On the GuardPoints tab, the **Multifactor Authentication** toggles for all the GuardPoints will be turned OFF. You can now enable MFA for individual GuardPoints.

MFA at GuardPoint Level

GuardPoint-level MFA can be enabled at the time of GuardPoint creation. Also, you can enable or disable it later.

▪ GuardPoints on Clients

When MFA is disabled at the client level, you can enable MFA for individual GuardPoints on clients. In this case, the CTE Agent processes the MFA configuration of individual GuardPoints. However, if client-level MFA is enabled, the MFA configuration of the client takes priority.

▪ GuardPoints on Client Groups

MFA cannot be enabled at the client group level. However, you can enable MFA for individual GuardPoints on client groups.

While propagating the MFA-enabled GuardPoints to the member clients, the CTE service on the CipherTrust Manager checks the MFA capability on the member clients. If a client is MFA-capable, the GuardPoints are added to the client. If a client is not MFA-capable, the GuardPoints are skipped.

Note

After GuardPoints are propagated to the member clients, the MFA configuration specified in the profiles associated with the member clients is used to send the security configuration to the CTE Agent.

Therefore, if the profiles of a client group and its member clients are different, the profiles of the member

clients are used.

Enabling MFA on GuardPoints

MFA for individual GuardPoints can only be enabled when the client-level MFA is disabled.

To enable MFA on a GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group on which you want to enable the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, turn ON the **Multifactor Authentication** toggle corresponding to the desired GuardPoint.

MFA is enabled on the selected GuardPoint.

Disabling MFA on GuardPoints

MFA can't be disabled on individual GuardPoints of a *client* if MFA is enabled at the client level. Before proceeding with disabling MFA for individual GuardPoints, make sure that MFA is *disabled* on the client. Refer to [Enabling or Disabling MFA on Client Level](#) for details.

MFA enabled on the GuardPoints created on client groups can be disabled directly.

To disable MFA at GuardPoint:

1. Open the **Transparent Encryption** application.
2. Select the client or client group on which you want to disable the GuardPoint.
 - Click a client under the **Client Name** column (**Clients > Clients**).
 - Click a client group under the **Client Group Name** column (**Clients > Client Groups**).
3. On the **GuardPoints** tab, click the expand icon (▸) corresponding to the desired GuardPoint.
4. Clear **Multifactor Authentication**.
5. Click **Apply**.

MFA is disabled at the GuardPoint level.

For steps, refer to [Enabling and Disabling MFA on GuardPoints](#).

Communication with CipherTrust Manager

A REST-based connection is created from a CTE client to the CipherTrust Manager. Although the connection is one-way, it imitates a two-way connection-like interaction between the CTE client and the CipherTrust Manager.

To understand communication between CTE and CipherTrust Manager when using a load balancer, refer to [Communication Workflow with CipherTrust Manager Behind a Load Balancer](#).

How the Communication Works

1. The CTE client registers with the CipherTrust Manager using a registration token and fingerprint of the server's "web" interface certificate.
2. When the CTE client registers, the CipherTrust Manager sends the security configuration to the CTE client. This configuration includes the list of nodes in the CipherTrust Manager cluster.
3. The CTE client sends the connection request to every node of the CipherTrust Manager cluster.
4. Every node holds the connection request until either of the following happens:
 - Any event that requests configuration push to the CTE client
 - A timeout of three minutes

For example, in a five-node CipherTrust Manager cluster, after registration with a particular node, the CTE client:

1. Receives security configuration from that CipherTrust Manager node.
2. Establishes a connection with all five nodes of the cluster.
3. If a directory browse operation is triggered on any of the cluster nodes, the node sends the browse request to the connection held by it.
4. The CTE client responds to the browse request and sends a new connection request.

When a CipherTrust Manager Node is Down

If a CipherTrust Manager node goes down:

1. If any other node pushes the security configuration to the CTE client due to some event (for example, policy change etc.), the security configuration does not include details of the failed node in it. With the new security configuration, the CTE client identifies the new node list and does not send the request to failed node.
2. Until the updated node list is pushed to the CTE client through the security configuration, the CTE client keeps on sending the connection requests to the failed node, which in turn, is going to fail.

When a New Node is Added to the Cluster

Whenever a new node is added to the CipherTrust Manager cluster:

1. The CipherTrust Manager sends the updated node list to the CTE client.
2. The CTE client establishes the connection with the new node and existing nodes in the list.

Communication Workflow with CipherTrust Manager Behind a Load Balancer

When a load balancer is configured in front of the CipherTrust Manager cluster nodes, the following workflow illustrates how requests and responses flow. Consider a 4-node CipherTrust Manager cluster, where a user browses an agent's filesystem via the CipherTrust Manager GUI. The request is routed to Node1 through the load balancer, while the agent is connected to Node2. Here's how the process unfolds:

1. **Initiating the Request:** The user selects the "Enter/Browse Path" option to browse a directory on the agent, and the request is directed to Node1.
2. **Notifying Other Cluster Nodes:** Node1 broadcasts the request to all nodes in the cluster, storing the details in the database. This ensures all nodes are aware of the request.
3. **Handling the Request:** Each node processes the notification. Only the node connected to the agent (Node2 in this case) takes action; the others disregard the request.
4. **Retrieving the Data:** Node2 fetches the requested data from the agent, records it in the database, and notifies all nodes that the request has been completed.
5. **Notifying the User:** Node1, which initially received the request, retrieves the data and delivers the results to the user's interface.

This system ensures that regardless of where a request originates, all nodes work together to fulfill the request. The process remains efficient and seamless with the load balancer directing traffic across the CipherTrust Manager cluster nodes.

Configuring Cluster Node Preference

A CTE administrator can configure preferred nodes of a CipherTrust Manager cluster for sending status updates from CTE clients. The administrator assigns a priority to every node of the cluster.

The cluster nodes can be categorized into tiers on the CipherTrust Manager GUI, with every tier assigned a priority. For example, Tier 1 is assigned higher priority than Tier 2. All tiers (for example, Tier 1 + Tier 2) can have a total of 20 nodes. This preference is configured through server settings in profiles. If not configured, the CipherTrust Manager continues working with the default settings. Refer to [Communication with CipherTrust Manager](#) for the default behavior.

After the server settings are configured, the CTE clients associated with the profile first try to send status updates to the top tier. If none of the nodes in the tier is reachable, the CTE clients try to send updates to the next tier.

This feature is applicable to the CipherTrust Manager clusters.

To configure the cluster node preference in a profile:

1. Open the **Transparent Encryption** application.

2. In the left pane, click **Settings > Profiles**.

3. Under **Name**, click the desired profile.

Alternatively, click the overflow icon () corresponding to the desired profile and click **Edit**.

4. Expand **SERVER SETTINGS**.

5. Modify the server settings, as appropriate. Refer to [Configuring Server Settings](#) for details.

6. Click **Update**.

Backup and Restore

CipherTrust Manager provides options to back up CTE policies and restore them to other CipherTrust Manager appliances. A CipherTrust Manager administrator with backup and restore permissions can fully or partially export CTE policies from one domain and import them into a different domain on the same CipherTrust Manager or a different CipherTrust Manager. The data under the backed up (exported) policies will remain encrypted.

This section covers the following topics:

- [Assumptions](#)
- [Backing up and Restoring Keys and CTE Policies](#)
- [Signing Files in Restored Signature Sets](#)

Perform the steps in the given order.

Assumptions

- Before restoring CTE policies into the same or a different CipherTrust Manager:
 - Restore all the keys associated with CTE policies.
 - Restore the backup keys.
- The policy backup file contains policies with the associated resources, including:
 - Security rules
 - Key rules
 - LDT rules
 - IDT rules
 - Policy elements (user sets, process sets, resource sets, and signature sets)
- The backed up policy data does not include:

- Keys that are associated with key rules. However, if the backup of keys and CTE policies is taken together, then the linked keys are included in the backup.
- Signatures associated with signature sets

Note

If the system, where the policies are being restored, contains any conflicting policy or policy elements:

- Policies with the same name are skipped.
- All policies using the conflicting policy elements are skipped.

Backing up and Restoring Keys and CTE Policies

Tip

CTE policies and keys used can be backed up *separately* (in different backup files) or *together* (in a single backup file.) If they are backed up separately, the key backup must be restored before the CTE policies.

Keys and CTE Policies are Backed up Together

When you want to back up the keys and CTE policies together:

1. Back up the keys and CTE policies.

- a. Create a domain scoped backup key. You can also use an existing backup key. This key is needed to encrypt the backup file.
- b. Download the domain scoped backup key. Ignore this step if you have already downloaded the key.
- c. Create a domain scoped backup of keys and CTE policies.
- d. Download the domain scoped backup of keys and CTE policies.

A backup file of keys and CTE policies will be downloaded. You need to restore this backup file to the destination CipherTrust Manager where you want to restore the backed up keys and CTE policies.

Now, transfer the downloaded backup key and the backup file to the destination CipherTrust Manager, as described below.

2. Restore the backup file.

- a. Transfer the backup key and files using Secure Copy Protocol (SCP) to the destination CipherTrust

Manager.

- b. [Inspect the backup key file.](#)
- c. [Upload the backup key file.](#)
- d. [Inspect the backup file.](#)
- e. [Upload the backup file.](#)
- f. [Restore the backup file.](#)
- g. [Verify that the backup file is restored successfully.](#)

Keys and CTE Policies are Backed up Separately

When you want to back up the keys and CTE policies separately:

1. Back up the CTE keys.

- a. [Create a domain scoped backup key.](#) You can also use an existing backup key. This key is needed to encrypt the exported backup file.
- b. [Download the domain scoped backup key.](#) Ignore this step if you have already downloaded the key.
- c. [Create a domain scoped key backup.](#)
- d. [Download the domain scoped key backup.](#)

A backup file of keys will be downloaded. You need to restore this backup file to the destination CipherTrust Manager where you want to restore the backed up keys.

Now, transfer the downloaded backup key and the backup file to the destination CipherTrust Manager, as described below.

2. Back up the CTE policies.

- a. [Create a domain scoped backup key.](#) You can also use an existing backup key. This key is needed to encrypt the exported backup file.
- b. [Download the domain scoped backup key.](#) Ignore this step if you have already downloaded the key.
- c. [Create a domain scoped CTE policy backup.](#)
- d. [Download the domain scoped CTE policy backup.](#)

A backup file of CTE policies will be downloaded. You need to restore this backup file to the destination CipherTrust Manager where you want to restore the backed up policies.

Now, transfer the downloaded backup key and the backup file to the destination CipherTrust Manager, as

described below.

3. Import the downloaded backup file.

- a. Transfer the backup key, key backup, CTE policy backup files using Secure Copy Protocol (SCP) to the destination CipherTrust Manager.
- b. Inspect the backup key file.
- c. Upload the backup key file.
- d. Inspect the key backup file.
- e. Upload the key backup file.
- f. Inspect the CTE policy backup file.
- g. Upload the CTE policy backup file.
- h. Restore the key backup file.
- i. Verify that the key backup file is restored successfully.
- j. Restore the CTE policy backup file.
- k. Verify that the CTE policy backup file is restored successfully.

Signing Files in Restored Signature Sets

The restored policy backup contains imported signature sets. As the signatures linked with the signature sets are not included in the backup, you need to sign the files in the signature sets. Refer to [Signing Files in a Signature Set](#) for details.

Integrating CTE Logging with Splunk

The Thales Security Intelligence app for Splunk is created and published to the Splunkbase repository. This app provides a number of security intelligence reports and enables search operations that can be used to extract information from the log streams produced by CTE agents and the CipherTrust Manager.

Read the subsequent sections for instructions to integrate the CTE audit logging with Splunk.

Prerequisites

Before proceeding, ensure that:

- CipherTrust Manager is up and running.
- CTE clients are registered with the CipherTrust Manager.
- You have a valid account on Splunkbase.

Integration Steps

To integrate CTE audit logs with Splunk:

1. [Install Splunk](#)
2. [Install Thales Security Intelligence App](#)
3. [Configure CipherTrust Manager to Forward Messages to Splunk](#)
4. [Configure Splunk Server](#)

After successful integration, the CTE agent logs will be forwarded to the configured Splunk server over the configured protocol.

Install Splunk

First of all, install the supported Splunk version on a target system. This release supports Splunk 7 and 8. Refer to the Splunk [Installation Manual](#) for details.

After you have installed Splunk successfully, install the Thales Security Intelligence app. Refer to [Install Thales Security Intelligence App](#) for details.

Install Thales Security Intelligence App

To install the Thales Security Intelligence app:

1. Log on to your Splunkbase account.
2. Search for the **Thales Security Intelligence** app.
3. Install the app.

Refer to the Splunk documentation for details.

The next step is to configure the CipherTrust Manager to forward CTE audit log messages to Splunk. Refer to [Configure CipherTrust Manager to Forward Messages to Splunk](#) for details.

Configure CipherTrust Manager to Forward Messages to Splunk

To configure the CipherTrust Manager for forwarding audit log messages to Splunk:

1. [Create Certificates for TLS Communication](#)
2. [Enable Syslog on CipherTrust Manager](#)
3. [Configure Syslog on CipherTrust Manager](#)

These steps are described below.

Create Certificates for TLS Communication

This step is required if you want to establish secure communication between the Splunk server and the CipherTrust Manager over the TLS protocol. For TCP and UDP protocols, this step is not required.

Create the CA certificate, client certificate, and a private key. These are required when configuring Syslog over TLS on the CipherTrust Manager. A server certificate is also required that you need to upload to the Splunk server.

The following steps provide examples to create the required certificates and the private key using OpenSSL.

On the Linux shell:

1. Set the subject of the certificate.

```
SUBJ=' /C=US/ST=Ca/L=SanJose/O=Testing/OU=QA/CN=Test '
```

2. Set the password.

```
PW='pass:password'
```

This password will be added to the `password` field of the `inputs.conf` file.

3. Generate a self-signed CA using OpenSSL.

```
openssl req -subj $SUBJ -new -days 365 -out ca.pem -passout $PW -batch -x509
```

The generated `ca.pem` file is the CA certificate. This certificate is stored at the current directory.

4. Generate the server certificate and sign it using the CA certificate created in step 3. Run the following commands:

```
openssl genrsa -out server.key 2048
openssl req -key server.key -new -out server.req -batch
echo 00 > file.srl
openssl x509 -req -in server.req -CA ca.pem -CAkey privkey.pem -CAserial file.srl -out server.pem -passin $PW
```

The generated `server.pem` file is the server certificate. This certificate will be uploaded to the Splunk server (refer to [Configure Splunk Server](#)).

5. Generate the client certificate and sign it using the CA certificate created in step 3. Run the following

commands:

```
openssl genrsa -out client.key 2048
openssl req -subj $SUBJ -key client.key -new -out client.req -days 365 -passout $PW -batch
openssl x509 -req -in client.req -CA ca.pem -CAkey privkey.pem -CAserial file.srl -out client.pem -passin $PW
```

The generated `client.pem` file is the client certificate. This certificate and the generated `client.key` file will be uploaded to the CipherTrust Manager.

Enable Syslog on CipherTrust Manager

To enable Syslog on the CipherTrust Manager:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Profiles**.
3. Under **Name**, click the profile linked to your CTE client. The edit view of the profile is displayed.
4. Expand **CLIENT LOGGING CONFIGURATION**.
5. Select **Syslog Enabled**.
6. Click **Apply**.

The Syslog setting is now enabled on the CipherTrust Manager. Next, you need to configure the Syslog settings on the CipherTrust Manager.

Configure Syslog on CipherTrust Manager

To configure Syslog on the CipherTrust Manager:

1. Expand **CLIENT SYSLOG CONFIGURATION**.
2. Specify the **Hostname or IP** address of the Splunk server.
3. Enter the **Port** of the Splunk server.
4. Ensure the **Message Format** is **RFC5424**.
5. Select the **Protocol**. This protocol acts as the transport protocol for the Syslog connection.

TLS is the preferred communication protocol.

6. (Applicable to the TLS protocol) Specify the certificates and key created in [Create Certificates for TLS Communication](#):

- **CA Certificate:** Click **Browse** to select the CA certificate, for example, `ca.pem`.
- **Certificate:** Click **Browse** to select the signed client certificate, for example, `client.pem`.
- **Private Key:** Click **Browse** to select the private key, for example, `client.key`.

7. Click **Apply**.

The Syslog server settings are configured on the CipherTrust Manager. Finally, you need to configure the Splunk server, as described below.

Configure Splunk Server

To configure the Splunk server:

1. Log on to your Splunk server.
2. Open the `inputs.conf` file in any text editor. The file is located at:
 - **Windows:** `C:\Program Files\Splunk\etc\system\local\inputs.conf`
 - **Linux:** `/opt/splunk/etc/system/local/inputs.conf`
3. Add the following content to the file:

```
[default]
host = <Splunk Server IP Address>

[tcp-ssl:<Splunk server port>]
listenOnIPv6 = yes
acceptFrom = *
sourcetype = rfc5424_syslog

[tcp:514]
listenOnIPv6 = yes
acceptFrom = *
sourcetype = rfc5424_syslog

[SSL]
password = password
requireClientCert = false
serverCert = <location for the server certificate (a .pem file)>
```

For example, location for the server certificate is:

- **Windows:** `C:\Program Files\Splunk\certs\server.pem`
- **Linux:** `/opt/splunk/certs/server.pem`

Here, `server.pem` is a sample name for the server certificate. Replace it with the name of your server certificate.

Refer to the Splunk [Admin Manual](#) for possible settings you can use to configure inputs in the `inputs.conf` file.

4. Copy the server certificate (for example, `server.pem`) to the `serverCert` location on the Splunk server. This is the same location you specified in the `inputs.conf` file above.
5. Restart the Splunk service. Refer to the Splunk [Admin Manual](#) for details.

The communication between the Splunk server and the CipherTrust Transparent Encryption service has been established.

Now, the CTE audit logs are visible on the app dashboards. Refer to the documentation on the Main tab of the **Thales Security Intelligence** app on the *Splunk server* on using "drill down" in reports, VSI Data Model and Pivot, searches, and [Thales Data Security Message Catalog](#).

Migrating CTE Configuration from Data Security Manager

This section describes steps to migrate configuration of CTE resources from a Data Security Manager (DSM) to a CipherTrust Manager.

Before proceeding with migration:

- Note that the password generation method of all *client groups* will be set to Generate after migration. If required, you can change the password method after migration. However, every client (standalone or in a client group) will retain its password and the password generation method as it is on the DSM.
- Ensure that no nested GuardPoints exist on the DSM. CipherTrust Manager doesn't support nested GuardPoints with different policies. As a result, client groups' GuardPoints can't be created during migration.
- To avoid key version mismatch on GuardPoints concerning DSM and CipherTrust Manager:
 - It is recommended to complete the end-to-end migration process in one go. Also, it is advised to pause or suspend LDT key rotation during migration.
 - If you plan to complete the migration later, ensure to extend the expiration date of the existing keys on DSM appropriately.

Prerequisites

- A sufficient number of CipherTrust Transparent Encryption (CTE) licenses is available on the CipherTrust Manager for clients to register successfully. For example, if you want to migrate 100 clients from the Data Security Manager (DSM), then at least 100 CTE licenses must be free on the CipherTrust Manager. Refer to [CTE Licensing Model](#) for details.
- DSM is up and running at the [supported](#) version. Refer to [DSM documentation](#) for details.

- A supported CTE version is configured with a supported DSM version. Refer to the [CTE Agent Quick Start Guide](#) specific to your platform for details.

Note

If you are running an unsupported version, upgrade your environment to the [supported](#) version before proceeding. Refer to the corresponding product documentation for upgrade instructions.

Supported Versions

Current Setup

Product	Version
CTE	7.1 and higher
DSM	6.4.5 and higher

Note

For the migration of LDT GuardPoints, the LDT clients must be running CTE Agent 7.1.1.55 or higher.

Target Setup

Product	Version
CTE	7.1 and higher
CipherTrust Manager	2.8 and higher

Supported Resources

CipherTrust Manager supports migration of the following CTE resources from a DSM backup file:

- Clients and client GuardPoints
- Client groups and client group GuardPoints
- Clients and client group associations
- User sets, resource sets, process sets, signature sets, and signatures
- Standard, Cloud Object Storage (COS), In-place Data Transformation (IDT), and Live Data Transformation (LDT) policies

- Client logging, upload logging, and Syslog settings
- LDT Quality of Service (QoS) and QoS schedules

Tip

Clients on the CipherTrust Manager are equivalent to *hosts* on the DSM.

Steps

To migrate the CTE configuration from the DSM to the CipherTrust Manager:

1. [Export and Import the Backup File](#)
2. [Verify Details of Migrated CTE Resources](#)
3. [Register CTE Clients with the CipherTrust Manager](#)
4. [Verify Access to GuardPoints](#)

Export and Import the Backup File

Export and import the backup file. Refer to [Exporting and Importing the Backup File](#) for details.

Caution

To minimize interruption of CTE client access to CTE keys, include the optional parameter `auto-cte-groups` with the `ksctl migrations apply` import command. This parameter automatically detects CTE keys and grants permission to access these keys to members of the `CTE Clients` group on CipherTrust Manager.

After migration, verify that the DSM keys are successfully migrated into the CipherTrust Manager domain.

Verify Details of Migrated CTE Resources

On the CipherTrust Manager GUI, verify details of the migrated CTE [resources](#).

The migrated resources can also be verified using the CTE reports available on the DSM and the CipherTrust Manager. Reports provide a comprehensive view of the migrated resources.

- A number of reports are available for the combination of clients, policies, GuardPoints, and encryption keys. Use these reports to match and verify the number of resources and their types on the DSM and the CipherTrust Manager.
- Both the DSM and the CipherTrust Manager provide options to download reports in the CSV format. So, if

needed, you can automate resource verification to parse and compare the report content.

Here is a mapping of CTE reports on the DSM and CipherTrust Manager to help verify migrated resources.

Resource	DSM Report	CipherTrust Manager Report
Clients	Hosts	Clients Health Report
Policies	Policy Key	Policies Keys Report
	Policy Host	Clients Policies Report
GuardPoints	GuardPoints	GuardPoints Report
	Hosts with GuardPoint Status	Client GuardPoint Status Report
Keys	Keys	Clients Keys Report
	Keys-Policy	Policies Keys Report

Refer to [Reports](#) for details on CTE reports available on the CipherTrust Manager. Refer to the DSM online help for details on CTE reports available on the DSM.

Verifying GuardPoints Configuration

GuardPoints that are applied to a client using a client group are created in the background. The original request is returned after initial validation of request parameters and migration proceeds further for other operations.

In some cases, creation of certain GuardPoints might fail later in the background due to various reasons. Any errors observed in the background cannot be updated in the migration status. The status is updated in the audit records of the CipherTrust Manager. So it is recommended to verify migration of CTE resources using the [CTE reports](#).

Verifying Profiles Configuration

Every migrated client is linked with a profile (named `profile_<dsm-hostname>_<dsm-domain-id>`) on the CipherTrust Manager. The profile contains information related to client logs, Syslog settings, and QoS configuration. If multiple clients have the same configuration on the DSM, they are linked with a single profile on the CipherTrust Manager. The following mapping helps you verify migration of client logging, Syslog, and QoS configuration.

Resource	Location on DSM	Location on CipherTrust Manager
Message Type	Hosts > FS/VDE Agent Log	Not displayed on the CipherTrust Manager GUI. You can verify them using the <code>/v1/transparent-encryption/profiles</code> APIs.
File Logging Settings	Hosts > FS/VDE Agent Log	Profiles > CLIENT LOGGING CONFIGURATION. Refer to Setting Client Log Configuration for details.
Syslog Settings	Hosts > FS/VDE Agent Log	Profiles > SYSLOG LOGGING CONFIGURATION. Refer to Setting Client Syslog Configuration for details.

Resource	Location on DSM	Location on CipherTrust Manager
Upload Logging Settings	Hosts > FS/VDE Agent Log	Profiles > CLIENT LOGGING CONFIGURATION. Refer to Setting Client Log Configuration for details.
Duplicate Message Suppression Settings	Hosts > FS/VDE Agent Log	Profiles > CLIENT LOGGING CONFIGURATION. Concise Logging settings are also displayed here. Refer to Setting Client Log Configuration for details.
LDT Quality of Service	Hosts > GuardPoints	Profiles > QUALITY OF SERVICE CONFIGURATION. Refer to Setting Quality of Service Configuration for details.
QoS Schedules	Hosts > GuardPoints	Profiles > QUALITY OF SERVICE CONFIGURATION > QoS Settings. Refer to Setting Quality of Service Configuration for details.

After you have successfully verified the CTE resources, proceed to the next step.

Register CTE Clients with the CipherTrust Manager

1. Ensure that the LDT GuardPoints, if any, are unguarded before re-registration of the migrated CTE clients.
2. Register your CTE clients with the CipherTrust Manager. Refer to [CTE Agent Quick Start Guide](#) specific to your platform for details.

Caution

- When registering a CTE client with the CipherTrust Manager, you must provide exactly the same client name with which that client was registered with the DSM before migration.
- Client names are case-sensitive, make sure that case-sensitivity is retained.
- If a different name is provided, the CipherTrust Manager considers it as a new client. The configurations migrated from the DSM are not propagated to this new client on the CipherTrust Manager.

After the CTE clients are successfully registered with the CipherTrust Manager, the migrated configuration is propagated to the CTE clients.

Verify Access to GuardPoints

When the initialization of the CTE clients is successful and the configuration is pushed to them, verify whether the GuardPoints are accessible according to the enforced policies.

Limitations

CTE resources of Container policies on the DSM cannot be migrated to the CipherTrust Manager using the backup/restore method. The Container policies are supported only on the DSM.

Migration Summary

This section provides a summary of the CTE resources migrated from the DSM to CipherTrust Manager, mapping of the resources that are handled differently between the two key managers. Also, the section provides any constraints applicable to the migrated resources and describes how to interpret the migration status.

Resource Mapping

This table describes how the DSM resources are mapped with resources on the CipherTrust Manager after migration.

DSM Resource	CipherTrust Manager Resource
Host	Client
Host Group	Client Group
Host Group - Host Association	Client Group - Client Association
User Sets	User Sets
Resource Sets	Resource Sets
Process Sets	Process Sets
Signature Sets	Signature Sets
Policy	Policy
Logging, QoS, and Syslog configuration	Profile
GuardPoints	GuardPoints

Migration Workflow and Exceptions/Deviations

Host | Client

Migration Workflow

- All related parameters configured on the DSM will be migrated as is to the CipherTrust Manager.
- Only the FS type hosts will be migrated to the CipherTrust Manager. Other host types, for example, VDE and Key, will NOT be migrated.
- After migration, every client needs to be registered with the CipherTrust Manager to receive its configuration.

Exceptions/Deviations

- Hosts marked for deletion on the DSM will NOT be migrated to the CipherTrust Manager.

Host Group | Client Group

Migration Workflow

- All related parameters (**except** the *client group password*) configured on the DSM will be migrated as is to the CipherTrust Manager.
- Host groups of only HDFS and NON-CLUSTER types will be migrated.

Exceptions/Deviations

- All host groups will be migrated with an auto-generated password (required for Challenge Response). Hosts with manual passwords configured on the DSM will also be migrated, but with a new auto generated password on the CipherTrust Manager. Manual password migration will be supported in a future CipherTrust Manager release.

If required, auto generated password could be changed to manual mode on the CipherTrust Manager interfaces after migration.

- Host groups' HDFS configurations for browsing HDFS nodes will NOT be migrated. The CipherTrust Manager does not support browsing of resource sets.

Host Group Association | Client Group - Client Association

Migration Workflow

All successfully migrated host will be migrated as members to the successfully migrated host groups according to the DSM configuration.

Exceptions/Deviations

- Configurations of hosts or host groups that could not be migrated due to any reason will NOT be migrated.
- GuardPoints of host groups will NOT be migrated as part of the migration activity. All GuardPoints of a host group will be automatically propagated in the background after successful association.

User Sets | User Sets

Migration Workflow

- All related parameters configured on the DSM will be migrated as is to the CipherTrust Manager.

Exceptions/Deviations

- Not applicable

Resource Sets | Resource Sets

Migration Workflow

- All related parameters configured on the DSM will be migrated as is to the CipherTrust Manager.

Exceptions/Deviations

- Not applicable

Process Sets | Process Sets

Migration Workflow

- All related parameters configured on the DSM will be migrated as is to the CipherTrust Manager.

Exceptions/Deviations

- Not applicable

Signature Sets | Signature Sets

Migration Workflow

- All related parameters configured on the DSM will be migrated as is to the CipherTrust Manager.
- All the associated signatures under each signature set will be migrated to the CipherTrust Manager.
- Signature sets will retain their last signing state on the DSM on the CipherTrust Manager after migration.

Exceptions/Deviations

- Not applicable

Policy | Policy

Migration Workflow

- All related parameters configured on the DSM will be migrated as is to the CipherTrust Manager.
- All policy elements, that is, security rules, key rules, data transformation rules, LDT rules, and IDT rules will be migrated as is to the CipherTrust Manager.

Exceptions/Deviations

- Policies will be migrated with version 0 to the CipherTrust Manager irrespective of their versions on the DSM.
- Policy audit records on the DSM will NOT be migrated to the CipherTrust Manager.

Logging, QoS, and Syslog configuration | Profile

Migration Workflow

- Logging, QoS, and Syslog configuration on the DSM will be migrated as a joint resource under profiles on the CipherTrust Manager. Profiles will be associated with the clients and client groups based on the DSM configuration. Every client or client group will have the same configuration for these resources/parameters. However, they will be controlled through a single resource called profile on the CipherTrust Manager.

-
- All the host/host groups having the same configuration on the DSM will be associated with the **same profile** on the CipherTrust Manager.
 - After migration, clients and client groups can be associated with different profiles or the existing profile can be modified appropriately.
 - After migration, any modifications in profiles will affect all the clients and client groups linked with the profile.

Exceptions/Deviations

- Syslog configuration used only for the CTE agents will be migrated. Syslog configuration used by the DSM for its log upload will NOT be migrated.
- If migration of these configurations fails due to any reason (for example, invalid TLS configuration on the DSM), the default profile will be associated with the migrated hosts and host groups.

GuardPoints | GuardPoints

Migration Workflow

- *Client GuardPoints*
 - All related parameters configured on the DSM will be migrated as is to the CipherTrust Manager.
- *ClientGroup GuardPoints*
 - All valid GuardPoints under a host group will be migrated as is to the CipherTrust Manager.

Exceptions/Deviations

- Efficient Storage GuardPoints (ESG) will NOT be migrated.
- *ClientGroup GuardPoints*

GuardPoints having invalid configuration that might be created due to limited restrictions on the DSM will either be modified before migration or dropped from the migration, as described below.

- GuardPoints with Secure Start enabled on non-Windows paths will NOT be migrated.
 - GuardPoints with Transform Sparse Region enabled with a non-LDT policy will be modified by disabling Sparse Region and then migrated with rest of the configuration intact.
 - GuardPoints with Automount enabled on Windows path will be modified by disabling Automount and then migrated with rest of the configuration intact.
 - *ClientGroup - Client Association GuardPoints*
 - Client group GuardPoints that are propagated to all member clients will NOT be migrated. They will be created in background after the association between the client groups and clients is successfully migrated.
 - Any modifications made to such GuardPoints on the DSM after their propagation on the client, will NOT be
-

available after migration. GuardPoints with the configuration available under the client group will be propagated as is on the CipherTrust Manager.

Important Notes on Migration

- Hosts marked for deletion on the DSM will NOT be migrated to the CipherTrust Manager.
- All host groups will be migrated with an auto-generated password.
- GuardPoints of host groups will NOT be migrated as part of the migration activity. All GuardPoints of a host group will be automatically propagated in the background after successful association.

Any modifications made to host group GuardPoints on the DSM on the client level after their propagation on the client, will NOT be available after migration. GuardPoints with the configuration available under the client group will be propagated as is on the CipherTrust Manager.

For example, a host group GuardPoint **HG_GP1** is enabled under a host group and propagated to the host. Later this GuardPoint is disabled on the host on the DSM. After that, if such data is migrated to the CipherTrust Manager, the corresponding GuardPoint will be created as an enabled GuardPoint on the client group and client on the CipherTrust Manager. The GuardPoint is enabled at the client group level, so the GuardPoint is propagated accordingly.

- Policies will be migrated with version **0**. Policy audit records will NOT be migrated.
- Time Sets will NOT be migrated. They are not supported on the CipherTrust Manager.
- Syslog configuration used only for the CTE agents will be migrated. Syslog configuration used by the DSM for its log upload will NOT be migrated.
- Efficient Storage and CIFS GuardPoints will NOT be migrated.
- GuardPoints with Secure Start enabled on non-Windows paths will NOT be migrated.

Interpreting Migration Status

After you have triggered the migration, you can track its progress by running the `ksctl migration status` command. This command returns the overview of all the migrated resources classified in multiple categories, for example, Number of Processed, Number of Ignored, and Number of Failed (Error) with the high-level reasons why a particular resource is ignored or failed during the migration process.

```
./ksctl migrations status
```

```
{
  "id": "06d3efbe-590b-4e55-ace5-96e9ba486246",
  "overall_status": "Failed",
  "source": "DSM",
```

```

"keys_status": {
  "status": "Completed",
  "num_processed": 0,
  "num_failed": 0,
  "num_ignored": 2,
  "error_details": [
    "Key uniquetohost exists for version 0, ignoring it",
    "Key uniquetohost_auto exists for version 0, ignoring it",
  ]
},
"keys_links_status": {
  "status": "",
  "num_processed": 0,
  "num_failed": 0,
  "num_ignored": 0
},
"domains_status": {
  "status": "Completed",
  "num_processed": 0,
  "num_failed": 0,
  "num_ignored": 1,
  "error_details": [
    "Domain dom1 already exists, not recreating it",
  ]
},
"cte_client_status": {
  "status": "Completed",
  "num_processed": 10,
  "num_failed": 0,
  "num_ignored": 2,
  "ignore_details": [
    "CTE Client keyagent-one migration Skipped. Reason: Only FS agent Hos
ts to be migrated. Skipping Host: keyagent-one",
    "CTE Client 10.164.15.216 already exists, not recreating it",
  ]
},
...
...
...
"cte_guard_point_status": {
  "status": "Failed",
  "num_processed": 34,
  "num_failed": 1,
  "num_ignored": 2,
  "error_details": [
    "failed to create CTE GuardPoint /test-1/ Err: Server error [16/NCERR
ResourceNotFound: Resource not found]: . HTTP code:404: 404 Not Found",
  ],
  "ignore_details": [
    "CTE GuardPoint https://s3.amazonaws.com/amithenrytestbucket6;http
s://s3.amazonaws.com/amithenrytestbucket777 already exists, not recreating it",
    "CTE GuardPoint E:\\my_test_1\\ already exists, not recreating it",
  ]
},
"cte_client_domain_sharing_status":{
  "status": "Completed",
  "num_processed": 1,
  "num_failed": 0,
  "num_ignored": 0
}

```



```

    },
    "cte_client_group_domain_sharing_status": {
      "status": "Completed",
      "num_processed": 1,
      "num_failed": 0,
      "num_ignored": 0
    }
  }
}

```

Important Notes on Migration Status

- The **error_details** and **ignore_details** parameters provide the high-level information about the reason of failure or skipping the resource from migration. For detailed information, review the CipherTrust Manager logs and audit records (for each domain).
- For resources such as GuardPoint, the number shown in the status will NOT include the client group-client association GuardPoints available in the backup. They are created in the background after successful association of clients and client groups.
- Status shown as **Failed** indicates an error with the resources shown under **num_failed**. Other resources with no issues under the same category are successfully processed and are not affected with overall status as failed.

For example, GuardPoints of hosts marked for deletion are not migrated and end up in the error section, as the linked host is not migrated itself. It leads to the overall status as failed for the GuardPoint migration, but all other GuardPoints under **num_processed** are successfully migrated.

- CTE reports offer a better alternative to verify the resources migrated from the DSM.

Permissions

This section provides the complete list of permissions required by a CipherTrust Manager user to perform create, read, update, delete, upload, and download operations on CTE resources.

Create Operations

Operation	Required Permissions
Create a CTE client	• CreateClientCTE • ReadClientCTE • ReadProfileCTE
Create a standard policy with existing policy elements and an existing key	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE

Operation	Required Permissions
	• CreateKeyRuleCTE • ReadKeyMetaCTE • CreateKeyMetaCTE • UpdateKeyMetaCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadKey
Create an LDT policy with existing policy elements and an existing key	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE • CreateKeyRuleCTE • ReadKeyMetaCTE • CreateKeyMetaCTE • UpdateKeyMetaCTE • CreateLDTRuleCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • ReadKey
Create an IDT policy with existing policy elements and an existing key	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE • CreateKeyRuleCTE • ReadKeyMetaCTE • CreateKeyMetaCTE • UpdateKeyMetaCTE • CreateLDTRuleCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • ReadKey • CreateIDTRuleCTE • ReadIDTRuleCTE
Create a COS policy with existing policy elements and an existing key	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE • CreateKeyRuleCTE • ReadKeyMetaCTE • CreateKeyMetaCTE

Operation	Required Permissions
	• UpdateKeyMetaCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadKey
Create a standard policy with permission to create policy elements and using an existing key	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE • CreateKeyRuleCTE • ReadKeyMetaCTE • CreateKeyMetaCTE • UpdateKeyMetaCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadKey • CreateSignatureSetCTE • CreateUserSetCTE • CreateProcessSetCTE • CreateResourceSetCTE
Create an LDT policy with permission to create policy elements and using an existing key	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE • CreateKeyRuleCTE • ReadKeyMetaCTE • CreateKeyMetaCTE • UpdateKeyMetaCTE • CreateLDTRuleCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • ReadKey • CreateSignatureSetCTE • CreateUserSetCTE • CreateProcessSetCTE • CreateResourceSetCTE
Create an IDT policy with permission to create policy elements and using an existing key	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE • CreateKeyRuleCTE • ReadKeyMetaCTE

Operation	Required Permissions
	• CreateKeyMetaCTE • UpdateKeyMetaCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadKey • CreateIDTRuleCTE • ReadIDTRuleCTE • CreateSignatureSetCTE • CreateUserSetCTE • CreateProcessSetCTE • CreateResourceSetCTE
Create a COS policy with permission to create policy elements and using an existing key	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE • CreateKeyRuleCTE • ReadKeyMetaCTE • CreateKeyMetaCTE • UpdateKeyMetaCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadKey • CreateSignatureSetCTE • CreateUserSetCTE • CreateProcessSetCTE • CreateResourceSetCTE
Create a client group	• CreateProfileCTE • ReadProfileCTE • CreateClientGroupCTE • ReadClientGroupCTE
Create a signature set superset	• CreateSignatureSetCTE • ReadSignatureSetCTE • ReadClientCTE • CreateSignatureCTE • ReadSignatureCTE
Create a user set superset	• CreateUserSetCTE • ReadUserSetCTE • ReadClientCTE
Create a process set superset	• CreateProcessSetCTE • ReadProcessSetCTE • CreateProcessSetSignatureSetAssociationCTE • CreateSignatureSetCTE • ReadSignatureSetCTE • ReadClientCTE • CreateSignatureCTE • ReadSignatureCTE • ReadProcessSetSignatureSetAssociationCTE • ReadProcessSetResourceSetAssociationCTE • CreateProcessSetResourceSetAssociationCTE

Operation	Required Permissions
Create a resource set	• CreateResourceSetCTE • ReadResourceSetCTE • ReadClientCTE
Create a CTE Profile	• CreateProfileCTE • ReadProfileCTE
Create an LDT Communication Group	• CreateLDTGroupCommServiceCTE • ReadLDTGroupCommServiceCTE • CreateLDTGroupCommServiceClientAssociationCTE • ReadLDTGroupCommServiceClientAssociationCTE • ReadClientsCTE
Create client group - client association	• CreateClientCTE • ReadClientCTE • UpdateClientCTE • CreateClientGroupCTE • ReadClientGroupCTE • UpdateClientGroupCTE • CreateClientGroupClientAssociationCTE • ReadClientGroupClientAssociationCTE • UpdateClientGroupClientAssociationCTE
Create a Storage Group	• CreateProfileCTE • ReadProfileCTE • CreateCSISStorageGroupCTE • ReadCSISStorageGroupCTE
Create Storage Group - client association	• CreateClientCTE • ReadClientCTE • UpdateClientCTE • CreateCSISStorageGroupCTE • ReadCSISStorageGroupCTE • UpdateCSISStorageGroupCTE • CreateCSISStorageGroupClientAssnCTE • ReadCSISStorageGroupClientAssnCTE
Add a GuardPolicy to a Storage Group	• CreateCSISStorageGroupCTE • ReadCSISStorageGroupCTE • UpdateCSISStorageGroupCTE • ReadPolicyCTE • UpdatePolicyCTE • ReadGuardPointCTE • UpdateGuardPointCTE • CreateGuardPointCTE
Create signatures in a signature set	• UpdatePolicyElementsCTE • ReadSignatureSetCTE • UpdateSignatureSetCTE • ReadSignatureCTE • CreateSignatureCTE • UpdateSignatureCTE • ReadSecurityRuleCTE • ReadProcessSetCTE • ReadSignatureRuleCTE • ReadGuardPointCTE • ReadClientCTE
Create a client group / client GuardPoint /	• ReadPolicyCTE

Operation	Required Permissions
Create GuardPoints using a CSV file	• ReadSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • CreatePolicyCTE • ReadClientGroupCTE • CreateGuardPointCTE • ReadClientCTE
Create a new security rule for a policy	• ReadKeyRuleCTE • ReadPolicyCTE • ReadResourceSetCTE • ReadGuardPointCTE • CreateSecurityRuleCTE • ReadSecurityRuleCTE • ReadUserSetCTE • ReadProcessSetCTE • UpdatePolicyCTE
Create a new key rule/ LDT rule / transformation rule for a policy	• UpdatePolicyCTE • ReadPolicyCTE • ReadSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • ReadResourceSetCTE • ReadGuardPointCTE • CreateKeyRuleCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadClientAndResourceMappingReadCTE
Create a new signature rule	• UpdatePolicyCTE • ReadPolicyCTE • ReadSignatureSetCTE • CreateSignatureRuleCTE • UpdatePolicyCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE

Update Operations

Operation	Required Permissions
Update an unregistered client / Enable capabilities/ Reset CTE client password	• ReadClientCTE • UpdateClientCTE
Update a client profile	• CreateProfileCTE • ReadProfileCTE • UpdateProfileCTE
Update authentication binaries for a client and a client group	• ReadClientCTE • UpdateClientCTE • ReadClientGroupCTE • UpdateClientGroupCTE • ReadClientGroupClientAssociationCTE

Operation	Required Permissions
Update a CTE policy	• ReadPolicyCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • ReadSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • CreatePolicyCTE • CreateKeyRuleCTE • ReadKeyMetaCTE • CreateKeyMetaCTE • UpdateKeyMetaCTE • CreateLDTRuleCTE • CreateSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • ReadKey • UpdatePolicyCTE • UpdateKeyRuleCTE • UpdateLDTRuleCTE • UpdateSecurityRuleCTE • UpdateIDTRuleCTE
Update a CTE client group	• ReadClientCTE • UpdateClientCTE • ReadClientGroupCTE • UpdateClientGroupCTE • CreateClientGroupClientAssociationCTE • ReadClientGroupClientAssociationCTE • UpdateClientGroupClientAssociationCTE
Update a signature set	• ReadSignatureSetCTE • ReadClientCTE • CreateSignatureCTE • ReadSignatureCTE • UpdateSignatureSetCTE • UpdateSignatureCTE • ReadClientAndResourceMappingReadCTE • UpdatePolicyElementsCTE • ReadPolicyCTE • ReadProcessSetSignatureSetAssociationCTE • ReadSignatureRuleCTE • ReadProcessSetCTE
Update a user set	• ReadUserSetCTE • UpdateUserSetCTE • ReadClientCTE • ReadClientAndResourceMappingReadCTE • UpdatePolicyElementsCTE
Update a process set	• UpdatePolicyElementsCTE • ReadProcessSetCTE • UpdateProcessSetCTE • ReadSignatureSetCTE • ReadProcessSetSignatureSetAssociationCTE • CreateProcessSetSignatureSetAssociationCTE • ReadProcessSetResourceSetAssociationCTE • CreateProcessSetResourceSetAssociationCTE

Operation	Required Permissions
Update a resource set	• ReadResourceSetCTE • UpdateResourceSetCTE • ReadClientCTE • ReadCTEClientAndResourceMappingRead • UpdatePolicyElementsCTE
Update a CTE profile	• ReadProfileCTE • UpdateProfileCTE • ReadUserSetCTE • ReadProcessSetCTE
Update an LDT Communication Group	• ReadLDTGroupCommServiceCTE • UpdateLDTGroupCommServiceCTE • ReadLDTGroupCommServiceClientAssociationCTE • ReadClientCTE
Update a CSI Storage Group	• ReadClientCTE • UpdateClientCTE • ReadCSIStorageGroupCTE • UpdateCSIStorageGroupCTE • ReadCSIStorageGroupClientAssnCTE • CreateCSIStorageGroupClientAssnCTE
Update a GuardPolicy in a Storage Group	• ReadClientCTE • UpdateClientCTE • ReadCSIStorageGroupCTE • UpdateCSIStorageGroupCTE • ReadPolicyCTE • UpdatePolicyCTE • ReadGuardPointCTE • UpdateGuardPointCTE
Modify existing Designated Primary Set parameters	• ReadClientGroupCTE • UpdateClientGroupCTE
Send an LDT suspend / resume request to a CTE client	• ReadClientCTE
Send an LDT suspend / resume request to a CTE client group	• ReadClientGroupCTE • ReadClientGroupClientAssociationCTE • UpdateClientGroupCTE
Turn off Preserve Sparse Region	• ReadGuardPointCTE • ReadPolicyCTE • ReadSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • ReadClientGroupCTE • UpdateGuardPointCTE • ReadClientCTE
Update Early Access on a client group GuardPoint	• ReadClientGroupCTE • ReadGuardPointCTE • UpdateGuardPointCTE
Update Early Access on a client GuardPoint	• ReadClientCTE • ReadGuardPointCTE • UpdateGuardPointCTE
Unguard single / bulk GuardPoint(s) from a client	• ReadClientGroupCTE

Operation	Required Permissions
group	• ReadGuardPointCTE • DeleteGuardPointCTE
Unguard a client GuardPoint	• ReadClientCTE • ReadGuardPointCTE • DeleteGuardPointCTE
Update a client group GuardPoint parameters	• ReadClientGroupCTE • ReadGuardPointCTE • DeleteGuardPointCTE
Update a client GuardPoint	• UpdateGuardPointCTE • ReadClientCTE • ReadGuardPointCTE • DeleteGuardPointCTE • UpdateClientCTE • ReadProfileCTE • ReadGuardPointCTE • ReadClientGroupClientAssociationCTE • ReadClientGroupCTE • ReadPolicyCTE • CreateGuardPointCTE • ReadKernelVersionCTE
Add a new Designated Primary Set (DPS) to a client group	• CreateClientGroupCTE • ReadClientGroupCTE
Add client(s) to client group	• ReadClientGroupCTE • UpdateClientCTE • ReadGuardPointCTE • ReadClientCTE • CreateClientGroupClientAssociationCTE • ReadSignatureSetCTE
Reset password for a CTE client group	• ReadClientGroupCTE • UpdateClientGroupCTE • ReadClientGroupClientAssociationCTE • ReadClientCTE • UpdateClientCTE
Update client settings for a client group	• ReadClientGroupCTE • UpdateClientGroupCTE • ReadSignatureSetCTE • ReadClientGroupClientAssociationCTE • ReadClientCTE
Update client group password	• PermissionCTEClientPasswordRead • PermissionCTEClientPasswordUpdate
Update a CTE client	• ReadClientCTE • UpdateClientCTE • ReadProfileCTE • ReadGuardPointCTE • ReadClientGroupClientAssociationCTE • ReadClientGroupCTE • ReadPolicyCTE • CreateGuardPointCTE • ReadKernelVersionCTE

Operation	Required Permissions
Update client password	• ReadClientPasswordCTE • UpdateClientPasswordCTE
Update the list of signatures to be added to the signature set	• UpdatePolicyElementsCTE • ReadSignatureSetCTE • UpdateSignatureSetCTE • ReadSignatureCTE • CreateSignatureCTE • UpdateSignatureCTE • ReadSecurityRuleCTE • ReadProcessSetCTE • ReadSignatureRuleCTE • ReadGuardPointCTE • ReadClientCTE
Update a user in a user set	• UpdatePolicyElementsCTE • ReadUserSetCTE • UpdateUserSetCTE
Update a security rule	• UpdatePolicyCTE • ReadPolicyCTE • ReadGuardPointCTE • UpdateSecurityRuleCTE • ReadSecurityRuleCTE • UpdateSecurityRuleCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • UpdatePolicyCTE
Update a Key rule	• UpdatePolicyCTE • ReadPolicyCTE • ReadGuardPointCTE • ReadResourceSetCTE • ReadKeyRuleCTE • UpdateKeyRuleCTE
Update a signature rule	• UpdatePolicyCTE • ReadPolicyCTE • ReadGuardPointCTE • ReadSignatureRuleCTE • UpdateSignatureRuleCTE • ReadSignatureSetCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE
Update an LDT key rule / Transformation rule	• UpdatePolicyCTE • ReadPolicyCTE • ReadResourceSetCTE • ReadLDTRuleCTE • UpdateLDTRuleCTE • ReadGuardPointCTE • UpdateKeyRuleCTE • ReadClientAndResourceMappingReadCTE • ReadUserSetCTE • ReadProcessSetCTE

Operation	Required Permissions
Add a client to an LDT Communication Group	• ReadLDTGroupCommServiceCTE • ReadClientCTE • CreateLDTGroupCommServiceClientAssociationCTE • UpdateClientCTE

Read Operations

Operation	Required Permissions
Read a CTE client / all operations for agent information	• ReadClientCTE
Read a CTE client and its profile	• ReadClientCTE • ReadProfileCTE
Read a CTE policy	• ReadPolicyCTE • ReadCTEClientAndResourceMappingRead • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSet • ReadSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • ReadIDTRuleCTE
Read a CTE client group	• ReadClientGroupCTE
Read a CTE client group and its profile	• ReadClientGroupCTE • ReadProfileCTE
Get client group - client association	• ReadClientCTE • ReadClientGroupCTE • ReadClientGroupClientAssociationCTE
Read a signature set	• ReadSignatureSetCTE
Read a user set	• ReadUserSetCTE
Read a process set	• ReadProcessSetCTE • ReadProcessSetSignatureSetAssociationCTE
Read a resource set	• ReadResourceSetCTE
Read signatures	• ReadSignatureCTE
Read a CTE profile	• ReadProfileCTE
Read an LDT Communication Group	• ReadLDTGroupCommServiceCTE
Read all reports	• ReadClientsReportCTE • ReadClientsKeysReportCTE • ReadClientsProfileReportCTE • ReadClientsGuardStatusReportCTE • ReadPolicyKeysReportCTE • ReadClientsPoliciesReportCTE • ReadGuardPointsReportCTE
Read a CSI Storage Group	• ReadCSIStorageGroupCTE

Operation	Required Permissions
Read clients in a Storage Group	• ReadClientCTE • ReadCSISStorageGroupCTE • ReadCSISStorageGroupClientAssnCTE
Get Storage Group - client association	• ReadClientCTE • ReadCSISStorageGroupCTE • ReadCSISStorageGroupClientAssnCTE
Read GuardPolicies in a Storage Group	• ReadCSISStorageGroupCTE • ReadPolicyCTE • ReadGuardPointsCTE
Get details of an existing / all Designated Primary Set(s) associated with a client group	• ReadGuardPointCTE • ReadClientGroupCTE
Get a kernel compatibility matrix	• ReadKernelVersionCTE
Get Challenge Response	• ReadClientCTE
Get details of client group GuardPoint(s)	• ReadGuardPointCTE • ReadClientGroupCTE
Get client GuardPoint(s) / get GuardPoint status	• ReadClientCTE • ReadGuardPointCTE
Get policy and user set association	• ReadUserSetCTE • ReadClientAndResourceMappingReadCTE
Get policy and process set association	• ReadProcessSetCTE • ReadClientAndResourceMappingReadCTE • ReadPolicyCTE
Get policy and resource set association	• ReadResourceSetCTE • ReadClientAndResourceMappingReadCTE • ReadPolicyCTE
Get the list of signatures added to a signature set	• ReadSignatureSetCTE • ReadSignatureCTE
Get latest client capabilities / query status update	• ReadClientCTE • UpdateClientCTE
Send / check / cancel a signature signing request to the client	• ReadSignatureSetCTE • ReadClientCTE
Get audit records of a policy	• ReadPolicyCTE
Get security rules	• ReadPolicyCTE • ReadSecurityRuleCTE
Get signature rules	• ReadPolicyCTE • ReadSignatureRuleCTE
Get a key rule / transformation rule	• ReadPolicyCTE • ReadKeyRuleCTE
Get an LDT key rule	• ReadPolicyCTE • ReadLDTRuleCTE
Get clients in the LDT Communication Group	• ReadLDTGroupCommServiceCTE • ReadClientCTE • CreateLDTGroupCommServiceClientAssociationCTE

Operation	Required Permissions
	• UpdateClientCTE

Delete Operations

Operation	Required Permissions
Delete a CTE client	• ReadClientCTE • DeleteClientCTE • UpdateClientCTE • ReadClientGroupCTE • ReadClientGroupClientAssociationCTE • DeleteClientGroupClientAssociationCTE • UpdateGuardPointCTE • ReadGuardPointCTE • DeleteGuardPointCTE
Unenroll a CTE client	• ReadClientCTE • UnenrollClientCTE • DeleteCSIClientCTE • ReadClientsPoliciesReportCTE • UpdateClientCTE • ReadGuardPointCTE • UpdateGuardPointCTE • ReadLDTGroupCommServiceCTE • DeleteLDTGroupCommServiceClientAssociationCTE • ReadLDTGroupCommServiceClientAssociationCTE
Delete a CTE policy	• DeletePolicyCTE • ReadPolicyCTE • ReadSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE
Delete a CTE client group	• ReadClientGroupCTE • ReadClientGroupClientAssociationCTE • ReadClientCTE • DeleteClientGroupCTE
Delete a signature set	• ReadSignatureSetCTE • DeleteSignatureSetCTE • DeletePolicyElementsCTE • ReadClientCTE • ReadClientGroupCTE
Delete a user set	• ReadUserSetCTE • DeleteUserSetCTE
Delete a process set	• ReadProcessSetCTE • DeleteProcessSetCTE • DeletePolicyElementsCTE
Delete a resource set	• ReadResourceSetCTE • DeleteResourceSetCTE • DeletePolicyElementsCTE
Delete a CTE profile	• ReadProfileCTE • DeleteProfileCTE

Operation	Required Permissions
Delete an LDT Communication Group	• ReadLDTGroupCommServiceCTE • ReadLDTGroupCommServiceClientAssociationCTE • DeleteLDTGroupCommServiceCTE
Delete client(s) from an LDT Communication Group	• ReadLDTGroupCommServiceCTE • ReadClientCTE • ReadLDTGroupCommServiceClientAssociationCTE • DeleteLDTGroupCommServiceClientAssociationCTE • UpdateClientCTE
Remove ClientGroup - Client association	• ReadClientCTE • UpdateClientCTE • ReadClientGroupCTE • UpdateClientGroupCTE • ReadClientGroupClientAssociationCTE • UpdateClientGroupClientAssociationCTE • DeleteClientGroupClientAssociationCTE • ReadSignatureSetCTE • ReadGuardPointCTE
Delete a CSI Storage Group	• ReadCSIStorageGroupCTE • DeleteCSIStorageGroupCTE
Delete a CSI client from a Storage Group	• ReadClientCTE • UpdateClientCTE • ReadCSIStorageGroupCTE • UpdateCSIStorageGroupCTE • ReadCSIStorageGroupClientAssnCTE • DeleteCSIStorageGroupClientAssnCTE
Delete a GuardPolicy from a CSI Storage Group	• ReadCSIStorageGroupCTE • UpdateCSIStorageGroupCTE • DeletePolicyCTE • ReadPolicyCTE • ReadGuardPointsCTE • DeleteGuardPointCTE
Delete the existing Designated Primary Set associated with a client group	• ReadSignatureSetCTE • ReadClientCTE • ReadClientGroupCTE • DeletePolicyElementsCTE • DeleteSignatureSetCTE
Delete a kernel compatibility matrix	• ReadKernelVersionCTE • DeleteKernelVersionCTE
Delete sources from a signature set	• ReadSignatureSetCTE • UpdatePolicyElementsCTE • UpdateSignatureSetCTE • ReadSignatureRuleCTE • ReadClientAndResourceMappingReadCTE • ReadPolicyCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE • UpdatePolicyCTE • ReadClientCTE • ReadProcessSetSignatureSetAssociationCTE

Operation	Required Permissions
Delete a signature from a signature set	• ReadSignatureSetCTE • UpdatePolicyElementsCTE • ReadSignatureCTE • DeleteSignatureCTE • ReadSecurityRuleCTE • ReadProcessSetCTE • ReadSignatureRuleCTE • ReadGuardPointCTE • ReadClientCTE
Delete a user from a user set	• UpdatePolicyElementsCTE • ReadUserSetCTE • UpdateUserSetCTE
Delete a process from a process set	• UpdatePolicyElementsCTE • ReadProcessSetCTE • UpdateProcessSetCTE • ReadProcessSetCTE • ReadSignatureSetCTE
Delete resources from a resource set	• UpdatePolicyElementsCTE • ReadResourceSetCTE • UpdateResourceSetCTE
Delete a Syslog server from a profile	• UpdateProfileCTE • ReadProfileCTE
Delete a security rule	• UpdatePolicyCTE • ReadPolicyCTE • ReadSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • DeleteSecurityRuleCTE • ReadClientAndResourceMappingReadCTE • ReadPolicyCTE • UpdatePolicyCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE
Delete a key rule / transformation rule	• UpdatePolicyCTE • ReadKeyRuleCTE • ReadPolicyCTE • ReadSecurityRuleCTE • ReadLDTRuleCTE • ReadGuardPointCTE • DeleteKeyRuleCTE • ReadClientAndResourceMappingReadCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE
Delete a signature rule	• UpdatePolicyCTE • ReadPolicyCTE • ReadGuardPointCTE • ReadSignatureRuleCTE • DeleteSignatureRuleCTE • ReadUserSetCTE

Operation	Required Permissions
	• ReadProcessSetCTE • ReadResourceSetCTE
Delete an LDT key rule	• UpdatePolicyCTE • ReadPolicyCTE • ReadSecurityRuleCTE • ReadKeyRuleCTE • ReadLDTRuleCTE • ReadLDTRuleCTE • ReadClientAndResourceMappingReadCTE • DeleteLDTRuleCTE • ReadUserSetCTE • ReadProcessSetCTE • ReadResourceSetCTE
Delete an IDT rule	• DeleteIDTRuleCTE

Upload Operations

Operation	Required Permissions
Upload the kernel compatibility matrix	• ReadKernelVersionCTE • CreateKernelVersionCTE

Download Operations

Operation	Required Permissions
Download all reports	• ReadClientsReportCTE • ReadClientsKeysReportCTE • ReadClientsProfileReportCTE • ReadClientsGuardStatusReportCTE • ReadPolicyKeysReportCTE • ReadClientsPoliciesReportCTE • ReadGuardPointsReportCTE

Quorum Control

CTE supports the quorum feature of the CipherTrust Manager. A CipherTrust Manager administrator can configure a quorum policy to have multiple approvers for supported operations. After the quorum policy is configured for an operation, all the approvers need to approve the operation before it can be successfully executed.

Refer to [Quorums](#) for details on the quorum feature of the CipherTrust Manager.

Supported Operations

Operation	Authorized Group for Approval
DeleteClientCTE	CTE Admins

Operation	Authorized Group for Approval
DeleteClientGroupCTE	CTE Admins
DeleteCSIStorageGroupCTE	CTE Admins
DeleteGuardPointCTE	CTE Admins
DeletePolicyCTE	CTE Admins
DeletePolicyElementsCTE	CTE Admins
DeleteProfileCTE	CTE Admins
UpdateClientGroupCTE	CTE Admins
UpdateCSIStorageGroupCTE	CTE Admins
UpdateGuardPointCTE	CTE Admins
UpdatePolicyCTE	CTE Admins
UpdatePolicyElementsCTE	CTE Admins
UpdateProfileCTE	CTE Admins
UpdateClientPasswordCTE	CTE Admins
UpdateClientGroupPasswordCTE	CTE Admins

Note

CTE for Kubernetes clients with healthy status cannot be deleted by the CipherTrust Manager Administrator. Only the CTE Agent can trigger their deletion. So, quorum is not supported for CTE for Kubernetes clients.

Supported APIs and Resources

Operation	APIs	Applicable to	Remarks
Delete clients (DeleteClientCTE)	- Single client deletion - Bulk client deletion	- FS (CTE and RWP) clients - CTE-U (CTE UserSpace) clients	Bulk client deletion behavior: Quorums are created for all resources. The administrators (approvers) need to approve quorum for all resources. Do not modify/delete the requested clients after a quorum request is created for bulk deletion. To make any changes, ensure that the quorum request is deleted.
Delete client groups (DeleteClientGroupCTE)	Delete client groups	- NON-CLUSTER groups - HDFS groups	-

Operation	APIs	Applicable to	Remarks
Update client groups (UpdateClientGroupCTE)	- Update client groups - Send LDT suspend/resume request to the CTE client groups	- NON- CLUSTER groups - HDFS groups	-
Delete client GuardPoints (DeleteGuardPointCTE)	- Single GuardPoint deletion - Bulk GuardPoint deletion	- FS (CTE and RWP) GuardPoints - CTE-U (CTE UserSpace) GuardPoints	Bulk GuardPoint deletion behavior: Quorums are created for all resources. The administrators (approvers) need to approve quorum for all resources. Do not modify/delete the requested GuardPoints after a quorum request is created for bulk deletion. To make any changes, ensure that the quorum request is deleted.
Delete client group GuardPoints (DeleteGuardPointCTE)	- Single GuardPoint deletion - Bulk GuardPoint deletion	- NON- CLUSTER groups - HDFS groups	Bulk client group GuardPoint deletion behavior: Quorums are created for all resources. The administrators (approvers) need to approve quorum for all resources. Do not modify/delete the requested GuardPoints after a quorum request is created for bulk deletion. To make any changes, ensure that the quorum request is deleted.
Update client GuardPoints (UpdateGuardPointCTE)	Single GuardPoint update	- FS (CTE and RWP) GuardPoints - CTE-U (CTE UserSpace) GuardPoints	Bulk update is not supported.
Update client group GuardPoints (UpdateGuardPointCTE)	Single GuardPoint update	- NON- CLUSTER groups - HDFS groups	Bulk update is not supported.
Delete Kubernetes storage group GuardPolicies (DeleteGuardPointCTE)	Delete GuardPolicies from Kubernetes storage groups	Kubernetes clients	-
Update Kubernetes storage group GuardPolicies (UpdateGuardPointCTE)	Single Kubernetes storage group GuardPolicy update	Kubernetes clients	-
Delete Kubernetes storage groups (DeleteCSISStorageGroup)	Single Kubernetes storage group deletion from Kubernetes clients	Kubernetes clients	-

Operation	APIs	Applicable to	Remarks
CTE)			
Update policy (UpdatePolicyCTE)	• Update a policy • Add, update, delete key rules • Add, update, delete security rules • Add, update, delete data transformation rules • Add, update, delete LDT rules • Update IDT rules • Add, update, and delete signature rules	• LDT policies • IDT policies • COS policies • CTE for Kubernetes policies • STANDARD policies	-
Delete policy elements (DeletePolicyElementsCTE)	Delete policy elements • Delete a resource set • Delete a user set • Delete a process set • Delete a signature set	Delete an element	Bulk deletion is not supported.
Update policy elements (UpdatePolicyElementsCTE)	Update policy elements • Update a resource set • Update a user set • Update a process set • Update a signature set • Add or remove a resource from a resource set • Add or remove a user from a user set • Add or remove a process from a process set • Add or remove a signature from a signature set	Single element update	Bulk update is not supported.
Delete profiles (DeleteProfileCTE)	Delete a profile	-	Bulk deletion is not supported.
Update profiles (UpdateProfileCTE)	Update a profile	-	Bulk update is not supported.

Workflow

This section provides the basic flow of the quorum process for the *DeleteClientCTE* operation. The process is similar for all the supported operations. This section assumes that a quorum policy, which requires two approvals for the DeleteClientCTE operation, is activated on the CipherTrust Manager.

1. Attempt to delete a client:
 - a. Open the **Transparent Encryption** application.
 - b. Click **Clients > Clients**.

- c. Under **Client Name**, click the overflow icon () corresponding to the client you want to delete.
- d. Click **Delete**. A dialog box appears prompting to confirm the action.
- e. Click **Delete**.

A dialog box appears stating that a quorum request has been made, and you need to get approval for this action.

The Quorum ID is displayed on the dialog box.

2. View details of the quorum.

- a. On the Requesting dialog box, click the **Go to Quorums Screen** link.

Alternatively, click **OK** on the Requesting dialog box and navigate to the Quorums page of the CipherTrust Manager GUI.

The Quorums page contains the Active Quorums and Inactive Quorums tabs. These tabs show quorum details such as the operation name, the requester who initiated the quorum, status and state of the quorum, and the quorum actions.

- b. Under the **Operation** column, expand **DeleteClientCTE: <client-name>**.

Information about the client to be deleted and the quorum approvers is displayed on the Quorum Client Info and Quorum Approvers tabs respectively.

- c. Click the **Quorum Approvers** tab to view details about the quorum approvers.

3. Approve the quorum. You, another CTE administrator, or a CipherTrust Manager Administrator can approve the quorum.

To approve the quorum:

- a. Under **Actions**, click the **Approve Quorum** icon () next to the desired **DeleteClientCTE: <client-name>** operation. The Approve Quorum dialog box is displayed.

If you are the last approver, the dialog box displays the message, *"This is the final approval. If you approve the quorum, the operation will be executed automatically."*

- b. (Optional) Specify a **Reason** for the approval.
- c. Click **Confirm** to approve the quorum. A message stating that the quorum is successfully approved is displayed.

Similarly, all the approvers need to approve the quorum for successful execution of the operation. The number of approvers is configured under **Approvals Needed** on the **Admin Settings > Quorum Policy** page.

When the last approver approves the quorum, the operation is removed from the Active Quorums tab and the client is deleted from the Clients page. The executed operation is displayed on the Inactive Quorums tab of

the Quorums page with the **executed** state.

The logs of the operation are available on the **Records > Server Records** page.

4. Verify the client deletion.
 - a. Open the **Transparent Encryption** application.
 - b. Click **Clients > Clients**.

Notice that the client is no longer listed on the Clients page. This indicates successful deletion of the client.

Confidential Computing

Confidential Computing is a cloud computing technology that can isolate and protect data on Confidential Virtual Machines (CVMs) or Trusted Domains (TDs) to protect them from a broad range of software attacks. Confidential Computing ensures that all data operations are executed within a Trusted Execution Environment.

Confidential Computing provisioning requires an attestation authority, such as Intel Trust Authority, to attest the CVMs or TDs and create a Trusted Execution Environment around them.

CTE makes Confidential Computing provisioning seamless, without the need to install or configure any additional tools on CTE clients. CTE together with CipherTrust Manager takes care of the attestation process to provision Confidential Computing on VMs running on CTE agents. If attestation fails, any access to the encrypted data guarded by CTE is prohibited.

Requirements & Specifications

Refer to [Requirements & Specifications](#) for details.

Prerequisite

Ensure that **Confidential Computing** is enabled for the CTE client to register it with the CipherTrust Manager. Refer to [prerequisites](#) for details.

Note

Ensure that the clocks on the CipherTrust Manager, client, and Intel server are synchronized. If they are not, [configure a Network Time Protocol Server](#).

Activate Confidential Computing on CTE Clients

To activate Confidential Computing on a CTE client, complete the following steps:

1. Create **Attestation Authority** connections in the CipherTrust Manager.

Note

To provision Confidential Computing on CTE clients, you require one **admin connection** (connection with administrator privileges) and one **non-admin connection** (connection without administrator privileges). The admin connection is necessary to retrieve the policies from the Attestation Authority, while the details of the non-admin connection are shared with the CTE agents.

- a. Log on to CipherTrust Manager.
- b. Go to **Access Management > Connections**.
- c. Select **+ Add Connection**.
- d. In the **Select Connection Type** section, select **More** and then select **Attestation Authority** from the **Select Connection** dropdown.
- e. Click **Next**.
- f. In the **General Info** section, enter the **Name** and **Description** for the connection.
- g. Click **Next**.
- h. In **Configure Connection** section, enter the following details:

Field Name	Description
URL	Provide the URL for connecting to the Attestation Authority.
Base URL	Provide base URL for the Attestation Authority.
API Key	Provide the allocated API key to establish connection with Attestation Authority.
Meta	Provide meta information in the JSON format.

Select the **Admin User** checkbox to create a connection with administrator privileges. By default, a connection without administrator privileges will be created.

- i. Click **Next**.
- j. In **Add Products** section, select the **CTE** checkbox.
- k. Click **Add Connection**.

To edit or delete the created connection, see [Attestation Authority Connection](#).

2. Create a Client Profile associated with above connection.
 - a. In CipherTrust Manager, click **Access Management > Add Client Profile**.
 - b. Enter **Profile Name** and **Description**.
 - c. Select **CA Type**: Local or External.
 - d. Select the respective Local or External CA in **Select <Local or External> CA**.
 - e. Enter the **Certificate Duration** for which the CA certificate will remain active.
 - f. Expand the **CONFIDENTIAL COMPUTING** section and add the following details:
 - a. Select **Attestation Authority Identifier**. Currently, only Intel Trust Authority (ITA) is supported.
 - b. Select **Cloud Provider**. The options are Azure and Google Cloud.
 - c. Select a non-admin connection in the **Attestation Connection** field.
 - d. Select an admin connection in the **Admin Connection** field. By default, this field remains blank. Selecting a value in this field allows you to select policies in the **Policy Names** field.

Note

Admin and non-admin type connections should belong to the same Attestation Authority.

- e. Select the policies in the **Policy Names** field. These policies are fetched from the Attestation Authority server. You can select multiple policies.
- f. Keep the default values for the remaining fields.
- g. (Optional) Click **Reset confidential computing form** to reset all the fields to the default values and input the information again.
- g. Click **Add Client Profile**.

To update or delete the created client profile, see [Managing Client Profiles](#).

3. [Create a registration token](#) associated to the above Client Profile. Retain this registration token.
4. Use the registration token during [installation and registration of CTE agents](#).

Ransomware Protection

Ransomware is a type of malicious software that is designed to block access to a computer system until a sum of money is paid. CTE Agent supports detection of Ransomware and protection of sensitive data from Ransomware.

Ransomware Protection is applied at GuardPoint, that is, at volume level for Windows and directory level for Linux. CTE Agent monitors the GuardPoints, analyzes the data, and looks for processes that might perform suspicious activities on the sensitive data. Examples of such processes are processes that try to encrypt files, open thousands of files, or change permissions on files. If a process displays suspicious behavior, then it is either blocked or audited (that is, flagged in a log file). The action taken is preconfigured by the CTE administrator in the [profile](#) linked to the client.

Licensing

Ransomware Protection is supported with RWP-enabled CTE clients. A CTE for Ransomware Protection license must be activated on the CipherTrust Manager to register an RWP-enabled CTE client. Refer to [CTE Licensing Model](#) for details.

Protection Modes

Based on the capabilities enabled during CTE registration, CTE clients can support the following protection modes:

- **Filesystem Protection (CTE):** Allows you to protect and encrypt files with policies.
- **Ransomware Protection (RWP) Only:** CTE is deployed to monitor GuardPoints for suspicious behavior from processes, and supports auditing or blocking of the processes.
- **Both filesystem and Ransomware Protection (CTE RWP):** Protects GuardPoints from Ransomware and allows you to protect and encrypt files with policies.

Ransomware Protection is available for *all* types of GuardPoints in the **RWP** and **CTE RWP** protection modes.

- The **RWP** protection mode doesn't support CTE file *encryption* and *protection*. Therefore, only Ransomware Protection Guardpoints are available in this mode, and these GuardPoints don't require any protection policies.
- The **CTE RWP** protection mode supports both Ransomware Protection and CTE file encryption. Therefore, all types of GuardPoints are available in the **CTE RWP** protection mode.

Use the [Ransomware Protection GuardPoints](#) to monitor or block Ransomware access attempts to the sensitive data stored on the CTE clients.

Protecting Non-Sensitive Data

Use the Ransomware Protection mode to protect systems that don't contain sensitive data, but have access to your network.

A use case of this scenario is when you have users with laptops who frequently use your network and access servers on it, but they do not have any sensitive data locally on their laptops. A system like this might belong to a salesperson who travels and frequently uses other networks to access the internet. When such users log on to your network, they access the sales network server and upload data to it. They could easily pick up a Ransomware from another network and accidentally upload it to your company's network.

Using the Ransomware Protection mode would protect the data on the GuardPoints from being infected with Ransomware.

Protecting Sensitive Data

The Ransomware Protection mode protects data on servers and endpoints from Ransomware attacks by auditing and blocking malicious IPs. Users can strengthen the security posture with CTE access and encryption policies and Ransomware protection for complete control on their data.

To protect sensitive data against Ransomware:

1. Ensure that the CTE Ransomware Protection license is activated and available on the CipherTrust Manager. Refer to [CTE Licensing Model](#) for details.
2. Install the CTE Agent with the Ransomware Protection capability enabled. The Ransomware Protection support uses the same registration process as CTE clients. Refer to [CTE Agent Linux and Windows Quick Start Guide](#) for information on installing and configuring CTE Agents.
3. Configure the Ransomware Protection settings in the linked client profile. Refer to [Setting Ransomware Protection Configuration](#) for details.
4. Create a Ransomware Protection GuardPoint on the volume for Windows and on the directory for Linux. Refer to the [Creating Ransomware GuardPoints](#) for details.

Disabling Ransomware Protection

To disable Ransomware Protection for all GuardPoints on the clients linked with a profile.

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings > Profiles**.
3. Under **Name**, click the desired profile.
4. Expand **RANSOMWARE PROTECTION CONFIGURATION**.
5. Select the **Operation** to **Disable**.

Note

- When you change the operation to **Disable** in a profile, Ransomware Protection for all GuardPoints on the linked clients is disabled.
- When you change the *profile* of a client to another profile with the operation set to **Disable**, Ransomware Protection for all GuardPoints on the client is disabled.

6. Click **Update**.

File Activity Monitoring (FAM)

File Activity Monitoring (FAM) catalogs, monitors, and secures unstructured data (files). It provides insights into data location, ownership, access history, permissions, protection, sharing, and sensitivity, enabling informed decisions about data protection.

A FAM Destination is where audit logs are sent. This can be a single Data Security Fabric (DSF) gateway (IP or hostname) or a group of DSF gateways (hostname suffix), such as `dsf-gateways.dsf.abcyz.com`. When using a group, each client sends logs to a unique hostname combining a client identifier and the FQDN suffix (for example, `clientid.dsf-gateways.dsf.abcyz.com`).

Viewing FAM Destination

To view the FAM destinations added to the CipherTrust Manager:

1. Open the **Transparent Encryption** application.
2. Click **Settings > FAM Destination**. The FAM destination page shows the list of FAM destinations added to the CipherTrust Manager. The page displays the following details:

Column	Description
Name	Name of the FAM destination.
Type	The type of the FAM destination.
Mode	The mode of the FAM destination. The supported modes are TCP and TLS.
Destination Address	The address of the FAM destination.
FQDN Suffix	A fully qualified domain name (FQDN) for the FAM destination.
Port	The port for the FAM destination.
Description	Description of the FAM destination.
TLS Verify	Whether TLS Verify is enabled. The value can be Yes or No. Applicable only when TLS mode is enabled.
Compress	Whether the data is compressed. Value can be Yes or No.

Unique to Client Keys

CTE on the CipherTrust Manager supports *Unique to Client* keys.

On the Data Security Manager (DSM), this feature is known as the Unique to Host keys.

A key is made unique to a client by using a token stored with the client record on the CipherTrust Manager. Unique to client keys provide greater security because a key compromised on one client does not compromise the keys on other clients.

Properties

- Unique to client keys are stored on the client for offline use. These keys are downloaded to the client and stored and encrypted using the client password.
- When the key is needed, it is decrypted and cached. If the client goes offline and is disconnected from the CipherTrust Manager, the current policy remains in effect because the encryption key is locally available in the system cache.
- If the CTE Agent cannot connect to the CipherTrust Manager after a reboot, any attempt to access the contents of an encrypted file on an unconnected client will not complete. The application will hang until the CTE Agent client password is entered in another terminal window. The application resumes execution after the password is provided.
- The key can also be re-established after a reboot without access to the CipherTrust Manager using the client password. You can specify the client password using the "vmsec passwd" utility, or, you can display the challenge string in challenge-response client deployments using the "vmsec challenge" utility.
- These keys are used for locally attached devices, as files encrypted by them can be read by only one client. Therefore, do not use "Unique to Client" keys in situations where data may be shared by multiple clients, such as in clustered environment or any environment that uses client mirroring.

Creating Unique to Client Keys

A unique to client key can be created when [adding key rules](#) during policy creation or on the Keys page of the CipherTrust Manager GUI, as described below.

To create a unique to client key:

1. Log on to the CipherTrust Manager with a user having permissions to manage CTE keys.
2. In the left pane, click **Keys**.
3. Create a key for use with **CTE**.

Tip

- When creating the key, make sure to select the **Unique to Client** check box under the CTE Property section.
- For a unique to client key, the **Persistent on Client** check box is selected automatically, and is non-editable. The key will be downloaded and stored (in an encrypted form) in persistent memory on the

client. This can be used in the event that a connection to the CipherTrust Manager is unreliable.

Refer to [Creating a New Key](#) for detailed instructions on creating a CTE key.

Limitation

A unique to client key will have different key values on different clients. If the key is used in a file system shared by different clients, it will cause data corruption.

So, it is recommended to not use a unique to client key to protect network shares. For example, when securing a CIFS path using an LDT communication group, the CIFS path should not be guarded with a policy having a Unique to Client key.

Load Balancer

This document describes the configuration steps to allow CTE agents communicate with a CipherTrust Manager cluster behind a network load balancer.

Prerequisites

Make sure a passthrough network load balancer is configured with the nodes of the CipherTrust Manager cluster. Refer to [Clusters and Nodes](#) for details on creating a CipherTrust Manager cluster.

Note

Only network load balancers with passthrough authentication are supported.

Configure the Load Balancer on CipherTrust Manager

After completing the prerequisites, you can configure the load balancer. Click the desired tab to view the instructions.

Using the UI

1. Login to the root domain as an Application Administrator.
2. Navigate to **Admin Settings > Properties**.
3. In **Load Balancer Address**, add an IP address or hostname for the load balancer to the **Value** field.
4. Click **Update** to update it.

Using the API

1. Authenticate to the REST API.
2. Go to the **Properties** section.
3. Update the name of the load balancer address.

Run the API

```
patch /v1/configs/properties/{name}
```

Example

```
/v1/configs/properties/LOAD_BALANCER_ADDRESS
```

Sample Output

```
{
  "name": "LOAD_BALANCER_ADDRESS" ,
  "value": "cte-cm-d91617b26a55d596.elb.us-east-1.amazonaws.com",
  "description": "Add IP/URL/Hostname of load balancer configured with CM. D
efault value is empty for CM."
}
```

Limitations

- If the nodes are configured with the load balancer, the configured Server Settings for the CTE Profiles on the CipherTrust Manager will not be applicable.

Refer to [Configuring Server Settings](#) for details.

- The Agent Information on the CipherTrust Manager will be unavailable for the CTE clients registered with the load balancer.
- If the load balancer configuration is deactivated and the CipherTrust Manager cluster is also removed, the agents registered with the load balancer need to be reregistered with the desired CipherTrust manager.
- When the load balancing setup changes to the non-load balancing mode, that is, when the load balancing configuration is removed, any configuration changes take time to reflect on the registered clients. If a client is down/unavailable, the configuration changes would not be updated for that client.

Workaround: To update the client with the configuration changes, reregister the client after it is up and running!

Operations

This section provides information on operations that the CTE Server Administrator performs on the CipherTrust Manager. These operations include registering CTE clients with the CipherTrust Manager, and protecting file system on a CTE client.

Registering Clients

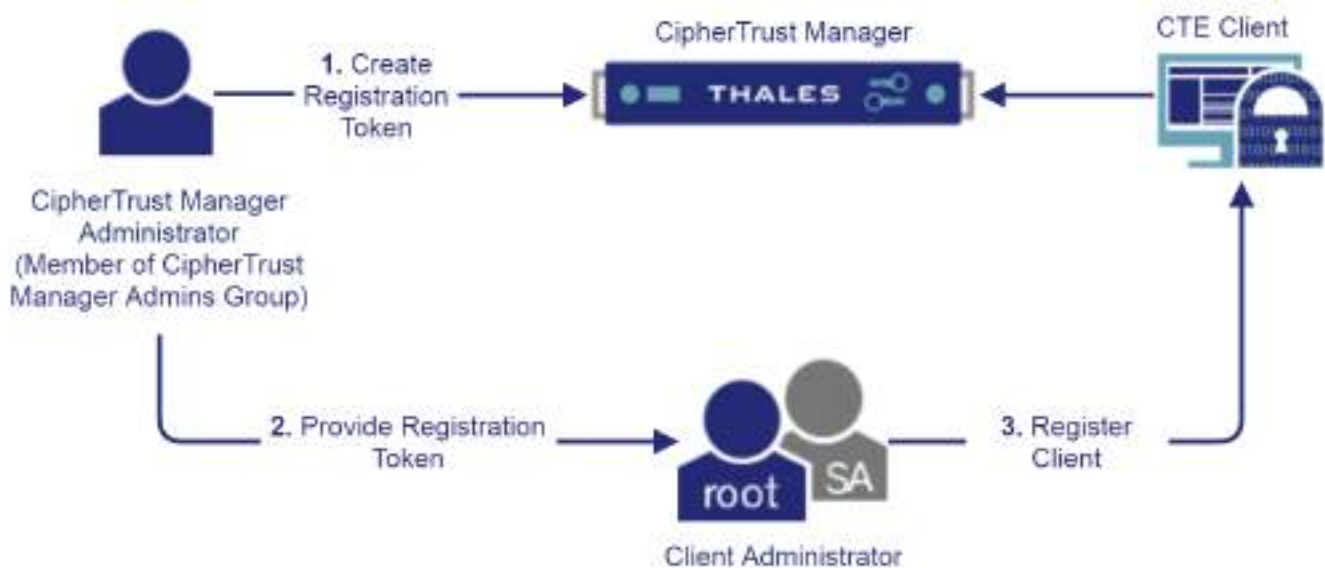
Registration is the process of configuring a CTE client with a CipherTrust Manager. This process creates SSL certificates for further communication between the CipherTrust Manager and the CTE client.

Warning

If you use a registration token created with a newly created Local CA, you must restart the CipherTrust Manager services before registering a CTE client. This step is required to ensure the new CA is loaded correctly by all services.

Registering a CTE client with the CipherTrust Manager requires a [registration token](#). Single registration token can be used to register any number of CTE clients. Refer to the [CTE Agent Quick Start Guide](#) specific to your platform for details.

The following diagram shows the process of registering CTE clients with the CipherTrust Manager:



By default, CipherTrust Manager issues a Local CA with Common Name "KeySecure Root CA" which is used by CTE for signing client certificates. This Local CA is, by default, marked as trusted by the "web" interface which is also used by CTE for client authentication. Make sure that the CA whose signature is used for registering CTE clients is trusted by the "web" interface. Refer to [Authentication Settings for NAE, KMIP, and Web Interfaces](#) for details.

Third party (external) CA certificates can also be used for securing communication between the CipherTrust Manager and CTE clients. Refer to [Using External CA Certificates](#) for details.

Using External CA Certificates

All local and external CAs that participate in securing communication between the CipherTrust Manager and CTE clients must be added to the list of trusted CAs for the "web" interface on the CipherTrust Manager. Refer to [Certificate Authority](#) for details.

To use an external CA certificate:

1. Create a registration token using the ID of the Local CA signed by the external CA. Refer to [Creating a Registration Token](#) for details.
2. Register the CTE clients using this registration token. The registration process will automatically use the Local CA signed by the external CA. Refer to the [CTE Agent Quick Start Guide](#) specific to your platform for details.

CA Certificates Renewal Notification

When the CA that signed a client certificate or the web interface certificate is modified, a compatible CTE client is notified of the change. The client can then generate or install a new certificate and update its truststore to ensure uninterrupted communication with CipherTrust Manager.

Note

Auto-Renewal Compatibility

Automatic CA certificate renewal notification is supported on CipherTrust Manager version 2.14 and later, when used with CTE version 7.5 and higher and CTE UserSpace version 10.2 and higher.

- This feature is enabled by the `CA_RENEWAL` capability, which can be set during agent installation.
- This feature is not available for CTE for Kubernetes clients.
- When you upgrade CipherTrust Manager to version 2.14 or higher, it uses client management profiles for registration tokens. The CA that was linked to a token used for an older client's registration will be linked to a client management profile.

Scenarios Requiring Manual Intervention

Manual intervention is required in the following scenarios where automatic renewal is not supported:

- **Unsupported Agent/CipherTrust Manager Versions:** If you are using CTE 7.4, CTE UserSpace 10.1, or any lower version, or your agent is registered with CipherTrust Manager 2.13 or lower, automatic notifications are not sent. If the certificate expires or is modified, you must reregister the client. Refer to [Reregistering CTE Clients](#) for instructions.
- **Upgrading CipherTrust Manager with Existing Agents:** If a compatible CTE Agent — such as CTE 7.5, CTE UserSpace 10.2, or later — was registered with CipherTrust Manager 2.13 or lower, the CipherTrust Manager is unaware of the agent's `CA_RENEWAL` capability after an upgrade to CipherTrust Manager 2.14+.

To resolve this, you must make the CipherTrust Manager aware of the agent's capabilities. You can do this in one of two ways:

- **Fetch Capabilities from CipherTrust Manager (Recommended):** In the CipherTrust Manager GUI, navigate to **Transparent Encryption > Settings > Client Information and Capabilities**, then click **Get Capability**. This action fetches the latest capabilities from all active clients without requiring a restart.
- **Reboot the CTE Agent:** Rebooting the CTE client causes it to reinitialize and send its capabilities to CipherTrust Manager, enabling future auto-renewal notifications.

Reregistering CTE Clients

In some cases, you need to change the CA certificate that was used to register a client with the CipherTrust Manager. If the CA used to generate the client certificate is about to expire or is modified, the CTE clients are notified of the CA certificate auto renewal.

Warning

If the client certificate is not renewed timely, it results in a connection failure. You need to reregister the client with the CipherTrust Manager.

While reregistering a client, you can enable capabilities even if they were disabled earlier.

To reregister a client with the CipherTrust Manager:

1. Create a new registration token. Use the ID of the trusted CA that will be used to sign the client certificate. By default, a local CA will be used to issue certificates. Refer to [Creating a Registration Token](#) for details.
2. Register the client again using the new registration token created in step 1. The client administrator reregisters the client with the CipherTrust Manager. Steps are similar to registering a new client with the CipherTrust Manager.

Protecting Data on Clients

After registration, the client can communicate with the CipherTrust Manager, and is ready for data protection using CTE. This section describes how CTE GuardPoints, policies, and policy elements work together to encrypt file systems.

Refer to [Common Scenarios](#) for prerequisites and procedures to encrypt data in the most common scenarios.

GuardPoints

A GuardPoint specifies the path on the client that is to be protected with different access and encryption policies. GuardPoint is configured by specifying the guard path, policy, and other policy/path specific configuration parameters.

A sample configuration of a GuardPoint is shown below:



Refer to [Managing GuardPoints](#) for details.

Policies

A policy is the resource where all the access privileges and key configuration is done to achieve the required use cases. Policies are categorized as:

- Standard Policies
- LDT Policies
- COS Policies
- IDT Policies

Refer to [Creating Policies](#) for details.

Standard Policies

Depending on the availability of data in GuardPoints, standard policies can be applied in two different scenarios.

- The GuardPoint **does not contain** any data. The data would be created after the GuardPoint is applied. These policies are also called production policies.

A sample production policy is shown below:

1 General Info

Name: ProductionPolicy

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*	User1		all_ops	permit,applykey	Yes

3 Key Rules

Resource Set	Key Name
	Key1

- The GuardPoint already **contains** data. The existing data is migrated to encrypted form by using the data transformation policy.

A sample data transformation policy is shown below:

1 General Info

Name: dataformplc

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit,applykey	Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	Key1

After the data is migrated, unguard the data transformation policy, apply the standard policy with same key (as used by the data transformation policy). A sample standard policy applied after unguarding a data transformation policy is shown below:

1 General Info

Name: UCT-Standard

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*	User1		all_ops	permit,applykey	Yes
*	User2		all_ops	permit	Yes
				deny	Yes

3 Key Rules

Resource Set	Key Name
	Key1

Data transformation policies are created by turning on the Data Transformation toggle when creating a Standard policy. These policies require downtime, so they are referred to as offline policies. If you do not want downtime, you can deploy LDT policies.

LDT Policies

As their name implies, LDT policies perform live transformation of data. They do not require any time downtime, so they are referred to as online policies. You can continue to work while the transformation of your data in GuardPoints is in progress. To benefit from LDT, you need to purchase an Add-On LDT license with the CTE Base license.

LDT policies can handle both these cases:

- The GuardPoint **does not contain** any data. No data is migrated. A production policy is applied to encrypt/decrypt the future data.
- The GuardPoint already **contains** data. The existing data is automatically migrated. After the data is migrated, the data is encrypted/decrypted like a production policy.

A sample LDT policy is shown below:

Name: UC1-LDT

Policy Type: ldt

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*			key_up	permit,applykey	No
*	User1		all_ops	permit,applykey	Yes
*	User2		all_ops	permit	Yes
				dany	Yes

3 Key Rules

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule
	clear_key	testldt	No

COS Policies

These policies are used to encrypt data and apply access rules on the GuardPoints on cloud. CTE supports Amazon S3 buckets.

A sample COS policy is shown below:

Name: RS3-COSPolicy

Policy Type: cloud_object_storage

Description:

2 Security Rules

User Set	Process Set	Action	Effect	Browsing
		all_ops	permit,applykey	No

3 Key Rules

Key Name
Key2

IDT Policies

These policies are used to create GuardPoints for Teradata clusters. Access to data is blocked during encryption or rekeying of data.

A sample IDT policy is shown below:

Name: IDT-Policy

Policy Type: in-place Data Transformation

Description:

1 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*				deny,audit	Yes

2 Key Rules

Current Key: clear_key

Transformation Key: testb1t6

Refer to [Protecting Teradata Appliances](#) for details on protecting Teradata appliances.

Policy Elements

To achieve different access privileges based on users, processes, and different resources (sub-directory/specific file formats), create these policy elements:

- User Sets
- Process Sets
- Resource Sets

Refer to [Creating Policy Elements](#) for details.

User Sets

Groups of single or multiple users that can be used as individual entities in policies to grant user specific privileges. A sample user set is shown below:

1 General Info

Name: UserSet1

Description:

2 Users / Groups

uname	UID	gname	GID	OS domain	
user1	1000	group1	1000		 Remove

Process Sets

Groups of single or multiple processes that can be used as individual entities in policies to grant process specific privileges.

1 General Info

Name: ProcessSet

Description:

2 Processes

Directory	File	Signature
/usr/bin	vi	

Resource Sets

Groups of single or multiple resources (sub-directory or specific file formats) that can be used as individual entities in policies to grant resource specific privileges.

1 General Info

Name: ResourceSet1

Description:

2 Resources

Directory	File	Include Sub Folders	File System Type
/	*.txt	Yes	Local File System

Certificate Renewal

If the CA that signed the client certificate or the web interface certificate is modified, the CTE client is notified about this change. The CTE client can now generate or install a new certificate and update the truststore for uninterrupted connections.

Refer to [CA Certificates Renewal Notification](#) for compatibility information.

Client Certificate Renewal

CTE Agents with the `CA_RENEWAL` capability support the CA renewal feature. When the CA (local or external) is updated in a client management profile, the `Client Profile updated` message is logged on the CipherTrust Manager. Also, all the clients linked with the updated client management profile are notified of the CA update. A message `RenewCerts - Renewal has been scheduled - OK` is generated in the VMD logs (client logs) on the linked clients.

Note

Client certificate renewal is applicable to all the **CA_RENEWAL** capable CTE clients in *all the domains* of the CipherTrust Manager.

Possible Scenarios

- Client with the **CA_RENEWAL** Capability is Active
- Client with the **CA_RENEWAL** Capability is Inactive
- Client with the **CA_RENEWAL** Capability is Registered with an Unsupported CipherTrust Manager Version
- Client Doesn't have the **CA_RENEWAL** Capability

Client with the **CA_RENEWAL** Capability is Active

A CTE client with the **CA_RENEWAL** capability is active. After the CA is updated in a client management profile:

1. The active client with the **CA_RENEWAL** capability linked with the updated profile receive the certificate renewal notification.
2. The CTE Agent generates a log of CA renewal, **RenewCerts: Renewal has been scheduled - OK**, in the client logs. The client continues to work properly after the CA renewal.

All the active and **CA_RENEWAL** capable CTE clients linked with the updated client management profile reflect the same behavior.

Client with the **CA_RENEWAL** Capability is Inactive

A CTE client with the **CA_RENEWAL** capability is inactive, that is, unable to communicate with the CipherTrust Manager it is registered with. In this case, if the CipherTrust Manager administrator updates the CA in the linked client management profile, the following message is generated in the CipherTrust Manager logs. This shows that the client can't be notified of the CA update.

```
Client cert updated. LONGPOLL connection is not available for client
```

The CA Renewal Notification ERROR message is also logged in the audit records on the CipherTrust Manager (**Records > Loki Audit Records > Server Records**).

Now, if the connection between the client and the CipherTrust Manager is restored:

- The CipherTrust Manager log shows that a **LONGPOLL** command of **RenewCertificates** is sent to the clients. This indicates that the communication between the CipherTrust Manager and the client is enabled. The client is notified of the CA update.
- The client log shows **RenewCerts: OK - Renewal has been scheduled**.

Note

If a client with the `CA_RENEWAL` capability is *inactive* (disabled or unreachable), the CipherTrust Manager can't notify the client of the certificate update. The CipherTrust Manager will retry notifying the client when it is *active* again.

Client with the `CA_RENEWAL` Capability is Registered with an Unsupported CipherTrust Manager Version

A CTE client with the `CA_RENEWAL` capability is registered with a CipherTrust Manager version that does not support certificate renewal notification. In this case, if the CA is updated in the linked client management profile, the CipherTrust Manager can't notify the linked clients of any CA updates.

Client Doesn't have the `CA_RENEWAL` Capability

A CTE Agent doesn't have the `CA_RENEWAL` capability. In this case, if the CA is updated in the linked client management profile, the CipherTrust Manager doesn't send CA update notifications to the client. An audit record is logged on the CipherTrust Manager.

When the CA in the linked client management profile is updated:

- A message `Client Profile updated` is displayed on the CipherTrust Manager GUI.
- A message `Client Cert updated. Cert renewal notification are not supported for the CTE Client` is logged on the CipherTrust Manager. The CA Renewal Notification ERROR message is also logged in the audit records on the CipherTrust Manager (**Records > Loki Audit Records > Server Records**).

Web Interface Certificate Renewal

When the CipherTrust Manager's web interface certificate is updated (or renewed), all the `CA_RENEWAL` capable CTE clients from *all the domains* of the CipherTrust Manager are notified of the changes in the web interface certificate.

Click the desired tab to view instructions to update the web interface certificate through the API or GUI.

API

To update the web interface certificate:

1. Add the new certificate to the list of upcoming interface certificates.

```
put /v1/configs/interfaces/web/renewal-certificate
```

In the `certificate` parameter, specify the certificate chain having the primary certificate, the CA, and its private key. Also, specify the `format` parameter.

After the upcoming certificate is updated successfully

- a. The active **CA_RENEWAL** capable clients receive notification of this update.
 - The CipherTrust Manager logs show that a **LONGPOLL** command of **RenewCertificates** is sent to the *active* clients. The clients are notified of the web interface certificate update.
 - The client log shows **RenewCerts: OK - CA trust store updated**.
- b. The CTE Agent updates the truststore with the new certificate chain. Both the old and the updated certificates are stored on the client at: **/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem**

2. Fetch the upcoming renewal certificate.

```
get /v1/configs/interfaces/web/renewal-certificate
```

The command returns the public portion (only public key and CA chain) of the upcoming renewal certificate in the PEM format.

3. When the current interface certificate is about to expire, apply the new certificate.

```
post /v1/configs/interfaces/{interface}/renewal-certificate/apply
```

Note

If the new certificate is not applied before the current certificate expires, the new certificate will be automatically applied when the current certificate expires.

GUI

To renew the web certificate:

Upload the updated web certificate

1. Go to **Admin Settings > Interfaces**.
 2. Click the Overflow Icon () next to the web interface.
 3. Click **Renewal Certificate Options...** The Interface Renewal Certificate Options on 'web' dialog box is displayed.
 4. Click **Upload/Generate** to upload a new server certificate.
 5. Click **OK**. The Upload/Generate Upcoming Certificate dialog box is displayed.
-

6. Select a certificate upload option. You can either upload the certificate using the **File Upload** option or paste the signed certificate and its private key content in the **Text** field.
7. Select **PEM** as **Format**.
8. Click **Upload Certificate**. The certificate is uploaded successfully.

Apply the new certificate

When the current interface certificate is about to expire, you need to apply the newly uploaded certificate.

1. Click the Overflow Icon () next to the web interface.
2. Click **Renewal Certificate Options...** The Interface Renewal Certificate Options on 'web' dialog box is displayed.
3. Click **Apply** to apply the upcoming renewal server certificate. The existing server certificate is replaced with the newly generated server certificate.

Note

If the new certificate is not applied before the current certificate expires, the new certificate will be automatically applied when the current certificate expires.

Refer to [managing upcoming server certificate](#) for details on upcoming server certificates.

Web Service Restart Required

When renewing the CipherTrust Manager web interface SSL certificate—including when using the "Automatically Renew the Upcoming Certificate" feature—a restart of the CipherTrust Manager web service is required to activate the new certificate.

- **Action Required:** Restart the web service through **Admin Settings > Services**.
- **Impact:** Until the web service is restarted, the new certificate will not be active, and "Failed to notify the CTE client" errors may appear in system logs.
- **After Upgrade:** This restart remains necessary even after upgrading the CipherTrust Manager to version 2.14 or higher.

After the CTE Agent has successfully updated the truststore and the updated web interface certificate is *applied* successfully, the **CA_RENEWAL** capable clients start communicating with the CipherTrust Manager over the renewed certificate.

Important Notes

- The CipherTrust Manager doesn't notify the clients that don't have the `CA_RENEWAL` capability. The following message is displayed in the CipherTrust Manager logs for such clients.

```
Web interface CA is updated but Auto-CA Renewal is not supported for the CTE Client
```

The CA Renewal Notification ERROR message is also logged in the audit records on the CipherTrust Manager (**Records > Loki Audit Records > Server Records**).

- When renewing a web interface SSL certificate that was signed by an external CA, re-registering older CTE Agents is not required if the certificate is renewed using the **same external CA signer**. This exception applies even to agents on versions 7.4.0 and lower.
- If the CA signer for the web interface certificate changes, or if you are using CTE or CipherTrust Manager versions that do not support automatic renewal notifications, manual re-registration of the CTE Agents is required.
- If the web interface SSL certificate was signed by an external CA and is renewed using the same external CA signer, then reregistering the CTE Agents is not required, even if they are on a version lower than 7.5.0.
- The CipherTrust Manager retries notifying all the `CA_RENEWAL` capable clients whether they are *active* or *inactive*.

If a client with the `CA_RENEWAL` capability is *inactive* (disabled or unreachable), the CipherTrust Manager can't notify the client of the certificate update (until it is active). The following message is displayed in the CipherTrust Manager logs.

```
Failed to notify the CTE client
```

The CA Renewal Notification ERROR message is also logged in the audit records on the CipherTrust Manager (**Records > Loki Audit Records > Server Records**).

The CipherTrust Manager retries notifying the client of the update when the client is active again (the connection is re-established). A `LONGPOLL` message `Sending pending event to CTE client` is displayed in the CipherTrust Manager logs.

After the client is notified of the update, the Agent updates the truststore. A message `RenewCerts: OK - CA trust store updated` is logged in the client logs.

Caution

- Restore the connectivity of inactive clients with the **CA_RENEWAL** capability before **applying** the updated web interface certificate. If the certificate is applied when a client is inactive, the client needs to be reregistered.
- In a clustered environment, all the CipherTrust Manager nodes must have the same certificate active. If the web interface certificate is renewed (updated and applied) at one node, the same certificate chain must be renewed on all nodes of the CipherTrust Manager cluster. Failure to do so can break the connectivity and the CTE clients need to be reregistered.

Common Scenarios

This section describes the common encryption scenarios in which paths can be encrypted using the CTE solution. Similarly, you can configure different types of policies with different combinations of policy elements to suit your requirements.

This section describes encryption using:

- User-based Access Privileges
- Process-based Access Privileges
- Signature-based Access Privileges for Processes
- Different Access Privileges for Subdirectory or Different File Formats
- Different Access Privileges for Combination of Users, Processes, and Resources

Prerequisites

- The CipherTrust Manager is up and running. Refer to the [CipherTrust Manager Deployment Guide](#) for details.
- A CTE base license is activated and installed. Refer to [Licensing](#) for details.
- (Optional) Add-on LDT license is activated and installed. This license is needed only if you want to deploy LDT policies. A CTE base license must be activated on the CipherTrust Manager. Refer to [Licensing](#) for details.
- The CTE Agent is installed on client machines where data is to be protected. The client machines are running a supported platform. Refer to the [CTE Agent Quick Start Guide](#) specific to your platform for details.

Note

Policy elements can be created either in advance or when creating the policy. Refer to [Creating Policy Elements](#) for details.

User-based Access Privileges

Encrypt a local path with the following access privileges:

- User set UserSet1 can encrypt/decrypt data in the GuardPoint.
- User set UserSet2 can access the ciphertext data but cannot encrypt or decrypt.
- All other user sets are denied access to the GuardPoint data.

Depending on the data availability (or downtime) and storage requirements in your setup, you can apply any of these policies:

- [Standard Production Policies](#)
- [Standard Data Transformation Policies](#)
- [LDT Policies](#)

Refer to [Data Transformation Techniques](#) for advantages and limitations of data transformation techniques. LDT policies require an add-on license to use them.

Standard Production Policies

If the GuardPoint does not contain any existing data, and the data would be created after the GuardPoint is applied:

1. Create a standard policy. Refer to [Creating Policies](#) for details.

1 General Info

Name: ProductionPolicy

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
+	User1		all_ops	permit,applykey	Yes

3 Key Rules

Resource Set	Key Name
	Key1

2. Apply a GuardPoint using the standard policy. Refer to [Creating Standard GuardPoints](#) for details.

Standard Data Transformation Policies

If the GuardPoint already contains data, and the existing data needs to be migrated to encrypted form by using the `dataxform` utility:

1. Create a data transformation policy. Refer to [Creating Policies](#) for details.

1 General Info

Name: dataxformplc

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
			key_op	permit,applykey	Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	Key1

2. Apply a GuardPoint using the data transformation policy. Refer to [Creating Standard GuardPoints](#) for details.
3. After the existing data is migrated, unguard the data transformation policy from the GuardPoint. Refer to [Removing GuardPoints](#) for details.
4. Create a standard policy with same key (as used by the data transformation policy in the first step). Refer to

Creating Policies for details.

1 General Info

Name: UCI-Standard

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*	User1		all_ops	permit,applykey	Yes
*	User2		all_ops	permit	Yes
				deny	Yes

3 Key Rules

Resource Set	Key Name
	Key1

Now, you must run the `dataxform --rekey --gp <GuardPath>` command on the CTE Agent. Refer to the [CTE Data Transformation Guide](#) specific to your platform for details.

5. Apply the GuardPoint using the standard policy created in the previous step. Refer to [Creating Standard GuardPoints](#) for details.

LDT Policies

If you have an add-on LDT license, you can achieve the combined effects of the standard production and standard data transformation policies by applying the LDT policies.

- If the GuardPoint already contains data, the policy migrates the existing data automatically. No need to run the `dataxform` utility manually. Later, the policy automatically encrypts/decrypts the data similar to a standard policy.
- If the GuardPoint does not contain any existing data, migration is not required. A standard (production) policy of encryption/decryption is applied automatically.

To apply an LDT policy:

1. Create an LDT policy. Refer to [Creating Policies](#) for details.

Name: UC1-LDT

Policy Type: ldt

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
*			key_up	permit,applykey	No
*	User1		all_ops	permit,applykey	Yes
*	User2		all_ops	permit	Yes
				deny	Yes

3 Key Rules

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule
	clear_key	testldt	No

2. Apply the GuardPoint using the LDT policy. Refer to [Creating LDT GuardPoints](#) for details.

Process-based Access Privileges

Encrypt a local path with the following access privileges:

- Process set ProcessSet1 can encrypt/decrypt data in the GuardPoint.
- Process set ProcessSet2 can access the ciphertext data but cannot encrypt or decrypt.
- All other process sets are denied access to the GuardPoint data.

Process-based policies are configured in exactly the same way the user-based policies are configured, as described in [User-based Access Privileges](#). The only difference is that instead of adding user sets add process sets to the Security Rules tab of the policy.

Depending on the data availability (or downtime) and storage requirements in your setup, you can apply any of these policies:

- [Standard Production Policies](#)
- [Standard Data Transformation Policies](#)
- [LDT Policies](#)

Refer to [Data Transformation Techniques](#) for advantages and limitations of data transformation techniques. LDT policies require an add-on license to use them.

Signature-based Access Privileges for Processes

Encrypt a local path with the following access privileges:

- Process Process1 with a particular signature can encrypt/decrypt data in the GuardPoint.
- All other processes are denied access to the GuardPoint data.

To apply a signature-based access policy for a process:

1. Create a signature set. When creating the set, add the source path of Process1. This process will be signed. Refer to [Creating Signature Sets](#).

1 General Info

Name: SignSet1

Description:

2 Sources

Source Directory

/usr/bin/vi

2. Sign the signature set. Use a CTE client having the desired process to sign the process. Refer to [Signing Files in a Signature Set](#) for details.



3. Create a process set. When creating the set, add the newly created signature set. Refer to [Creating Process Sets](#) for details.

1 General Info

Name: UC-3-ProcessSet

Description:

2 Processes

Directory	File	Signature	
/usr/bin/	vi	SignSet1	***

4. Configure process-based access policies. Refer to [Process-based Access Privileges](#) for details.

Different Access Privileges for Subdirectory or Different File Formats

Encrypt a local path with the following access privileges:

- Encrypt/decrypt only a subdirectory, subdir1, under the GuardPath.
- Deny access to all other files and directories under the GuardPoint.

To achieve this use case, you need to add a resource set to the policy. In a resource set, you can provide details about the subdirectories or specific file formats that need to be handled differently under a GuardPoint.

To achieve this use case:

1. Create a resource set. Specify the details of the subdirectory (subdir1) in the resources. Refer to [Creating Resource Sets](#) for details.

1 General Info

Name: UC4_ResourceSet_SubDir1

Description:

2 Resources

Directory	File	Include Sub Folders	File System Type
/subdir1/	*	Yes	Local File System

Note

Paths specified in a resource set should be relative to the GuardPath. Do not provide absolute path for the resources.

2. Create the desired policy type. Make sure to add the resource set created in the previous step. This is done to enforce the desired access policy. Refer to [Creating Policies](#) for details.

1 General Info

Name: UC4-Policy

Policy Type: Standard

Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
+ UC4_ResourceSet_SubDir1			all_ops	permit_applykey	Yes
				deny	Yes

3 Key Rules

Resource Set	Key Name
UC4_ResourceSet_SubDir1	Key1

3. Apply the GuardPoint using the policy created in the previous step. Refer to [Managing GuardPoints](#) for details.

Different Access Privileges for Combination of Users, Processes, and Resources

Encrypt a local path with the following access privileges:

- Allow only the process usrbn.exe being run by User1 to encrypt/decrypt text files (*.txt) present under the GuardPath.
- Deny access to all other users and processes.

To achieve this use case:

1. Created the required resource set. Refer to [Creating Resource Sets](#) for details.
2. Create the required user set. Refer to [Creating User Sets](#) for details.
3. Create the required process set. Refer to [Creating Process Sets](#) for details.
4. Create the desired policy type using the resource set, the user set, and the process set created above. Refer

to [Creating Policies](#) for details.

1 General Info

Name: UCS-Combination-Policy
Policy Type: Standard
Description:

2 Security Rules

Resource Set	User Set	Process Set	Action	Effect	Browsing
Text_ResourceSet	User1	UsrBin_ProcessSet	all_ops	permit,applykey	Yes
				deny	Yes

3 Key Rules

Resource Set	Key Name
Text_ResourceSet	Key1

5. Apply the GuardPoint using the policy created in the previous step. Refer to [Managing GuardPoints](#) for details.

Reports

Reports provide an easy and quick method to answer queries such as:

- How many clients are registered with the CipherTrust Manager?
- What is the health status of clients?
- How many keys are used for protecting data?
- What keys and policies are linked?
- How many GuardPoints are applied on a client?
- What key is used to protect a specific GuardPoint?
- What CTE resources belong to a specific CipherTrust Manager domain?

Use the **Domain Sharing Data** toggle button to include/exclude information about CTE resources shared across domains.

Dashboard

The dashboard on the Reports page shows the following information:

- **TOTAL CLIENTS:** Shows the total count of registered and unregistered clients on the CipherTrust Manager.
- **CTE LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption* licenses out of

available licenses.

- **CTE-U LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for UserSpace* licenses out of available licenses.
- **K8S LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for Kubernetes* licenses out of available licenses.
- **TOTAL GUARDPOINTS:** Shows the total count of GuardPoints configured on the registered and unregistered clients on the CipherTrust Manager.
- **ACTIVE GUARDPOINTS:** Shows the count of active GuardPoints on the CipherTrust Manager.
- **INACTIVE GUARDPOINTS:** Shows the count of inactive GuardPoints on the CipherTrust Manager.

Download Formats

View the latest CTE reports and download them as PDF and CSV documents on your local machines. The PDF and CSV formats present reports in easy-to-understand tabular forms.

Important Note on CSV Reports

If the names of CTE resources include special characters like equals (=), plus (+), minus (-), at (@), tab (0x09), and carriage return (0x0D), the resources are renamed in the downloaded CSV reports by applying the following rules:

- Every cell is wrapped in double quotes
- Every cell is prepended with a single quote
- Every double quote is escaped using an additional double quote

For example, a resource named `=A+B " ; , =C+D` is renamed as `" '=A+B ' "' ; , =C+D"` in the downloaded CSV report.

Report Types

The Reports page shows different types of CTE reports on the following tabs:

Tab	Description
Clients	Shows the health status of the CTE clients available on the CipherTrust Manager. Refer to Clients Health Report .
Clients Keys	Shows the keys used for protecting GuardPoints on the CTE clients available on the CipherTrust Manager. Refer to Clients Keys Report .
Clients Profiles	Shows the mapping of clients with the profiles they are linked to on the CipherTrust Manager. Refer to Clients Profiles Report .
Clients Policies	Shows the mapping of clients with the policies applied

Tab	Description
	to them on the CipherTrust Manager. Refer to Clients Policies Report .
Policies Keys	Shows the list of keys used by the CTE policies. A key can be used by multiple policies, similarly, a policy can have multiple keys. Refer to Policies Keys Report .
GuardPoints	Shows the GuardPoints applied to the CTE clients available on the CipherTrust Manager. Refer to GuardPoints Report .
Clients GuardPoints Status	Shows the status of GuardPoints applied to the CTE clients available on the CipherTrust Manager. Refer to Clients GuardPoint Status Report .

Filtering Reports

Use the "Search by" box to search for records in the reports by different resources or CipherTrust Manager domains.

When searching for records by domain names, specify the complete and exact domain name including case-sensitivity. For example, searching for "test", "test-domain", and "Test-Domain" will return different search results.

However, search by other resources support regular expressions and case-insensitivity. For example, when searching the Clients reports by Name, if you type the letter "t", the search results will display all the reports that have the letter "t" in their names, regardless of the order, complete name, and case-sensitivity.

The records can also be filtered using the on-screen filters. To filter the records, click the Filter icon (), selected/clear the desired option, and click **OK**. When a filter is applied, the icon changes to ().

To hide/show desired columns in the report, click the Custom View icon (), select/clear the check box against the desired column, and click **OK**.

Clients Health Report

The Clients Health Report shows the health status of the CTE clients available on the CipherTrust Manager. You can download the report as a PDF or CSV document, as required. Refer to [Downloading the Report](#).

Use the "Search by" box to search for records in the report by Client Name or Domain. When searching for records by domain names, specify the complete and exact domain name including case-sensitivity. For example, searching for "test", "test-domain", and "Test-Domain" will return different search results.

Viewing the Report

To view the Clients Health Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients** tab.

The report shows all or some of the following columns:

Column	Description
Domain	Name of the CipherTrust Manager domain to which the record belongs. If the Domain Sharing Data toggle is turned ON, the report displays all the domains where the resource is shared.
Client Name	Name of the client on the CipherTrust Manager.
Status	Status of the client. The status can be: • Unregistered • Error • Warning • Healthy • Expunged Refer to Client States for details.
Client Type	Type of the client: • FS: CTE client • CSI: CTE for Kubernetes client • CTE-U: CTE UserSpace client
OS Type	Operating system running on the client - AIX, LINUX, WINDOWS, UNKNOWN, FREEBSD. UNKNOWN is displayed for unregistered or manually added clients. FREEBSD is supported by CTE UserSpace.
Details	Versions of the platform and kernel installed on the client, for example, RHEL7.8 - 3.10.0-1127.el7.x86_64. For Windows clients and unregistered or manually added clients, the field is empty. The Details column shows hyphen-separated (-) combination of these fields: • Details-OS Sub Type: Variant of the operating system running on the client, for example, RHEL7.8. • Details-OS Kernel: Version of the kernel running on the client, for example, 3.10.0-1127.el7.x86_64. To view/hide their values, click the custom view icon (⚙️), select/clear the desired column, and click OK .
Client Version	Version of the CTE Agent installed on the client, for example, 7.2.0.xxxx. For unregistered or manually added clients, the field is empty.
Client Description	Description of the client.
Client Group Name	Name of the client group associated with the client.
Total GuardPoints	Total number of GuardPoints applied on the client.
Enabled GuardPoints	Number of enabled/active GuardPoints on the client.

Downloading the Report

Download the report as a PDF or CSV document. Based on the displayed columns and applied filters, the downloaded report shows all or some of the columns listed in [Viewing the Report](#).

Reports provide an easy and quick method to answer queries such as:

- How many clients are registered with the CipherTrust Manager?
- What is the health status of clients?
- How many keys are used for protecting data?
- What keys and policies are linked?
- How many GuardPoints are applied on a client?
- What key is used to protect a specific GuardPoint?
- What CTE resources belong to a specific CipherTrust Manager domain?

Use the **Domain Sharing Data** toggle button to include/exclude information about CTE resources shared across domains.

Dashboard

The dashboard on the Reports page shows the following information:

- **TOTAL CLIENTS:** Shows the total count of registered and unregistered clients on the CipherTrust Manager.
- **CTE LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption* licenses out of available licenses.
- **CTE-U LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for UserSpace* licenses out of available licenses.
- **K8S LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for Kubernetes* licenses out of available licenses.
- **TOTAL GUARDPOINTS:** Shows the total count of GuardPoints configured on the registered and unregistered clients on the CipherTrust Manager.
- **ACTIVE GUARDPOINTS:** Shows the count of active GuardPoints on the CipherTrust Manager.
- **INACTIVE GUARDPOINTS:** Shows the count of inactive GuardPoints on the CipherTrust Manager.

Download Formats

View the latest CTE reports and download them as PDF and CSV documents on your local machines. The PDF and CSV formats present reports in easy-to-understand tabular forms.

Important Note on CSV Reports

If the names of CTE resources include special characters like equals (=), plus (+), minus (-), at (@), tab (0x09), and carriage return (0x0D), the resources are renamed in the downloaded CSV reports by applying the following rules:

- Every cell is wrapped in double quotes
- Every cell is prepended with a single quote
- Every double quote is escaped using an additional double quote

For example, a resource named `=A+B' " ; , =C+D` is renamed as `" '=A+B' " " ; , =C+D` in the downloaded CSV report.

To download the report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients** tab.
4. Download the report:
 - Click **Download CSV** to download the report as a CSV file. The file is named `<DOMAIN>_cte_client_health_<TIMESTAMP>.csv`, for example, `root_cte_client_health_2021-01-12T06_52_51Z.csv`.
 - Click **Download PDF** to download the report as a PDF file. The file is named `<DOMAIN>_cte_client_health_<TIMESTAMP>.pdf`, for example, `root_cte_client_health_2021-01-12T06_55_09Z.pdf`.

Note

If the CipherTrust Manager is part of a cluster environment, the filename of the downloaded report (CSV and PDF) will also include the cluster ID.

If the downloaded report is a CSV file, the file will be named `<CLUSTER ID><DOMAIN>_cte_client_health_<TIMESTAMP>.csv`, for example, `51.26.30.11_root_cte_client_health_2021-01-12T06_52_51Z.csv`. The PDF file will also be named in the same way.

The downloaded PDF document shows the **Report Name** as *Clients Health Report* and time the report is **Generated At**.

Clients Keys Report

The Clients Keys Report shows the keys used for protecting GuardPoints on the CTE clients available on the CipherTrust Manager. You can download the report as a PDF or CSV document, as required. Refer to [Downloading the Report](#).

Use the "Search by" box to search for records in the report by Client Name, Key Name, or Domain. When searching for records by domain names, specify the complete and exact domain name including case-sensitivity.

For example, searching for "test", "test-domain", and "Test-Domain" will return different search results.

Viewing the Report

To view the Clients Keys Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Keys** tab.

The report shows all or some of the following columns:

Column	Description
Domain	Name of the CipherTrust Manager domain to which the record belongs. If the Domain Sharing Data toggle is turned ON, the report displays all the domains where the resource is shared.
Client Name	Name of the client on the CipherTrust Manager.
Description	Description of the client.
Key Name	Name of the key.

Downloading the Report

Download the report as a PDF or CSV document. Based on the displayed columns and applied filters, the downloaded report shows all or some of the columns listed in [Viewing the Report](#).

Reports provide an easy and quick method to answer queries such as:

- How many clients are registered with the CipherTrust Manager?
- What is the health status of clients?
- How many keys are used for protecting data?
- What keys and policies are linked?
- How many GuardPoints are applied on a client?
- What key is used to protect a specific GuardPoint?
- What CTE resources belong to a specific CipherTrust Manager domain?

Use the **Domain Sharing Data** toggle button to include/exclude information about CTE resources shared across domains.

Dashboard

The dashboard on the Reports page shows the following information:

- **TOTAL CLIENTS:** Shows the total count of registered and unregistered clients on the CipherTrust Manager.
- **CTE LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption* licenses out of available licenses.
- **CTE-U LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for UserSpace* licenses out of available licenses.
- **K8S LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for Kubernetes* licenses out of available licenses.
- **TOTAL GUARDPOINTS:** Shows the total count of GuardPoints configured on the registered and unregistered clients on the CipherTrust Manager.
- **ACTIVE GUARDPOINTS:** Shows the count of active GuardPoints on the CipherTrust Manager.
- **INACTIVE GUARDPOINTS:** Shows the count of inactive GuardPoints on the CipherTrust Manager.

Download Formats

View the latest CTE reports and download them as PDF and CSV documents on your local machines. The PDF and CSV formats present reports in easy-to-understand tabular forms.

Important Note on CSV Reports

If the names of CTE resources include special characters like equals (=), plus (+), minus (-), at (@), tab (0x09), and carriage return (0x0D), the resources are renamed in the downloaded CSV reports by applying the following rules:

- Every cell is wrapped in double quotes
- Every cell is prepended with a single quote
- Every double quote is escaped using an additional double quote

For example, a resource named `=A+B' " ; , =C+D` is renamed as `"' =A+B' " " " ; , =C+D"` in the downloaded CSV report.

To download the report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Keys** tab.
4. Download the report:

- Click **Download CSV** to download the report as a CSV file. The file is named `<DOMAIN>_cte_client_keys_<TIMESTAMP>.csv`, for example, `root_cte_client_keys_2021-01-12T06_56_30Z.csv`.
- Click **Download PDF** to download the report as a PDF file. The file is named `<DOMAIN>_cte_client_keys_<TIMESTAMP>.pdf`, for example, `root_cte_client_keys_2021-01-12T06_56_30Z.pdf`.

Note

If the CipherTrust Manager is part of a cluster environment, the filename of the downloaded report (CSV and PDF) will also include the cluster ID.

If the downloaded report is a CSV file, the file will be named `<CLUSTER ID><DOMAIN>_cte_client_health_<TIMESTAMP>.csv`, for example, `51.26.30.11_root_cte_client_health_2021-01-12T06_52_51Z.csv`. The PDF file will also be named in the same way.

The downloaded PDF document shows the **Report Name** as *Clients Keys Report* and time the report is **Generated At**.

Clients Profiles Report

The Clients Profile Report shows the mapping of clients with the profiles they are linked to on the CipherTrust Manager. A client can be linked to a single profile at once. However, multiple clients can be linked to a single profile. You can download the report as a PDF or CSV document, as required. Refer to [Downloading the Report](#).

Use the "Search by" box to search for records in the report by Client Name, Profile Name, or Domain. When searching for records by domain names, specify the complete and exact domain name including case-sensitivity. For example, searching for "test", "test-domain", and "Test-Domain" will return different search results.

Viewing the Report

To view the Clients Profiles Report:

- Open the Transparent Encryption application.
- In the left pane, click **Reports**. The Reports page is displayed.
- Click the **Clients Profiles** tab.

The report shows all or some of the following columns:

Column	Description
Domain	Name of the CipherTrust Manager domain to which the record belongs. If the Domain Sharing Data toggle is

Column	Description
	turned ON, the report displays all the domains where the resource is shared.
Client Name	Name of the client on the CipherTrust Manager.
Profile Name	Name of the profile the client is linked to.
Description	Description of the linked profile.

Downloading the Report

Download the report as a PDF or CSV document. Based on the displayed columns and applied filters, the downloaded report shows all or some of the columns listed in [Viewing the Report](#).

Reports provide an easy and quick method to answer queries such as:

- How many clients are registered with the CipherTrust Manager?
- What is the health status of clients?
- How many keys are used for protecting data?
- What keys and policies are linked?
- How many GuardPoints are applied on a client?
- What key is used to protect a specific GuardPoint?
- What CTE resources belong to a specific CipherTrust Manager domain?

Use the **Domain Sharing Data** toggle button to include/exclude information about CTE resources shared across domains.

Dashboard

The dashboard on the Reports page shows the following information:

- **TOTAL CLIENTS:** Shows the total count of registered and unregistered clients on the CipherTrust Manager.
- **CTE LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption* licenses out of available licenses.
- **CTE-U LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for UserSpace* licenses out of available licenses.
- **K8S LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for Kubernetes* licenses out of available licenses.
- **TOTAL GUARDPOINTS:** Shows the total count of GuardPoints configured on the registered and unregistered clients on the CipherTrust Manager.

- **ACTIVE GUARDPOINTS:** Shows the count of active GuardPoints on the CipherTrust Manager.
- **INACTIVE GUARDPOINTS:** Shows the count of inactive GuardPoints on the CipherTrust Manager.

Download Formats

View the latest CTE reports and download them as PDF and CSV documents on your local machines. The PDF and CSV formats present reports in easy-to-understand tabular forms.

Important Note on CSV Reports

If the names of CTE resources include special characters like equals (=), plus (+), minus (-), at (@), tab (0x09), and carriage return (0x0D), the resources are renamed in the downloaded CSV reports by applying the following rules:

- Every cell is wrapped in double quotes
- Every cell is prepended with a single quote
- Every double quote is escaped using an additional double quote

For example, a resource named `=A+B " ; , =C+D` is renamed as `" '=A+B ' "' ; , =C+D"` in the downloaded CSV report.

To download the report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Profiles** tab.
4. Download the report:
 - Click **Download CSV** to download the report as a CSV file. The file is named `<DOMAIN>_cte_client_profile_<TIMESTAMP>.csv`, for example, `root_cte_client_profile_2021-01-12T07_05_03Z.csv`.
 - Click **Download PDF** to download the report as a PDF file. The file is named `<DOMAIN>_cte_client_profile_<TIMESTAMP>.pdf`, for example, `root_cte_client_profile_2021-01-12T07_07_10Z.pdf`.

Note

If the CipherTrust Manager is part of a cluster environment, the filename of the downloaded report (CSV and PDF) will also include the cluster ID.

If the downloaded report is a CSV file, the file will be named `<CLUSTER`

ID><DOMAIN>_cte_client_health_<TIMESTAMP>.csv, for example, **51.26.30.11_root_cte_client_health_2021-01-12T06_52_51Z.csv**. The PDF file will also be named in the same way.

The downloaded PDF document shows the **Report Name** as *Clients Profile Report* and time the report is **Generated At**.

Clients Policies Report

The Clients Policies Report shows the mapping of clients with the policies applied to them on the CipherTrust Manager. You can download the report as a PDF or CSV document, as required. Refer to [Downloading the Report](#).

Use the "Search by" box to search for records in the report by Client Name, Policy Name, or Domain. When searching for records by domain names, specify the complete and exact domain name including case-sensitivity. For example, searching for "test", "test-domain", and "Test-Domain" will return different search results.

Viewing the Report

To view the Clients Policies Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Policies** tab.

The report shows all or some of the following columns:

Column	Description
Domain	Name of the CipherTrust Manager domain to which the record belongs. If the Domain Sharing Data toggle is turned ON, the report displays all the domains where the resource is shared.
Client Name	Name of the client on the CipherTrust Manager. Click the up/down arrow icon to sort the report list by client name.
Policy Name	Name of the applied policy. Click the up/down arrow icon to sort the report list by policy name.
Policy Description	Description of the applied policy.
Transformation Policy	Displays whether the listed policy is a transformation policy or not.
Client Type	Type of the client: • FS: CTE client • CSI: CTE for Kubernetes client • CTE-U: CTE UserSpace client

Column	Description
OS Type	Operating system running on the client - AIX, LINUX, WINDOWS, UNKNOWN, FREEBSD. UNKNOWN is displayed for unregistered or manually added clients. FREEBSD is supported by CTE UserSpace.
Policy Type	Type of the policy. The type can be: • Standard • Live Data Transformation • Cloud Object Storage • In-place Data Transformation • CSI
Guard Enabled	Whether a GuardPoint is enabled.
Learn Mode	Whether Learn Mode is enabled on the policy.
Last Update	Displays the most recent time of policy update. Click the up/down arrow icon to sort the report list based on the time of last update.

Downloading the Report

Download the report as a PDF or CSV document. Based on the displayed columns and applied filters, the downloaded report shows all or some of the columns listed in [Viewing the Report](#).

Reports provide an easy and quick method to answer queries such as:

- How many clients are registered with the CipherTrust Manager?
- What is the health status of clients?
- How many keys are used for protecting data?
- What keys and policies are linked?
- How many GuardPoints are applied on a client?
- What key is used to protect a specific GuardPoint?
- What CTE resources belong to a specific CipherTrust Manager domain?

Use the **Domain Sharing Data** toggle button to include/exclude information about CTE resources shared across domains.

Dashboard

The dashboard on the Reports page shows the following information:

- **TOTAL CLIENTS:** Shows the total count of registered and unregistered clients on the CipherTrust Manager.
- **CTE LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption* licenses out of available licenses.

-
- **CTE-U LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for UserSpace* licenses out of available licenses.
 - **K8S LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for Kubernetes* licenses out of available licenses.
 - **TOTAL GUARDPOINTS:** Shows the total count of GuardPoints configured on the registered and unregistered clients on the CipherTrust Manager.
 - **ACTIVE GUARDPOINTS:** Shows the count of active GuardPoints on the CipherTrust Manager.
 - **INACTIVE GUARDPOINTS:** Shows the count of inactive GuardPoints on the CipherTrust Manager.

Download Formats

View the latest CTE reports and download them as PDF and CSV documents on your local machines. The PDF and CSV formats present reports in easy-to-understand tabular forms.

Important Note on CSV Reports

If the names of CTE resources include special characters like equals (=), plus (+), minus (-), at (@), tab (0x09), and carriage return (0x0D), the resources are renamed in the downloaded CSV reports by applying the following rules:

- Every cell is wrapped in double quotes
- Every cell is prepended with a single quote
- Every double quote is escaped using an additional double quote

For example, a resource named `=A+B' " ; , =C+D` is renamed as `" '=A+B' '" " ; , =C+D"` in the downloaded CSV report.

To download the Clients Policies Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Profiles** tab.
4. Download the report:
 - Click **Download CSV** to download the report as a CSV file. The file is named `<DOMAIN>_cte_clients_policies_<TIMESTAMP>.csv`, for example, `root_cte_clients_policies_2021-01-12T07_08_43Z.csv`.
 - Click **Download PDF** to download the report as a PDF file. The file is named `<DOMAIN>_cte_clients_policies_<TIMESTAMP>.pdf`, for example, `root_cte_clients_policies_2021-01-12T07_08_50Z.pdf`.

Note

- If the CipherTrust Manager is part of a cluster environment, the filename of the downloaded report (CSV and PDF) will also include the cluster ID.

If the downloaded report is a CSV file, the file will be named <CLUSTER ID><DOMAIN>_cte_client_health_<TIMESTAMP>.csv, for example, **51.26.30.11_root_cte_client_health_2021-01-12T06_52_51Z.csv**. The PDF file will also be named in the same way.

- Exclude at least two columns to download the report in the PDF format. Use the gear icon (⚙️) to select which fields should appear in the report.

The downloaded PDF document shows the **Report Name** as *Clients Policies Report* and time the report is **Generated At**.

Policies Keys Report

The Policies Keys Report shows the list of keys used by the CTE policies. A key can be used by multiple policies, similarly, a policy can have multiple keys. You can download the report as a PDF or CSV document, as required. Refer to [Downloading the Report](#).

Use the "Search by" box to search for records in the report by Policy Name, Key Name, or Domain. When searching for records by domain names, specify the complete and exact domain name including case-sensitivity. For example, searching for "test", "test-domain", and "Test-Domain" will return different search results.

Viewing the Report

To view the Policies Keys Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Policies** tab.

The report shows all or some of the following columns:

Column	Description
Domain	Name of the CipherTrust Manager domain to which the record belongs. The Domain Sharing Data toggle does not affect the Policies Keys report.
Policy Name	Name of the policy.
Description	Description of the policy.
Policy Type	Type of the policy. The type can be:

Column	Description
	• Standard • Live Data Transformation • Cloud Object Storage • In-place Data Transformation • CSI
Key Name	Key used by the policy.

Downloading the Report

Download the report as a PDF or CSV document. Based on the displayed columns and applied filters, the downloaded report shows all or some of the columns listed in [Viewing the Report](#).

Reports provide an easy and quick method to answer queries such as:

- How many clients are registered with the CipherTrust Manager?
- What is the health status of clients?
- How many keys are used for protecting data?
- What keys and policies are linked?
- How many GuardPoints are applied on a client?
- What key is used to protect a specific GuardPoint?
- What CTE resources belong to a specific CipherTrust Manager domain?

Use the **Domain Sharing Data** toggle button to include/exclude information about CTE resources shared across domains.

Dashboard

The dashboard on the Reports page shows the following information:

- **TOTAL CLIENTS:** Shows the total count of registered and unregistered clients on the CipherTrust Manager.
- **CTE LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption* licenses out of available licenses.
- **CTE-U LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for UserSpace* licenses out of available licenses.
- **K8S LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for Kubernetes* licenses out of available licenses.
- **TOTAL GUARDPOINTS:** Shows the total count of GuardPoints configured on the registered and unregistered clients on the CipherTrust Manager.

- **ACTIVE GUARDPOINTS:** Shows the count of active GuardPoints on the CipherTrust Manager.
- **INACTIVE GUARDPOINTS:** Shows the count of inactive GuardPoints on the CipherTrust Manager.

Download Formats

View the latest CTE reports and download them as PDF and CSV documents on your local machines. The PDF and CSV formats present reports in easy-to-understand tabular forms.

Important Note on CSV Reports

If the names of CTE resources include special characters like equals (=), plus (+), minus (-), at (@), tab (0x09), and carriage return (0x0D), the resources are renamed in the downloaded CSV reports by applying the following rules:

- Every cell is wrapped in double quotes
- Every cell is prepended with a single quote
- Every double quote is escaped using an additional double quote

For example, a resource named `=A+B " ; , =C+D` is renamed as `" '=A+B ' "' ; , =C+D"` in the downloaded CSV report.

To download the Policies Keys Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Profiles** tab.
4. Download the report:
 - Click **Download CSV** to download the report as a CSV file. The file is named `<DOMAIN>_cte_policies_keys_<TIMESTAMP>.csv`, for example, `root_cte_policies_keys_2021-01-12T07_11_57Z.csv`.
 - Click **Download PDF** to download the report as a PDF file. The file is named `<DOMAIN>_cte_policies_keys_<TIMESTAMP>.pdf`, for example, `root_cte_policies_keys_2021-01-12T07_13_23Z.pdf`.

Note

If the CipherTrust Manager is part of a cluster environment, the filename of the downloaded report (CSV and PDF) will also include the cluster ID.

If the downloaded report is a CSV file, the file will be named `<CLUSTER`

ID><DOMAIN>_cte_client_health_<TIMESTAMP>.csv, for example, **51.26.30.11_root_cte_client_health_2021-01-12T06_52_51Z.csv**. The PDF file will also be named in the same way.

The downloaded PDF document shows the **Report Name** as *Policies Keys Report* and time the report is **Generated At**.

GuardPoints Report

The GuardPoints Report shows the GuardPoints applied to the CTE clients available on the CipherTrust Manager. A client can have multiple GuardPoints. Similarly, a GuardPoint can be applied to multiple clients. You can download the report as a PDF or CSV document, as required. Refer to [Downloading the Report](#).

Use the "Search by" box to search for records in the report by Client Name, Policy Name, or Domain. When searching for records by domain names, specify the complete and exact domain name including case-sensitivity. For example, searching for "test", "test-domain", and "Test-Domain" will return different search results.

Viewing the Report

To view the GuardPoints Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **GuardPoints** tab.

The report shows all or some of the following columns:

Column	Description
Domain	Name of the CipherTrust Manager domain to which the record belongs. If the Domain Sharing Data toggle is turned ON, the report displays all the domains where the resource is shared.
Client Name	Name of the client on the CipherTrust Manager.
Policy Name	Name of the applied policy.
Guard Path	Path where the GuardPoint is applied.
Guard Type	Type of the GuardPoint. The type can be: • Auto Directory • Manual Directory • Auto Raw Device • Manual Raw Device • Auto Cloud Storage • Manual Cloud Storage • Ransomware Protection Only
Guard Enabled	Whether a GuardPoint is enabled. Value can be Yes or

Column	Description
	No.

Downloading the Report

Download the report as a PDF or CSV document. Based on the displayed columns and applied filters, the downloaded report shows all or some of the columns listed in [Viewing the Report](#).

Reports provide an easy and quick method to answer queries such as:

- How many clients are registered with the CipherTrust Manager?
- What is the health status of clients?
- How many keys are used for protecting data?
- What keys and policies are linked?
- How many GuardPoints are applied on a client?
- What key is used to protect a specific GuardPoint?
- What CTE resources belong to a specific CipherTrust Manager domain?

Use the **Domain Sharing Data** toggle button to include/exclude information about CTE resources shared across domains.

Dashboard

The dashboard on the Reports page shows the following information:

- **TOTAL CLIENTS:** Shows the total count of registered and unregistered clients on the CipherTrust Manager.
- **CTE LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption* licenses out of available licenses.
- **CTE-U LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for UserSpace* licenses out of available licenses.
- **K8S LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for Kubernetes* licenses out of available licenses.
- **TOTAL GUARDPOINTS:** Shows the total count of GuardPoints configured on the registered and unregistered clients on the CipherTrust Manager.
- **ACTIVE GUARDPOINTS:** Shows the count of active GuardPoints on the CipherTrust Manager.
- **INACTIVE GUARDPOINTS:** Shows the count of inactive GuardPoints on the CipherTrust Manager.

Download Formats

View the latest CTE reports and download them as PDF and CSV documents on your local machines. The PDF and CSV formats present reports in easy-to-understand tabular forms.

Important Note on CSV Reports

If the names of CTE resources include special characters like equals (=), plus (+), minus (-), at (@), tab (0x09), and carriage return (0x0D), the resources are renamed in the downloaded CSV reports by applying the following rules:

- Every cell is wrapped in double quotes
- Every cell is prepended with a single quote
- Every double quote is escaped using an additional double quote

For example, a resource named `=A+B ' " ; , =C+D` is renamed as `" ' =A+B ' " " ; , =C+D "` in the downloaded CSV report.

To download the GuardPoints Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **GuardPoints** tab.
4. Download the report:
 - Click **Download CSV** to download the report as a CSV file. The file is named `<DOMAIN>_cte_guardpoints_<TIMESTAMP>.csv`, for example, `root_cte_guardpoints_2021-01-12T07_15_38Z.csv`.
 - Click **Download PDF** to download the report as a PDF file. The file is named `<DOMAIN>_cte_guardpoints_<TIMESTAMP>.pdf`, for example, `root_cte_guardpoints_2021-01-12T07_17_21Z.pdf`.

Note

If the CipherTrust Manager is part of a cluster environment, the filename of the downloaded report (CSV and PDF) will also include the cluster ID.

If the downloaded report is a CSV file, the file will be named `<CLUSTER ID><DOMAIN>_cte_client_health_<TIMESTAMP>.csv`, for example, `51.26.30.11_root_cte_client_health_2021-01-12T06_52_51Z.csv`. The PDF file will also be named in the same way.

The downloaded PDF document shows the **Report Name** as *GuardPoints Report* and time the report is **Generated At**.

Clients GuardPoint Status Report

The Clients GuardPoint Status Report shows the status of GuardPoints applied to the CTE clients available on the CipherTrust Manager. The report also shows the states of the GuardPoints and whether they are enabled or not. You can download the report as a PDF or CSV document, as required. Refer to [Downloading the Report](#).

Use the "Search by" box to search for records in the report by Client Name, Policy Name, or Domain. When searching for records by domain names, specify the complete and exact domain name including case-sensitivity. For example, searching for "test", "test-domain", and "Test-Domain" will return different search results.

Viewing the Report

To view the Clients GuardPoint Status Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Guard Status** tab.

The report shows all or some of the following columns:

Column	Description
Domain	Name of the CipherTrust Manager domain to which the record belongs. If the Domain Sharing Data toggle is turned ON, the report displays all the domains where the resource is shared.
Client Name	Name of the client on the CipherTrust Manager.
Policy Name	Name of the applied policy.
Key Name	Name of the key used to protect the GuardPoint.
Guard Path	Path where the GuardPoint is applied.
Guard State	State of the GuardPoint. The state can be: • Active • Inactive • Unknown • Disabled
Guard Enabled	Whether a GuardPoint is enabled. Value can be Yes or No.

Downloading the Report

Download the report as a PDF or CSV document. Based on the displayed columns and applied filters, the downloaded report shows all or some of the columns listed in [Viewing the Report](#).

Reports provide an easy and quick method to answer queries such as:

-
- How many clients are registered with the CipherTrust Manager?
 - What is the health status of clients?
 - How many keys are used for protecting data?
 - What keys and policies are linked?
 - How many GuardPoints are applied on a client?
 - What key is used to protect a specific GuardPoint?
 - What CTE resources belong to a specific CipherTrust Manager domain?

Use the **Domain Sharing Data** toggle button to include/exclude information about CTE resources shared across domains.

Dashboard

The dashboard on the Reports page shows the following information:

- **TOTAL CLIENTS:** Shows the total count of registered and unregistered clients on the CipherTrust Manager.
- **CTE LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption* licenses out of available licenses.
- **CTE-U LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for UserSpace* licenses out of available licenses.
- **K8S LICENSES USED:** Shows the count of consumed *CipherTrust Transparent Encryption for Kubernetes* licenses out of available licenses.
- **TOTAL GUARDPOINTS:** Shows the total count of GuardPoints configured on the registered and unregistered clients on the CipherTrust Manager.
- **ACTIVE GUARDPOINTS:** Shows the count of active GuardPoints on the CipherTrust Manager.
- **INACTIVE GUARDPOINTS:** Shows the count of inactive GuardPoints on the CipherTrust Manager.

Download Formats

View the latest CTE reports and download them as PDF and CSV documents on your local machines. The PDF and CSV formats present reports in easy-to-understand tabular forms.

Important Note on CSV Reports

If the names of CTE resources include special characters like equals (=), plus (+), minus (-), at (@), tab (0x09), and carriage return (0x0D), the resources are renamed in the downloaded CSV reports by applying the following rules:

- Every cell is wrapped in double quotes

- Every cell is prepended with a single quote
- Every double quote is escaped using an additional double quote

For example, a resource named `=A+B' " ; , =C+D` is renamed as `"' =A+B' '" " ; , =C+D"` in the downloaded CSV report.

To download the Clients GuardPoint Status Report:

1. Open the Transparent Encryption application.
2. In the left pane, click **Reports**. The Reports page is displayed.
3. Click the **Clients Guard Status** tab.
4. Download the report:
 - Click **Download CSV** to download the report as a CSV file. The file is named `<DOMAIN>_cte_clients_gp_status_<TIMESTAMP>.csv`, for example, `root_cte_clients_gp_status_2020-11-30T13_29_25Z.csv`.
 - Click **Download PDF** to download the report as a PDF file. The file is named `<DOMAIN>_cte_clients_gp_status_<TIMESTAMP>.pdf`, for example, `root_cte_clients_gp_status2021-01-12T07_18_55Z.pdf`.

Note

If the CipherTrust Manager is part of a cluster environment, the filename of the downloaded report (CSV and PDF) will also include the cluster ID.

If the downloaded report is a CSV file, the file will be named `<CLUSTER ID><DOMAIN>_cte_client_health_<TIMESTAMP>.csv`, for example, `51.26.30.11_root_cte_client_health_2021-01-12T06_52_51Z.csv`. The PDF file will also be named in the same way.

The downloaded PDF document shows the **Report Name** as *Clients GuardPoint Status Report* and time the report is **Generated At**.

Troubleshooting

This section describes how to handle the issues that you might face when using CTE with the CipherTrust Manager.

Connection Issues

Symptoms	Possible Cause and Remediation
- Client status is Error - Configuration changes are not pushed to the client - Requests like Browse file system are failing	Analyze the CTE logs, identify connection failure reasons, and rectify them: - Look for the issues in the <code>/var/log/vormetric/server_comms.log</code> file on the CTE agent. This file contains information about the CipherTrust Manager's communication with the client. - Identify the cause of the issue. - Restart <code>vmd</code> to get the latest <code>init</code>.
Client status is Error This can occur for CTE clients running version 7.4.0 or lower when a CipherTrust Manager node in a cluster goes down.	With CTE Agent versions 7.4.0 and lower, this issue occurs because they lack the functionality for the default server health check setting (<code>server_response_rate</code> set to 0). This capability was introduced in a later version. Workaround: In the client's profile, change <code>server_response_rate</code> from the default of 0 to a value between 1 and 100 using the <code>/v1/transparent-encryption/profiles/</code> API. This parameter sets a health threshold. For example, a value of 75 means the server is considered healthy if 75% or more of its API calls succeed. If the success rate drops below this threshold, the agent marks the server as unhealthy.

Registration Issues

Symptoms	Possible Cause and Remediation
Registration fails with conflict errors	Conflict errors occur when a client with the given name already exists on the CipherTrust Manager. To fix these issues: - Delete the existing client entry from the CipherTrust Manager. - Unenroll the existing client if you want to register it with another CipherTrust Manager. NOTE: A conflict error might occur even if no CTE client with the given name exists on the CipherTrust Manager. This happens because the client's entry, which was added during registration, is no longer associated with the CTE client due to any failure in enrollment. To resolve this issue: - Run the API <code>/v1/transparent-encryption/clients/delete</code> with the flag <code>delete_stale_clients</code> set to <code>true</code>. DON'T specify any other parameters when running the API. Alternatively, run the command <code>ksctl cte clients bulk-delete --delete-stale-clients true</code> on the CLI. This cleans up the stale client entries. - Retry registration with the same name.

Symptoms	Possible Cause and Remediation
Reregistration fails with capabilities related errors	Capabilities cannot be disabled during reregistration with the CipherTrust Manager. To disable the CTE Agent capabilities, delete the client from the CipherTrust Manager and register again with these capabilities disabled.

Backup and Restore Issues

Symptoms	Possible Cause and Remediation
Reregistration issues after CipherTrust Manager is restored on a new CipherTrust Manager appliance	After the backup of a CipherTrust Manager is restored to another CipherTrust Manager, CTE client reregistration does not work as expected. To work around this issue: 1. Before taking the backup, disable or stop the LDT GuardPoints on the current CipherTrust Manager. 2. Back up the CipherTrust Manager. 3. Restore the backup to another CipherTrust Manager. 4. Unenroll the client using the UnEnroll option on the details view of the Clients page. 5. Reregister the CTE client with the restored CipherTrust Manager.

Licensing Issues

Symptoms	Possible Cause and Remediation
• Registration fails with licensing errors • LDT feature cannot be used • CTE configurations are read-only	Registration can fail if the number of purchased licenses are consumed or the validity of a license is expired. This is applicable for all types of licenses: the base license (CTE - TransparentEncryption), the CTE for Kubernetes license (CTE - KubernetesProtection), and the add-on license (CTE - LiveDataTransformation). • To enable LDT at the time of registration (or later), make sure that you have a valid base license and a valid add-on LDT license. • After a license is expired: – A new client cannot be registered. – Existing operations on registered clients remain in tact. Their existing security configurations are pushed as and when required.

Configuration Issues

Symptoms	Possible Cause and Remediation
Mismatched log levels between the CipherTrust Manager configuration and client logs	Try these: • Check the configuration in the linked profile on the CipherTrust Manager. • Validate the vmd configuration on the CTE client by running: <pre>vmsec vmdconfig</pre>

API Examples

This section provides examples to use different CTE APIs to perform the following tasks:

- [Creating Keys](#)
- [Creating Policy Elements](#)
- [Creating Policies](#)
- [Creating GuardPoints](#)
- [LDT Use Cases](#)

For description of different response codes returned when running CTE APIs, refer to [API Response Codes](#).

Creating Keys

This section describes steps to create an encryption key using the CTE API.

Overview

Keys in a CTE policy must fulfill the following conditions. The keys should:

- Have the **CTE Clients** group permissions
- Be exportable
- Be non-versioned/versioned
- Be of the type "CBC" / "CBC_CS1" or "XTS"

Note

The XTS keys are required for creating GuardPoints with In-place Data Transformation (IDT) policies.

- Have metadata with the following details:

```
{
  "cte": {
    "is_used": <true/false>,
    "cte_versioned": <true/false>,
    "encryption_mode": <"CBC"/"CBC_CS1"/"XTS">,
    "persistent_on_client": <true/false>
  },
  "ownerId": "string",
  "permissions": {
    "ReadKey": [
      "CTE Clients"
    ],
    "ExportKey": [
      "CTE Clients"
    ]
  }
}
```

CTE supports standard, LDT, COS, and IDT policies. Click the following tabs for policy-specific key requirements.

Standard

Keys for Standard Policies

- Standard policies support only non-versioned keys.
- Keys should have the CTE Clients group access.
- CTE Clients group should have the Read Key and Export Key permissions.
- Standard policies support "CBC" / "CBC_CS1" keys.

API

```
/v1/vault/keys2/
```

Sample

```
{
  "name": "Standard_pol_key",
  "algorithm": "aes",
  "size": 256,
  "undeletable": true,
```

```

"unexportable": false,
"meta": {
  "ownerId": "local|f02d8ec9-34dd-42fd-99e7-85cb7f18180c",
  "permissions": {
    "DecryptWithKey": [
      "CTE Clients"
    ],
    "EncryptWithKey": [
      "CTE Clients"
    ],
    "ExportKey": [
      "CTE Clients"
    ],
    "MACVerifyWithKey": [
      "CTE Clients"
    ],
    "MACWithKey": [
      "CTE Clients"
    ],
    "ReadKey": [
      "CTE Clients"
    ],
    "SignVerifyWithKey": [
      "CTE Clients"
    ],
    "SignWithKey": [
      "CTE Clients"
    ],
    "UseKey": [
      "CTE Clients"
    ]
  },
  "cte": {
    "persistent_on_client": true,
    "encryption_mode": "CBC",
    "cte_versioned": false
  }
},
"xts": false
}

```

LDT

Keys for LDT Policies

- LDT policies support only "CBC" and "CBC_CS1" keys.
- Keys should have the CTE Clients group access.
- CTE Clients group should have the Read Key and Export Key permissions.
- LDT policies support only non-versioned keys in the "current_key" field.
- LDT policies support only versioned keys in the "transformation_key" field.

API

```
/v1/vault/keys2/
```

Sample

Click the tabs to view the samples for the current key and transformation key.

Current Key

Sample for the Current Key

```
{
  "name": "LDT_Current_Key",
  "algorithm": "aes",
  "size": 256,
  "undeletable": true,
  "unexportable": false,
  "meta": {
    "ownerId": "local|f02d8ec9-34dd-42fd-99e7-85cb7f18180c",
    "permissions": {
      "DecryptWithKey": [
        "CTE Clients"
      ],
      "EncryptWithKey": [
        "CTE Clients"
      ],
      "ExportKey": [
        "CTE Clients"
      ],
      "MACVerifyWithKey": [
        "CTE Clients"
      ],
      "MACWithKey": [
        "CTE Clients"
      ],
      "ReadKey": [
        "CTE Clients"
      ],
      "SignVerifyWithKey": [
        "CTE Clients"
      ],
      "SignWithKey": [
        "CTE Clients"
      ],
      "UseKey": [
        "CTE Clients"
      ]
    },
    "cte": {
      "persistent_on_client": true,
      "encryption_mode": "CBC",
      "cte_versioned": false
    }
  },
}
```



```
"xts": false
}
```

Transformation Key

Sample for the Transformation Key

```
{
  "name": "LDT_transformation_key",
  "algorithm": "aes",
  "size": 256,
  "undeletable": true,
  "unexportable": false,
  "meta": {
    "ownerId": "local|f02d8ec9-34dd-42fd-99e7-85cb7f18180c",
    "permissions": {
      "DecryptWithKey": [
        "CTE Clients"
      ],
      "EncryptWithKey": [
        "CTE Clients"
      ],
      "ExportKey": [
        "CTE Clients"
      ],
      "MACVerifyWithKey": [
        "CTE Clients"
      ],
      "MACWithKey": [
        "CTE Clients"
      ],
      "ReadKey": [
        "CTE Clients"
      ],
      "SignVerifyWithKey": [
        "CTE Clients"
      ],
      "SignWithKey": [
        "CTE Clients"
      ],
      "UseKey": [
        "CTE Clients"
      ]
    },
    "cte": {
      "persistent_on_client": true,
      "encryption_mode": "CBC",
      "cte_versioned": true
    }
  },
  "xts": false
}
```

COS

Keys for COS Policies

- Keys should have the CTE Clients group access.
- CTE Clients group should have the Read Key and Export Key permissions.
- COS policies support only non-versioned keys.
- COS policies support only "CBC_CS1" keys.

API

```
/v1/vault/keys2/
```

Sample

```
{
  "name": "COS_Key",
  "algorithm": "aes",
  "size": 256,
  "undeletable": true,
  "unexportable": false,
  "meta": {
    "ownerId": "local|f02d8ec9-34dd-42fd-99e7-85cb7f18180c",
    "permissions": {
      "DecryptWithKey": [
        "CTE Clients"
      ],
      "EncryptWithKey": [
        "CTE Clients"
      ],
      "ExportKey": [
        "CTE Clients"
      ],
      "MACVerifyWithKey": [
        "CTE Clients"
      ],
      "MACWithKey": [
        "CTE Clients"
      ],
      "ReadKey": [
        "CTE Clients"
      ],
      "SignVerifyWithKey": [
        "CTE Clients"
      ],
      "SignWithKey": [
        "CTE Clients"
      ],
      "UseKey": [
```

```

    "CTE Clients"
  ]
},
"cte": {
  "persistent_on_client": true,
  "encryption_mode": "CBC_CS1",
  "cte_versioned": false
}
},
"xts": true
}

```

IDT

Keys for IDT Policies

- Keys should have the CTE Clients group access.
- CTE Clients group should have the Read Key and Export Key permissions.
- IDT policies support only the "XTS" encryption mode.
- IDT policies support only non-versioned keys in the "current_key" and "transformation_key" fields.
- IDT policies are used for IDT-capable devices.

API

```
/v1/vault/keys2/
```

Sample

Click the tabs to view the samples for the current key and transformation key.

Current Key

Sample for the Current Key

```

{
  "name": "IDT_Policy_Current_key",
  "algorithm": "aes",
  "size": 256,
  "undeletable": true,
  "unexportable": false,
  "meta": {
    "ownerId": "local|f02d8ec9-34dd-42fd-99e7-85cb7f18180c",
    "permissions": {
      "DecryptWithKey": [
        "CTE Clients"
      ]
    }
  }
}

```

```

    "EncryptWithKey": [
      "CTE Clients"
    ],
    "ExportKey": [
      "CTE Clients"
    ],
    "MACVerifyWithKey": [
      "CTE Clients"
    ],
    "MACWithKey": [
      "CTE Clients"
    ],
    "ReadKey": [
      "CTE Clients"
    ],
    "SignVerifyWithKey": [
      "CTE Clients"
    ],
    "SignWithKey": [
      "CTE Clients"
    ],
    "UseKey": [
      "CTE Clients"
    ]
  },
  "cte": {
    "persistent_on_client": true,
    "encryption_mode": "XTS",
    "cte_versioned": false
  }
},
"xts": true,
"id": "694bf52e-d0c2-4416-b615-feab9ce27940"
}

```

Transformation Key

Sample for the Transformation Key

```

{
  "name": "IDT_Policy_Transformation_Key",
  "algorithm": "aes",
  "size": 256,
  "undeletable": true,
  "unexportable": false,
  "meta": {
    "ownerId": "local|f02d8ec9-34dd-42fd-99e7-85cb7f18180c",
    "permissions": {
      "DecryptWithKey": [
        "CTE Clients"
      ],
      "EncryptWithKey": [
        "CTE Clients"
      ],
      "ExportKey": [
        "CTE Clients"
      ],
    ]
  }
}

```

```

    "MACVerifyWithKey": [
      "CTE Clients"
    ],
    "MACWithKey": [
      "CTE Clients"
    ],
    "ReadKey": [
      "CTE Clients"
    ],
    "SignVerifyWithKey": [
      "CTE Clients"
    ],
    "SignWithKey": [
      "CTE Clients"
    ],
    "UseKey": [
      "CTE Clients"
    ]
  },
  "cte": {
    "persistent_on_client": true,
    "encryption_mode": "XTS",
    "cte_versioned": false
  }
},
"xts": true,
"id": "d32d1b65-5a09-403e-921d-8d1c8db39a75"
}

```

Deleting CTE Keys

- A CTE key cannot be deleted if it is being used in a policy.
- The CTE Admins and Key Admins group permissions are required to delete a CTE key.

API

```
/v1/vault/keys2/{id} [DELETE]
```

Creating Policy Elements

Policy rule criteria consist of resource sets, user sets, signature sets, process sets, action, and effect, and are called policy elements. These elements should exist on the CipherTrust Manager before you can use them in security policies. This section describes steps to create policy elements using the CTE API.

Click the following tabs for details on policy elements.

User Sets

Creating User Sets

- The `name` field is mandatory for creating a user set.
- Any number of users can be added to a single user set.
- Add users by specifying `uname`, `gname`, `uid`, or `gid`.

The following sample creates a user set, `UserSet1` having two users, `user1` and `user2`.

API

```
/v1/transparent-encryption/usersets
```

Sample

```
{
  "name": UserSet1,
  "users": [
    {
      "gid": 1001,
      "gname": "user1",
      "os_domain": "Linux",
      "uid": 1001,
      "uname": "user1"
    },
    {
      "gid": 1002,
      "gname": "user2",
      "os_domain": "Linux",
      "uid": 1002,
      "uname": "user2"
    }
  ]
}
```

Resource Sets

Creating Resource Sets

- The `name` field is mandatory for creating a resource set.
- The `type` field determines the type of the resource set. The type can be `Directory` or `Classification`. The default type is `Directory`.
- Any number of resources can be added to a single resource set.

- Add resources by specifying paths using `directory` and/or `file` fields. For `Directory` type resource sets, you can specify whether to include subdirectories by using `include_subfolders`. Set to `true` to include subdirectories, set to `false` to exclude.
- Set `hdfs` to `true` for an HDFS path.

The following samples create two resource sets, `ResourceSet1` and `ResourceSetHDFS1` of the type `Directory` having two resources.

API

```
/v1/transparent-encryption/resourcesets
```

Sample

```
{
  "name": "ResourceSet1",
  "resources": [
    {
      "directory": "/home/test-user/dir1/",
      "file": "*.txt",
      "include_subfolders": true
    },
    {
      "directory": "/home/test-user/dir2/",
      "file": "*.bin",
      "include_subfolders": true
    }
  ],
  "type": "Directory"
}
```

Sample (HDFS)

```
{
  "name": "ResourceSetHDFS1",
  "resources": [
    {
      "directory": "/home/test-user/dir3/",
      "file": "*.txt",
      "include_subfolders": true,
      "hdfs": true
    },
    {
      "directory": "/home/test-user/dir4/",
      "file": "*.bin",
      "include_subfolders": true,
      "hdfs": true
    }
  ],
  "type": "Directory"
}
```

Signature Sets

Creating Signature Sets

- The **name** field is mandatory for creating a signature set.
- Any number of sources can be added to a single signature set.

The following sample creates a signature set, **SignatureSet1** having a **source_list** of two processes, **/usr/bin** and **/usr/sbin**.

API

```
/v1/transparent-encryption/signaturesets
```

Sample

```
{
  "name": "SignatureSet1",
  "source_list": [
    "/usr/bin",
    "/usr/sbin"
  ]
}
```

Process Sets

Creating Process Sets

- The **name** field is mandatory for creating a process set.
- Any number of processes can be added to a single process set.
- Add processes by specifying their details using **signature**, **directory**, and/or **file**.

The following sample creates a process set, **ProcessSet1** having two processes with their **signature**, **directory**, and process **file** name.

API

```
/v1/transparent-encryption/processsets
```

Sample

```
{
  "name": "ProcessSet1",
```



```

"processes": [
  {
    "signature": "SignatureSet1",
    "directory": "/home/testUser",
    "file": "*"
  },
  {
    "signature": "SignatureSet2",
    "directory": "/home/kyloTest",
    "file": "kylo.bin"
  }
]
}

```

Creating Policies

This section describes steps to create policies using the CTE API. CTE supports Standard, LDT, COS, and IDT policies. Different types of policies can have different types of security and key rule requirements, as described in the sections below. Also, key uses can be different based on the types of policies they are used with. Refer to [Creating Keys](#) for details.

Click the following tabs for policy-specific details, requirements, and samples.

Standard

Creating Standard Policies

A STANDARD policy should contain security rules and/or key rules. At least one of these rules must be added to the standard policy.

The security rules define the access permissions based on the policy elements (user sets, resource set, and process sets). The key rules define what key is used for encryption and decryption of data.

In the following sample, in the security rule:

- All users in the user set "Sample_User_Set1" have read/write access on the processes in the process set "Sample_Process_Set1" and resources in the resource set "Sample_Resource_Set1".
- When a user of "Sample_User_Set1" performs any operation, the policy with the key "Sample_StandardPolicyKey" is applied.

API

```
/v1/transparent-encryption/policies/
```

Sample

```

{
  "never_deny": false,
  "security_rules": [

```

```

    {
      "process_set_id": "Sample_Process_Set1",
      "resource_set_id": "Sample_Resource_Set1",
      "user_set_id": "Sample_User_Set1",
      "exclude_user_set": false,
      "exclude_resource_set": false,
      "exclude_process_set": false,
      "partial_match": true,
      "action": "read,write",
      "effect": "permit,audit,applykey"
    },
    {
      "process_set_id": "",
      "resource_set_id": "",
      "user_set_id": "",
      "exclude_user_set": false,
      "exclude_resource_set": false,
      "exclude_process_set": false,
      "partial_match": true,
      "action": "all_ops",
      "effect": "deny,audit"
    }
  ],
  "policy_type": "Standard",
  "key_rules": [
    {
      "key_id": "Sample_StandardPolicyKey"
    }
  ],
  "name": "Sample_Standard_Policy",
  "description": "This is a sample for a Standard policy."
}

```

LDT

Creating LDT Policies

An LDT policy should contain at least one non-exclusion key rule. The security rules define the access permissions based on the policy elements (user sets, resource set, and process sets).

An LDT policy has two sets of keys, one is the current key and the other is transformation key.

- **Current key:** The key with which the data is encrypted before any transformation. If the data is in plaintext, then the current key should be set as "clear_key".
- **Transformation key:** The key with which the data is to be encrypted. This key must be VERSIONED so that multiple key versions can be created as and when required.

In the following sample, in the security rule:

- All users in the user set "Sample_User_Set1" have "all_ops" access on the processes in the process set "Sample_Process_Set1" and resources in the resource set "Sample_Resource_Set1".
- The key rule indicates that the data on which encryption will be performed is plaintext (the current key as

"clear_key"). The data will be encrypted with the transformation key "Sample_LDTPolicyKey".

API

```
/v1/transparent-encryption/policies/
```

Sample

```
{
  "never_deny": false,
  "security_rules": [
    {
      "action": "key_op",
      "effect": "permit,applykey",
      "type": "default"
    },
    {
      "process_set_id": "Sample_Process_Set1",
      "resource_set_id": "Sample_Resource_Set1",
      "user_set_id": "Sample_User_Set1",
      "exclude_user_set": false,
      "exclude_resource_set": false,
      "exclude_process_set": false,
      "partial_match": true,
      "action": "all_ops",
      "effect": "permit,audit,applykey"
    }
  ],
  "policy_type": "LDT",
  "ldt_key_rules": [
    {
      "is_exclusion_rule": false,
      "current_key": {
        "key_id": "clear_key"
      },
      "transformation_key": {
        "key_id": "Sample_LDTPolicyKey"
      }
    }
  ],
  "name": "Sample_LDT_Policy",
  "description": "This is a sample for an LDT policy."
}
```

COS

Creating COS Policies

A COS policy should contain security rules and/or key rules. At least one of these rules must be added to the COS policy.

The security rules define the access permissions based on the policy elements (user sets, resource set, and process sets). The key rules define what key is used for encryption and decryption of data.

Note

COS policies support the "CBC_CS1" keys only.

In the following sample, in the security rule:

- All users in the user set "Sample_User_Set1" have read/write access on the processes in the process set "Sample_Process_Set1" and resources in the resource set "Sample_Resource_Set1".
- When a user of "Sample_User_Set1" performs any operation, the policy with the key "Sample_COSPolicyKey" is applied.

API

```
/v1/transparent-encryption/policies/
```

Sample

```
{
  "never_deny": false,
  "security_rules": [
    {
      "process_set_id": "Sample_Process_Set1",
      "resource_set_id": "Sample_Resource_Set1",
      "user_set_id": "Sample_User_Set1",
      "exclude_user_set": false,
      "exclude_resource_set": false,
      "exclude_process_set": false,
      "action": "all_ops",
      "effect": "permit,audit,applykey"
    }
  ],
  "policy_type": "Cloud_Object_Storage",
  "key_rules": [
    {
      "key_id": "Sample_COSPolicyKey"
    }
  ],
  "name": "Sample_COS_Policy",
  "description": "This is a sample for a COS policy."
}
```

IDT**Creating IDT Policies**

An IDT policy should contain security rules and/or key rules. At least one of these rules must be added to the standard policy.

The security rules define the access permissions based on the policy elements (user sets, resource set, and process sets). The key rules define what key is used for encryption and decryption of data.

Note

IDT policies support the "XTS" keys only.

In the following sample, in the security rule:

- All users in the user set "Sample_User_Set1" have read/write access on the processes in the process set "Sample_Process_Set1" and resources in the resource set "Sample_Resource_Set1".
- When a user of "Sample_User_Set1" performs any operation, the policy linked with the key "Sample_IDTPolicyKey" is applied.

API

```
/v1/transparent-encryption/policies/
```

Sample

```
{
  "never_deny": false,
  "security_rules": [
    {
      "process_set_id": "Sample_Process_Set1",
      "resource_set_id": "Sample_Resource_Set1",
      "user_set_id": "Sample_User_Set1",
      "exclude_user_set": false,
      "exclude_resource_set": false,
      "exclude_process_set": false,
      "partial_match": true,
      "action": "all_ops",
      "effect": "permit,audit,applykey"
    }
  ],
  "policy_type": "IDT",
  "idt_key_rules": [
    {
      "current_key": "clear_key",
      "transformation_key": "Sample_IDTPolicyKey"
    }
  ],
  "name": "Sample_IDT_Policy",
  "description": "This is a sample for an IDT policy."
}
```

LDT Use Cases

This section describes various LDT scenarios using the CTE APIs.

Suspend/Resume Rekey

The LDT rekey operation can be paused and resumed on the protected LDT clients. Run the `ldtpause` API with `"paused": true` to pause, and `"paused": false` to resume the operation.

API

```
/v1/transparent-encryption/clients/{id}/ldtpause
```

Sample

```
{  
  "paused": <true/false>  
}
```

Key Rotation

On a path guarded using an LDT policy, you can create a new version of the key used for encryption. This triggers the rekey operation on the client for the GuardPath using the rotated key.

API

```
/v1/vault/keys2/{id}/versions
```

Decrypting LDT-protected GuardPoints

This section describes steps to decrypt an LDT-protected GuardPoint using the CTE APIs.

Note

- Reverse migration/decryption is **not** supported for network shares.

To decrypt an LDT-protected GuardPoint:

1. Get the LDT policy currently being used by the GuardPoint.

Run the API

```
get /v1/transparent-encryption/clients/<client-name>/guardpoints
```

Example

```
get /v1/transparent-encryption/clients/ldt-client-name/guardpoints
```

This API returns the list of GuardPoints applied to the client. Copy the value of LDT `"policy_name"` (for example, `ldt-policy`) applied to the desired LDT GuardPoint.

2. Get the key linked to the LDT policy.

Run the API

```
get /v1/transparent-encryption/policies/<ldt-policy-name>/ldtkeyrules
```

Example

```
get /v1/transparent-encryption/policies/ldt-policy/ldtkeyrules
```

This API returns the LDT key rules of the LDT policy. Copy the value of `"key_id"` (for example, `current-key`). This key is used to encrypt the LDT GuardPoint.

3. Clone the current (latest) version of the key to a non-versioned CTE key.

Run the API

```
post /v1/vault/keys2/<current-key-name>/clone
```

Request Parameters

```
{
  "newKeyName": "<clone-key-name>",
  "meta": {
    "cte": {
      "persistent_on_client": true,
      "cte_versioned": false,
      "encryption_mode": "<enc-mode>"
    }
  }
}
```

Note

Make sure that "cte_versioned" is set to false.

Example

```
post /v1/vault/keys2/current-key/clone
{
  "newKeyName": "cloned-key",
  "meta":
  {
    "cte":
    {
      "persistent_on_client":true,
      "cte_versioned":false,
      "encryption_mode":"CBC"
    }
  }
}
```

A new key with the specified name (for example, `cloned-key`) is created with version 0.

4. Create a new LDT policy (for example, `new-ldt-policy`). In "ldt_key_rules", set:
 - The cloned key (`cloned-key`) as the "key_id" for "current_key".
 - `clear_key` as the "key_id" for "transformation_key".

Run the API

```
post /v1/transparent-encryption/policies
```

Request Parameters

```
{
  "name":"<new-ldt-policy-name>",
  "policy_type":"LDT",
  "never_deny":false,
  "security_rules":[
    {
      "effect":"permit,applykey",
      "action":"key_op"
    },
  ],
}
```



```

    {
      "effect": "permit, applykey, audit",
      "action": "all_ops",
      "partial_match": true
    }
  ],
  "ldt_key_rules": [
    {
      "resource_set_id": "<resource-set>",
      "current_key": {
        "key_id": "<clone-key-name>"
      },
      "transformation_key": {
        "key_id": "clear_key"
      }
    }
  ]
}

```

Example

```

post /v1/transparent-encryption/policies
{
  "name": "new-ldt-policy",
  "policy_type": "LDT",
  "never_deny": false,
  "security_rules": [
    {
      "effect": "permit, applykey",
      "action": "key_op"
    },
    {
      "effect": "permit, applykey, audit",
      "action": "all_ops",
      "partial_match": true
    }
  ],
  "ldt_key_rules": [
    {
      "resource_set_id": "",
      "current_key": {
        "key_id": "cloned-key"
      },
      "transformation_key": {

```

```

        "key_id": "clear_key"
      }
    }
  ]
}

```

A new LDT policy with the name `new-ldt-policy` is created.

5. Remove the LDT GuardPoint.

Run the API

```

patch /v1/transparent-encryption/clients/<client-name>/guardpoints/<GuardPoint-resource-id>/unguard/

```

Example

```

patch /v1/transparent-encryption/clients/ldt-client-name/guardpoints/a724ed5d-b5c5-45f3-8b8f-77ec3ec976d1/unguard

```

6. On the CTE client, remove the existing CTE-LDT attributes on the GuardPoint.

Run the Command

```

voradmin ldt attr delete <GuardPoint>

```

Example

```

voradmin ldt attr delete /ldt_path

```

The LDT metadata has been removed from all files in the GuardPoint `/ldt_path`.

7. Create a new GuardPoint for the directory using the new policy.

Run the API

```

post /v1/transparent-encryption/clients/<client-name>/guardpoints

```

Request Parameters

```

{
  "guard_paths": ["/<GuardPath>"],

```

```

    "guard_point_params":
    {
        "is_idt_capable_device":false,
        "guard_point_type":"directory_auto",
        "policy_id":"<new-ldt-policy-name>",
        "preserve_sparse_regions":true
    }
}

```

Example

```

post /v1/transparent-encryption/clients/ldt-client-name/guardpoints
{
    "guard_paths":["/ldt_path"],
    "guard_point_params":
    {
        "is_idt_capable_device":false,
        "guard_point_type":"directory_auto",
        "policy_id":"new-ldt-policy",
        "preserve_sparse_regions":true
    }
}

```

- Wait for the rekey to complete. You can check the rekey status, as described below.

Run the API

```
get /v1/transparent-encryption/clients/<client-name>/guardpoints
```

Example

```
get /v1/transparent-encryption/clients/ldt-client-name/guardpoints
```

When the **"rstatus"** status becomes **"Rekeyed"**, the rekey (decryption) is complete.

Note

- If you have selected **directory_auto**, data transformation begins as soon as the client gets the new policy information from the key manager.
- If you have selected **directory_manual**, use the **secfsd -guard <GuardPoint>** command

on the client to begin data transformation.

9. Remove the GuardPoint. This ensures rekey is no longer triggered for any new data added to the specified GuardPath.

Run the API

```
patch /v1/transparent-encryption/clients/<client-name>/guardpoints/<GuardPoint-resource-id>/unguard/
```

Example

```
patch /v1/transparent-encryption/clients/ldt-client-name/guardpoints/77ec9ec67d3-c5b5-435f-7b8f-a275de45e/unguard
```

Creating GuardPoints

This section describes steps to protect create GuardPoints using the CTE APIs.

To create a GuardPoint:

1. Create keys (non-versioned and/or versioned keys) required for your policy. Standard and COS policies require one key while LDT and IDT policies require two keys. Refer to [Creating Keys](#) for details.
2. Create a policy with the keys created in the previous step. Refer to [Creating Policies](#) for details.
3. Create a GuardPoint using the policy.

Refer to the following sections for the API and sample for creating a GuardPoint. Also, for creating GuardPoints for supported CTE capabilities, refer to [GuardPoint Features](#).

API

```
/v1/transparent-encryption/clients/{clientId}/guardpoints
```

Sample

```
{
  "guard_paths": [
    <GuardPath_Name>
  ],
  "guard_point_params": {
```

```

    "guard_point_type": "directory_auto"/"directory_manual",
    "policy_id": <policy_name>
  }
}

```

Refer to [Creating Policies](#) for information on creating GuardPoints for different policy types.

GuardPoint Features

Depending on the capabilities enabled on the LDT client, you can use Preserve Sparse Region, Secure Start, and LDT over CIFS when creating GuardPoints. The following table lists the platforms and policies they are supported with.

Feature	Supported Platform	Supported Policies
Preserve Sparse Region	Windows, Linux	LDT
Secure Start	Windows	Standard, LDT
LDT over CIFS	Windows	LDT

Click the following tabs for samples to create GuardPoints with these features.

Preserve Sparse Region

The default value is `True`.

Note

The value cannot be changed to `True` if you have set it `False` for a GuardPoint.

```

{
  "guard_paths": [
    <GuardPath_Name>
  ],
  "guard_point_params": {
    "guard_point_type": "directory_auto"/"directory_manual",
    "policy_id": <policy_name>,
    "preserve_sparse_regions": True/False
  }
}

```

Secure Start

```

{
  "guard_paths": [
    <GuardPath_Name>
  ],
  "guard_point_params": {
    "guard_point_type": "directory_auto"/"rawdevice_auto",

```

```

    "policy_id": <policy_name>,
    "early_access": True/False
  }
}

```

LDT over CIFS

```

{
  "guard_paths": [
    <GuardPath_Name>
  ],
  "guard_point_params": {
    "guard_point_type": "directory_auto",
    "policy_id": <policy_name>,
    "cifs_enabled": True/False,
    "network_share_credentials_id":<CIFS connection manager name> (Applicable
if 'cifs_enabled' parameter is TRUE)
  }
}

```

API Response Codes

This section lists the response codes returned by the CTE APIs. The section describes the response codes, corresponding messages, and possible corrective actions to be taken for them.

Clients API

patch /v1/transparent-encryption/clients/{id}/resetpassword

Resets a client's password.

Response Code	Messages	Corrective Actions
400 Bad Request	Client is marked for deletion. Cannot modify CTE Client	Specify a client that is not marked for deletion. The clients marked for deletion cannot be modified.
401 Unauthorised	Unauthorised: Bearer token malformed: Token is expired by 50s	Refresh the authentication token. The current token has expired.
404 Not Found	Resource not found	Specify a valid client ID. A client with the specified ID does not exist.
422 Unprocessable Entity	Client has MANUAL password_creation_method. Cannot generate automatic password	Change the password creation method to MANUAL , and then reset the password.

Client Groups APIs

post /v1/transparent-encryption/clientgroups

Creates a client group.

Response Code	Messages	Corrective Actions
400 Bad Request	Invalid name supplied. The name must consist of alpha-numeric characters; it must start with an alpha character; and the only non-alpha-numeric characters allowed are underscore (_) and dash (-).	Specify a valid client group name.
401 Unauthorized	Unauthorized: Bearer token malformed: Token is expired by 50s	Refresh the authentication token. The current token has expired.
404 Not Found	ClientGroup Profile set Failed: Failed to get CTE profile for ProfileID: <profile-id>. Err: record not found	Specify a valid profile ID.
409 Conflict	Could not create clientgroup as it already exists	Specify a different name for the group. A client group with the specified name already exists.
422 Unprocessable Entity	Validation errors:\ncluster_type: cluster_type is a required field	Specify the cluster type.
422 Unprocessable Entity	Validation errors:\ncluster_type: Key: 'CreateClientGroupParams.cluster_type' Error:Field validation for 'cluster_type' failed on the 'eq=NON-CLUSTER eq=HDFS' tag.	Specify a valid cluster type, NON-CLUSTER or HDFS . The specified cluster type is invalid.

post /v1/transparent-encryption/clientgroups/{id}/clients

Adds a client to a client group.

Response Code	Messages	Corrective Actions
400 Bad Request	Client <client-name> is marked for deletion. Cannot add client to clientgroup. Rejecting complete request	Specify a client that is not marked for deletion. The clients marked for deletion cannot be added to a client group.
401 Unauthorized	Unauthorized: Bearer token malformed: Token is expired by 50s	Refresh the authentication token. The current token has expired.
409 Conflict	Failed to create Client-ClientGroup Association. Error:could not create clientgroupclientassn as it already exists	Ensure that the association of the specified client and the group does not exist. The specified client is already part of the client group.
422 Unprocessable Entity	Failed to get CTE ClientGroup:	Specify a valid client group ID.

Response Code	Messages	Corrective Actions
	record not found	
422 Unprocessable Entity	Failed to get CTE Client: record not found	Specify a valid <code>client_id</code> list.
422 Unprocessable Entity	Validation errors:\nclient_list: client_list must contain at least 1 item	Specify at least one client ID in the <code>client_id</code> list.

How to Configure the External CA for CTE

CipherTrust Transparent Encryption can now use an external certificate, available at a user-defined path, to communicate with CipherTrust Manager.

Prerequisites

- The external certificate must be on the file system and in the PEM format.
- A key pair must already exist for the client and:
 - Must have encryption type of either `sha256WithRSAEncryption` or `ecdsa-with-SHA384`
 - Must be encrypted with a passphrase

Initial Setup

1. Obtain your external CA certificate.
2. Create a certificate using the external CA certificate and key.

CipherTrust Manager Setup

To setup CipherTrust Manager to communicate through an external certificate:

1. Import the CA certificate into the CipherTrust Manager:
 - Navigate to **CA > External > Add External CA**.
 - In the dialog, paste the content of `<ca_certificate_name>.pem` and provide a user-friendly name.

See [Using an Externally Generated Server Certificate for an Interface](#) for more information.
2. Add the CA certificate to trusted sources for the web interface. Go to **Admin Settings > Interfaces > web > Edit > External Trusted CAs**.
3. Restart the web server. Navigate to **Admin Settings > Services > web > Restart**.
4. [Create a Registration Token](#) for the CTE agent.

CTE Agent Setup

1. Create a directory on the system to hold required files, for example:

- Linux/AIX: /root/cert_files
- Windows: c:\temp\cert_files

2. Copy or create the following files in the directory:

- client_cert.pem
- client_key.pem
- passphrase (plain text)

3. (Linux/AIX) Set the environment variable:

```
export EXTERNAL_CERT_DIR=/root/cert_files
```

Registering the Client

- If the agent is installed but registration is pending:
 - Linux/AIX: Run `register_host`
 - Windows: Run `c:\> register_host.exe -extcertdir=c:\temp\cert_files`
- If the agent is not yet installed, and you want to install it and register the client:
 - Linux/AIX: Run `./vee-fs-<release>-<build>-<system>.bin`
 - Windows: Run `c:\> installer.exe -extcertdir=c:\temp\cert_files`

Post Registration

During registration:

1. The certificate file is uploaded to the CipherTrust Manager.
2. The certificate and key files are imported into the CTE PEM store.
3. The key is decoded using the passphrase and re-encoded securely.

After successful registration, the input files should be removed.

Certificate Renewal

- The certificate directory path is stored in `agent.conf` (via `EXTERNAL_CERT_DIR` or `-extcertdir`).
- ~60 days before expiration, CTE agent checks for updated certificate files in this directory.
 - If present, the new certificate is pushed to CipherTrust Manager and applied.
 - If not, a **WARNING** is logged (and/or uploaded to CipherTrust Manager per the logging settings) and retry occurs every 24 hours.

To manually update the certificate set, run the following command. Note that this command does not update the saved path in `agent.conf` for future automatic renewals.

```
vmutil -a vmd -d <ext_cert_Dir> updatecerts
```

If you wish to permanently change the directory path for new certificates, you must update the `EXTERNAL_CERT_DIR` entry in the `agent.conf` file and then restart the `vmd` service.

Note

- If certificate is not updated before expiry, communication may fail and re-registration will be required.
- The renewed certificate must have **exactly the same common name** as the original, or CipherTrust Manager will reject it.

Reference: [Using external certificates for communication between CTE Agent and CipherTrust Manager](#)

How to Change Local CA or External CA for CTE

How to Change Local CA

The CipherTrust Manager allows you to renew the local CA certificates in the certificate chain when they are about to expire.

When a local CA in the certificate chain expires, the entire certificate chain validation fails.

In such scenarios, the user has to create a new CA and renew the client/server certificates or both using the new CA.

When to Renew

To avoid any service downtime, it is recommended to prepare the new Local CA certificate chain in advance before the CA expiration. During the overlapping period, the new server certificate chain as described in the below section should be downloaded and added to the trust store in the client's setup.

How to Renew on the Web Console UI

The CA certificate chain renewal process contains the following steps:

1. Create a new local CA using the same attributes as an existing CA.
2. Renew server certificates issued by the original local CA.

Create a New Local CA Using the Same Attributes as Existing CA

1. Log on to CipherTrust Manager as a user in the Admins group, such as **admin**.
2. Navigate to **CA > Local**.
3. In the **Local Certificate Authorities** table, find the local CA to copy attributes from. Click the corresponding overflow icon (ellipsis) and select **Renew**.

A CSR with the same attributes as the local CA is present in the **Pending CAs** table.

Sign the CSR to Make the New Local CA Active

- **Self-sign:**
 - a. Find the desired CSR in the Pending CAs table.
 - b. Click the overflow icon and select **Self-sign**.
 - c. Set a **Duration (days)**. Default is 365.

Caution

When a CA expires, all the certificates it has issued also expire. If you use a Local CA for client and server certificates that access CipherTrust Manager, you must replace the certificate chain across multiple interfaces and clients before the Local CA expires to maintain communication. When setting the CA duration, consider how often your organization is prepared to perform this maintenance.

- d. Click **Save**. The new Local CA appears in the table.

- **Sign with an Existing Local CA:**
 - a. Find the desired CSR in the Pending CAs table.
 - b. Copy or download the CSR.
 - a. Click the overflow icon.

-
- b. Select either of the following:
 - **Copy CSR** to copy the CSR contents to the clipboard.
 - **Download CSR** to download the CSR as a file.
 - c. In the Local Certificate Authorities table, find the signing CA and click its name.
 - d. Click **Upload CSR** and:
 - a. Specify the **Display name** for the new CA.
 - b. In the **CSR** field, paste CSR text.
 - c. Choose **CA** as Certificate Purpose.
 - e. Set the **Duration in days** before the new CA will expire.

Caution

When a CA expires, all the certificates it has issued also expire. If you use a Local CA for client and server certificates that access CipherTrust Manager, you must replace the certificate chain across multiple interfaces and clients before the Local CA expires to maintain communication. When setting the CA duration, consider how often your organization is prepared to perform this maintenance.

- f. Click **Issue Certificate**.
- g. Copy or download the new CA certificate.
 - a. Find the new CA certificate in the **Certificates issued by** table.
 - b. Click the corresponding overflow icon.
 - c. Select either **Copy** to copy the CA certificate contents to the clipboard, or **Download** to download the CA certificate as a file.
- h. Return to **CA > Local**, locate the CSR in the **Pending CAs** table, click the corresponding overflow icon, and select **Install**.
- i. Choose **Local CA** as Parent CA Type.
- j. From the **Select Local Parent CA** drop-down, select the local CA that signed the CA certificate.
- k. Paste certificate text in the **Certificate** field.
- l. Click **Save**.

▪ Sign with an External CA:

- a. Make sure the external CA is added via **CA > External**. An external CA must exist on this page. If no external CA exists, add one.
- b. Navigate to **CA > Local**.
- c. Find the desired CSR in the Pending CAs table.
- d. Copy or download the CSR.
 - a. Click the overflow icon.
 - b. Select either of the following:
 - **Copy CSR** to copy the CSR contents to the clipboard.
 - **Download CSR** to download the CSR as a file.
- e. Sign the CSR *externally*, then retain the signed certificate.

Caution

When a CA expires, all the certificates it has issued also expire. If you use a Local CA for client and server certificates that access CipherTrust Manager, you must replace the certificate chain across multiple interfaces and clients before the Local CA expires to maintain communication. When setting the CA duration, consider how often your organization is prepared to perform this maintenance.

- f. Return to **CA > Local**, find the CSR in the Pending CAs table, click the corresponding overflow icon, and select **Install**.
- g. Choose **External CA** as Parent CA Type.
- h. From the **Select External Parent CA** drop-down, select the external CA that signed the CA certificate.
- i. Paste certificate text in the **Certificate** field.
- j. Click **Save**.

The new local CA is now created and visible in the Local Certificate Authorities table. Note down the CA's name for renewing certificates.

Renew Server Certificate Using New Local CA

1. Issue a new server certificate from the new CA. See [Issuing Certificate Signed by Local CA](#) for details.
 2. Create a certificate chain in PEM or PKCS12 format with the following in the given order:
-

-
- a. Server certificate
 - b. Intermediate CAs (in hierarchy order). Start with the intermediate CA that issued the server certificate. Next, add the issuer of the intermediate CA, if any. Continue adding any intermediate CAs higher up the hierarchy, each time adding the issuer of the last certificate you uploaded.
 - c. Intermediate CAs, ordered from the one that signed the server certificate up to the one signed by the root CA.
 - d. Root CA

Note

In PEM format, include the server certificate's private key first. In PKCS#12 format, include it last.

3. Upload the chain on CipherTrust Manager's [interface](#) associated with the clients.
 - a. Log on to CipherTrust Manager as a user in the Admins group, such as [admin](#).
 - b. Go to **Admin Settings > Interfaces**.
 - c. In the table, find the interface associated with the clients.
 - Most clients authenticate to the web interface.
 - NAE clients authenticate to the original nae interface, or additional NAE interfaces created later.
 - KMIP clients authenticate to the original kmip interface, or additional KMIP interfaces created later.
 - d. Upload the renewal certificate. See [Upload renewal server certificate](#) for details.

For clients, the uploaded certificate chain is available for [download](#).

4. Add the downloaded certificate to the client trust store.

Now, the clients can use this new chain to set up their environment.

5. (Optional) After the clients have been updated with the new certificate chain, [apply](#) the new certificate chain on CipherTrust Manager. This immediately replaces the existing server certificates with the newly generated server certificates.

If not applied manually, the new certificate chain will auto-apply when the CA expires.

See [Renewing Local CA certificate](#) for details.

How to Change External CA

To use an external CA as a trusted entity:

1. Log on to CipherTrust Manager as a user in the Admins group, such as **admin**.
2. Navigate to **CA > External**.
3. Click **+ Add External CA**.
4. Specify a Display Name.
5. Specify a certificate (upload or paste).
 - Upload: Select **File Upload > Upload Certificate** to upload the certificate file.
 - Paste: Select **Text** and paste the certificate content in the text field.
6. Click **Add External CA**.

See [Adding an External CA](#) for details.

How to Renew the Client Certificates

Renewing the Local CA

Client certificates are automatically renewed starting 60 days before expiration. The agent retries daily until successful.

You can also renew the client certificates manually:

- **Linux:** `./vmutil -a vmd renewcerts`
- **Windows:** `vmutil -a vmd renewcerts` (`vmutil` is located at `C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin`)

Renewing the External CA

Client certificates from an external CA are not automatically renewed. To renew:

1. Place the new certificate and key files in the designated folder on the client.
2. Run the following command:
 - **Linux:** `./vmutil -a vmd updatecerts`
 - **Windows:** `vmutil -a vmd updatecerts` (`C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin`)

References

- [Certificate Renewal](#)
- [Automatic Renewal of Client Certificates](#)

CipherTrust Batch Data Transformation

Secure Static Data Masking



Static Data Masking

Static Data Masking refers to the process of transforming selected data in various data stores to unreadable or unusable forms, typically order to utilize data sets while preventing misuse of sensitive data.

CipherTrust Batch Data Transformation offers high-performance static data masking with centralized encryption key management as part of the [CipherTrust Data Security Platform](#). It leverages the power of [CipherTrust Application Data Protection](#) and [CipherTrust Tokenization](#) to protect vast quantities of data quickly. It also can be used as a high-performance encryption or tokenization solution for compliance.

The breadth of use cases for static data masking is surprisingly large. These first four begin with “masking sensitive data”:

1. Prior to third-party data sharing
2. In databases shared with development, QA, R&D, or data science/analytics teams
3. Before adding a data set to a data lake or big data environment
4. In advance of starting big data extract, transform and load (ETL) operations

Batch Data Transformation has many other use cases beyond Static Data Masking. Here are a couple of examples:

- Preparing a database for tokenization or encryption deployment
- Rekeying data in a database following a new key version or key rotation

Key Advantages

Secure, cost-effective static data masking

Not every static data masking solution is secure. With Batch Data Transformation, you can depend on the security of centralized key management provided by [CipherTrust Manager](#), which can provide up to FIPS 140-2 Level 3 key security. Meanwhile, every investment in the Data Security Platform makes it more valuable to you.

Accelerate Transformation of Existing Sensitive Data

Following deployment and execution of [CipherTrust Data Discovery and Classification](#), you can protect sensitive information in database columns quickly and efficiently using either encryption or tokenization with minimal disruption, effort and cost.

Enable database sharing with reduced risk

Static data masking enables you to remove sensitive information before sharing with third-party developers and big data environments while maintaining data integrity and still supporting mission-critical testing and analytical activities.

Static Data Masking where you need it

Batch Data Transformation and its data protection tools are all software and completely cloud friendly. You can mask data on premises and use it in the cloud, mask data in the cloud and use it there, or secure data in one cloud and use it in another.

The CipherTrust Data Security Platform provides a wide range of data protection capabilities from on-premises to cloud, enabling secure digital transformations.

Batch Data Transformation Key Features

Efficient and Flexible Encryption

Large volumes of data are encrypted quickly with Batch Data Transformation in conjunction with CipherTrust Application Data Protection installed on the same server. Policy files define encryption options including standard AES encryption or format preserving encryption, while identifying the database columns to be protected and the number of records in each batch. Data filtering enables creation of customized destination record subsets.

Batch Data Transformation offers a choice in encryption “operating modes”:

- Encryption keys provided by CipherTrust Manager are cached on the Batch Data Transformation server where encryption occurs
- Encryption operations can occur on CipherTrust Manager. This mode is available for the highest security transformation environments where there is a requirement to retain the key in the key source

Flexible Tokenization

An alternative to encryption in Batch Data Transformation is tokenization. Batch Data Transformation can utilize the CipherTrust Tokenization Server to tokenize select database columns. Detokenization is supported so that applications can access the clear data again when required, or, irreversible tokenization can ensure that third parties never gain access to original sensitive data.

Flexible Conversion Between Data Stores

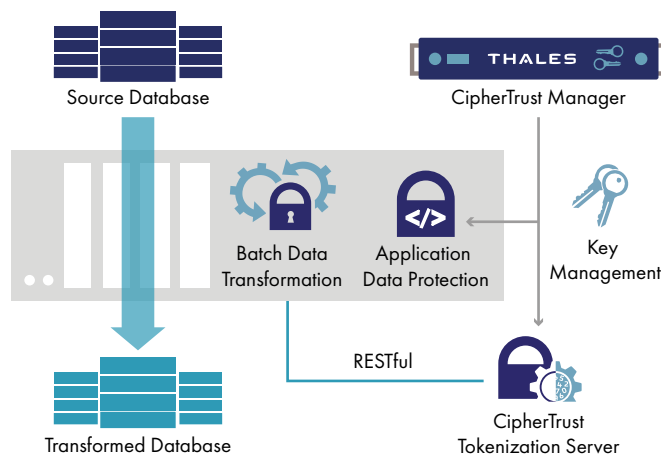
CipherTrust Batch Data Transformation can protect data while it is moving, for example, from a database to various flat file formats or in reverse. CipherTrust Batch Data Transformation supports:

- Flat-file (CSV) to flat-file
- Flat-file to Database
- Database to flat-file
- Database to Database

Supported databases include

- Oracle
- Microsoft SQL Server
- Oracle MySQL
- IBM DB2
- SAP HANA

Transformation from a source database is read-only, so production databases may be used transparently.



CipherTrust Data Security Platform

CipherTrust Tokenization is part of the CipherTrust Data Security Platform, which unifies data discovery, classification, data protection, and unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations and reduces risk across your business. You can rely on Thales CipherTrust Data Security Platform to help you discover, protect and control your organization's sensitive data

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.



CipherTrust Batch Data Transformation (BDT)

Version: v3.0.0 (latest)

30 January 2026

Contents

- Administration 3
 - Quick Start 5
 - Alternative Deployment Methods 31
 - Deploy BDT in Kubernetes Environment (without Helm Chart) 31
 - Deploy BDT as a Standalone Container 36
 - Transformation Process 41
 - Tasks..... 46
 - How to protect data 46
 - How to reveal data 58
 - How to reprotect data 66
 - Change key manager 74
 - Change application 75
 - View logs in Kubernetes environment..... 75
 - Monitoring BDT health 76
 - Renewing client certificate 77
 - Advanced Topics 77
 - Environment Variables 77
 - Concepts 78
 - Protection Policy 80
 - BDT Logging 84
 - Fixed-length Format File 84
 - Supported Encoding 85
 - Behavior of BDT on Container Shutdown 90
 - Unprocessed Record File 91
 - Using Text Qualifier Characters in Input Files 91
 - Using JDBC Driver URLs 92
 - Thread Count and Batch Sizes 94
 - Troubleshooting 94

Administration

CipherTrust Batch Data Transformation (BDT) is a high-performance, scalable, and containerized data security solution designed to securely process large volumes of sensitive data in bulk. It leverages advanced protection mechanisms, such as encryption, tokenization, and data masking, ensuring that sensitive information is protected across various files and databases.

BDT integrates seamlessly with [Application Data Protection](#) on CipherTrust Manager, enabling organizations to centrally configure, manage, and enforce data-centric cryptographic policies and job configurations in a reusable, human-readable format, providing flexibility and ease of management. Jobs can be initiated directly from CipherTrust Manager, where users can also monitor the intermediate status of the data transformation process.

BDT offers flexibility in how data is processed, allowing transformations either in place (within the same location) or by generating transformed data in a separate file or database. This adaptability makes it an ideal solution for organizations looking to securely manage and transform large-scale sensitive data, ensuring both scalability and efficiency.

Specifications

Supported Transformations

BDT supports the following transformations:

Database to database (DB-to-DB)

Protects, reveals, or reprotects the data of a database table and move it to another database. Multiple tables can be transformed in a single execution. You can choose table columns and specify what action needs to be performed on a particular column.

Database to file (DB-to-File)

Protects, reveals, or reprotects the data of a database table and move it to another file. You can choose table columns and specify what action needs to be performed on a particular column.

File to database (File-to-DB)

Protects, reveals, or reprotects the data of a file and move it to another database. You can choose file columns and specify what action needs to be performed on a particular column.

File to file (File-to-File)

Protects, reveals, or reprotects the data of a file and move it to another file. You can choose file columns and specify what action needs to be performed on a particular column.

In-Place Transformation

BDT also supports **In-Place Transformation**, where the *source and destination tables are same and transformation takes place within the same table of the database*. This transformation is only applicable to database. For In-Place transformation to work, a **Primary Key column** must be available in the table.

For SQL Server, primary key should be a non-clustered index key.

Supported File Formats

BDT accepts the input and output files in the following formats:

- CSV
- Fixed-length format

Supported Databases

- MySQL
- Oracle
- IBM Db2
- SAP HANA
- Microsoft SQL Server
- PostgreSQL

For supported database versions, refer to [Release Notes](#).

Supported Algorithms

- FPE/AES
- FPE/FF1v2
- FPE/FF3
- FPE/FF3-1
- AES/CBC/NoPadding
- AES/CBC/PKCS5Padding
- AES/ECB/NoPadding
- AES/ECB/PKCS5Padding
- AES/GCM (Support available in CipherTrust Manager 2.22 and higher versions)

Supported Operations

- Protect

-
- Reveal
 - Reprotect

Licensing

BDT is licensed per deployed instance. Licenses for BDT are part of the Flex Connector Premium. Refer to [Batch Data Transformation Licensing Model](#) for details.

Quick Start

This section describes how to get BDT up and running in less than 10 minutes using a Helm Chart. Refer to [Alternative Deployment Methods](#) for instructions on deployment as a standalone container or deployment without a Helm Chart.

Prerequisites

- Kubernetes environment is up and running and kubectl is installed.
- Helm is installed. Refer to <https://helm.sh/docs/intro/install/> for details.
- CipherTrust Manager 2.19 or higher is up and running. Refer to [CipherTrust Manager Deployment](#) for details.
- Docker hub must be accessible.
- BDT image repository, [thalesciphertrust/ciphertrust-batch-data-transformation](#), is accessible. This repository contains images for BDT. The image path with the **latest** tag always points to the latest release.

Note

- The instructions provided in this section are for deploying BDT in the default namespace.
- The user is responsible for maintaining the **security of their deployment environment**.
- This sample values are enclosed within `< >`, for example, `<target_directory>`. Replace these values with the actual values per your environment.

Following section provides instructions for deploying BDT within the Kubernetes Pod for both **File-to-File** and **DB-to-DB** transformations. Click the tab of your choice.

DB-to-DB

Steps for DB-to-DB

1. Create a BDT application from the **Application Data Protection** tile on CipherTrust Manager. Click the desired tab to view the instructions.
-

GUI

To create an application from CipherTrust Manager's UI, follow this [link](#).

The application is created on the CipherTrust Manager and a registration token is returned in response. This token is passed in the deployment scripts to register BDT client on the CipherTrust Manager as shown in the below steps.

API

API: `/v1/data-protection/client-profiles`

Request

```
{
  "name": "client_profile_bdt",
  "app_connector_type": "BDT",
  "heartbeat_threshold": 5,
  "configurations":

  {

    "log_level": "WARN",
    "heartbeat_interval": 300,
    "heartbeat_timeout_count":5,
    "thread_count": 1,
    "batch_size": 1000
  }
}
```

Response

```
{
  "id": "9f3edcb1-38e8-4bc7-8c41-99e897560328",
  "uri": "kylo:kylo:adp-management:client-profiles:client-profile-bdt-9f3edcb1-38e8-4bc7-8c41-99e897560328",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-24T03:26:15.949341161Z",
  "updatedAt": "2025-03-24T03:26:15.949341161Z",
  "name": "client_profile_bdt",
  "app_connector_type": "BDT",
  "configurations": {
    "thread_count": 1,
    "batch_size": 1000,
  }
}
```



```

    "enable_performance_metrics": true,
    "tls_to_appserver": {
      "tls_skip_verify": true,
      "tls_enabled": false
    },
    "auth_method_used": {
      "scheme_name": "Basic"
    },
    "symmetric_key_cache_enabled": true,
    "symmetric_key_cache_expiry": 43200,
    "size_of_connection_pool": 300,
    "load_balancing_algorithm": "round-robin",
    "connection_timeout": 30000,
    "connection_read_timeout": 7000,
    "connection_idle_timeout": 600000,
    "connection_retry_interval": 600000,
    "maximum_idle_connection": 10000,
    "maximum_idle_connection_per_host": 10000,
    "dial_timeout": 10,
    "dial_keep_alive": 60,
    "log_level": "WARN",
    "log_rotation": "Daily",
    "log_size_limit": "100K",
    "log_max_backup_index": -1,
    "log_type": "Console",
    "log_gmt": false,
    "heartbeat_interval": 300,
    "heartbeat_timeout_count": 5
  },
  "csr_parameters": {
    "csr_cn": "Application Data Protection"
  },
  "ca_id": "04d7f146-684b-47a2-a2c2-e8690be50e18",
  "enable_client_autorenewal": false,
  "client_management_profile_id": "0a3b495c-26c2-4a1a-a722-f46bec47e
689",
  "registration_token_id": "0850f54a-dc42-4f3e-a2d3-0b49e19c5ece",
  "meta": {
    "has_active_clients": false,
    "status": "Healthy"
  }
}

```

In response, a *registration token* is returned. The registration token is passed in the deployment script to

register BDT client on the CipherTrust Manager as shown in the below steps.

2. Download and copy the following files:

- `deployment.yaml` to `<target_directory>/templates`.

Warning

The `deployment.yaml` file should not be modified.

- `values.yaml` to `<target_directory>`.
- `Chart.yaml` to `<target_directory>`.

3. Navigate to the `<target_directory>`.

Before proceeding to the next step, we recommend reviewing the concept of [environment variables](#). While the variable names may differ, their purpose and usage remain consistent.

4. In the `values.yaml` file, update the following values:

- `kmsHost`: IP address of your CipherTrust Manager instance.
- `regToken`: Registration token generated on the CipherTrust Manager.
- `dbCertValue`: **(Optional)** Certificate value required for SSL connection with databases.
- `jdbcDriverDownloadUrl`: **(Optional)** URL or location from where BDT will download/load the driver jars required for JDBC connection.

5. Deploy the BDT application in your Kubernetes environment. This section uses `bdt` as the release name.

- When you are in the `<target_directory>`, run the below command:

```
helm install bdt .
```

- When you are in some other directory, run the below command:

```
helm install bdt <target_directory>
```

Note

Here, `<target_directory>` is the location where you have kept all the configuration files.

The status `DEPLOYED` indicates a successful deployment.

Verify the deployment

1. List the deployed BDT pods.

```
kubectl get pods
```

The output should list the deployed BDT pod.

2. Test your deployment.

```
curl -X GET http://<node ip>:32082/liveness
```

Replace `<node ip>` with the actual IP address of your Kubernetes node where the BDT pod is deployed.

Additional commands

- To get the IP address of your Kubernetes node, you can run the following command.

```
kubectl get nodes -o wide
```

- To fetch BDT logs, run the following command.

```
kubectl logs -f <bdp pod name>
```

Sample Transformation

This section explains how to perform a **db-to-db** transformation, demonstrated using an Oracle database. The high-level steps include:

- Creating data source
- Creating access policy
- Creating protection policy
- Creating job configuration

- Running job
- Viewing job status

Tip

The transformation steps provided in this example can be performed using the CipherTrust Manager UI or API playground.

Create data source

Here, we are using the option where the source and destination data-sources are same.

GUI

To create a data source from CipherTrust Manager's UI, follow this [link](#).

API

API: `post /v1/data-protection/data-sources`

Create source data-source

Request

```
{
  "name": "Oracle_ds1",
  "description": "",
  "type": "Oracle",
  "database_properties": {
    "password": "asdf1234",
    "username": "USER5",
    "connection_url": "jdbc:oracle:thin:@<db_host_ip>:orcl",
  }
}
```

Response

```
{
  "id": "17a6f8d0-5db4-4435-984f-fc2a5dbac72e",
  "uri": "kylo:kylo:adp-management:data-sources:oracle_ds1-17a6f8d0-5db4-4435-984f-fc2a5dbac72e",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-07-08T03:27:35.049159948Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "Oracle_ds1",
  "description": "",
  "type": "Oracle",
}
```

```
"database_properties": {
  "connection_url": "jdbc:oracle:thin:@<db_host_ip>:orcl",
}
```

In response, ID of *source data-source* (17a6f8d0-5db4-4435-984f-fc2a5dbac72e) is returned.

Create access policy

GUI

To create access policy from CipherTrust Manager's UI, follow this [link](#).

API

API: `post /v1/data-protection/access-policies`

API Request

```
{
  "name": "ap",
  "description": "access policy description",
  "default_reveal_type": "Plaintext",
  "default_error_replacement_value": "",
  "user_set_policy": [
    {
      "user_set_id": "39738cd0-c7f9-4450-99ea-96b5257d0700",
      "reveal_type": "Plaintext"
    }
  ]
}
```

API Response

```
{
  "id": "396eb554-d167-46f4-a8a5-8a2c9a99648d",
  "uri": "kylo:kylo:adp-management:access-policies:ap-396eb554-d167-46f4-a8a5-8a2c9a99648d",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-07-08T04:28:18.702065393Z",
  "updatedAt": "2025-07-08T04:28:18.706185882Z",
  "created_by": "local|5bb48a34-b391-4886-8f7c-31f7ac6f2fd9",
  "name": "ap1",
  "description": "access policy description",
  "default_reveal_type": "Plaintext",
  "default_error_replacement_value": "",
  "default_masking_format_id": null,
  "user_set_policy": [
    {
      "user_set_id": "39738cd0-c7f9-4450-99ea-96b5257d0700",
```

```

        "reveal_type": "Plaintext",
        "error_replacement_value": null,
        "masking_format_id": null
    },
    ],
    "version": 1
}

```

In response, ID of *access policy* (396eb554-d167-46f4-a8a5-8a2c9a99648d) is returned.

Create protection policy

When creating protection policy, the key should exist on the CipherTrust Manager, if it does not exist, create one following the instructions mentioned [here](#).

Note

Ensure the key used in protection policy has correct permissions. For more details on key permissions, refer to [Supported key types](#).

The protection policy will be created with the following specifications:

- **Algorithm:** AES/CBC/PKCS5Padding
- **Versioning:** Internal

GUI

To create protection policy from CipherTrust Manager's UI, follow this [link](#).

API

API: `post /v1/data-protection/protection-policies`

API Request

```

{
  "name": "ppinternal1",
  "key": "bdtkey",
  "algorithm": "AES/CBC/PKCS5Padding",
  "use_external_versioning": false,
  "access_policy_name": "ap"
}

```

API Response

```

{

```

```

    "id": "9b2237ea-315f-4e20-96e6-38e6be76cb8c",
    "uri": "kylo:kylo:adp-management:protection-policies:ppinternal1-9b2237ea-315f-4e20-96e6-38e6be76cb8c",
    "account": "kylo:kylo:admin:accounts:kylo",
    "createdAt": "2025-07-08T03:37:39.934151665Z",
    "updatedAt": "2025-07-08T03:37:39.920679472Z",
    "name": "ppinternal1",
    "version": 1,
    "latest_version": true,
    "key": "bdtkey",
    "algorithm": "AES/CBC/PKCS5Padding",
    "use_external_versioning": false,
    "disable_versioning": false,
    "access_policy_name": "ap"
  }

```

In response, ID of *protection policy* (9b2237ea-315f-4e20-96e6-38e6be76cb8c) is returned.

Create job configuration

Here, we are creating a job configuration to protect *latitude* using the protection policy *ppinternal1*. Similarly, you can also reveal and reprotect any columns by changing the operation type as required.

GUI

To create job configuration from CipherTrust Manager's UI, follow this [link](#).

API

API: `post /v1/data-protection/bdt/job-configurations`

API Request

```

{
  "name": "ora-ora-pr",
  "source_id": "17a6f8d0-5db4-4435-984f-fc2a5dbac72e",
  "destination_id": "17a6f8d0-5db4-4435-984f-fc2a5dbac72e",
  "tables": [
    {
      "source_table": "EXPORT18",
      "source_schema": "",
      "destination_table": "EXPORT20",
      "destination_schema": "",
      "create_destination_table": true,
      "columns": [
        {
          "source_column_name": "latitude",
          "operation": "protect",
          "protection_policy": "ppinternal1"
        }
      ]
    }
  ]
}

```

API Response

```
{
  "id": "f448f111-adeb-46e1-ad56-d9d67e723e27",
  "uri": "kylo:kylo:adp-management:bdp-job-configurations:ora-ora-pr-f448f111-adeb-46e1-ad56-d9d67e723e27",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-07-08T03:40:23.784226773Z",
  "updatedAt": "2025-07-08T03:40:23.784226773Z",
  "version": 1,
  "name": "ora-ora-pr",
  "description": "",
  "case_sensitive": false,
  "source_id": "17a6f8d0-5db4-4435-984f-fc2a5dbac72e",
  "destination_id": "17a6f8d0-5db4-4435-984f-fc2a5dbac72e",
  "in_place_update": false,
  "unprocessed_record_file": "",
  "tables": [
    {
      "id": "7c176862-4109-4820-a31a-36bff6c02eea",
      "uri": "kylo:kylo:adp-management:bdp-job-configurations-tables:7c176862-4109-4820-a31a-36bff6c02eea",
      "account": "kylo:kylo:admin:accounts:kylo",
      "createdAt": "2025-07-08T03:40:23.792579732Z",
      "updatedAt": "2025-07-08T03:40:23.787905169Z",
      "source_table": "EXPORT18",
      "source_schema": "",
      "destination_table": "EXPORT20",
      "destination_schema": "",
      "create_destination_table": true,
      "subset": {
        "limit": 0,
        "offset": 0,
        "recurrency": 1,
        "order_by": "",
        "order": "ASC",
        "filters": null
      },
      "columns": [
        {
          "id": "0ce7ebf9-e6ac-44d9-bd96-29838fa632a9",
          "uri": "kylo:kylo:adp-management:bdp-job-configurations-tables-columns:0ce7ebf9-e6ac-44d9-bd96-29838fa632a9",
          "account": "kylo:kylo:admin:accounts:kylo",
          "createdAt": "2025-07-08T03:40:23.803205011Z",
          "updatedAt": "2025-07-08T03:40:23.801725918Z",
          "source_column_name": "latitude",
          "operation": "protect",
          "protection_policy": "ppinternal1"
        }
      ]
    }
  ],
  "meta": {
    "job_running": false
  }
}
```

In response, ID of the job configuration (f448f111-adeb-46e1-ad56-d9d67e723e27) is returned.

Run job

Here, we will run the job by passing the job configuration ID (generated in [Create job configuration](#)) and client profile ID (generated in step 1) in the API request. To run a job, at least **one healthy BDT client** must be registered with the application.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

API

There is slight difference in the Run Job API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `post /v1/data-protection/run-job`

API Request

```
{
  "job_configuration_id": "f448f111-adeb-46e1-ad56-d9d67e723e27",
  "client_profile_id": "9f3edcb1-38e8-4bc7-8c41-99e897560328"
}
```

API Response

```
{
  "job_status_id": "29994ae1-acd0-415b-bf92-a23cf68a3fb8"
}
```

In response, a job status ID (29994ae1-acd0-415b-bf92-a23cf68a3fb8) is returned, use this ID to check the intermediate status of the job.

API call in CM 2.20 and higher versions

API: `post /v1/data-protection/bdt/job-configurations/{id}/run`

API Request

```
post /v1/data-protection/bdt/job-configurations/{f448f111-adeb-46e1-ad56-d9d67e723e27}/run
{ "client_profile_id": "9f3edcb1-38e8-4bc7-8c41-99e897560328" }
```

API Response

```
{
  "job_status_id": "29994ae1-acd0-415b-bf92-a23cf68a3fb8"
}
```

In response, a job status ID (29994ae1-acd0-415b-bf92-a23cf68a3fb8) is returned, use this ID to check the intermediate status of the job.

Check job status

Here, you will check the status of the job by passing the job status ID generated in [above step](#) in the API request.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

API

There is slight difference in the Job Status API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `get /v1/data-protection/job-status/{id}`

API Request

```
{
  /v1/data-protection/job-status/{29994ae1-acd0-415b-bf92-a23cf68a3fb8}
}
```

In response, information about the job in various stages, total number of records processed, error messages are returned.

API call in CM 2.20 and higher versions

API: `get /v1/data-protection/jobs/{id}`

API Request

```
/v1/data-protection/jobs/29994ae1-acd0-415b-bf92-a23cf68a3fb8
```

In response, information about the job in various stages, total number of records processed, error messages are returned.

Verify results

After the job status gets completed, Check the destination table, *EXPORT20* for transformed data. The column

named *latitude* will contain the protected data as shown here:

Input Data	Protected Data
latitude	latitude
38.631913	1002008eb.QbvK1B
38.478902	1002008bX.lyin02
38.618305	1002008Oq.238Xpk
38.616835	10020088g.ZnhFEO
38.51947	1002008zQ.9RjXy
38.662595	1002008qg.xrjv8K
38.681659	1002008Ns.Sz5Hc6
38.535092	1002008kl.Elfmor
38.621188	1002008Qq.elSZHs
38.700909	1002008NT.QXs6S8
38.637663	1002008IG.f1U4xg
38.470746	1002008j4.qQLRIV

In the output, you can see that the version header is prepended to the ciphertext (1002008eb.QbvK1B).

File-to-File

Steps for File-to-File

1. Create a BDT application from the **Application Data Protection** tile on CipherTrust Manager. Click the desired tab to view the instructions.

GUI

To create an application from CipherTrust Manager's UI, follow this [link](#).

The application is created on the CipherTrust Manager and a registration token is returned in response. This token is passed in the deployment scripts to register BDT client on the CipherTrust Manager as shown in the below steps.

API

API: `/v1/data-protection/client-profiles`

Request

```
{
  "name": "client_profile_bdt",
  "app_connector_type": "BDT",
  "heartbeat_threshold": 5,
  "configurations":
```

```
{
  "log_level": "WARN",
  "heartbeat_interval": 300,
  "heartbeat_timeout_count": 5,
  "thread_count": 1,
  "batch_size": 1000
}
```

Response

```
{
  "id": "9f3edcb1-38e8-4bc7-8c41-99e897560328",
  "uri": "kylo:kylo:adp-management:client-profiles:client-profile-bd
t-9f3edcb1-38e8-4bc7-8c41-99e897560328",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-24T03:26:15.949341161Z",
  "updatedAt": "2025-03-24T03:26:15.949341161Z",
  "name": "client_profile_bdt",
  "app_connector_type": "BDT",
  "configurations": {
    "thread_count": 1,
    "batch_size": 1000,
    "enable_performance_metrics": true,
    "tls_to_appserver": {
      "tls_skip_verify": true,
      "tls_enabled": false
    },
    "auth_method_used": {
      "scheme_name": "Basic"
    },
    "symmetric_key_cache_enabled": true,
    "symmetric_key_cache_expiry": 43200,
    "size_of_connection_pool": 300,
    "load_balancing_algorithm": "round-robin",
    "connection_timeout": 30000,
    "connection_read_timeout": 7000,
    "connection_idle_timeout": 600000,
    "connection_retry_interval": 600000,
    "maximum_idle_connection": 10000,
    "maximum_idle_connection_per_host": 10000,
  }
}
```

```

        "dial_timeout": 10,
        "dial_keep_alive": 60,
        "log_level": "WARN",
        "log_rotation": "Daily",
        "log_size_limit": "100K",
        "log_max_backup_index": -1,
        "log_type": "Console",
        "log_gmt": false,
        "heartbeat_interval": 300,
        "heartbeat_timeout_count": 5
    },
    "csr_parameters": {
        "csr_cn": "Application Data Protection"
    },
    "ca_id": "04d7f146-684b-47a2-a2c2-e8690be50e18",
    "enable_client_autorenewal": false,
    "client_management_profile_id": "0a3b495c-26c2-4a1a-a722-f46bec47e
689",
    "registration_token_id": "0850f54a-dc42-4f3e-a2d3-0b49e19c5ece",
    "meta": {
        "has_active_clients": false,
        "status": "Healthy"
    }
}

```

In response, a *registration token* is returned. The registration token is passed in the deployment script to register BDT client on the CipherTrust Manager as shown in the below steps.

2. Download and copy the following files:

- `deployment.yaml` to `<target_directory>/templates`.

Warning

The `deployment.yaml` file should not be modified.

- `values.yaml` to `<target_directory>`.
- `Chart.yaml` to `<target_directory>`.

3. Navigate to the `<target_directory>`.

Before proceeding to the next step, we recommend reviewing the concept of *environment variables*.

While the variable names may differ, their purpose and usage remain consistent.

4. In the `values.yaml` file, update the following values:

- `kmsHost` is the IP address of your CipherTrust Manager instance.
- `regToken` is the registration token generated on the CipherTrust Manager.
- `volumeHostPath` is the location of the directory on the host machine where input file exists. In this sample we are using the same path for generating output file. If required, you can mount different paths.
- `volumeMountPath` is the path of directory inside the BDT container to be mounted to the `volumeHostPath`.

Caution

Volume mounting is mandatory in the following cases during deployment to allow BDT to read or create a file.

- When using file as source/destination
- When configuring unprocessed record file path
- When loading the JDBC driver from the host machine

Use `/opt/app/tmp/` to map the external volume with container. Ensure the BDT container has permission to read, write, and execute on the mounted volume else, **the deployment will fail**.

5. Deploy the BDT application in your Kubernetes environment. This section uses `bdt` as the release name.

- When you are in the `<target_directory>`, run the below command:

```
helm install bdt .
```

- When you are in some other directory, run the below command:

```
helm install bdt <target_directory>
```

Note

Here, `<target_directory>` is the location where you have kept all the configuration files.

The status `DEPLOYED` indicates a successful deployment.

Verify the deployment

1. List the deployed BDT pods.

```
kubectl get pods
```

The output should list the deployed BDT pod.

2. Test your deployment.

```
curl -X GET http://<node ip>:32082/liveness
```

Replace `<node ip>` with the actual IP address of your Kubernetes node where the BDT pod is deployed.

Additional commands

- To get the IP address of your Kubernetes node, you can run the following command.

```
kubectl get nodes -o wide
```

- To fetch BDT logs, run the following command.

```
kubectl logs -f <bdp pod name>
```

Sample Transformation

This section explains how to perform a File-to-File transformation, demonstrated using a CSV file. The high-level steps include:

- Creating data source
- Creating access policy
- Creating protection policy
- Creating job configuration
- Running job
- Viewing job status

Tip

The transformation steps provided in this example can be performed using the CipherTrust Manager UI or API playground.

Important Points

- We have provided the following sample files with this example.
 - **Input.csv:** Contains the data to be processed. Download and save this file on the host machine specified during volume mapping when deploying BDT.
 - **Output.csv:** Contains the processed data. This file will get created on the host machine specified during volume mapping when deploying BDT.
- Column of the `input.csv` file that to be protected: *latitude*.

Create data source**GUI**

To create a data source from CipherTrust Manager's UI, follow this [link](#).

API

API: `post /v1/data-protection/data-sources`

Create source data-source**Request**

```
{
  "name": "sourcefile",
  "description": "source details",
  "type": "CSV File",
  "file_properties":
    {"file_path": "/opt/app/tmp/input/inputProtect.csv", "delimiter": ",", "column_count": 12, "has_header_row": true}
}
```

Response

```
{
  "id": "5c22a447-f8dd-4c4c-af7d-149123ecf974",
  "uri": "kylo:kylo:adp-management:data-sources:sourcefile-5c22a447-f8dd-4c"
```



```

4c-af7d-149123ecf974",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-20T11:08:05.940999Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "sourcefile",
  "description": "source details",
  "type": "CSV File",
  "file_properties": {
    "file_path": "/opt/app/tmp/input/input.csv",
    "delimiter": ",",
    "qualifier": "\"",
    "column_count": 12,
    "has_header_row": true,
    "encoding": null,
    "record_length": null,
    "line_separator": null
  }
}

```

In response, ID of *sourcefile* (5c22a447-f8dd-4c4c-af7d-149123ecf974) is returned.

Create destination data-source

Request

```

{
  "name": "destinationfile",
  "description": "destination details",
  "type": "CSV File",
  "file_properties": {
    "file_path": "/opt/app/tmp/output/outputProtect-2025-03-26.10.35.15.348.csv",
    "delimiter": ",",
    "column_count": 12,
    "has_header_row": true
  }
}

```

Response

```

{
  "id": "9b9520e2-2d86-46bd-a615-375b689ee03b",
  "uri": "kylo:kylo:adp-management:data-sources:destinationfile-9b9520e2-2d86-46bd-a615-375b689ee03b",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-20T10:56:19.706092Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "destinationfile",
  "description": "destination details",
  "type": "CSV File",
  "file_properties": {
    "file_path": "/opt/app/tmp/output/output.csv",
    "delimiter": ",",
    "qualifier": "\"",
    "column_count": 12,
    "has_header_row": true,
    "encoding": null,

```

```

    "record_length": null,
    "line_separator": null
  }
}

```

In response, ID of *destinationfile* (9b9520e2-2d86-46bd-a615-375b689ee03b) is returned.

Create access policy

GUI

To create access policy from CipherTrust Manager's UI, follow this [link](#).

API

API: `/v1/data-protection/access-policies`

Request

```

{
  "name": "access_policy",
  "description": "access policy ",
  "default_reveal_type": "Plaintext"
}

```

Response

```

{
  "id": "24e1f7eb-63a8-4b9f-abc3-0295098ad98f",
  "uri": "kylo:kylo:adp-management:access-policies:access-policy-24e1f7eb-63a8-4b9f-abc3-0295098ad98f",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-18T11:30:54.511291Z",
  "updatedAt": "2025-03-18T11:30:54.513016Z",
  "created_by": "local|238dfbe5-dff4-4c56-8474-480fb3c51701",
  "name": "access_policy",
  "description": "",
  "default_reveal_type": "Plaintext",
  "default_error_replacement_value": "",
  "default_masking_format_id": null,
  "user_set_policy": [],
  "version": 1
}

```

In response, ID of the access policy (24e1f7eb-63a8-4b9f-abc3-0295098ad98f) is returned.

Create protection policy

When creating protection policy, the key should exist on the CipherTrust Manager, if it does not exist, create one following the instructions mentioned [here](#).

Note

Ensure the key used in protection policy has correct permissions. For more details on key permissions, refer to [Supported key types](#).

The protection policy will be created with the following specifications:

- **Algorithm:** FPE/FF1v2
- **Versioning:** Internal version
- **Character set:** Alphanumeric

GUI

To create protection policy from CipherTrust Manager's UI, follow this [link](#).

API

API: `post /v1/data-protection/protection-policies`

API Request

```
{
  "name": "fpeProtectionPolicy",
  "description": "FPE protection policy",
  "key": "aakey",
  "algorithm": "FPE/FF1v2/UNICODE",
  "tweak": "121212121212",
  "tweak_algorithm": "SHA1",
  "character_set_id": "2d00cfdb-c422-46ac-8a05-6152806a5715",
  "access_policy_name": "access_policy"
}
```

API Response

```
{
  "id": "ed2efc0b-bf78-4b0f-bb0a-2077475fe5ba",
  "uri": "kylo:kylo:adp-management:protection-policies:fpeprotectionpolicy-v10-ed2efc0b-bf78-4b0f-bb0a-2077475fe5ba",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-04-02T06:29:16.772448Z",
  "updatedAt": "2025-04-02T06:29:16.771811Z",
  "name": "fpeProtectionPolicy",
  "version": 10,
  "latest_version": true,
  "description": "",
  "key": "aakey",
  "iv": "",
}
```

```

    "tweak": "121212121212",
    "tweak_algorithm": "SHA1",
    "character_set_id": "2d00cfdb-c422-46ac-8a05-6152806a5715",
    "character_set": {
      "id": "2d00cfdb-c422-46ac-8a05-6152806a5715",
      "uri": "kylo:kylo:adp-management:character-sets:alphanumeric-2d00cfdb-c422-46ac-8a05-6152806a5715",
      "account": "kylo:kylo:admin:accounts:kylo",
      "createdAt": "2025-01-31T07:15:53.167752Z",
      "updatedAt": "2025-01-31T07:15:53.167752Z",
      "name": "Alphanumeric",
      "description": "",
      "range": "0030-0039,0041-005A,0061-007A",
      "encoding": "UTF-8",
      "predefined": true
    },
    "masking_format_id": "",
    "algorithm": "FPE/FF1v2/UNICODE",
    "use_external_versioning": false,
    "disable_versioning": false,
    "access_policy_name": "access_policy",
    "prefix": "",
    "data_format": "",
    "nonce": "",
    "tag_length": 0,
    "allow_small_input": true
  }
}

```

In response, ID of protection policy (ed2efc0b-bf78-4b0f-bb0a-2077475fe5ba) is returned.

Create job configuration

Here, we are creating a job configuration to protect column *latitude* using the protection policy *fpeProtectionPolicy*. Similarly, you can also reveal and reprotect any columns by changing the operation type as required.

GUI

To create job configuration from CipherTrust Manager's UI, follow this [link](#).

API

API: `post /v1/data-protection/bdt/job-configurations`

API Request

```

{
  "name": "job configuration for file",
  "in_place_update": false,
  "source_id": "5c22a447-f8dd-4c4c-af7d-149123ecf974",
  "destination_id": "9b9520e2-2d86-46bd-a615-375b689ee03b",
  "tables": [
    {
      "columns": [

```

```

    { "source_column_name": "latitude", "operation": "protect",      "protection_p
olicy": "fpeProtectionPolicy"}
    ]
  }
}

```

API Response

```

{
  "id": "142b84d8-22ba-4b66-8fec-16076911ec7a",
  "uri": "kylo:kylo:adp-management:bdt-job-configurations:job-configuratio
n-for-file-142b84d8-22ba-4b66-8fec-16076911ec7a",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-18T11:43:40.577668Z",
  "updatedAt": "2025-04-04T09:14:59.905281Z",
  "version": 26,
  "name": "job configuration for file",
  "description": "",
  "case_sensitive": false,
  "source_id": "5c22a447-f8dd-4c4c-af7d-149123ecf974",
  "destination_id": "9b9520e2-2d86-46bd-a615-375b689ee03b",
  "in_place_update": false,
  "unprocessed_record_file": "/opt/app/tmp/unProcessedRecordFiles/",
  "tables": [
    {
      "id": "2eefe155-7bee-41a9-aacf-546c52f75880",
      "uri": "kylo:kylo:adp-management:bdt-job-configurations-tables:2e
efe155-7bee-41a9-aacf-546c52f75880",
      "account": "kylo:kylo:admin:accounts:kylo",
      "createdAt": "2025-04-04T08:11:39.328142Z",
      "updatedAt": "2025-04-04T08:11:39.327642Z",
      "source_table": "",
      "source_schema": "",
      "destination_table": "",
      "destination_schema": "",
      "create_destination_table": false,
      "subset": {
        "limit": 0,
        "offset": 0,
        "recurrency": 1,
        "order_by": "",
        "order": "ASC",
        "filters": []
      },
      "columns": [
        {
          "id": "dfd71200-1c83-40c5-921d-e941496a72b2",
          "uri": "kylo:kylo:adp-management:bdt-job-configurations-t
ables-columns:dfd71200-1c83-40c5-921d-e941496a72b2",
          "account": "kylo:kylo:admin:accounts:kylo",
          "createdAt": "2025-04-04T08:11:39.332823Z",
          "updatedAt": "2025-04-04T08:11:39.332262Z",
          "source_column_name": "latitude",
          "operation": "protect",

```

```

        "protection_policy": "fpeProtectionPolicy"
      }
    ]
  },
  "meta": {
    "job_running": false
  }
}

```

In response, ID of the job configuration (142b84d8-22ba-4b66-8fec-16076911ec7a) is returned.

Tip

Multiple columns can be configured in a single job configuration, and each column can be associated with different protection policies.

Run job

Here, we will run the job by passing the job configuration ID (generated in above step) and client profile ID (generated in step 1) in the API request. To run a job, at least **one healthy BDT client** must be registered with the application.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

API

There is slight difference in the Run Job API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `post /v1/data-protection/run-job`

API Request

```

{
  "job_configuration_id": "142b84d8-22ba-4b66-8fec-16076911ec7a",
  "client_profile_id": "9f3edcb1-38e8-4bc7-8c41-99e897560328"
}

```

API Response

```

{ "job_status_id": "a960a20c-4852-4fee-a18b-302710f67170" }

```

In response, a job status ID (a960a20c-4852-4fee-a18b-302710f67170) is returned, use this ID to check the intermediate status of the job.

API call in CM 2.20 and higher versions

API: `post /v1/data-protection/bdt/job-configurations/{id}/run`

API Request

```
post /v1/data-protection/bdt/job-configurations/{142b84d8-22ba-4b66-8fec-16076911ec7a}/run
{ "client_profile_id": "9f3edcb1-38e8-4bc7-8c41-99e897560328" }
```

API Response

```
{ "job_status_id": "a960a20c-4852-4fee-a18b-302710f67170" }
```

In response, a *job_status_id* (a960a20c-4852-4fee-a18b-302710f67170) is returned. Use this ID to check the status of the job.

Check job status

Here, you will check the status of the job by passing the job status ID (generated in above step) in the API request.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

API

There is slight difference in the Job Status API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `get /v1/data-protection/job-status/{id}`

Pass the *job_status_id* (generated in step 5) in the API request.

API Request

```
{
/v1/data-protection/job-status/{a960a20c-4852-4fee-a18b-302710f67170}
}
```

In response, information about the job in various stages, total number of records processed, error messages are returned.

API call in CM 2.20

API: `get /v1/data-protection/jobs/{id}`

Pass the `job_status_id` (generated in step 5) in the API request.

API Request

```
/v1/data-protection/jobs/a960a20c-4852-4fee-a18b-302710f67170
```

In response, information about the jobs in various stages, total number of records processed, error messages are returned.

Verify results

After the job status gets completed, Check the [Output.csv](#) for transformed data.

Note

For transformations, where destination is file, the output file name (provided on UI) will also contain a timestamp appended to it. For example, `<output-name-as-per-ui>-2025-04-01.17.57.01.521.csv`

- For CSV file, the output file will be formatted as: `<file-name>-<timestamp>.csv`
- For fixed length file, the output file will be formatted as: `<file-name>-<timestamp>.txt`

In the **Input.csv** file, the *latitude* column was in plaintext, after transformation, the data is in ciphertext.

Before Transformation	After Transformation
latitude	latitude
38.631913	1002008eb.QbvK1B
38.478902	1002008bX.lyin02
38.618305	1002008Oq.238Xpk
38.616835	10020088g.ZnhFEO
38.51947	1002008zQ.9RjXy
38.662595	1002008qg.xrjv8K
38.681659	1002008Ns.Sz5Hc6
38.535092	1002008kl.Elfmor
38.621188	1002008Qq.elSZHs
38.700909	1002008NT.QXs6S8
38.637663	1002008IG.f1U4xg
38.470746	1002008j4.qQLRIV

In the output, you can see that the version header is prepended to the ciphertext (1002008eb.QbvK1B).

Next Topics

- [Tasks](#)
- [Advanced Topics](#)

Alternative Deployment Methods

This section offers the following alternative deployment methods for BDT:

- [Deploy BDT in Kubernetes Environment \(without Helm Chart\)](#)
- [Deploy BDT as a Standalone Container](#)

Deploy BDT in Kubernetes Environment (without Helm Chart)

This section describes steps to deploy BDT in a Kubernetes pod without using a Helm Chart.

Tip

You can use any orchestration tool for deployment.

Prerequisites

- Kubernetes environment is up and running and kubectl is installed.
- CipherTrust Manager 2.19 or higher is up and running. Refer to [CipherTrust Manager Deployment](#) for details.
- BDT image repository, [thalesciphertrust/ciphertrust-batch-data-transformation](#), is accessible. This repository contains images for BDT. The image path with the **latest** tag always points to the latest release.

Note

The user is responsible for maintaining the **security of their production environment**.

Steps to Deploy BDT within your Kubernetes Pod

1. Create an BDT application on CipherTrust Manager. Click the desired tab to view the instructions.

GUI

To create an application from CipherTrust Manager's UI, follow this [link](#).

The application is created on the CipherTrust Manager and a registration token is returned in response. This token is passed in the deployment scripts to register BDT client on the CipherTrust Manager as shown in the below steps.

API

API: `/v1/data-protection/client-profiles`

Request

```
{
  "name": "client_profile_bdt",
  "app_connector_type": "BDT",
  "heartbeat_threshold": 5,
  "configurations":
  {
    "log_level": "INFO",
    "heartbeat_interval": 30,
    "heartbeat_timeout_count": 3,
    "thread_count": 2,
    "batch_size": 10
  }
}
```

Response

```
{
  "id": "9f3edcb1-38e8-4bc7-8c41-99e897560328",
  "uri": "kylo:kylo:adp-management:client-profiles:client-profile-bd
t-9f3edcb1-38e8-4bc7-8c41-99e897560328",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-24T03:26:15.949341161Z",
  "updatedAt": "2025-03-24T03:26:15.949341161Z",
  "name": "client_profile_bdt",
  "app_connector_type": "BDT",
  "configurations": {
    "thread_count": 2,
    "batch_size": 10,
    "enable_performance_metrics": true,
    "tls_to_appserver": {
      "tls_skip_verify": true,

```

```

        "tls_enabled": false
    },
    "auth_method_used": {
        "scheme_name": "Basic"
    },
    "symmetric_key_cache_enabled": true,
    "symmetric_key_cache_expiry": 43200,
    "size_of_connection_pool": 300,
    "load_balancing_algorithm": "round-robin",
    "connection_timeout": 30000,
    "connection_read_timeout": 7000,
    "connection_idle_timeout": 600000,
    "connection_retry_interval": 600000,
    "maximum_idle_connection": 10000,
    "maximum_idle_connection_per_host": 10000,
    "dial_timeout": 10,
    "dial_keep_alive": 60,
    "log_level": "INFO",
    "log_rotation": "Daily",
    "log_size_limit": "100K",
    "log_max_backup_index": -1,
    "log_type": "Console",
    "log_gmt": false,
    "heartbeat_interval": 30,
    "heartbeat_timeout_count": 3
},
"csr_parameters": {
    "csr_cn": "Application Data Protection"
},
"ca_id": "04d7f146-684b-47a2-a2c2-e8690be50e18",
"enable_client_autorenewal": false,
"client_management_profile_id": "0a3b495c-26c2-4a1a-a722-f46bec47e
689",
"registration_token_id": "0850f54a-dc42-4f3e-a2d3-0b49e19c5ece",
"meta": {
    "has_active_clients": false,
    "status": "Healthy"
}
}

```

In response, a *registration token* is returned. The registration token is passed in the deployment script to register BDT client on the CipherTrust Manager as shown in the below steps.

2. Create the secret using the following command.

```
kubectl create secret generic <bdt secret name> --from-literal=regtoken=<registration token>
```

3. Create a deployment file, for example, `<bdt-deployment.yaml>` with the following content.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: bdt-deployment
  labels:
    app: bdt
spec:
  replicas: 1
  selector:
    matchLabels:
      app: bdt
  template:
    metadata:
      labels:
        app: bdt
    spec:
      containers:
        - name: bdt-container
          image: <bdt-image-name>
          imagePullPolicy: IfNotPresent
          env:
            - name: KMS_HOST
              value: "<key manager ip>"
            - name: REG_TOKEN
              valueFrom:
                secretKeyRef:
                  name: <bdt secret name>
                  key: regtoken
          volumeMounts:
            - mountPath: <container mount path>
              name: bdt-volume
      volumes:
        - name: bdt-volume
          hostPath:
            path: <host path to mount>
            type: Directory
```

Note

- The <container mount path> should exist inside the container's home directory (/opt/app/tmp/). For example, <container mount path> can be /opt/app/tmp/input/ for input files. Similarly, volumes for output and unprocessed record files can also be mapped.
- To run database-related transformations, you might need to configure more environment variables, click [here](#) for details.

Caution

Volume mounting is mandatory in the following cases during deployment to allow BDT to read or create a file.

- When using file as source/destination
- When configuring unprocessed record file path
- When loading the JDBC driver from the host machine

Use /opt/app/tmp/ to map the external volume with container. Ensure the BDT container has permission to read, write, and execute on the mounted volume else, **the deployment will fail**.

4. Apply the deployment configuration.

```
kubectl apply -f <bdtd-deployment.yaml>
```

5. Create a service to expose the BDT pod, for example, <bdtd-service.yaml> with the following content.

```
apiVersion: v1
kind: Service
metadata:
  name: bdt-service
  labels:
    app: bdt
spec:
  selector:
    app: bdt
  type: NodePort
  ports:
```

```
- port: 8080
  nodePort: 32085
```

6. Apply the service configuration.

```
kubectl apply -f <bdt-service.yaml>
```

7. Check whether your deployment is ready.

```
kubectl get deployments
```

8. Verify the deployment.

```
curl -X GET http://<node ip>:32085/liveness
```

The following response indicates a successful deployment.

```
{
  "status": "OK"
}
```

BDT is now deployed successfully and is ready to protect, reveal, and reprotect data. Refer to [Tasks](#) for details.

Deploy BDT as a Standalone Container

This article covers the steps involved in deploying BDT as a standalone container in Docker. Refer to [Alternative Deployment Methods](#) for other methods of deploying BDT.

Prerequisites

- Docker Container Runtime Environment (CRE) is ready.
- Docker version 24.0.1 or higher is installed.
- CipherTrust Manager 2.19 or higher is up and running. Refer to [CipherTrust Manager Deployment](#) for details.
- BDT image repository, [thalesciphertrust/ciphertrust-batch-data-transformation](#), is accessible. This repository contains images of BDT. The image path with the **latest** tag always points to the latest release.

Note

The user is responsible for maintaining the **security of their production environment**.

Steps to Deploy BDT as Standalone Container

1. Create an BDT application on CipherTrust Manager. Click the desired tab to view the instructions.

GUI

To create an application from CipherTrust Manager's UI, follow this [link](#).

The application is created on the CipherTrust Manager and a registration token is returned in response. This token is passed in the deployment scripts to register BDT client on the CipherTrust Manager as shown in the below steps.

API

API: `/v1/data-protection/client-profiles`

Request

```
{
  "name": "client_profile_bdt",
  "app_connector_type": "BDT",
  "heartbeat_threshold": 5,
  "configurations":
  {
    "log_level": "INFO",
    "heartbeat_interval": 30,
    "heartbeat_timeout_count":3,
    "thread_count": 2,
    "batch_size": 10
  }
}
```

Response

```
{
```

```

    "id": "9f3edcb1-38e8-4bc7-8c41-99e897560328",
    "uri": "kylo:kylo:adp-management:client-profiles:client-profile-bd
t-9f3edcb1-38e8-4bc7-8c41-99e897560328",
    "account": "kylo:kylo:admin:accounts:kylo",
    "createdAt": "2025-03-24T03:26:15.949341161Z",
    "updatedAt": "2025-03-24T03:26:15.949341161Z",
    "name": "client_profile_bdt",
    "app_connector_type": "BDT",
    "configurations": {
      "thread_count": 2,
      "batch_size": 10,
      "enable_performance_metrics": true,
      "tls_to_appserver": {
        "tls_skip_verify": true,
        "tls_enabled": false
      },
      "auth_method_used": {
        "scheme_name": "Basic"
      },
      "symmetric_key_cache_enabled": true,
      "symmetric_key_cache_expiry": 43200,
      "size_of_connection_pool": 300,
      "load_balancing_algorithm": "round-robin",
      "connection_timeout": 30000,
      "connection_read_timeout": 7000,
      "connection_idle_timeout": 600000,
      "connection_retry_interval": 600000,
      "maximum_idle_connection": 10000,
      "maximum_idle_connection_per_host": 10000,
      "dial_timeout": 10,
      "dial_keep_alive": 60,
      "log_level": "INFO",
      "log_rotation": "Daily",
      "log_size_limit": "100K",
      "log_max_backup_index": -1,
      "log_type": "Console",
      "log_gmt": false,
      "heartbeat_interval": 30,
      "heartbeat_timeout_count": 3
    },
    "csr_parameters": {
      "csr_cn": "Application Data Protection"
    },
    "ca_id": "04d7f146-684b-47a2-a2c2-e8690be50e18",

```



```

        "enable_client_autorenewal": false,
        "client_management_profile_id": "0a3b495c-26c2-4a1a-a722-f46bec47e
689",
        "registration_token_id": "0850f54a-dc42-4f3e-a2d3-0b49e19c5ece",
        "meta": {
            "has_active_clients": false,
            "status": "Healthy"
        }
    }
}

```

In response, a *registration token* is returned. The registration token is passed in the deployment script to register BDT client on the CipherTrust Manager as shown in the below steps.

2. Pull the BDT image to the container environment as shown below:

```
docker pull thalesciphertrust/ciphertrust-batch-data-transformation:latest
```

3. Create a **docker-compose.yml** file by copying the following content. You can modify the parameters as needed:

```

services:

  bdt:
    container_name: bdt
    volumes:
      - <host_location_for_input>:/opt/app/tmp/<subdirectory_for_input>
      - <host_location_for_output>:/opt/app/tmp/<subdirectory_for_output>
    image: <bdt_image_name>
    ports:
      - "<host_port>:8080"
    environment:
      KMS_HOST: "<kms_host>"
      KMS_PORT: "443"
      REG_TOKEN: "<registration_token>"

```

Note

The BDT container listens for healthz and liveness probes on port 8080.

You can also download the [docker-compose.yml](#) file modify according to your needs.

Here,

- `<host_port>`: Any available port on the host machine.
- `<kms_host>`: The IP address or host name of the key manager.
- `<bdtd_image_name>`: Name of the BDT image pulled.
- `<registration_token>`: Registration token generated [here](#).
- `<host_location_for_input>`: Location of the directory on the host machine where input file exists.
- `<host_location_for_output>`: Location of the directory on the host machine where output file exists.

Note

Similarly, you can also map the location of the directory for unprocessed record file.

- `<subdirectory_for_input>`: Directory location inside the container where `<host_location_for_input>` will be mounted. This location must reside inside the `/opt/app/tmp` path of the **container**. Use this location in the **File Path** field with input file name when [creating data source](#).
- `<subdirectory_for_output>`: Directory location inside the container where `<host_location_for_output>` will be mounted. This location must reside inside the `/opt/app/tmp` path of the **container**. Use this location in the **File Path** field with output file name when [creating data source](#).

To run database-related transformations, you will need to configure different environment variables in your deployment files, click [here](#) for details.

Caution

Volume mounting is mandatory in the following cases during deployment to allow BDT to read or create a file.

- When using file as source/destination
- When configuring unprocessed record file path
- When loading the JDBC driver from the host machine

Use `/opt/app/tmp/` to map the external volume with container. Ensure the BDT container has permission to read, write, and execute on the mounted volume else, **the deployment will fail**.

4. Run the below command from the location where you have downloaded the `docker-compose.yml` file to bring the BDT container up and running.

```
docker compose up
```

5. Run the following command to stop the BDT container.

```
docker compose down
```

Verify your deployment

Run the following command to verify your deployment:

```
curl <BDT instanceip>:<host_port>/healthz
```

Replace `<BDT instanceip>` and `<host_port>` with the actual values from your BDT deployment.

BDT is now deployed successfully and is ready to protect, reveal, and reprotect data. Refer to [Tasks](#) for details.

Transformation Process

This section outlines the complete transformation process for data source types — Files and Databases. The transformation can include protect, reveal, or reprotect operation.

- The protect operation protects the plaintext data and returns the ciphertext based on the protection policy selected in the job configuration.
- The reveal operation returns the output based on the default reveal format configured in access policy.
- The reprotect operation protects the plaintext data with the latest version of the protection policy and returns the ciphertext based on the protection policy selected in the job configuration.

Prerequisites

- BDT application must be registered on the CipherTrust Manager. Refer to [Quick Start](#) for details.
- BDT must be deployed. Refer to [Quick Start](#) for details.
- A compatible CipherTrust Manager must be up and running. Refer to [CipherTrust Manager Deployment](#) for

details.

Steps

Tip

The transformation steps provided in this example can be performed using the CipherTrust Manager UI or API playground.

1. Create source and destination data-sources. A data source is required to specify the details of input and output data sources that are part of the transformation process. The data source can be database or file.

GUI

To create a data source from CipherTrust Manager's UI, follow this [link](#).

API

`/data-protection/data-sources`

- a. Access the API playground.
- b. In the left pane of the API playground, click **Data Protection**.
- c. Under **Data Sources**, click **Create**. The Create section of the API playground is displayed in the right pane.
- d. In the body field, specify required parameters with their values.

Expand schema under the body field for names and types of fields. Hover your mouse over each field to view its description. The parameter names and casing in the body field must match with those shown in the schema. Also, ensure that parameters and their values are specified in double quotes.

- e. Click **POST**.
2. Create access policy. The access policies contain set of rules that govern how the protected data will be revealed to users.

GUI

To create access policy from CipherTrust Manager's UI, follow this [link](#).

API

`/data-protection/access-policies`

- a. Access the API playground.

-
- b. In the left pane of the API playground, click **Data Protection**.
 - c. Under **Access Policies**, click **Create**. The Create section of the API playground is displayed in the right pane.
 - d. In the body field, specify required parameters with their values.

Expand schema under the body field for names and types of fields. Hover your mouse over each field to view its description. The parameter names and casing in the body field must match with those shown in the schema. Also, ensure that parameters and their values are specified in double quotes.

- e. Click **POST**.
3. Create protection policy. A protection policy defines a set of rules that govern the cryptographic operations. The protection policy includes entities such as algorithm, key, IV, access policy name, and character set.

GUI

To create protection policy from CipherTrust Manager's UI, follow this [link](#).

API

`data-protection/protection-policies`

- a. Access the API playground.
- b. In the left pane of the API playground, click **Data Protection**.
- c. Under **Protection Policies**, click **Create**. The Create section of the API playground is displayed in the right pane.
- d. In the body field, specify required parameters with their values.

Expand schema under the body field for names and types of fields. Hover your mouse over each field to view its description. The parameter names and casing in the body field must match with those shown in the schema. Also, ensure that parameters and their values are specified in double quotes.

- e. Click **POST**.
4. Create job configuration. A job configuration is required to specify details about the data to be transformed and the destination where the transformed data will be stored.

GUI

To create job configuration from CipherTrust Manager's UI, follow this [link](#).

API

`/data-protection/bdt/job-configurations`

- a. Access the API playground.
- b. In the left pane of the API playground, click **Data Protection**.
- c. Under **BDT Job Configurations**, click **Create**. The Create section of the API playground is displayed in the right pane.
- d. In the body field, specify required parameters with their values.
 - To protect, select **operation** type as **protect**.
 - To reveal, select **operation** type as **reveal**.
 - To reprotect, select **operation** type as **reprotect**.

Tip

Multiple columns can be configured in a single job configuration, and each column can be associated with different protection policies.

Expand schema under the body field for names and types of fields. Hover your mouse over each field to view its description. The parameter names and casing in the body field must match with those shown in the schema. Also, ensure that parameters and their values are specified in double quotes.

- e. Click **POST**.
5. Run job. To run a job, at least one **active client must be registered with the application**.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

API

```
data-protection/bdt/job-configurations/{id}/run
```

- a. Access the API playground.
- b. In the left pane of the API playground, click **Data Protection**.
- c. Under **BDT Job Configurations**, click **Run Job**. The Create section of the API playground is displayed in the right pane.
- d. In the body field, specify required parameters with their values.

Expand schema under the body field for names and types of fields. Hover your mouse over each field to view its description. The parameter names and casing in the body field must match with those shown in

the schema. Also, ensure that parameters and their values are specified in double quotes.

- e. Click **POST**.
6. Check status of the job. The job status provides the information about the various stages of jobs, total number of records processed, error messages, and so on.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

API

```
/data-protection/jobs/{id}
```

- a. Access the API playground.
- b. In the left pane of the API playground, click **Data Protection**.
- c. Under **Jobs**, click **get**. Enter the query parameters with which you want to filter the jobs.
- d. Click **GET**.

Verify Results

After the job status gets completed, Check the destination data data-source for transformed data.

Note

- For transformations, where *destination is file*, the output file name (provided on UI) will also contain a timestamp appended to it. For example, <output-name-as-per-ui>-2025-04-01.17.57.01.521.csv
 - For CSV file, the output file will be formatted as: <file-name>-<timestamp>.csv
 - For fixed length file, the output file will be formatted as: <file-name>-<timestamp>.txt
- For *database and file related transformation*, if you have configured **Unprocessed Record File Path**, the *unprocessed record file* will be created with the following formats:
 - Database: <job_id>-<source_table>-<timestamp>.txt
 - File: <job_id>-<timestamp>.txt

Tasks

This section describes BDT tasks:

- [How to protect data](#)
- [How to reveal data](#)
- [How to reprotect data](#)
- [Change key manager](#)
- [Change application](#)
- [View logs in Kubernetes environment](#)
- [Monitor BDT health](#)
- [Renew client certificate](#)

How to protect data

This section outlines the complete File-to-File transformation process for CSV files. The example provided here demonstrates how to protect data of a CSV file. The protect operation protects the plaintext data and returns the ciphertext based on the protection policy selected in the job configuration. The protection policy provides different functionalities as described [here](#); the output will change according to these functionalities.

Important Points

- We have provided the following sample files with this example.
 - [Input.csv](#): Contains the data to be processed. Download and save this file on the host machine specified during volume mapping when deploying BDT.
 - [Output.csv](#): Contains the processed data. This file will get created on the host machine specified during volume mapping when deploying BDT.
- Column of the `input.csv` file that to be protected: *latitude*.
- Type of protection policy used: Internal version.
- Algorithm: FPE/FF1v2.
- Character set: Alphanumeric.

Prerequisites

- BDT application must be registered on the CipherTrust Manager. Refer to [Quick Start](#) for details.

- BDT must be deployed. Refer to [Quick Start](#) for details.
- A compatible CipherTrust Manager must be up and running. Refer to [CipherTrust Manager Deployment](#) for details.

Steps

The transformation steps provided in this example can be performed using the [CipherTrust Manager UI](#) or [API playground](#).

1. Create source and destination data-sources. The source data-source contains the data to be processed while the destination data-source will store the processed data.

API

API: `post /v1/data-protection/data-sources`

Create source data-source

Request

```
{
  "name": "sourcefile",
  "description": "source details",
  "type": "CSV File",
  "file_properties":
    {
      "file_path": "/opt/app/tmp/input/inputProtect.csv", "delimiter": ",",
      "column_count": 12, "has_header_row": true
    }
}
```

Response

```
{
  "id": "5c22a447-f8dd-4c4c-af7d-149123ecf974",
  "uri": "kylo:kylo:adp-management:data-sources:sourcefile-5c22a447-f8dd-4c4c-af7d-149123ecf974",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-20T11:08:05.940999Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "sourcefile",
  "description": "source details",
  "type": "CSV File",
  "file_properties": {
```

```

        "file_path": "/opt/app/tmp/input/input.csv",
        "delimiter": ",",
        "qualifier": "\"",
        "column_count": 12,
        "has_header_row": true,
        "encoding": null,
        "record_length": null,
        "line_separator": null
    }
}

```

In response, ID of *sourcefile* (5c22a447-f8dd-4c4c-af7d-149123ecf974) is returned.

Create destination data-source

Request

```

{
  "name": "destinationfile",
  "description": "destination details",
  "type": "CSV File",
  "file_properties":
    {
      "file_path": "/opt/app/tmp/output/outputProtect-2025-03-26.10.35.15.348.csv",
      "delimiter": ",",
      "column_count": 12,
      "has_header_row": true
    }
}

```

Response

```

{
  "id": "9b9520e2-2d86-46bd-a615-375b689ee03b",
  "uri": "kylo:kylo:adp-management:data-sources:destinationfile-9b9520e2-2d86-46bd-a615-375b689ee03b",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-20T10:56:19.706092Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "destinationfile",
  "description": "destination details",
  "type": "CSV File",
  "file_properties": {
    "file_path": "/opt/app/tmp/output/output.csv",
    "delimiter": ",",

```

```

        "qualifier": "\"",
        "column_count": 12,
        "has_header_row": true,
        "encoding": null,
        "record_length": null,
        "line_separator": null
    }
}

```

In response, ID of *destinationfile* (9b9520e2-2d86-46bd-a615-375b689ee03b) is returned.

GUI

To create a data source from CipherTrust Manager's UI, follow this [link](#).

Similarly, you can also create data sources for fixed length file and databases. For fixed length file follow the [link](#). For databases, refer to [Managing Data Sources](#).

2. Create access policy

API

API: /v1/data-protection/access-policies

Request

```

{
  "name": "access_policy",
  "description": "access policy ",
  "default_reveal_type": "Plaintext"
}

```

Response

```

{
  "id": "24e1f7eb-63a8-4b9f-abc3-0295098ad98f",
  "uri": "kylo:kylo:adp-management:access-policies:access-policy-24e1f7eb-63a8-4b9f-abc3-0295098ad98f",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-18T11:30:54.511291Z",
  "updatedAt": "2025-03-18T11:30:54.513016Z",
  "created_by": "local|238dfbe5-dff4-4c56-8474-480fb3c51701",
  "name": "access_policy",
}

```

```

    "description": "",
    "default_reveal_type": "Plaintext",
    "default_error_replacement_value": "",
    "default_masking_format_id": null,
    "user_set_policy": [],
    "version": 1
  }

```

In response, ID of the access policy (24e1f7eb-63a8-4b9f-abc3-0295098ad98f) is returned.

GUI

To create access policy from CipherTrust Manager's UI, follow this [link](#).

3. Create protection policy.

API

API: `post /v1/data-protection/protection-policies`

API Request

```

{
  "name": "fpeProtectionPolicy",
  "description": "FPE protection policy",
  "key": "aakey",
  "algorithm": "FPE/FF1v2/UNICODE",
  "tweak": "121212121212",
  "tweak_algorithm": "SHA1",
  "character_set_id": "2d00cfdb-c422-46ac-8a05-6152806a5715",
  "access_policy_name": "access_policy"
}

```

API Response

```

{
  "id": "ed2efc0b-bf78-4b0f-bb0a-2077475fe5ba",
  "uri": "kylo:kylo:adp-management:protection-policies:fpeprotectionpolicy-v10-ed2efc0b-bf78-4b0f-bb0a-2077475fe5ba",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-04-02T06:29:16.772448Z",
  "updatedAt": "2025-04-02T06:29:16.771811Z",
  "name": "fpeProtectionPolicy",

```

```

    "version": 10,
    "latest_version": true,
    "description": "",
    "key": "aakey",
    "iv": "",
    "tweak": "121212121212",
    "tweak_algorithm": "SHA1",
    "character_set_id": "2d00cfdb-c422-46ac-8a05-6152806a5715",
    "character_set": {
      "id": "2d00cfdb-c422-46ac-8a05-6152806a5715",
      "uri": "kylo:kylo:adp-management:character-sets:alphanumeric-2d00cfdb-c422-46ac-8a05-6152806a5715",
      "account": "kylo:kylo:admin:accounts:kylo",
      "createdAt": "2025-01-31T07:15:53.167752Z",
      "updatedAt": "2025-01-31T07:15:53.167752Z",
      "name": "Alphanumeric",
      "description": "",
      "range": "0030-0039,0041-005A,0061-007A",
      "encoding": "UTF-8",
      "predefined": true
    },
    "masking_format_id": "",
    "algorithm": "FPE/FF1v2/UNICODE",
    "use_external_versioning": false,
    "disable_versioning": false,
    "access_policy_name": "access_policy",
    "prefix": "",
    "data_format": "",
    "nonce": "",
    "tag_length": 0,
    "allow_small_input": true
  }

```

GUI

To create protection policy from CipherTrust Manager's UI, follow this [link](#).

A protection policy, named `fpeProtectionPolicy` is created and this policy will be used to protect data as shown the in next step.

Note

Ensure the key used in protection policy has correct permissions. For more details on key permissions, refer to [Supported key types](#).

4. Create job configuration.

API

API: `post /v1/data-protection/bdt/job-configurations`

API Request

```
{
  "name": "job configuration for file",
  "in_place_update": false,
  "source_id": "5c22a447-f8dd-4c4c-af7d-149123ecf974",
  "destination_id": "9b9520e2-2d86-46bd-a615-375b689ee03b",
  "tables": [
    {
      "columns": [
        {
          "source_column_name": "latitude", "operation": "protect", "protectio
n_policy": "fpeProtectionPolicy"
        }
      ]
    }
  ]
}
```

API Response

```
{
  "id": "142b84d8-22ba-4b66-8fec-16076911ec7a",
  "uri": "kylo:kylo:adp-management:bdt-job-configurations:job-configurat
ion-for-file-142b84d8-22ba-4b66-8fec-16076911ec7a",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-03-18T11:43:40.577668Z",
  "updatedAt": "2025-04-04T09:14:59.905281Z",
  "version": 26,
  "name": "job configuration for file",
  "description": "",
}
```

```

"case_sensitive": false,
"source_id": "5c22a447-f8dd-4c4c-af7d-149123ecf974",
"destination_id": "9b9520e2-2d86-46bd-a615-375b689ee03b",
"in_place_update": false,
"unprocessed_record_file": "/opt/app/tmp/unProcessedRecordFiles/",
"tables": [
  {
    "id": "2eefe155-7bee-41a9-aacf-546c52f75880",
    "uri": "kylo:kylo:adp-management:bdt-job-configurations-table
s:2eefe155-7bee-41a9-aacf-546c52f75880",
    "account": "kylo:kylo:admin:accounts:kylo",
    "createdAt": "2025-04-04T08:11:39.328142Z",
    "updatedAt": "2025-04-04T08:11:39.327642Z",
    "source_table": "",
    "source_schema": "",
    "destination_table": "",
    "destination_schema": "",
    "create_destination_table": false,
    "subset": {
      "limit": 0,
      "offset": 0,
      "recurrency": 1,
      "order_by": "",
      "order": "ASC",
      "filters": []
    },
    "columns": [
      {
        "id": "dfd71200-1c83-40c5-921d-e941496a72b2",
        "uri": "kylo:kylo:adp-management:bdt-job-configuration
s-tables-columns:dfd71200-1c83-40c5-921d-e941496a72b2",
        "account": "kylo:kylo:admin:accounts:kylo",
        "createdAt": "2025-04-04T08:11:39.332823Z",
        "updatedAt": "2025-04-04T08:11:39.332262Z",
        "source_column_name": "latitude",
        "operation": "protect",
        "protection_policy": "fpeProtectionPolicy"
      }
    ]
  }
],
"meta": {
  "job_running": false
}

```

```
}
```

In response, ID of the job configuration (142b84d8-22ba-4b66-8fec-16076911ec7a) is returned.

GUI

To create job configuration from CipherTrust Manager's UI, follow this [link](#).

To protect, select **operation** type as **protect**.

Tip

Multiple columns can be configured in a single job configuration, and each column can be associated with different protection policies.

5. Run job.

To run a job, at least one **active client must be registered with the application**.

API

There is slight difference in the Run Job API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `post /v1/data-protection/run-job`

API Request

```
{
  "job_configuration_id": "142b84d8-22ba-4b66-8fec-16076911ec7a",
  "client_profile_id": "9f3edcb1-38e8-4bc7-8c41-99e897560328"
}
```

API Response

```
{ "job_status_id": "a960a20c-4852-4fee-a18b-302710f67170" }
```

In response, a job status ID (a960a20c-4852-4fee-a18b-302710f67170) is returned, use this ID to check the intermediate status of the job.

API call in CM 2.20 and higher versions

API: `post /v1/data-protection/bdt/job-configurations/{id}/run`

API Request

```
post /v1/data-protection/bdt/job-configurations/{142b84d8-22ba-4b66-8fec-16076
911ec7a}/run
{ "client_profile_id": "9f3edcb1-38e8-4bc7-8c41-99e897560328" }
```

API Response

```
{ "job_status_id": "a960a20c-4852-4fee-a18b-302710f67170" }
```

In response, a *job_status_id* (a960a20c-4852-4fee-a18b-302710f67170) is returned. Use this ID to check the status of the job.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

6. Check status of the job.

API

There is slight difference in the `Job Status` API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `get /v1/data-protection/job-status/{id}`

Pass the *job_status_id* (generated in step 5) in the API request.

API Request

```
{
  /v1/data-protection/job-status/{a960a20c-4852-4fee-a18b-302710f67170}
}
```

API call in CM 2.20 and higher version

API: `get /v1/data-protection/jobs/{id}`

Pass the `job_status_id` (generated in step 5) in the API request.

API Request

```
/v1/data-protection/jobs/a960a20c-4852-4fee-a18b-302710f67170
```

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

In response, information about the jobs in various stages, total number of records processed, error messages are returned.

Verify Results

After the job status gets completed, check the [Output.csv](#) for transformed data.

Note

For transformations, where destination is file, the output file name (provided on UI) will also contain a timestamp appended to it. For example, `<output-name-as-per-ui>-2025-04-01.17.57.01.521.csv`

- For CSV file, the output file will be formatted as: `<file-name>-<timestamp>.csv`
- For fixed length file, the output file will be formatted as: `<file-name>-<timestamp>.txt`

In the **Input.csv** file, the *latitude* column was in plaintext, after transformation, the data is in ciphertext.

Before Transformation	After Transformation
latitude	latitude
38.631913	1002008eb.QbvK1B
38.478902	1002008bX.lyin02
38.618305	1002008Oq.238Xpk
38.616835	10020088g.ZnhFEO
38.51947	1002008zQ.9RjXy
38.662595	1002008qg.xrjv8K
38.681659	1002008Ns.Sz5Hc6
38.535092	1002008kl.Elfmor
38.621188	1002008Qq.elSZHs
38.700909	1002008NT.QXs6S8
38.637663	1002008IG.f1U4xg
38.470746	1002008j4.qQLRIV

In the output, you can see that the version header is prepended to the ciphertext (1002008eb.QbvK1B).

Protect Use cases

Protect with Prefix

To configure prefix, enter a user friendly name in the **Prefix** text-box when configuring [protection policy](#).

Example

Protection Policy Type: Internal version

Prefix: geo-

Character Set: Alphanumeric

Input data: 38.689999

Ciphertext: 1002008geo-eb.QbvK1B

Protect Luhn compliant data

To protect luhn compliant data, the **Luhn toggle** must be turned on when configuring [protection policy](#). To use, this functionality, following points must be considered:

- It is only compatible with **All digits character set (0-9)** and **FPE algorithms**.
- The luhn check requires **minimum3 characters** to perform crypto operations.

Example

Protection Policy Type: Internal version

Character Set: All digits (0030-0039)

Input data: 1234567812345670

Ciphertext: 9262746894652355

Note

The generated ciphertext is also luhn complaint. To check if a number is valid luhn, starting from the rightmost digit, double every other digit, and if the doubled value is greater than 9, add its digits. Then, sum all the digits (including the original and doubled ones) and check if the sum is divisible by 10.

Protect with static masking format

The static masking format allows you to preserve starting and ending characters of the input data. It is only applicable with FPE algorithms.

To configure static masking format, select the desired format when configuring [protection policy](#).

Example

Protection Policy Type: Internal version

Static masking format: Preserve LAST_FOUR characters

Character Set: Alphanumeric (0030-0039, 0041-005A, 0061-007A)

Note

Any character outside the given character set range will be preserved in the output.

Input Data: 3526 HIGH ST

Ciphertext: 10020080j37 PaGH ST (last 4 characters are preserved.)

How to reveal data

This section outlines the complete File-to-File transformation process for CSV files. The example provided here demonstrates how to reveal data of a CSV file. The reveal operation returns the data based on the default reveal format defined in the [access policy](#).

Note

Currently, the default reveal format supported by BDT is only *plaintext*.

Important Points

- We have provided the following sample files with this example.
 - **Input.csv:** Contains the data to be processed. Download and save this file on the host machine specified during volume mapping when deploying BDT.
 - **Output.csv:** Contains the processed data. This file will get created on the host machine specified during volume mapping when deploying BDT.
- Column of the `input.csv` file that will be revealed in this demo is: *latitude*.
- We will use the same protection policy for reveal that was used during protect (**fpeProtectionPolicy**) else, data can't be revealed.

Prerequisites

- BDT application must be registered on the CipherTrust Manager. Refer to [Quick Start](#) for details.

- BDT must be deployed. Refer to [Quick Start](#) for details.
- A compatible CipherTrust Manager must be up and running. Refer to [CipherTrust Manager Deployment](#) for details.

Steps

The transformation steps provided in this example can be performed using the [CipherTrust Manager UI](#) or [API playground](#).

1. Create source and destination data-sources. The source data-source contains the data to be processed while the destination data-source will store the processed data. The output of protect operation will act as input for the reveal operation.

API

API: `post /v1/data-protection/data-sources`

Create source data-source

Request

```
{
  "name": "sourcefileforreveal",
  "description": "source details",
  "type": "CSV File",
  "file_properties": {
    "file_path": "/opt/app/tmp/input/inputReveal.csv", "delimiter":
    ",", "column_count": 12, "has_header_row": true}
}
```

Response

```
{
  "id": "24fad7da-d288-47cb-b93b-815760cad19f",
  "uri": "kylo:kylo:adp-management:data-sources:sourcefileforreveal-24fa
d7da-d288-47cb-b93b-815760cad19f",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-04-10T10:30:54.678120212Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "sourcefileforreveal",
  "description": "source details",
  "type": "CSV File",
  "file_properties": {
```

```

        "file_path": "/opt/app/tmp/input/inputReveal.csv",
        "delimiter": ",",
        "qualifier": "\"",
        "column_count": 12,
        "has_header_row": true,
        "encoding": null,
        "record_length": null,
        "line_separator": null
    }
}

```

In response, ID of *sourcefile* (24fad7da-d288-47cb-b93b-815760cad19f) is returned.

Create destination data-source

Request

```

{
  "name": "destinationfileforreveal",
  "description": "destination details",
  "type": "CSV File",
  "file_properties":
    {
      "file_path": "/opt/app/tmp/output/outputReveal-2025-03-26.11.01.5
5.639.csv", "delimiter": ",", "column_count": 12, "has_header_row": true
    }
}

```

Response

```

{
  "id": "c1e06436-2ae9-48a3-b3c7-79f6c909b3ef",
  "uri": "kylo:kylo:adp-management:data-sources:destinationfileforreveal-c1e06436-2ae9-48a3-b3c7-79f6c909b3ef",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-04-10T10:33:47.6178149Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "destinationfileforreveal",
  "description": "destination details",
  "type": "CSV File",
  "file_properties": {
    "file_path": "/opt/app/tmp/output/outputReveal-2025-03-26.11.01.5

```

```
5.639.csv",
    "delimiter": ",",
    "qualifier": "\"",
    "column_count": 12,
    "has_header_row": true,
    "encoding": null,
    "record_length": null,
    "line_separator": null
  }
}
```

In response, ID of *destinationfile* (c1e06436-2ae9-48a3-b3c7-79f6c909b3ef) is returned.

GUI

To create a data source from CipherTrust Manager's UI, follow this [link](#).

Similarly, you can also create data sources for fixed length file and databases. For fixed length file follow the [link](#). For databases, refer to [Managing Data Sources](#).

2. Create job configuration.

API

API: `post /v1/data-protection/bdt/job-configurations`

API Request

```
{
  "name": "job configuration for reveal",
  "in_place_update": false,
  "source_id": "24fad7da-d288-47cb-b93b-815760cad19f",
  "destination_id": "c1e06436-2ae9-48a3-b3c7-79f6c909b3ef",
  "tables": [
    {
      "columns": [
        {
          "source_column_name": "latitude", "operation": "reveal", "protection_policy": "fpeProtectionPolicy"
        }
      ]
    }
  ]
}
```

API Response

```
{
  "id": "210cfdec-37d5-44f3-b9e0-fa4663030f74",
  "uri": "kylo:kylo:adp-management:bdt-job-configurations:job-configuration-
for-reveal-210cfdec-37d5-44f3-b9e0-fa4663030f74",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-04-10T10:40:08.615309848Z",
  "updatedAt": "2025-04-10T10:40:08.615309848Z",
  "version": 1,
  "name": "job configuration for reveal",
  "description": "",
  "case_sensitive": false,
  "source_id": "24fad7da-d288-47cb-b93b-815760cad19f",
  "destination_id": "c1e06436-2ae9-48a3-b3c7-79f6c909b3ef",
  "in_place_update": false,
  "unprocessed_record_file": "",
  "tables": [
    {
      "id": "c2756724-9983-43dd-89d5-93bc9737552e",
      "uri": "kylo:kylo:adp-management:bdt-job-configurations-tables:c27
56724-9983-43dd-89d5-93bc9737552e",
      "account": "kylo:kylo:admin:accounts:kylo",
      "createdAt": "2025-04-10T10:40:08.623659657Z",
      "updatedAt": "2025-04-10T10:40:08.622902571Z",
      "source_table": "",
      "source_schema": "",
      "destination_table": "",
      "destination_schema": "",
      "create_destination_table": false,
      "subset": {
        "limit": 0,
        "offset": 0,
        "recurrency": 1,
        "order_by": "",
        "order": "ASC",
        "filters": null
      },
      "columns": [
        {
          "id": "67074d83-cd41-4481-bdb7-0d798736fb52",
          "uri": "kylo:kylo:adp-management:bdt-job-configurations-ta
bles-columns:67074d83-cd41-4481-bdb7-0d798736fb52",
          "account": "kylo:kylo:admin:accounts:kylo",
```



```

        "createdAt": "2025-04-10T10:40:08.630819232Z",
        "updatedAt": "2025-04-10T10:40:08.628260173Z",
        "source_column_name": "latitude",
        "operation": "reveal",
        "protection_policy": "fpeProtectionPolicy"
      }
    ]
  },
  "meta": {
    "job_running": false
  }
}

```

In response, ID of the job configuration (210cfdec-37d5-44f3-b9e0-fa4663030f74) is returned.

GUI

To create job configuration from CipherTrust Manager's UI, follow this [link](#).

To reveal, select **operation** type as **reveal**.

Tip

Multiple columns can be configured in a single job configuration, and each column can be associated with different protection policies.

3. Run job.

To run a job, at least one **active client must be registered with the application**.

API

There is slight difference in the Run Job API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `post /v1/data-protection/run-job`

API Request

```
{
```

```
"job_configuration_id": "210cfdec-37d5-44f3-b9e0-fa4663030f74",
"client_profile_id": "ab2e3f89-b277-4821-9939-4e5ee6e82352"
}
```

API Response

```
{ "job_status_id": "a960a20c-4852-4fee-a18b-302710f67170" }
```

In response, a job status ID (a960a20c-4852-4fee-a18b-302710f67170) is returned, use this ID to check the intermediate status of the job.

API call in CM 2.20 and higher versions

API: `post /v1/data-protection/bdt/job-configurations/{id}/run`

Pass the job configuration ID (generated in step 2) and client profile ID (generated in deployment steps) in the API request.

API Request

```
post /v1/data-protection/bdt/job-configurations/{210cfdec-37d5-44f3-b9e0-fa4663030f74}/run
{"client_profile_id": "ab2e3f89-b277-4821-9939-4e5ee6e82352"}
```

API Response

```
{ "job_status_id": "bf2a71d7-8c7f-438a-8a87-35c0bb351383" }
```

In response, a *job_status_id* (bf2a71d7-8c7f-438a-8a87-35c0bb351383) is returned. Use this ID to check the status of the job.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

4. Check status of the job.

API

There is slight difference in the `Job Status` API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `get /v1/data-protection/job-status/{id}`

API Request

```
{
  /v1/data-protection/job-status/{bf2a71d7-8c7f-438a-8a87-35c0bb351383}
}
```

In response, information about the job in various stages, total number of records processed, error messages are returned.

API call in CM 2.20 and higher versions

API: `get /v1/data-protection/jobs/{id}`

Pass the `job_status_id` (generated in step 3) in the API request.

API Request

```
/v1/data-protection/jobs/bf2a71d7-8c7f-438a-8a87-35c0bb351383
```

In response, information about the job in various stages, total number of records processed, error messages are returned.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

In response, information about the jobs in various stages, total number of records processed, error messages are returned.

Verify Results

After the job status gets completed, check the [Output.csv](#) for transformed data.

Note

For transformations, where destination is file, the output file name (provided on UI) will also contain a timestamp appended to it. For example, `<output-name-as-per-ui>-2025-04-01.17.57.01.521.csv`

- For CSV file, the output file will be formatted as: `<file-name>-<timestamp>.csv`

- For fixed length file, the output file will be formatted as: <file-name>-<timestamp>.txt

In the **Input.csv** file, the *latitude* column was in ciphertext, after transformation, the data is in plaintext.

Before Transformation	After Transformation
latitude	latitude
1002008eb.QbvK1B	38.631913
1002008bX.lyin02	38.478902
1002008Oq.238Xpk	38.618305
10020088g.ZnhFEO	38.616835
1002008zQ.9RjXy	38.51947
1002008qg.xrjv8K	38.662595
1002008Ns.Sz5Hc6	38.681659
1002008kl.Elfmor	38.535092
1002008Qq.eISZHs	38.621188
1002008NT.QXs6S8	38.700909
1002008lG.f1U4xg	38.637663
1002008j4.qQLRIV	38.470746

How to reprotect data

This section outlines the complete File-to-File transformation process for CSV files. The example provided here demonstrates how to reprotect data of a CSV file. The reprotect operation protects the plaintext data with the **latest version of the protection policy** and returns the ciphertext based on the protection policy selected in the job configuration.

Important Points

- We have provided the following sample files with this example.
 - Input.csv:** Contains the data to be processed. Download and save this file on the host machine specified during volume mapping when deploying BDT.
 - Output.csv:** Contains the processed data. This file will get created on the host machine specified during volume mapping when deploying BDT.
- Column of the `input.csv` file that will be reprotected in this example is: *latitude*.
- We will modify some of the attributes of the protection policy that was used during protect (**fpeProtectionPolicy**). Doing this will increment the version of the protection policy.
- BDT application must be registered on the CipherTrust Manager. Refer to [Quick Start](#) for details.

- BDT must be deployed. Refer to [Quick Start](#) for details.
- A compatible CipherTrust Manager must be up and running. Refer to [CipherTrust Manager Deployment](#) for details.

Steps

The transformation steps provided in this example can be performed using the [CipherTrust Manager UI](#) or [API playground](#).

1. Create source and destination data-sources. The source data-source contains the data to be processed while the destination data-source will store the processed data.

API

API: `post /v1/data-protection/data-sources`

Request

```
{
  "name": "sourcefileforreprotect",
  "description": "source details",
  "type": "CSV File",

  "file_properties":
    {
      "file_path": "/opt/app/tmp/input/inputReprotect", "delimiter": ",", "column_count": 12, "has_header_row": true
    }
}
```

Response

```
{
  "id": "060f5f02-0020-4391-8622-986a17a67242",
  "uri": "kylo:kylo:adp-management:data-sources:sourcefilefor-reprotect-060f5f02-0020-4391-8622-986a17a67242",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-04-10T11:45:11.181451365Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "sourcefileforreprotect",
  "description": "source details",
  "type": "CSV File",
  "file_properties": {
    "file_path": "/opt/app/tmp/input/inputReprotect",
```

```

        "delimiter": ",",
        "qualifier": "\"",
        "column_count": 12,
        "has_header_row": true,
        "encoding": null,
        "record_length": null,
        "line_separator": null
    }
}

```

In response, ID of *sourcefileforreprotect* (060f5f02-0020-4391-8622-986a17a67242) is returned.

Request

```

{
  "name": "destinationfileforreprotect",
  "description": "destination details",
  "type": "CSV File",
  "file_properties":
    {
      "file_path": "/opt/app/tmp/output/outputReprotect-2025-03-26.10.54.05.32
6.csv", "delimiter": ",", "column_count": 12, "has_header_row": true
    }
}

```

Response

```

{
  "id": "f1092d62-c64d-4dd5-ba21-0a30a1b7d17f",
  "uri": "kylo:kylo:adp-management:data-sources:destinationfileforreprotect-f1092d62-c64d-4dd5-ba21-0a30a1b7d17f",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-04-10T11:46:54.504532806Z",
  "updatedAt": "0001-01-01T00:00:00Z",
  "name": "destinationfileforreprotect",
  "description": "destination details",
  "type": "CSV File",
  "file_properties": {
    "file_path": "/opt/app/tmp/output/outputReprotect-2025-03-26.10.54.05.326.csv",
    "delimiter": ",",
    "qualifier": "\"",

```

```

        "column_count": 12,
        "has_header_row": true,
        "encoding": null,
        "record_length": null,
        "line_separator": null
    }
}

```

In response, ID of *destinationfileforreprotect* (f1092d62-c64d-4dd5-ba21-0a30a1b7d17f) is returned.

GUI

To create a data source from CipherTrust Manager's UI, follow this [link](#).

Similarly, you can also create data sources for fixed length file and databases. For fixed length file follow the [link](#). For databases, refer to [Managing Data Sources](#).

2. Update protection policy. The updated protection policy will be used to reprotect data.
3. Create job configuration.

API

API: `post /v1/data-protection/bdt/job-configurations`

API Request

```

{
  "name": "job configuration for reprotect",
  "in_place_update": false,
  "source_id": "060f5f02-0020-4391-8622-986a17a67242",
  "destination_id": "f1092d62-c64d-4dd5-ba21-0a30a1b7d17f",
  "tables": [
    {
      "columns": [
        {
          "source_column_name": "latitude", "operation": "reprotect", "protect
ion_policy": "fpeProtectionPolicy"
        }
      ]
    }
  ]
}

```

API Response

```
{
  "id": "7e5a96f6-d8ff-4e07-8017-62329e52c22f",
  "uri": "kylo:kylo:adp-management:bdt-job-configurations:job-configuration-
for-reprotect-7e5a96f6-d8ff-4e07-8017-62329e52c22f",
  "account": "kylo:kylo:admin:accounts:kylo",
  "createdAt": "2025-04-10T11:59:26.798803671Z",
  "updatedAt": "2025-04-10T11:59:26.798803671Z",
  "version": 1,
  "name": "job configuration for reprotect",
  "description": "",
  "case_sensitive": false,
  "source_id": "060f5f02-0020-4391-8622-986a17a67242",
  "destination_id": "f1092d62-c64d-4dd5-ba21-0a30a1b7d17f",
  "in_place_update": false,
  "unprocessed_record_file": "",
  "tables": [
    {
      "id": "0d77a4cc-6b7e-49de-a7f0-6ea4fbab0439",
      "uri": "kylo:kylo:adp-management:bdt-job-configurations-tables:0d7
7a4cc-6b7e-49de-a7f0-6ea4fbab0439",
      "account": "kylo:kylo:admin:accounts:kylo",
      "createdAt": "2025-04-10T11:59:26.803556607Z",
      "updatedAt": "2025-04-10T11:59:26.802711961Z",
      "source_table": "",
      "source_schema": "",
      "destination_table": "",
      "destination_schema": "",
      "create_destination_table": false,
      "subset": {
        "limit": 0,
        "offset": 0,
        "recurrency": 1,
        "order_by": "",
        "order": "ASC",
        "filters": null
      },
      "columns": [
        {
          "id": "54c8a33c-a06b-4308-99c3-9326b79db087",
          "uri": "kylo:kylo:adp-management:bdt-job-configurations-ta
bles-columns:54c8a33c-a06b-4308-99c3-9326b79db087",
          "account": "kylo:kylo:admin:accounts:kylo",
```



```

        "createdAt": "2025-04-10T11:59:26.808796141Z",
        "updatedAt": "2025-04-10T11:59:26.807903746Z",
        "source_column_name": "latitude",
        "operation": "reprotect",
        "protection_policy": "fpeProtectionPolicy"
      }
    ]
  },
  "meta": {
    "job_running": false
  }
}

```

In response, ID of the job configuration (7e5a96f6-d8ff-4e07-8017-62329e52c22f) is returned.

GUI

To create job configuration from CipherTrust Manager's UI, follow this [link](#).

To reprotect, select **operation** type as **reprotect**.

Tip

Multiple columns can be configured in a single job configuration, and each column can be associated with different protection policies.

4. Run job.

To run a job, at least one **active client must be registered with the application**.

API

There is slight difference in the Run Job API call depending on the CipherTrust Manager version you are using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `post /v1/data-protection/run-job`

Pass the job configuration ID (generated in step 4) and client profile ID (generated in deployment steps) in the API request.

API Request

```
{
  "job_configuration_id": "7e5a96f6-d8ff-4e07-8017-62329e52c22f",
  "client_profile_id": "ab2e3f89-b277-4821-9939-4e5ee6e82352"
}
```

API Response

```
{ "job_status_id": "b960a20c-4852-4fee-a18b-302710f67170" }
```

In response, a job status ID (b960a20c-4852-4fee-a18b-302710f67170) is returned, use this ID to check the intermediate status of the job.

API call in CM 2.20 and higher versions

API: `post /v1/data-protection/bdt/job-configurations/{id}/run`

Pass the job configuration ID (generated in step 4) and client profile ID (generated in deployment steps) in the API request.

API Request

```
post /v1/data-protection/bdt/job-configurations/{7e5a96f6-d8ff-4e07-8017-6
2329e52c22f}/run
{ "client_profile_id": "ab2e3f89-b277-4821-9939-4e5ee6e82352" }
```

API Response

```
{ "job_status_id": "b960a20c-4852-4fee-a18b-302710f67170" }
```

In response, a *job_status_id* (b960a20c-4852-4fee-a18b-302710f67170) is returned. Use this ID to check the status of the job.

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

5. Check status of the job.

API

There is slight difference in the `Job Status` API call depending on the CipherTrust Manager version you are

using. Choose the preferred tab to view the details.

API call in CM 2.19

API: `get /v1/data-protection/job-status/{id}`

Pass the `job_status_id` (generated in step 5) in the API request.

API Request

```
{  
  /v1/data-protection/job-status/{b960a20c-4852-4fee-a18b-302710f67170}  
}
```

API call in CM 2.20 and higher versions

API: `get /v1/data-protection/jobs/{id}`

Pass the `job_status_id` (generated in step 5) in the API request.

API Request

```
/v1/data-protection/jobs/b960a20c-4852-4fee-a18b-302710f67170
```

GUI

To run a job from CipherTrust Manager's UI, follow this [link](#).

In response, information about the jobs in various stages, total number of records processed, error messages are returned.

Verify Results

After the job status gets completed, Check the [Output.csv](#) for transformed data.

Note

For transformations, where destination is file, the output file name (provided on UI) will also contain a timestamp appended to it. For example, `<output-name-as-per-ui>-2025-04-01.17.57.01.521.csv`

- For CSV file, the output file will be formatted as: `<file-name><timestamp>.csv`
- For fixed length file, the output file will be formatted as: `<file-name><timestamp>.txt`

In the **Input.csv** file, the *latitude* column was protected with older version of protection policy (1002008), after transformation, the data is reprotected with the latest version of protection policy (1003008).

Before Transformation	After Transformation
latitude <pre>1002008eb.QbvK1B 1002008bX.lyin02 1002008Oq.238Xpk 10020088g.ZnhFEO 1002008zQ.9RjXy 1002008qg.xrjv8K 1002008Ns.Sz5Hc6 1002008kl.Elfmor 1002008Qq.eISZHs 1002008NT.QXs6S8 1002008lG.f1U4xg 1002008j4.qQLRIV</pre>	latitude <pre>1003008eb.QbvK1B 1003008bX.lyin02 1003008Oq.238Xpk 10030088g.ZnhFEO 1003008zQ.9RjXy 1003009qg.xrjv8K 1003008Ns.Sz5Hc6 1003008kl.Elfmor 1003008Qq.eISZHs 1003008NT.QXs6S8 1003008lG.f1U4xg 1003008j4.qQLRIV</pre>

In the output, you can see that the incremented version header is prepended to the ciphertext (1003008eb.QbvK1B).

Change key manager

This article describes how to change a key manager. BDT uses the CipherTrust Manager as a trusted key manager.

For Kubernetes deployment with Helm

1. In the `values.yaml` file, under the `env` section, update the value of `kmsHost` with a valid IP address or hostname of the CipherTrust Manager.
2. Update your BDT deployment.

```
helm upgrade <helm chart name> <path of helm chart>
```

For Kubernetes deployment without Helm

1. In the BDT deployment file (for example, `<bdtd-deployment.yaml>`), update the value of `KMS_HOST` with a valid IP address or hostname of the CipherTrust Manager.
2. Update your BDT deployment.

```
kubect1 replace -f <bdtd-deployment.yaml>
```

For Standalone deployment

1. Stop the existing container.
2. In the environment variable, update the `KMS_HOST` field with a valid IP address or hostname of the CipherTrust Manager
3. Start the container.

```
docker run -e KMS_HOST=<new-IP address or host name of kms> -e REG_TOKEN=<registration_token> -p <host-port>:<bdp-port> <bdp_image_name>
```

Change application

This section provides instructions to change the application you want to redeploy BDT with.

1. Define the new application on the CipherTrust Manager and generate a new registration token. Refer to [Defining applications](#) for details.
2. Redeploy BDT to use the new application. Refer to the following sections for instructions on deploying BDT based on your deployment.
 - [With helm deployment](#)
 - [Without helm chart deployment](#)
 - [Standalone deployment](#)

Note

If you are making changes in the existing application BDT is configured with, no need to redeploy BDT. The configuration will be reflected based on the [heartbeat configuration](#).

View logs in Kubernetes environment

A log serves as the record that captures every minute details of what your application did.

To fetch BDT specific logs in *Kubernetes* (with and without helm) deployment from *sysout*, you can use the following command:

```
kubectl logs <pod_name> -c <bdp_container_name>
```

To fetch BDT specific logs in *standalone* deployment, use the following command:

```
docker logs <container_id>
```

Monitoring BDT health

BDT provides `healthz` and `liveness` probes to monitor BDT health.

`healthz` Probe

Checks the current health status of the BDT container and reports whether BDT is serving the requests.

- If the status code `200` (`status is OK`) is returned, BDT is running fine. You can proceed with your operations.
- If the status code `503` (`Container is not healthy`), BDT can't process any requests but it is recoverable. Check the issue in the BDT logs and fix it to recover from the error state.

Example

```
GET https://<BDT instanceip>:<port>/healthz
```

Output

```
{  
  "status": "OK"  
}
```

In the above API call, replace `<BDT instanceip>` and `<port>` with the actual values from your BDT deployment.

`liveness` Probe

Checks the liveness of the BDT container whether BDT is running healthy.

- If the status code `200` (`status is OK`) is returned, BDT is running fine. You can proceed with your operations.
- If the status code `503` is returned, BDT can't process any requests and isn't recoverable. In this case, you need to restart or redeploy the BDT container.

Example

```
GET https://<BDT instanceip>:<port>/liveness
```

Output

```
{  
  "status": "OK"  
}
```

In the above API call, replace `<BDT_instanceip>` and `<port>` with the actual values from your BDT deployment.

Renewing client certificate

While creating the application on CipherTrust Manager, the Application Data Protection admin configures the Certificate Duration (in days). When the certificate expiry duration ranges from 90-60 days, the client logs the `Client certificate will expire in <number> Days` notification message daily. To renew the client certificate, use either of the ways:

Auto renew

When the [Certificate Auto Renewal](#) toggle is enabled and the client certificate is between 60 and 1 day before expiration, it is auto-renewed, and the message `Client certificate renewed successfully` is returned.

Manual renew

When the [Certificate Auto Renewal](#) toggle is not enabled and the client certificate is between 60 and 1 day before expiration, the certificate will expire. To renew it manually, restart your container.

Advanced Topics

This section describes advanced BDT topics.

- [Environment Variables](#)
- [Concepts](#)
- [Protection Policy](#)
- [BDT Logging](#)
- [Using Fixed-Length Record Format](#)
- [Supported Encoding](#)
- [Behavior of BDT on Container Shutdown](#)
- [Unprocessed Record File](#)
- [Using JDBC Driver URLs](#)
- [Thread Count and Batch Sizes](#)

Environment Variables

Variable	Description	Optional/Mandatory
KMS_HOST	IP address or hostname of the	Mandatory

Variable	Description	Optional/Mandatory
	CipherTrust Manager.	
KMS_PORT	Port on which BDT communicates with the CipherTrust Manager. The default port is 443.	Optional
REG_TOKEN	Registration token used to register a BDT client on the CipherTrust Manager.	Mandatory
DB_CERT_VALUE	Comma separated certificate values in <i>.pem</i> format required to make a secure JDBC connection with databases.	Optional
JDBC_DRIVER_DOWNLOAD_URL	The URL or location from where BDT will download/load the driver jars required to make a JDBC connection with the database. Click here for more details.	Optional

Concepts

Application

An application, configured on the CipherTrust Manager, contains the necessary settings that are required to protect/reveal/reprotect data. Refer to [Managing Application](#) for details.

Access policy

Access policies contain set of rules that govern how the protected data will be revealed to users. Since there is no concept of users in BDT, the data will be revealed based on the default reveal format configured in the access policy.

Note

For BDT, it is recommended to configure the default reveal format as plaintext.

Refer to [Managing Access Policy](#) for details.

Dynamic Masking

Creates masking format for the reveal operation. Dynamic masking format determines how the output of the reveal operation is displayed to the application users. Refer to [Masking Format](#) for details.

Heartbeat

Heartbeat is a lightweight mechanism that allows BDT to poll the CipherTrust Manager for any change in configurations. Refer to [Heartbeat Configuration](#)

Note

- Every transformation will run with the latest configurations.
- For BDT, only protection policy configurations get reflected with heartbeat in a running transformation. Modifications done in all other configurations can not get reflected in a running transformation.
- The time on both the client and server machines must be synchronized. To achieve this, NTP (Network Time Protocol) should be configured. Follow [instructions](#) to set up NTP.

Behavior of BDT when heartbeat timeout count is reached

If the count of the continuous skipped heartbeat becomes equivalent to the value of `Heartbeat Timeout Count` parameter, the BDT client enters a revoked state after a maximum of 5 minutes. At this point, its liveness and health probes become false. In this scenario, BDT does not transform data. This safeguard ensures the crypto operations are not performed when the container's state is unhealthy and unrecoverable.

Note

If a client is processing a job and in-between its heartbeat timeout count has reached due to any issue on the Key Manager, the client enters a revoked state. The CipherTrust Manager will stop running the job linked to that client. The job status page may not reflect the actual progress of that stopped job.

Behavior of BDT when client gets deleted, revoked, or expired

If a client gets deleted, revoked or expired on Key Manager, the liveness and health probes become false. In this scenario, BDT does not transform data. This safeguard ensures the crypto operations are not performed when the container's state is unhealthy and unrecoverable.

Note

- When a client gets deleted on Key Manager, the status of its running job will no longer get updated on the [Job Status](#) page. As a result, the associated job configuration can't be reused to run a new job.
- The deleted, revoked, or expired client will be in healthy state for maximum 5 minutes.

Key Caching

The key caching feature allows BDT to securely cache a copy of the in-use key that it received from the CipherTrust Manager using the REST protocol. Key caching is limited for the value set in the `Key Cache Expiry` parameter while creating an application to perform cryptographic operations locally.

See the `Key Cache Expiry` parameter under the BDT tab [here](#) for details.

Key States

A key state determines which operations can be performed using that key. Refer to [Key States](#) for details. Based on the key states, BDT will throw error for the following key states.

Compromised Key State: Cannot Protect with Compromised Key Version

Deactivated Key State: Cannot perform operation with Deactivated Key Version

Protection Policy

Protection policy defines a set of rules that govern the cryptographic operations. The protection policy includes entities such as algorithm, key, IV, access policy name, and character set. Refer to [Managing Protection Policy](#) for details.

Protection policy specifications

Internal versioning protection policy

It is a type of protection policy where the version header is prepended with the ciphertext. For example, 1001000B1E06A7C20585E0F5A13233953B4971D. The protected text reserves 7 digits for version header. The permissible version header range is 1001000 - 1999999.

- The first digit is reserved for type
- The next 3 digits are reserved for protection policy version
- The last 3 digits are reserved for key version.

Important Notes

- The length of the ciphertext will increase after prepending the 7-digit version header to it. So, the *length of the column* receiving the ciphertext will increase by 7.
- In case of protect operation for Fixed Length File, the white spaces at the end of the plaintext will be removed to ensure the version header is prepended to the ciphertext.

External versioning protection policy

It is a type of protection policy where the version header is not part of the ciphertext and it is stored in a different column. Specify the column name (where you want to insert the version header value) in the *Version header column*. Refer to [Managing Job Configuration](#) for details.

Important Notes

Protect operation

- For transformations where destination is database, the version header column should exist in the destination table. Else, the following error will be thrown:

```
Version header column <version header name> not present in destination table.
```

Note

If **Create Destination** check-box is selected, BDT will create the column with the name specified in the version header column parameter (if it is not already in source) with datatype as VARCHAR (7). For Oracle, the datatype will be VARCHAR2 (7).

- If the destination table already contains the column with the same name as the version header column value, BDT will use that column to add the version header value.
- For transformations where destination is file, if the version header column is already present in the source, the column data will be overwritten with version header value. If version header column doesn't exist, BDT will create column in the output file.
- For Fixed length file transformation, following points will be taken into consideration:
 - If the version header column value length is greater than 7, BDT will add spaces in the version header value.
 - If the version header column value length is less than 7, BDT will add spaces in the version header column name.
 - If the version header column already present in destination, the column length of the original column will be used.

Reveal Operation

If the version header column is not null or does not exist in the source table or input file, BDT throws the following error:

```
Version header column is not present in source.
```

Disable versioning protection policy

It is a type of policy where information about version header is not returned with the ciphertext. In this scenario, only *Version 0* of a key can be used to protect data.

Luhn check

A luhn check is a method to validate identification of numbers. Protection policy is configured to protect or reveal luhn complaint data. This check is only compatible with All digits character set (0-9) and FPE algorithms. The luhn

check requires minimum 3 characters to perform crypto operations. For configuring luhn data format, refer to [Creating Protection Policy](#).

Prefix

It is a user friendly name that helps user identify the type of data being protected. This value is specified while creating a protection policy. For configuring prefix, refer to [Creating Protection Policy](#).

Note

In case of protect operation for Fixed Length File, the white spaces at the end of the plaintext will be removed to ensure the prefix is prepended to the ciphertext.

Static masking format

Allows you to preserve starting and ending characters of the input data. The remaining characters will be protected based on the selected algorithm. It is only applicable for FPE algorithms. Refer to [Masking Format](#) for details.

Allow Small Input Value

Support available in CipherTrust Manager future releases

Support to handle small character input will be available in CipherTrust Manager 2.22 and higher versions.

Format-preserving algorithms require a character set during cryptographic operations. When the effective input length does not meet the minimum length criteria supported by the underlying algorithm, an error is thrown. To handle this scenario, use the **Allow Small Input** parameter. This parameter allows BDT to process small input.

Conversely, if the Allow Small Input parameter is disabled and user attempts to protect a small input value, BDT doesn't process it and returns the `Input buffer is too short (len=1), it has to be at least 2 bytes long` error.

This parameter is only supported with FPE and Random2 algorithms.

Random nonce

Support for Random Nonce in AES algorithms will be available in CipherTrust Manager 2.22 and higher versions.

A random nonce is a randomly generated nonce (IV) that can be used only once in cryptographic operations. It can be internal, external, or disabled.

Internal random nonce: The nonce generated during protect is returned with the ciphertext. The structure of ciphertext is as follows: `versionheader + prefix + nonce + ciphertext`. Internal random nonce works with internal and disabled protection policies.

External random nonce: The nonce generated during protect is not part of the ciphertext and it is stored in a different column. Specify the column name (where you want to insert the random nonce value) when creating job configuration. External random nonce works with external and disabled protection policies.

Disable random nonce: In this case, nonce is not returned with the ciphertext. Disable nonce can be used with internal, external, or disabled protection policy.

Important Notes

Protect Operation

- For transformations where destination is database, the random nonce column should exist in the destination table. Else, the following error will be thrown:

```
Random nonce column <random nonce column name> not present in destination table.
```

Note

If **Create Destination** check-box is selected, BDT will create the column with the name specified in the random nonce column parameter (if it is not already in source) with datatype as VARCHAR (32). For Oracle, the datatype will be VARCHAR2 (32).

- If the destination table already contains the column with the same name as the random nonce column value, BDT will use that column to add the random nonce value.
- For transformations where destination is file, if the random nonce column is already present in the source, the column data will be overwritten with random nonce value. If random nonce column doesn't exist, BDT will create column in the output file.
- For Fixed length file transformation, following points will be taken into consideration:
 - If the random nonce column value length is greater than 32, BDT will add spaces in the random nonce value.
 - If the random nonce column value length is less than 32, BDT will add spaces in the random nonce column name.
 - If the random nonce column already present in destination, the column length of the original column will be used.

Reveal Operation

If the random nonce column is not null or does not exist in the source table or input file, BDT throws the following error:

```
Random nonce column is not present in source.
```

BDT Logging

Logs contain information about the events happening inside your application. Logs can be very helpful when trying to troubleshoot a problem. The BDT logging framework is designed in such a way that it can be integrated with most of the third-party external loggers such as Splunk and Datadog. The BDT logs are captured on the console. Users are free to choose any logging agent that works with the containerized solutions. A logging agent fetches the logs from the BDT console and pushes them to the user configured environment.

Application logs: Capture implementation level details required by the developer to understand what happened or how the application responded during a specific event. The application logs are printed in text format. Click [here](#) to know more.

Log level specifies the level of logging to be performed by the application. Following table describes the supported log levels with their description.

Log Level	Description
INFO	Records error messages, warnings, and informational messages.
WARN	Records error messages and warnings.
ERROR	Records only error messages.
DEBUG	Records diagnostic information.

These log levels are configurable and can be changed from the [CipherTrust Manager UI](#).

Format of Application Log

The log format determines how the contents of a log should be interpreted. Below is the sample of an application log:

```
bdt | 2025-01-15 08:53:30:577 INFO [main] - BDT is registered successfully on ke  
y manager  
bdt | 2025-01-15 08:53:30:578 WARN [main] - Connection not secure  
bdt | 2025-01-15 08:53:30:598 INFO [main] - Started HTTP server on port 80
```

Fixed-length Format File

Some systems may require fixed-length record formats. As described by IBM:

"In fixed-length or fixed-format records, each field starts and ends at the same place in every record. A data file that contains data records of equal and constant length might be organized as follows.

```
aaabbbbccccdddgghhhh
```

The data illustrated above has three records. Each record has a field of three characters followed by a field of four characters, so the total record length is seven characters. The file does not contain any separation between records; delimiters are unnecessary because all fields have the same length."

Reference: [IBM® Informix® 12.10](#)

In the above example, the records are not separated with a newline character (↵). For such types of file, line separator should not be enabled in the data source. Refer to [Managing Data Source](#) for details.

Fixed-length file only works with FPE algorithms.

References

We have provided samples of fixed length file where records are separated with a newline character (↵) followed by its data source configuration.

- [Fixed length file where records are separated with a newline character](#)
- [Fixed length data source configuration sample](#)

Supported Encoding

The following table lists the standard encoding supported by Oracle Java. BDT uses these encodings to read input files.

Encoding Set

Encoding	Description
Cp858	Variant of Cp850 with Euro character
Cp437	MS-DOS United States, Australia, New Zealand, South Africa
Cp775	PC Baltic
Cp850	MS-DOS Latin-1
Cp852	MS-DOS Latin-2
Cp855	IBM Cyrillic
Cp857	IBM Turkish
Cp862	PC Hebrew
Cp866	MS-DOS Russian
ISO8859_1	ISO-8859-1, Latin Alphabet No. 1
ISO8859_2	Latin Alphabet No. 2
ISO8859_4	Latin Alphabet No. 4
ISO8859_5	Latin/Cyrillic Alphabet
ISO8859_7	Latin/Greek Alphabet (ISO-8859-7:2003)
ISO8859_9	Latin Alphabet No. 5
ISO8859_13	Latin Alphabet No. 7
ISO8859_15	Latin Alphabet No. 9
KOI8_R	KOI8-R, Russian

Encoding	Description
KOI8_U	KOI8-U, Ukrainian
ASCII	American Standard Code for Information Interchange
UTF8	Eight-bit Unicode (or UCS) Transformation Format
UTF-16	Sixteen-bit Unicode (or UCS) Transformation Format, byte order identified by an optional byte-order mark
UnicodeBigUnmarked	Sixteen-bit Unicode (or UCS) Transformation Format, big-endian byte order
UnicodeLittleUnmarked	Sixteen-bit Unicode (or UCS) Transformation Format, little-endian byte order
UTF_32	32-bit Unicode (or UCS) Transformation Format, byte order identified by an optional byte-order mark
UTF_32BE	32-bit Unicode (or UCS) Transformation Format, big-endian byte order
UTF_32LE	32-bit Unicode (or UCS) Transformation Format, little-endian byte order
UTF_32BE_BOM	32-bit Unicode (or UCS) Transformation Format, big-endian byte order, with byte-order mark
UTF_32LE_BOM	32-bit Unicode (or UCS) Transformation Format, little-endian byte order, with byte-order mark
Cp1250	Windows Eastern European
Cp1251	Windows Cyrillic
Cp1252	Windows Latin-1
Cp1253	Windows Greek
Cp1254	Windows Turkish
Cp1257	Windows Baltic
UnicodeBig	Sixteen-bit Unicode (or UCS) Transformation Format, big-endian byte order, with byte-order mark
Cp737	PC Greek
Cp874	IBM Thai
UnicodeLittle	Sixteen-bit Unicode (or UCS) Transformation Format, little-endian byte order, with byte-order mark
Big5	Big5, Traditional Chinese
Big5_HKSCS	Big5 with Hong Kong extensions, Traditional Chinese (incorporating 2001 revision)
EUC_JP	JISX 0201, 0208 and 0212, EUC encoding Japanese
EUC_KR	KS C 5601, EUC encoding, Korean
GB18030	Simplified Chinese, PRC standard
EUC_CN	GB2312, EUC encoding, Simplified Chinese

Encoding	Description
GBK	GBK, Simplified Chinese
Cp838	IBM Thailand extended SBCS
Cp1140	Variant of Cp037 with Euro character
Cp1141	Variant of Cp273 with Euro character
Cp1142	Variant of Cp277 with Euro character
Cp1143	Variant of Cp278 with Euro character
Cp1144	Variant of Cp280 with Euro character
Cp1145	Variant of Cp284 with Euro character
Cp1146	Variant of Cp285 with Euro character
Cp1147	Variant of Cp297 with Euro character
Cp1148	Variant of Cp500 with Euro character
Cp1149	Variant of Cp871 with Euro character
Cp037	USA, Canada (Bilingual, French), Netherlands, Portugal, Brazil, Australia
Cp1026	IBM Latin-5, Turkey
Cp1047	Latin-1 character set for EBCDIC hosts
Cp273	IBM Austria, Germany
Cp277	IBM Denmark, Norway
Cp278	IBM Finland, Sweden
Cp280	IBM Ital
Cp284	IBM Catalan/Spain, Spanish Latin America
Cp285	IBM United Kingdom, Ireland
Cp297	IBM France
Cp420	IBM Arabic
Cp424	IBM Hebrew
Cp500	EBCDIC 500V1
Cp860	MS-DOS Portuguese
Cp861	MS-DOS Icelandic
Cp863	MS-DOS Canadian French
Cp864	PC Arabic
Cp865	MS-DOS Nordic
Cp868	MS-DOS Pakistan
Cp869	IBM Modern Greek
Cp870	IBM Multilingual Latin-2

Encoding	Description
Cp871	IBM Iceland
Cp918	IBM Pakistan (Urdu)
ISO2022CN	GB2312 and CNS11643 in ISO 2022 CN form, Simplified and Traditional Chinese (conversion to Unicode only)
ISO2022JP	JIS X 0201, 0208, in ISO 2022 form, Japanese
ISO2022KR	ISO 2022 KR, Korean
ISO8859_3	Latin Alphabet No. 3
ISO8859_6	Latin/Arabic Alphabet
ISO8859_8	Latin/Hebrew Alphabet
JIS_X0201	JIS X 0201
JIS_X0212-1990	JIS X 0212
SJIS	Shift-JIS, Japanese
TIS620	TIS620, Thai
Cp1255	Windows Hebrew
Cp1256	Windows Arabic
Cp1258	Windows Vietnamese
MS932	Windows Japanese
Big5_Solaris	Big5 with seven additional Hanzi ideograph character mappings for the Solaris zh_TW.BIG5 locale
EUC_JP_LINUX	JISX 0201, 0208, EUC encoding Japanese
EUC_TW	CNS11643 (Plane 1-7,15), EUC encoding, Traditional Chinese
EUC_JP_Solaris	JISX 0201, 0208, 0212, EUC encoding Japanese
Cp1006	IBM AIX Pakistan (Urdu)
Cp1025	IBM Multilingual Cyrillic: Bulgaria, Bosnia, Herzegovina, Macedonia (FYR)
Cp1046	IBM Arabic - Windows
Cp1097	IBM Iran (Farsi)/Persian
Cp1098	IBM Iran (Farsi)/Persian (PC)
Cp1112	IBM Latvia, Lithuania
Cp1122	IBM Estonia
Cp1123	IBM Ukraine
Cp1124	IBM AIX Ukraine
Cp1381	IBM OS/2, DOS People's Republic of China (PRC)

Encoding	Description
Cp1383	IBM AIX People's Republic of China (PRC)
Cp33722	IBM-eucJP - Japanese (superset of 5050)
Cp834	IBM EBCDIC DBCS-only Korean
Cp856	IBM Hebrew
Cp875	IBM Greek
Cp921	IBM Latvia, Lithuania (AIX, DOS)
Cp922	IBM Estonia (AIX, DOS)
Cp930	Japanese Katakana-Kanji mixed with 4370 UDC, superset of 5026
Cp933	Korean Mixed with 1880 UDC, superset of 5029
Cp935	Simplified Chinese Host mixed with 1880 UDC, superset of 5031
Cp937	Traditional Chinese Host mixed with 6204 UDC, superset of 5033
Cp939	Japanese Latin Kanji mixed with 4370 UDC, superset of 5035
Cp942	IBM OS/2 Japanese, superset of Cp932
Cp942C	Variant of Cp942
Cp943	IBM OS/2 Japanese, superset of Cp932 and Shift-JIS
Cp943C	Variant of Cp943
Cp948	OS/2 Chinese (Taiwan) superset of 938
Cp949	PC Korean
Cp949C	Variant of Cp949
Cp950	PC Chinese (Hong Kong, Taiwan)
Cp964	AIX Chinese (Taiwan)
Cp970	AIX Korean
ISCII91	ISCII91 encoding of Indic scripts
ISO2022_CN_CNS	CNS11643 in ISO 2022 CN form, Traditional Chinese (conversion from Unicode only)
ISO2022_CN_GB	GB2312 in ISO 2022 CN form, Simplified Chinese (conversion from Unicode only)
x-iso-8859-11	Latin/Thai Alphabet
x-JIS0208	JIS X 0208
JISAutoDetect	Detects and converts from Shift-JIS, EUC-JP, ISO 2022 JP (conversion to Unicode only)
x-Johab	Korean, Johab character set

Encoding	Description
MacArabic	Macintosh Arabic
MacCentralEurope	Macintosh Latin-2
MacCroatian	Macintosh Croatian
MacCyrillic	Macintosh Cyrillic
MacDingbat	Macintosh Dingbat
MacGreek	Macintosh Greek
MacHebrew	Macintosh Hebrew
MacIceland	Macintosh Iceland
MacRoman	Macintosh Roman
MacRomania	Macintosh Romania
MacSymbol	Macintosh Symbol
MacThai	Macintosh Thai
MacTurkish	Macintosh Turkish
MacUkraine	Macintosh Ukraine
MS950_HKSCS	Windows Traditional Chinese with Hong Kong extensions
MS936	Windows Simplified Chinese
PCK	Solaris version of Shift_JIS
x-SJIS_0213	Shift_JISX0213
Cp50220	Windows Codepage 50220 (7-bit implementation)
Cp50221	Windows Codepage 50221 (7-bit implementation)
MS874	Windows Thai
MS949	Windows Korean
MS950	Windows Traditional Chinese
x-windows-iso2022jp	Variant ISO-2022-JP (MS932 based)

Behavior of BDT on Container Shutdown

Container shutdown can be either graceful or not.

Graceful Shutdown

For BDT, a shutdown is considered graceful when it receives a `SIGINT` (Interrupt) or `SIGTERM` (Terminate) signal.

In case of graceful shutdown, following actions take place:

- The BDT client stops accepting the new requests and is deleted from the single pane of glass.
- The BDT server shuts down and the container is terminated.
- Any licenses in use are automatically released.

Note

In the scenarios, when shutdown is not graceful, the container is immediately terminated without deleting the client. You can either wait for the CipherTrust Manager to delete the client (When the BDT client skips sending heartbeat, it first enters into warning state. If the number of missed heartbeat count becomes equal to Heartbeat Timeout Count, CipherTrust Manager revokes the client) or can manually delete the client from the single pane of glass. Any licenses in use will be automatically released post client deletion.

Unprocessed Record File

The unprocessed record file holds details of the records that failed during processing. You can configure the location of this file when creating a [job configuration](#) on the CipherTrust Manager. If you specify the location for *Unprocessed Record File Path*, files with below formats (based on the source type) will be created at the specified location.

Source type	File format
Database	<code><job_id>-<source_table>-<timestamp>.txt</code> Example: <code>50cc3d07-ff29-474f-b9b5-bbf484a354ce-SOURCETABLE-2025-05-08.11.44.17.159.txt</code>
File	<code><job_id>-<timestamp>.txt</code> Example: <code>5b6542d4-a867-40a0-a34a-ac56e2bdf622-2025-05-08.04.31.29.535.txt</code>

The location of directory for unprocessed record file should exist inside container's directory structure that is `/opt/app/tmp`. To access this file outside the container, you must mount this path to a host location. For more information on volume mounting refer to [quick start](#).

It is recommended that the *Unprocessed Record File Path* be configured only if required, as it contains sensitive information. If configured, you must delete the created file after use or manage its access control to prevent the sensitive information from invalid access.

Note

The column order in the unprocessed record file when *in-place transformation* is enabled is as follows:

First, the columns to be encrypted as specified in the job configuration, followed by the primary keys.

Using Text Qualifier Characters in Input Files

A text qualifier character can be used to mark the start and end of a column field in a file that is input to the BDT utility. This is useful when the field value itself contains a character that would normally act as a field delimiter.

Use the qualifier to indicate to BDT that the data following the delimiter is part of the same field, and not the beginning of the next field.

Any printable ASCII character can be specified as a text qualifier, except for the backslash (\) character. Also note that the qualifier character cannot be the same as the delimiter character.

For example, in the following input file, the comma is the delimiter character, but it is also part of the address field. To let BDT know that the text after the comma is also part of the same field, the value must be enclosed with a text qualifier.

Example

Data before adding text qualifier:

```
#bash

Firstname, Lastname, Address
James,Brown,1745 E. New St., Apt. 22,Chicago
Scott,Smith,400 South Warren Street,Trenton
```

Data after adding text qualifier:

```
James,Brown,"1745 E. New St., Apt. 22,Chicago"
Scott,Smith,"400 South Warren Street,Trenton"
```

Using JDBC Driver URLs

A `JDBC_DRIVER_DOWNLOAD_URL` is an environment variable that specifies URL or a physical location from where container will download/load the driver jars required to make a JDBC connection with the database. If loading the driver from a physical location make sure the location is mounted inside the mount point `'/opt/app/tmp'` of the container.

Note

Ensure the location from which these URLs are retrieved while processing a job is accessible from the machine where the container is deployed.

Its value consists of comma-separated key-value pairs formatted as:

- **<Key Name>=<url>**

Specify unauthenticated URLs only. Authenticated URLs are not supported.

Note

You can provide URLs for multiple databases simultaneously, formatted like this: `<Key`

```
Name1>=<url1>, <Key Name2>=<url2>
```

- **<Key Name>=<Mounted Path>**

For specifying location to load the JDBC driver, you first need to mount the location of driver at host machine to the container's location (/opt/app/tmp/) when starting the container. Refer to quick start for details.

The following table lists the mapping of supported databases and their respective **KeyName**.

Database Name	Key Name
Oracle	ORACLE
Microsoft SQL Server	MSSQL
MySQL	MYSQL
PostgreSQL	POSTGRESQL
IBM Db2	DB2
SAP HANA	SAPHANA

Note

Key Name is case sensitive.

If the `JDBC_DRIVER_DOWNLOAD_URL` value is not specified during deployment, BDT will use the following default URLs.

Database Name	Default URLs
Oracle	https://repo1.maven.org/maven2/com/oracle/database/jdbc/ojdbc17/23.7.0.25.01/ojdbc17-23.7.0.25.01.jar
Microsoft SQL Server	https://repo1.maven.org/maven2/com/microsoft/sqlserver/mssql-jdbc/12.8.1.jre8/mssql-jdbc-12.8.1.jre8.jar
MySQL	https://repo1.maven.org/maven2/mysql/mysql-connector-java/8.0.30/mysql-connector-java-8.0.30.jar
PostgreSQL	https://repo1.maven.org/maven2/org/postgresql/postgresql/42.7.4/postgresql-42.7.4.jar
IBM Db2	https://repo1.maven.org/maven2/com/ibm/db2/jcc/db2jcc/db2jcc4/db2jcc-db2jcc4.jar
SAP HANA	https://repo1.maven.org/maven2/com/sap/cloud/db/jdbc/ngdbc/2.22.12/ngdbc-2.22.12.jar

Note

When default drivers are used, the MSSQL and MYSQL drivers establish the JDBC connection over SSL.

Thread Count and Batch Sizes

To best configure thread count and batch size, use the following principles:

1. Identify the ideal thread count for your environment depending on your system configuration. BDT gives optimal performance with 16 threads on four core machines. Setting thread count too low or too high will slow down the application.
2. Decide on batch size, configured based on available memory, size of individual record, and configured thread count. Setting batch size too high may result in an out-of-memory error.
3. Use the following formula to calculate the approximate maximum memory utilization by BDT:

$$\text{thread count} * \text{batch size} * \text{record size} = \text{memory utilization}$$

Therefore, thread count and batch size will be less than or equal to about 60% of available memory. The remaining memory is required to run BDT and to maintain transformed batches in the write queue.

Example

If you have 4GB available memory and individual record size of approximately 50MB, you can set either:

- Batch size to 50 and thread count to 1, utilizing $50 * 50\text{MB} = 2500\text{MB}$, approximately 60% of memory.
- Batch size to 10 and thread count to 3, utilizing $10 * 3 * 100\text{MB} = 3000\text{MB}$.

Troubleshooting

This section describes the issues you may run into and how to resolve them. If you face an issue that is not listed here, contact [Thales Customer Support](#).

Error/Issue	Possible Cause and Fix
Resource doesn't exist on Key Manager.	Make sure the resources associated to the job (such as job configuration, data sources, and protection policy) exist on Key Manager.
Client is unable to fetch latest policy even after synchronizing time between client and server.	To get the latest updates, the heartbeat interval must be longer than the delay between the client and server.
Failed to update BDT job status on CipherTrust Manager.	BDT failed to update the job status on CipherTrust Manager. Check liveness probe of the container. If it returns

Error/Issue	Possible Cause and Fix
	HTTP code 503, BDT can't process more jobs. In such scenarios, restart the container.
JDBC driver jar does not exist at location.	JDBC driver JAR is missing from the specified location. Ensure the JAR file exists in the specified location with the exact file name when a job is being processed.
Invalid value provided in database certificate value.	The provided database CA certificate is malformed. Make sure the database CA certificate is a valid certificate in <i>.PEM</i> format.
Failed to download the driver.	The required JDBC driver for database connection could not be downloaded. Ensure to specify correct JDBC driver download URL.
Could not parse JDBC driver download URL.	Unable parse JDBC driver download URL due to following reasons: — Empty or null key value pair in JDBC driver URL. —Invalid key-value pair. Ensure to provide correct JDBC driver download URL. See Using JDBC Driver URLs .
The job could not be stopped successfully.	Unable to stop the job, as it may have already completed or stopped.
Job configuration does not exists.	The job configuration associated with the job is deleted from CipherTrust Manager. Ensure job configuration exists on the CipherTrust Manager.
Primary key column not found. Can't perform in-place update.	Occurs when the Primary Key column is not available in the source/destination table in case of in-place update.
A deadlock error occurs during an in-place transformation in the Microsoft SQL Server database when the table has a primary key with a varchar datatype.	Using a primary key of a varchar datatype can slow down comparisons compared to integer datatypes, potentially leading to a deadlock. Therefore, it is recommended to modify the table to have a primary key of integer datatype. After the transformation is over, these changes can be reverted. 1. Identify the primary key constraint name. <pre>SELECT name FROM sys.key_constraints WHERE type = 'PK' AND parent_object_id = OBJECT_ID('table_name');</pre> 2. Drop composite primary key constraint from the table. <pre>ALTER TABLE table_name DROP CONSTRAINT <constraint_name>;</pre> The <code><constraint name></code> is obtained as the output of 1st query. 3. Alter table to create a new primary column of integer type. <pre>Alter table <table_name> add</pre>

Error/Issue	Possible Cause and Fix
	<pre><new_primary_column> int primary key identity(1,1)</pre> 4. Run the transformation. It will run successfully. 5. Delete the new primary key created in step 3. — Identify its constraint name using the query mentioned in step 1. — Drop the constraint using query mentioned in step 2. 6. Alter the table to add the composite primary key constraint back. <pre>ALTER TABLE <table_name> ADD CONSTRAINT <constraint_name> PRIMARY KEY (<column_name1>, <column_name2>);</pre>



CipherTrust Manager

Version: v2.22 (latest)

30 January 2026

Contents

- Batch Data Transformation (BDT) 3
 - Protection Profiles 3
 - BDT Policies 5
 - BDT Containers 10

Batch Data Transformation (BDT)

The Batch Data Transformation tile of the CipherTrust Manager lets you create data encryption profiles and policies that can be used to standardize your encryption policies across several Thales products. This feature ensures consistency and centralizes control over the types of encryption being used.

Batch Data Transformation currently supports:

- **Protection Profiles** that let you specify the encryption information for a specific input column in a BDT (Batch Data Policy) policy. Future releases will support Protection Profiles for other Thales products, such as the CipherTrust Tokenization Server. For details about creating Protection Policies, refer to [Protection Profiles](#).
- **BDT Policies** that work with the Batch Data Transformation (BDT) utility. BDT policies contain all the information BDT needs to transform and rekey data, and the policies you define in CipherTrust Manager can replace the locally-stored `bdt.config` file. For details, refer to [BDT Policies](#).

Note

BDT policies are supported BDT 2.3 onward.

Protection Profiles

Protection Profiles contain all information needed to perform a cryptographic operation, and they can be used to specify the encryption information for a specific input column in a BDT policy.

Creating a Protection Profile

1. Log on to the CipherTrust Manager as an administrator.
2. On the app selection menu, click **Batch Data Transformation** and select **Protection Profiles**.
3. Click **Create Protection Profile**. The Create Protection Policy wizard is displayed.
4. Enter the following information:

Field	Description
Name	A user defined name for this Protection Profile. The name must be unique.
Description	An optional description of the profile.
Key Name	Click Select and select the name of the key that you want to use. If you need to create a new key, you

Field	Description
	can click Create a New Key on the Select Key page.
Tweak	An optional 16-digit tweak for the encryption key.
IV	An optional 32-digit initialization vector for the encryption key.
Algorithm	The algorithm to use. This can be: • FPE (also called FF3) • FF1 • AES_CBC_PAD • AES_CTR • DESede (also called 3DES, Triple-DES, and DES-EDE)
Mode	Only applicable if the Algorithm is set to DESede. This can be: • CBC (the default) • ECB
Padding	Only applicable if the Algorithm is set to DESede. This can be: • NoPadding • PKCS5Padding
Character Set	The character set that will be encrypted by this profile. Thales provides the following default character sets: • Alphanumeric • All printable ASCII • All digits You can also make as many custom character sets as you need. For details, see Creating a Character Set.
Allow null or single character inputs	If this option is enabled, null or single-character inputs will be passed through to the output without being encrypted. If this option is not selected, the row transformation will fail. This option applies to FPE or FF1 algorithm encryption only. It is ignored if the Algorithm is set to Random.

5. Review the Protection Profile settings and click **Save** when you are done.

Creating a Character Set

1. Log on to the CipherTrust Manager as an administrator.
2. In the left pane, expand **Data Protection** and select **Character Sets**.
3. Click **Create Character Set** and enter the following information:

Field	Description
Name	A user defined name for this character set. The name must be unique.
Unicode Character Range	The Unicode characters included in this character set in HEX format. This field can contain a range of characters, a single Unicode character, or a comma-separated list consisting of any number of ranges and single characters. Examples: • Basic Latin: 0000–007F • Digits: 0031–0039 • Greek: 0370–03FF • Greek and all digits: 0E00–0E7F, 0030–0039 • Greek and the single digit 9: 0E00–0E7F, 0039 As you specify the range, a check mark icon next to the field label indicates that the entry uses valid HEX format. An exclamation mark icon indicates that the value is not valid HEX. You cannot create the character set unless you have a valid HEX expression in this field.

4. When you are done, click **Create**.

BDT Policies

The Batch Data Transformation utility (BDT) provides a policy-based data transformation and re-key service. While you can create a local `bdt.config` file that contains the required encryption information in different sections, you can also define BDT policies in CipherTrust Manager and then use those same policies wherever they are needed.

Creating a BDT Policy

1. Log on to the CipherTrust Manager as an administrator.
2. In the left pane, click **Data Protection > BDT Policies**.
3. Click **Create BDT Policy**. The Create BDT Policy wizard is displayed.

4. Enter the following information:

Field	Description
Name	A user defined name for this BDT policy. The name must be unique.
Description	An optional description of the policy.
FPE Mode	If you are using Format-Preserving Encryption (FPE), enter the FF3-encoding mechanism you want to use. The options are: • ASCII: The default encryption mode. ASCII supports only ASCII characters and is faster than UTF • UTF: Required when using FPE to encrypt Unicode characters. NOTE: The ASCII encryption mode is separate from ASCII character encoding.
In Place Update	Applies only if the source container points to a database. Enable this option if you want BDT to transform the data in place instead of specifying a different destination to hold the transformed data. If you enable this option, BDT transforms the data directly in the source database table and CipherTrust Manager does not display the Add Destination page in the wizard. If you <i>do not</i> enable this option, you can specify any container as the destination on the Add Destination wizard page. NOTE: If you enable this option and you also specify a destination table on the Data Transformation page of this wizard, the destination table is ignored.
Create Bad Record File	Enable this option if you want BDT to create a .failed file that contains information about the input records that could not be transformed.

When you are done, click **Next**. The **Add Source** screen is displayed.

5. Select the container that specifies the database or file that you want to transform. If you want to create a new container, click **Create Container**. For details, see [BDT Containers](#).

When you are done, click **Next**.

6. If you selected the **In Place Update** option on the **General Info** screen, proceed to the next step. Otherwise,

on the **Add Destination** screen, select the container that specifies the database or file into which you want BDT to write the transformed data. If you want to create a new container, click **Create Container**. For details, see [BDT Containers](#).

Note

If you want BDT to write the transformed data to a new table in the source database, the Source and Destination containers should be the same. You will be able to specify the destination table name in the next step.

When you are done, click **Next**. The **Data Transformation** screen is displayed.

- Click **Create Table** and enter the following information.

Note

- You must create a table even if you are using a CSV file or a fixed length file as the input. For these entities, the **Source Table** name field should be left blank.
- This step only specifies the database table names. You will specify the columns you want to use later in this procedure.

Field	Description
Source Table	If the source container points to a database, enter the name of the database table containing the columns that you want to transform. If the source container points to a CSV file or a fixed length file, leave the Source Table field blank.
Destination Table	Applies only when the In Place Update option is not enabled. If that option is enabled, BDT ignores this field. If the destination container points to a database, enter the name of the database table into which you want BDT to write the results of the transformation process. If you want BDT to create the destination table for you, enable the Create Destination Table option. If the destination container points to a CSV file or a fixed length file, leave the Destination Table field

Field	Description
	blank.
In Place Error	Specifies what to do when the In Place Update transformation option is selected and some records fail the transform process. The options are: • <code>rollback</code>: Roll back all changes. The source table returns unchanged to its initial state. • <code>commit</code>: Update the source column with transformed values and replace any failed records with either null or plain text depending on the value selected in the Error Placeholder field. • <code>exit</code>: Keeps source table as it is, with some values already transformed. This allows you to resolve the cause of the failure and restart the transformation (with the <code>-r</code> option).
Error Placeholder	This option applies only if In Place data transformation encounters an error and the In Place Error field is set to <code>commit</code>. The options are: • <code>NULL</code>: Sets the record value to null if the transformation fails. Use caution when selecting this option, as the original plain text data will be lost. • <code>PLAIN_TEXT</code>: Retains the original record contents if transformation fails.

- Repeat the previous step to add any other database tables you want to add to this BDT policy.

When you are done specifying the tables, click **Next**.

- Review the policy settings and click **Save** when you are done.

Now, specify the columns you want BDT to process. Refer to [Specifying Columns to Process](#).

Specifying Columns to Process

To specify which columns you want BDT to process in the input database table, CSV file, or fixed length file:

- On the BDT Policies page, click on the policy name.
- In the **Tables** section, expand the table for which you want to add column information.
- Click **Create Column** and enter the following information:

Field	Description
Name	The name of the column.

Field	Description
Action	This can be ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, or REKEY. If you select REKEY, CipherTrust Manager displays two sections, one for the decryption of the existing data and one for the encryption of the same data with the new key. Do not change the Action that is automatically selected in these sections. When you specify the Decryption options, make sure they exactly match how the existing data is encrypted or the rekey operation will not succeed.
Protection Profile	The Protection Profile to use for this column. For details, see Protection Profiles .
Token Template	If you are using a CipherTrust Tokenization Server and you do not have a Protection Profile, you can use this field to specify a CTS template token. This option is only available if the Action is Tokenize, Detokenize, or Rekey. NOTE: If you specify a Protection Profile and a Token Template, CipherTrust Manager ignores the Token Template and uses the Protection Profile.
Token Group	The CTS token group associated with the template specified in the Token Template field. This option is only available if the Action is Tokenize, Detokenize, or Rekey.
Header	The cipher header version for determining the key version. The supported header versions are: V1_5, V1_5_Base64, V2_1, and V2_7.
Tweak Source	Specifies a column in the source database or file that contains the tweak. This allows you to use a different tweak for each row. If you specify a tweak source and a Protection Profile, this value overrides the tweak in the Protection Profile.
IV Source	Specifies a column in the source database or file that contains the IV (initialization vector). This allows you to use a different IV for each row. If you specify an IV source and a Protection Profile, this value overrides the IV in the Protection Profile.

Field	Description
Input Encoding	Specifies how to decode input and create byte array from it. Valid options are BASE2, BASE16, BASE64, UTF8, UTF16LE, UTF16BE, UTF32LE, or UTF32BE. NOTE: BASE2 is supported only with database Blob data type columns.
Output Encoding	Specifies how to encode output byte array to a string. Valid options are BASE16, BASE64, UTF8, UTF16LE, UTF16BE, UTF32LE, or UTF32BE.

- When you are done, click **Create**.
- Repeat this step for any other columns you want BDT to process.

BDT Containers

A container is the connection and encoding information for the input or destination associated with a BDT policy. Containers can point to databases, CSV files, or fixed length files, and they can be created as standalone entities or on-the-fly during BDT policy creation. Whichever method you use, CipherTrust Manager adds the container to the list of available containers for all BDT policies, so make sure you use a descriptive name so that the container can be easily identified in the list.

If you want to create a container during the creation of a BDT policy, click **Create Container** on the **Add Source** or **Add Destination** page of the Create BDT Policy wizard, then see the appropriate section below based on the type of container you want to create.

If you want to create a container as a standalone entity, do the following:

- Log on to the CipherTrust Manager as an administrator.
- In the left pane, click **Data Protection > Containers**.
- Click **Create Container**.
- Refer to one of the following sections depending on the type of container you want to create.
 - Creating a Database Container
 - Creating a CSV Container
 - Creating a Fixed Length File Container

Creating a Database Container

- Enter a user-defined name for the container in the **Name** field. This name must be unique, and it should be descriptive enough that you can easily find this container in the list of available containers.
- In the **Type** field, select one of the following:

- DB2
- ORACLE
- SQL_SERVER
- MYSQL
- HANA

3. Enter the following connection information for the database:

Field	Description
Connection URL	The URL BDT should use to access the database. For example, <code>jdbc:mysql://localhost:3306/world</code>
Username	The user name BDT should use to access the database.
Password	The password for the user account.
Driverclass	The JDBC connection driver class, for example, <code>com.mysql.jdbc.Driver</code>

4. Click **Create**.

Creating a CSV Container

1. Enter a user-defined name for the container in the **Name** field. This name must be unique, and it should be descriptive enough that you can easily find this container in the list of available containers.
2. In the **Type** field, select **CSV_FILE**.
3. Enter the following information for the CSV file:

Field	Description
Delimiter	The character that is used to divide one column from the next in the input file. Any printable ASCII character (except for backslash \) can be used as a delimiter, in addition to space (), tab, and Ctrl-A. NOTE: The delimiter and qualifier characters cannot be the same.
Qualifier	(Optional) The character to enclose fields that contain a delimiter character. Any printable ASCII character (except for backslash \) can be used as a

Field	Description
	qualifier. NOTE: The delimiter and qualifier characters cannot be the same.
File Path	The filepath relative to the <i>inputDir</i> or <i>outputDir</i> path in the BDT config file. The BDT config file resides on the local host where BDT will be running.
Encoding	Used to set character encoding, for example, to enable IBM's EBCDIC. If this container is used as the input source, the encoding type must match the input file. If this container is used as a destination, this is the encoding method BDT will use for the output and failed record files. • If you are using IBM's EBCDIC encoding, set encoding to <i>ibm500</i>. • If you are encrypting ASCII files, set the encoding to <i>ASCII</i>. For a complete list of supported encoding options, see Oracle Documentation .
Column Count	The total number of columns in the input file. This count should include all columns in the input file, regardless of whether the column has a transform rule defined for it or not.
Has Header Row	If you enable this check box, BDT will treat the first row as header row. Values from this row will be treated as column names. The same column names should be mentioned in the transformation action.
Unescape Input	If you enable this check box, BDT will consider delimiter and qualifier characters in the input preceded by a backslash (\) as normal characters and part of the input data. If you are using the BDT output file as input to another process, enable this option.

Creating a Fixed Length File Container

1. Enter a user-defined name for the container in the **Name** field. This name must be unique, and it should be descriptive enough that you can easily find this container in the list of available containers.
2. In the **Type** field, select **FIXED_LENGTH_FILE**.

3. Enter the following information for the fixed length file:

Field	Description
File Path	The filepath relative to the inputDir or outputDir path in the BDT configuration file. The BDT configuration file resides on the local host where BDT will be running.
Encoding	Used to set character encoding, for example, to enable IBM EBCDIC. If this container is used as the input source, the encoding type must match the input file. If this container is used as a destination, this is the encoding method BDT will use for the output and failed record files. • If you are using IBM's EBCDIC encoding, set encoding to ibm500. • If you are encrypting ASCII files, set the encoding to ASCII. For a complete list of supported encoding options, see Oracle Documentation.
Column Count	The total number of columns in the file. This count should include all columns in the input file, regardless of whether the column has a transform rule defined for it or not.
Has Header Row	If you enable this option, BDT will treat the first row as header row. Values from this row will be treated as column names. The same column names should be used in the transformation action.
Unescape Input	If you enable this check box, BDT will consider delimiter and qualifier characters in the input preceded by a backslash (\) as normal characters and part of the input data. If you are using the BDT output file as input to another process, enable this option.
Line Separator	If you enable this option, BDT assumes that the records in the input data are separated by a line separator.
Record Length	The length of one full row in the fixed length file.
Column Position Info	The position of the columns that you want to transform with this BDT policy. For each column, use the following format: <pre>[{"column": "n", "startIndex": "x", "endIndex": "y"}]</pre> Multiple column definitions should be separated with a comma. For example, to specify column 0 with a starting index of 0 and an ending index of 10 along with column 1 with a starting index of 10 and an ending index of 26, you would enter: <pre>[{"column": 0, "startIndex": 0, "endIndex": 10}, {"column": 1, "startIndex": 10, "endIndex": 26}]</pre> If the column definitions are valid, CipherTrust

Field	Description
	Manager displays a green triangle with a white check mark in the corner of this field. If the definitions are not valid, the icon changes to a red triangle with a black X. You cannot save the container until the column definitions are valid.

Product Brief

CipherTrust Batch Data Transformation (BDT)

cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Batch Data Transformation (BDT) is a bulk transformation tool that is used offline to protect/re-protect data inside your data store. BDT can be part of an ongoing extract and transform operation. BDT may also be the primary means of doing annual key rotations on existing data, and part of the process to securely move production data into QA and staging for test purposes while tokenizing it for protection.

Gain transparent field-level encryption, tokenization, data generalization, data masking or redaction without needing to know anything about cryptography. Developers do not need to be involved. All DevOps needs to do is deploy BDT in communication with the source it is going to protect. The source can be either a database or a file. Your Data Security Admin will handle all data protection including creation of policies for rapid data transformation.

You keep months of Developer time, and Security gains the ability to close vulnerability gaps efficiently.

To sustain your compliance and your capacity per sprint, we removed Developer (Dev) involvement from data transformation.

Data multiplies, but team members don't. So that you can focus on more exciting projects, you need an automated process to prepare an existing database to transform data from clear text to protected text, re-encrypt data to the most current key using version metadata, and move data to Data Lakes or Data Warehouses.

Organizations tell us traditional encryption, tokenization, data generalization, data masking and redaction solutions require their Devs to handle fire drills when ciphers, keys or parameters need to change—taking Devs away from roadmap and/or innovative topics for a minimum of two months each and every time an update is needed for ciphers, keys or parameters.

Their Devs get pulled into projects that are a minimum of two calendar months because the Devs have to change source code, and DBAs/Devs have to migrate current data to the new ciphers/keys/parameters. After all changes are submitted, all of the code must be tested and re-tested until it passes all tests. The Devs are required to become cryptographers and change source code for every individual piece of sensitive data in every database column multiplied by every service protecting data. As a result, organizations report that they typically dedicate resources to revenue generating projects and delay their data protection updates for two years, resulting in a weakened security posture, increases in failed audits and more security breaches.

CipherTrust Batch Data Transformation (BDT) removes the need to learn cryptography and automates batch data transformation to encrypt/decrypt, tokenize/detokenize, or re-key large volumes of data quickly. BDT empowers you to perform data transformation on your schedule of choice with no Developer involvement.

DBAs or Data Security Admins configure BDT's policies and initiate data transformation. Using BDT removes the need to write and maintain scripts to read data from source, protect data and then move the transformed data to target systems.

BDT reduces your workload with centrally-managed policies that define encryption options including standard AES encryption or format preserving encryption, while identifying the database columns

to be protected and the number of records in each batch. Data filtering enables creation of customized destination record subsets.

Since transformation from a source database is read-only, BDT uses production databases transparently.

Data Security Admins manage the policies, entering ciphers, keys or parameters. They update data protection in real time, making a selection from a dropdown menu in the GUI or by REST API. Vulnerability gaps are reduced from months to less than a minute.

Since there are no changes to code, no Dev or Test involvement is required to update ciphers/keys/parameters.

Benefits

Increase Developer Capacity

- Devs are not involved in data transformation. Instead of managing security workflows, automation allows developers to focus on higher-value tasks, such as delivering business logic and innovation
- Human error decreases due to no changes to source code for the initial setup or for updates
- Dev and Test are not involved so vulnerability gaps for sensitive data can be closed in minutes after discovery

Security Experts Manage Security

- Data Security Admins configure protection policies and BDT jobs, identifying which columns of sensitive data need to be Protected/Revealed with which policy and the target column or data source for the transformed data
- Data Security Admins can initiate jobs and view job status using the CM GUI or REST APIs
- Data Security Admins can define centrally-managed access policies describing how people see data, including static data masking and redaction
- Data Security Admins can leverage crypto agility to change ciphers, parameters and keys in real time without taking Devs off of other projects

- Visibility on a single pane of glass shows where protection is deployed

Continuous Compliance

- Compliance teams can easily demonstrate compliance without involving Devs – the audit will be more complete, accurate and faster. Includes tracking of all data access for easy integration with SIEM tools
- Separation of Duties aligns with compliance regulations

Ease of use

- Deploy centrally and scale automatically using containers
- Automate batch transformations and control the schedule
- Flexible data extraction/ingestion

Crypto Agility

BDT supports crypto agility for data protection due to the convergence of three design elements:

- Centrally-managed Protection and Access Policies
- No changes to code, ever
- Separation of duties

Crypto agility enables Data Security Admins to change ciphers, keys and parameters in real time.

High Speed Transformation

Flexible Conversion Between Data Stores

BDT can protect data while it is moving, for example, from a database to a comma-separated values (CSV) file or in reverse. BDT supports:

- File to File
- File to Database
- Database to File
- Database to Database

Supports:

- Databases (Oracle, Microsoft SQL Server, IBM Db2, MySQL, SAP Hana)
- CSV files
- Fixed Length files

Views and Triggers can be built to associate the UDFs to Inserts or Queries automatically.

Diagram 1 shows BDT deployed as a docker container. BDT can be scaled up to provide high availability and performance.

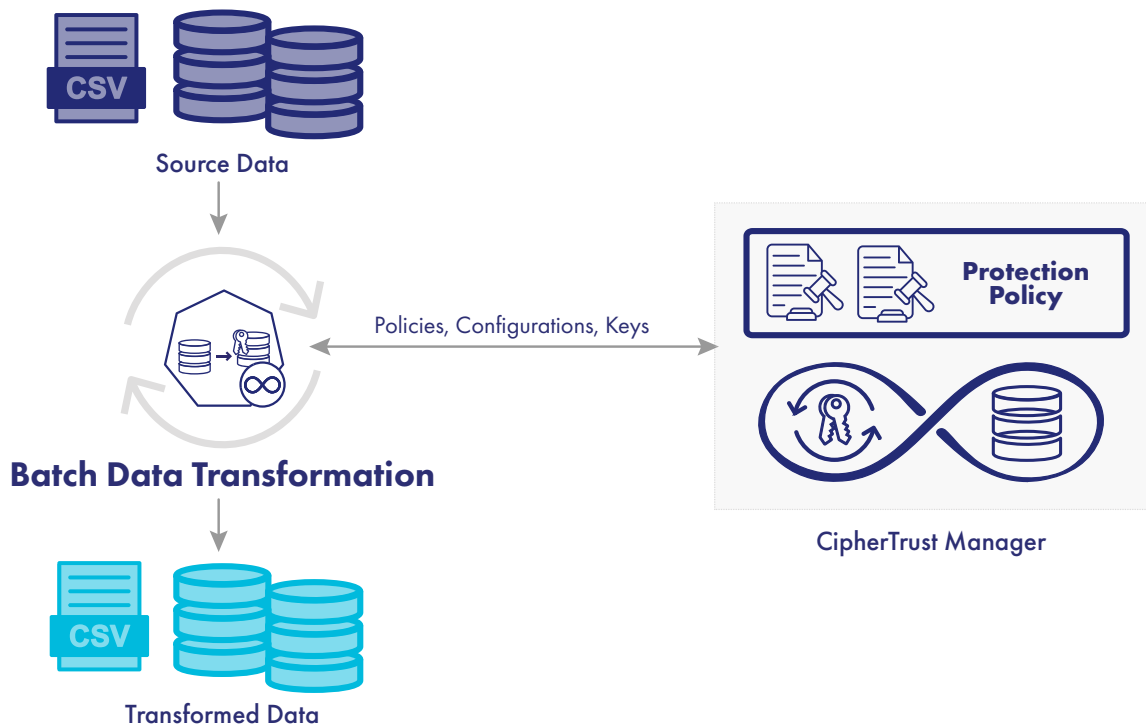


Diagram 1: Extract, Transform, Load (ETL) – CipherTrust Manager handles configuration, policies and keys for BDT.

Protection Policies

We enable the Data Security Admin to define a protection policy by selecting from an ever-growing list of NIST-sanctioned algorithms. The Access Policies can be automated for onboarding/offboarding.

Create Protection Policy

A protection policy specifies how a piece of data should be protected.

Name *

BDT Policy 1

Luhn 

Algorithm *

FPE/FF3-1

Key *

bdt-app-1

Select

Character Set *

Alphanumeric

Select

Access Policy *

bdt-app1-access-policy

Select

Masking Format

FIRST_SIX

Select

Tweak Algorithm 

NONE

Tweak *

55556445466

Prefix 

Prefix

☐ Disable Versioning 

Version Header 

☒ Internal ☐ External

Cancel

Create

Add Access Policy

1 General Info 2 User Set Rules 3 Default Reveal Format 4 Confirmation



Please Review

Before adding the access policy, review all the details.

GENERAL INFO

Name bdt-app1-access-policy [Edit](#)

Description

USER SET RULES

[Edit](#)

User Set	Reveal Format	Masking Format	Error Replacement Value

bdt-app1-us	Plaintext	N/A	N/A

1 User Set Rule 5 per page

DEFAULT REVEAL FORMAT

[Edit](#)

Reveal Format Ciphertext

Masking Format N/A

Error Replacement Value N/A

[Back](#)

Save

Protect Data Across Apps, APIs and Databases

BDT is one of several centrally-managed Thales data protection offerings. CipherTrust Application Data Protection SDK (CADP SDK) offers field-level data protection to developers as a simple-to-integrate library. CipherTrust RESTful Data Protection (CRDP) is a RESTful service that offers field-level data protection across cloud and on-premises applications. CipherTrust Data Protection Gateway (DPG) is a Gateway that transparently intercepts RESTful API calls and protects data with no code changes required on the RESTful service or clients.

CipherTrust Database Protection (CDP) offers transparent, column-level data protection for a wide range of databases.

All centrally-managed Connectors support Static Data Masking and Redaction. CADP, CRDP and DPG additionally support Dynamic Data Masking.

BDT complements our other CipherTrust data protection solutions by automating batch data transformation processes.

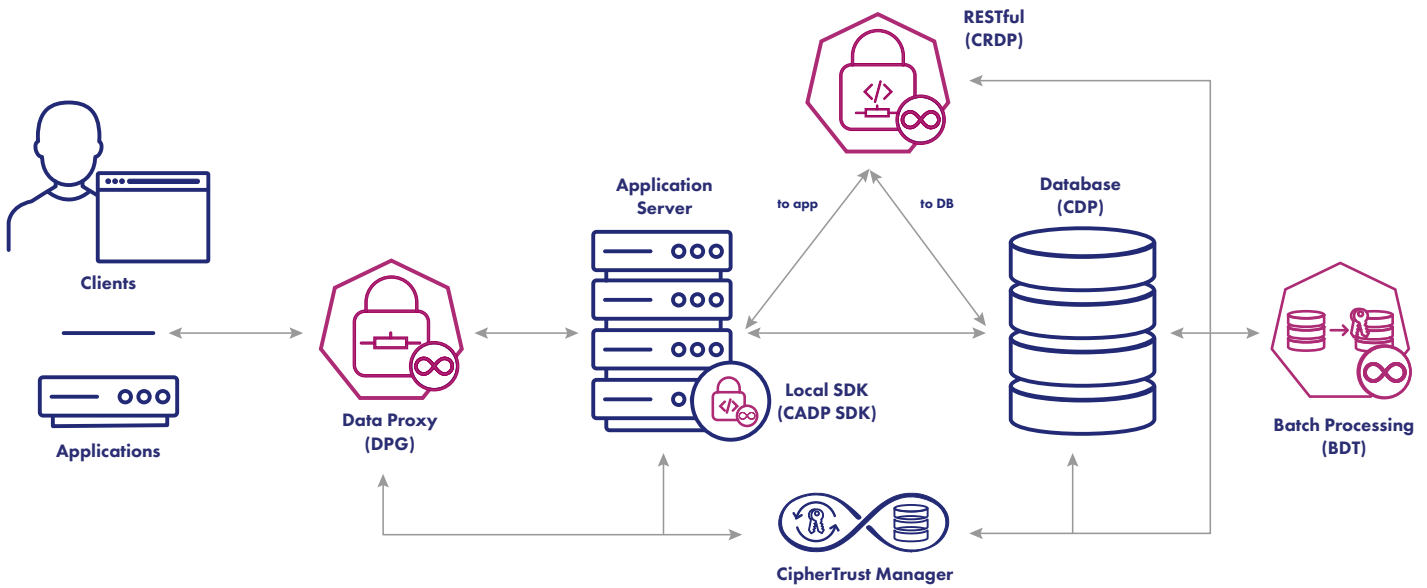


Diagram 2: BDT can be used with DPG, CADP, CRDP and CDP to transform data in files or databases and rotate keys to maintain security compliance. BDT can connect to a database or to a server. Diagram 2 shows Connection to a database.

CipherTrust Data Security Platform

BDT is part of the CipherTrust Data Security Platform (CDSP), which unifies data discovery, classification, protection and monitoring with unprecedented granular access controls and centralized key management. Protecting your sensitive data with CDSP decreases time to compliance, simplifies data security operations, secures cloud migrations and reduces risk across your business. You can rely on the Thales CipherTrust Data Security Platform to help you discover, protect, control and monitor your organization's sensitive data, wherever the data resides.

ESG Statement

The Thales CipherTrust Batch Data Transformation (BDT) containerized solution makes a smaller carbon footprint than a full server solution or virtual appliance because BDT elastically scales, in alignment with Thales' ESG (environmental, social, and governance) commitment to a greener, safer world.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Vormetric Data Security Platform

Batch Data Transformation 2.0 ***Installation and User Guide***

Document version 1

JANUARY 2018

Vormetric Data Security Platform

Batch Data Transformation 2.0

Installation and User Guide

January 2018

Document version 1

Copyright (C) 2009- 2018 Vormetric, Inc. All rights reserved.

NOTICES, LICENSES, AND USE RESTRICTIONS

Vormetric is a registered trademark of Thales eSecurity, Inc. in the United States (U.S.) and a registered trademark or trademark in other countries. Microsoft, Windows, Windows XP, Windows NT, SQL Server and the Windows logo are registered trademarks or trademarks of Microsoft Corporation in the U.S. and or other countries.

UNIX is a registered trademark of The Open Group in the U.S. and a registered trademark or trademark in other countries. Linux is a registered trademark of Linus Torvalds in the U.S., and a registered trademark or trademark in other countries.

Oracle, Oracle ASM, Solaris, SPARC, Oracle Enterprise Linux and Java are registered trademarks of Oracle Corporation in the United States (U.S.) and a registered trademark or trademark in other countries (DO THE SAME FOR THE REMAINING COMPANIES)

IBM, IBM logo, ibm.com, AIX, DB2, PowerPC, DB2 Universal Database are trademarks of International Business Machines Corporation in the U.S., other countries, or both.

Intel, Intel logo, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the U.S. and other countries.

HP-UX is registered trademark of Hewlett-Packard Company in the U.S., other countries, or both.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S., other countries, or both.

X Window System is a trademark of the Massachusetts Institute of Technology.

Red Hat and Red Hat Enterprise Linux, are trademarks of Red Hat, Inc., registered in the United States and other countries.

SUSE and SLES are a registered Trademarks of Novell, Inc.

All other products described in this document are registered trademarks or trademarks of their respective holders in the United States or in other countries.

The software ("Software") and documentation contains confidential and proprietary information that is the property of Thales eSecurity, Inc. The Software and documentation are furnished under license from Thales and may be used only in accordance with the terms of the license. No part of the Software and documentation may be reproduced, transmitted, translated, or reversed engineered, in any form or by any means, electronic, mechanical, manual, optical, or otherwise.

The license holder ("Licensee") shall comply with all applicable laws and regulations (including local laws of the country where the Software is being used) pertaining to the Software including, without limitation, restrictions on use of products containing encryption, import or export laws and regulations, and domestic and international laws and regulations pertaining to privacy and the protection of financial, medical, or personally identifiable information. Without limiting the generality of the foregoing, Licensee shall not export or re-export the Software, or allow access to the Software to any third party including, without limitation, any customer of Licensee, in violation of U.S. laws and regulations, including, without limitation, the Export Administration Act of 1979, as amended, and successor legislation, and the Export Administration Regulations issued by the Department of Commerce, or in violation of the export laws of any other country.

Any provision of any Software to the U.S. Government is with "Restricted Rights" as follows: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277.7013, and in subparagraphs (a) through (d) of the Commercial Computer-Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR Supplement, when applicable. The Software is a "commercial item" as that term is defined at 48 CFR 2.101, consisting of "commercial computer software" and "commercial computer software documentation", as such terms are used in 48 CFR 12.212 and is provided to the U.S. Government and all of its agencies only as a commercial end item. Consistent with 48 CFR 12.212 and DFARS 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Software with only those rights set forth herein. Any provision of Software to the U.S. Government is with Limited Rights. Thales is Thales eSecurity, Inc. at Suite 710, 900 South Pine Island Road, Plantation, FL 33324.

Vormetric Transparent Encryption Installation and Configuration Guide

THALES, PROVIDES THIS SOFTWARE AND DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND ANY WARRANTIES ARISING OUT OF CONDUCT OR INDUSTRY PRACTICE. ACCORDINGLY, THALES DISCLAIMS ANY LIABILITY, AND SHALL HAVE NO RESPONSIBILITY, ARISING OUT OF ANY FAILURE OF THE SOFTWARE TO OPERATE IN ANY ENVIRONMENT OR IN CONNECTION WITH ANY HARDWARE OR TECHNOLOGY, INCLUDING, WITHOUT LIMITATION, ANY FAILURE OF DATA TO BE PROPERLY PROCESSED OR TRANSFERRED TO, IN OR THROUGH LICENSEE'S COMPUTER ENVIRONMENT OR ANY FAILURE OF ANY TRANSMISSION HARDWARE, TECHNOLOGY, OR SYSTEM USED BY LICENSEE OR ANY LICENSEE CUSTOMER. THALES SHALL HAVE NO LIABILITY FOR, AND LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST, ANY SHORTFALL IN PERFORMANCE OF THE SOFTWARE, OTHER HARDWARE OR TECHNOLOGY, OR FOR ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AS A RESULT OF THE USE OF THE SOFTWARE IN ANY ENVIRONMENT. LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST ANY COSTS, CLAIMS, OR LIABILITIES ARISING OUT OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY. NO PROVISION OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY SHALL BE BINDING ON THALES.

Protected by U.S. patents: 6,678,828; 6,931,530; 7,143,288; 7,283,538; 7,334,124

Vormetric Data Security includes a restricted license to the embedded IBM DB2 database. That license stipulates that the database may only be used in conjunction with the Vormetric Security Server. The license for the embedded DB2 database may not be transferred and does not authorize the use of IBM or 3rd party tools to access the database directly.

Contents

Preface	1
Documentation Version History	1
Assumptions	1
Vormetric Data Security Platform—Overview	2
How to Search Documentation Sets	3
Service Updates and Support Information	4
1 Overview	5
Overview	5
Architecture	6
System Requirements	7
Input data requirements	7
2 Installing and Configuring BDT	9
Installation (Linux)	9
Installation (Windows)	10
Installed Software Directory Structure	10
Edit the bdt.config File	11
Overview	11
Example bdt.config file	11
About characterSets	13
Default characterSets names and range values	13
VTS server authentication	14
VTS client authentication	14
3 Using Batch Data Transformation	15
Running BDT	15

Overview of running BDT	15
Output file format	16
BDT command syntax	16
Example BDT commands	17
Example 1: Run the BDT utility	17
Example 2: Display help	17
Example 3: Set BDT passwords in bdt.config file	17
Example 3b: Set database passwords in a BDT policy file	18
Example 4: Validate configuration	18
Example 5: Transform input file	18
Example 6: Skip validation	19
Example 7: Set BDT passwords and transform data	19
Example 8: List source tables, columns (for db transformations)	19
Example 9: List destination tables, columns (for db transformations)	19
Creating a BDT Policy	19
Top-level policy attributes	20
The source/destination attributes	20
For databases	20
For CSV files	20
For fixed-length files	22
The tables attributes	23
About Format-Preserving Encryption (FPE)	24
Sample policy	24
Policy actions	26
ENCRYPT policy action	26
DECRYPT policy action	29
TOKENIZE policy action	29
DETOKENIZE policy action	30
REKEY policy action	30
(Semi-optional) Set character encoding	32
(Optional) Define fixed-length record format	33
Example policy	37
Using Text Qualifier Characters in Input Files	43
Transforming Databases	44
Overview	44

Terminology	44
Supported databases	44
Example 1: Transforming database table columns	44
DbToDbTransformation.policy sample	44
Example 2: Transforming database tables to files	46
DBToFileTransformation.policy sample	46
Example 3: Transforming input file to database table	47
FileToDBTransformation.policy sample	47
Filtering Input Data	49
Example: Filter input rows from a source file	49
Example: Filter database table rows	50
Monitoring and Troubleshooting	51
Log files	51
Thread count and batch size best practices	51

PREFACE

The *Batch Data Transformation Installation and User Guide* describes how to install, configure, and use Vormetric Batch Data Transformation.

Documentation Version History

The following table describes the documentation changes made for each document version.

Documentation Changes

Product/Document Version	Date	Changes
2.0 v1	1/19/18	Added support for database transformations, fixed-length file format support details, added AES_CTR and FF1 algorithm support. New policy file attributes added and described. 80% of guide material changed or edited.
1.1 v1	11/15/17	(Internal-only release) Added FF1 encryption, character encoding, fixed-length formatting,
1.0 v1	12/16/16	First release of document.

Assumptions

This documentation assumes:

- Familiarity with Vormetric Application Encryption (VAE)
- Familiarity with Vormetric Token Server (VTS)
- Some knowledge of format-preserving encryption, tokenization, or cipher block chaining principles, depending on which technique you will use for Batch Data Transformation.

Vormetric Data Security Platform—Overview

The Vormetric Data Security (VDS) Platform protects data wherever it resides. The platform solves security and compliance issues with encryption, key management, privileged user access control, and security intelligence logging. It protects data in databases, files, and Big Data nodes across public, private, hybrid clouds and traditional infrastructures.

Figure 1: The Vormetric “Solar System”



The platform consists of products that share a common, extensible infrastructure. At the heart of the platform is the Data Security Manager (DSM), which coordinates policies, keys, and the collection of security intelligence, all of which is managed and observed through your browser. In addition to the DSM, the Vormetric Data Security Platform consists of the following:

- **Vormetric Application Encryption (VAE)** provides a framework to deliver application-layer encryption such as column- or field-level encryption in databases, Big Data, or PaaS applications. VAE is an application encryption library providing a standards-based API to do

cryptographic and encryption key management operations into existing corporate applications.

- **Vormetric Cloud Encryption Gateway (VCEG)** safeguards files in cloud-storage environments, including Amazon S3 and Box. VCEG encrypts sensitive data before it is saved to the cloud, enabling security teams to establish visibility and control around cloud assets.
- **Vormetric Key Management (VKM)** centralizes 3rd-party encryption keys and stores certificates securely. It provides standards-based enterprise encryption key management for Transparent Database Encryption (TDE), KMIP-compliant devices, and offers vaulting and inventory of certificates.
- **Vormetric Protection for Teradata Database** provides granular controls to secure assets in Teradata environments. It simplifies the process of using column-level encryption in your Teradata database. It provides documented, standards-based APIs and user-defined functions (UDFs) for cryptographic and key management operations.
- **Vormetric Security Intelligence** provides comprehensive logging combined with Security Information Event Management (SIEM) systems to detect advanced persistent threats and insider threats. In addition, the logs satisfy compliance and regulatory audits.
- **Vormetric Tokenization with Dynamic Data Masking (VTS)** replaces sensitive data in your database with unique identification symbols called tokens. This reduces the number of places that clear-text sensitive data reside, and thus reduces the scope of complying with PCI DSS and corporate security policies.
- **Vormetric Transparent Encryption (VTE)** secures any database, file, or volume across your enterprise without changing the applications, infrastructure, or user experience.

How to Search Documentation Sets

Technical information for Vormetric products can be spread across many documents. Instead of searching through each individual document to find the information you need, you can use the following procedure to search all of the VTE documents with a single search in Windows (the same process should work for UNIX/Linux):

1. Copy all the .pdf files of a specific product into a single directory. For example, using the Vormetric Transparent Encryption:

```
C:\Documents\PDFs\5.2.3>dir
Admin_Guide_V1.pdf
Agent_Install_& Config_Guide_v2.pdf
Data_Transformation_Guide_v1.pdf
DSM_Automation_Reference_v1.pdf
DSM_Install_Guide_v1.pdf
Event_&_Log_Messages_Ref_v1.pdf
```


GettingStarted_v1.pdf
 VSI_Reference_v1.pdf
 RN_DSM.pdf
 RN_Linux.pdf
 RN_RHEL7.pdf
 RN_UNIX.pdf
 RN_Windows.pdf
 VDSCompatibilityMatrix.pdf

2. Bring up Adobe Reader or Adobe Acrobat.
3. Open any pdf file from that directory: **File > Open > Select File.**
4. Click **Edit > Advanced Search.**
5. Under "*Where would you like to search?*" click "**All PDF Documents in**", then select the directory containing all the VTE PDF files. In this case, C:\Documents\PDFs\5.2.3
6. In the "*What word or phrase would you like to search for?*" enter the search phrase and click search.

You can do this with any set of PDF files.

Service Updates and Support Information

The license agreement that you have entered into to acquire the Thales products ("License Agreement") defines software updates and upgrades, support and services, and governs the terms under which they are provided. Any statements made in this guide or collateral documents that conflict with the definitions or terms in the License Agreement, shall be superseded by the definitions and terms of the License Agreement. Any references made to "upgrades" in this guide or collateral documentation can apply either to a software update or upgrade.

For support and troubleshooting issues:

- <http://help.thalesecurity.com>
- <http://support.vormetric.com>
- support@thalesecurity.com
- (877) 267-3247

For Thales Sales:

- <http://go.thalesecurity.com/contact-data-security-specialist-form.html>
- sales@thalesec.net
- (408) 433-6000

Overview

The Batch Data Transformation utility (BDT) provides a policy-based data transformation and re-key service. This chapter contains the following sections:

- [“Overview” on page 5](#)
- [“Architecture” on page 6](#)
- [“System Requirements” on page 7](#)

Overview

The Batch Data Transformation utility (BDT) is a command-line tool that you can use to achieve these main goals:

- Encrypt production data quickly and securely
- Re-key encrypted data
- Migrate data out of a production environment

BDT provides a policy-based data transformation and re-key service. The utility's actions are based on policies, which are defined in policy files. For each action or group of actions that you want to do with the utility, you define a policy file. Each policy file contains one or more configuration sections. Each section defines an action and its attributes. For more information, see [“Creating a BDT Policy” on page 19](#).

BDT 2.0 supports the following transformation options:

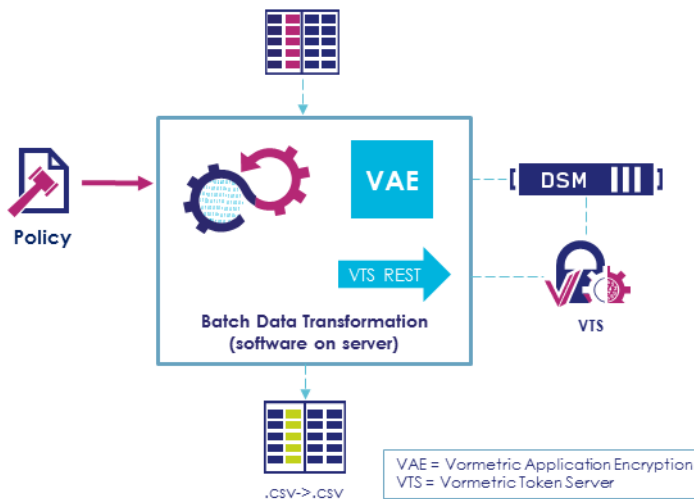
- File to file
- File to database table
- Database table to file
- Database to database

To run the Batch Data Transformation utility, invoke it from the command line. See [“Running BDT” on page 15](#).

Architecture

The BDT utility makes use of other Vormetric technology, including Vormetric Application Encryption (VAE) and the Vormetric Tokenization Server (VTS). It can encrypt and decrypt data using format-preserving encryption (FPE), either FF3 or FF1, or Advanced Encryption Standard (AES) block cipher, either cipher block chaining (AES_CBC_PAD) or counter (AES_CTR) modes. Or it can tokenize data using the VTS. In this version of BDT, the user can also designate specific source and destination database tables and columns.

BDT also supports character encoding, such as EBCDIC, and the option of fixed-length and .csv file formats.



System Requirements

Please refer to the *Vormetric Batch Data Transformation 2.0 Release Notes* for system requirements, including:

- Compatible VAE/DSM versions
- Compatible VTS/DSM versions
- Supported databases

BDT supports the same operating systems as Vormetric Application Encryption (VAE), and has a few additional special requirements:

- Java Runtime Environment (JRE) 1.8+
- 4 cores
- 16 GB RAM

Input data requirements

- Per-column data size limit: 128K
- The input data file can contain quoted and unquoted values. Both "field1_Value" and field2_Value are recognized as data values. To use quoted values, you must specify the double quote character as a text qualifier. (See [“Using Text Qualifier Characters in Input Files” on page 43.](#))
- Fields must be separated by the delimiter character specified in the policy file. (See [“Creating a BDT Policy” on page 19.](#))
- If a field value contains the delimiter character, the value must be enclosed by text qualifier characters, as specified in the policy file. (See [“Using Text Qualifier Characters in Input Files” on page 43.](#))
- If a field value contains the text qualifier, the entire value must be enclosed in text qualifier characters.
- Another way to deal with field values having delimiter or qualifier characters is to escape those character using the backslash (\) instead of enclosing the field in text qualifier characters. When using this technique, set the `unescapeInput` attribute in the policy file to true. For example:

Jon, Smith, 400\, \"West Avenue, 5000

If the field value has a backslash character, it must also be escaped using an additional backslash character.



Installing and Configuring BDT

This chapter tells how to install Batch Data Transformation on Windows or Linux and how to modify the software configuration settings. Be sure your system is compatible, as listed in [“System Requirements” on page 7](#).

This chapter contains the following sections:

- [“Installation \(Linux\)” on page 9](#)
- [“Installation \(Windows\)” on page 10](#)
- [“Installed Software Directory Structure” on page 10](#)
- [“Edit the bdt.config File” on page 11](#)

Installation (Linux)

1. Download the BDT distribution.
`wget https://<path to download site>/bdt-2.0.0.tar.gz`
2. Create a BDT home directory at a convenient location.
`cd /usr/local/bin`
`mkdir bdt`
3. Extract the distribution to the BDT home directory.
`sudo tar -xzf filename.tgz -C /usr/local/bin/bdt`
4. Add the Java bin directory path to the PATH environment variable. Edit the `.bashrc` file for the admin user and add the following lines:
`export JAVA_HOME=/usr/lib/java/jre`
`export PATH=$JAVA_HOME/bin:$PATH`
5. Verify installation by checking to be sure the installation directories appear; see [“Installed Software Directory Structure” on page 10](#).

Installation (Windows)

1. Download the BDT distribution file `bdt-2.0.0.zip` through the web browser using the URL obtained from your sales representative.
2. Create a BDT home directory at a convenient location. Use the File Explorer “New Folder” button to create a new folder named BDT under the folder `C:\Program Files`.
3. Extract the distribution to the BDT home directory. Use winzip, pkunzip, 7zip, or your other favorite file compression/extraction utility.
4. Add the Java bin directory path to the PATH environment variable:
 - a. Start the Control Panel
 - b. Click System
 - c. Click Advanced System Settings
 - d. Click the Environment Variables button.
 - e. Under System Variables, select Path, then click Edit.



Be **very careful** not to delete any of the existing text here.

Hit the “End” button, then append this to what’s already in the value:

`;C:\Program Files\BDT`

- f. Click OK.
5. Verify installation by checking to be sure the installation directories appear; see [“Installed Software Directory Structure” on page 10](#).

Installed Software Directory Structure

The directory structure of the installed software is as follows:

bin	Executable scripts for validating configuration, testing and execution.
conf	Default configuration files. Includes <code>bdt.config</code> and logging properties.
lib	Required JAVA library dependencies.
log	Log file directory.
samples	Sample policy and configuration files.

Edit the bdt.config File

Overview

The configuration of the BDT utility is stored in JSON format in the file `bdt.config`. Edit this file to change settings to refer to your own environment and to tune the performance of the utility.

Refer to the [“Example bdt.config file” on page 11](#).

At the top of the file are several global configuration settings, followed by settings that configure the main underlying tools used by BDT:

- The first few lines contain settings for the Batch Data Transformation utility itself. These include `inputDirectory`, `outputDirectory`, `threadCount`, and `batchSize`.
- The `vts{}` object contains settings to customize the behavior of the Vormetric Tokenization Server.
NOTE: When running BDT for the first time, follow the steps in [“Example 3: Set BDT passwords in bdt.config file” on page 17](#) to store encrypted pin and passwords in `bdt.config`.
- The `vae{}` object contains settings related to Vormetric Application Encryption. Note that you will encode and enter the `pin` value using the steps in [“Example 3: Set BDT passwords in bdt.config file” on page 17](#).
- The `characterSets{}` object was added to `bdt.config` to improve compatibility with the Vormetric Tokenization Server (VTS). See [“About characterSets” on page 13](#).

Example bdt.config file

```
{
  "inputDirectory": "/home/user/input",
  "outputDirectory": "/home/user/output",
  "threadCount": 20,                      /* maximum running threads to transform file */
  "batchSize": 1000,                     /* Number of records processed in batch */
  "vts": {
    "hostName": "vtshost",                /* hostname of a machine where tokenization server is
      running */
    "userName": "vtsuser",                /* VTS username */
    "password": "",                       /* VTS password. Don't put plain text here. Use bdt -e option
      to put encrypted value here */
  }
}
```




```

"tokenUrl": "https://vtshost/vts/rest/v2.0/tokenize",      /* VTS tokenize rest
  url */
"detokenUrl": "https://vtshost/vts/rest/v2.0/detokenize", /* VTS detokenize rest
  url */
"ssl" : {
  "server" : {                                           /*ssl configuration for
    server*/
    "sslmode" : "DEFAULT",                               /* ssl mode (DEFAULT, ALLOW_ALL
    - allow everything, SPECIFY_SSL_CERT - communicate if server cert exist in
    specified truststore)*/
    "verifyHostname" : true,                             /* whether to do host
    name verification */
    "truststore": "",                                   /* truststore file path,
    truststore should have server cert. Applicable only for SPECIFY_SSL_CERT
    mode*/
    "password" : ""                                     /* truststore file password.
    Applicable only for SPECIFY_SSL_CERT mode*/
  },
  "client" : {                                           /* ssl configuration for
    client*/
    "sslmode" : "DEFAULT",                               /* ssl mode (DEFAULT/ALLOW_ALL -
    don't send client authentication, SPECIFY_SSL_CERT - send client
    authentication certs specified keystore)*/
    "keystore": "",                                     /* keystore file path.
    keystore should have client key and certificate */
    "storepassword" : "",                               /* keystore file password
    */
    "keypassword" : ""                                  /* key file password.
    usually same as keystore password.*/
  }
}
},
"vae": {
  "libPath": "", /* Vae lib path. empty means platform specific default path */
  "pin": "" /* Vae lib pin. Don't put plain text here. Use bdt -e option to put
    encrypted value here. */
},
"characterSets":[                                       /*configurable list of charset names and their range*/
  {
    "latin":["0020-007E"]
  }
]

```

```
    },  
    {  
      "digits":["0030-0039"]  
    },  
    {  
      "alphabets":["0041-005A", "0061-007A"]  
    },  
    {  
      "alphanumeric":["0030-0039", "0041-005A", "0061-007A"]  
    }  
  ]  
}
```

About characterSets

In earlier versions of BDT, users could specify a character set range in a policy file. Now, use the `characterSets` attribute at the `bdt.config` level to define a character set name (such as “digits”) and a range, entered as a name/value pair. Four defaults are listed; users can also define their own name and range for a character set.

Default characterSets names and range values

The sample `bdt.config` file includes the following sample `characterSets` name/value definitions. Value is a list of numeric code ranges for this character set, specified in hex representation. For example, numeric characters range from 0030 to 0039 in hex, which is 48-57 in decimal.

Name	Value (Range)
latin	"0020-007E"
digits	"0030-0039"
alphabets	"0041-005A", "0061-007A"
alphanumeric	"0030-0039", "0041-005A", "0061-007A"

VTS server authentication

You must set up SSL for secure communication between the BDT utility and the Tokenization Server (VTS). In the `vts{}` section of `bdt.config`, the `server{}` object contains the following settings related to SSL authentication:

<code>sslmode</code>	One of the following values: DEFAULT - Trust only a standard valid certificate issued by a Certificate Authority (CA). If the certificate is expired, self-signed, or invalid, communication with the VTS server fails. SPECIFY_SSL_CERT - Trust standard certificates and certificates stored in the provided trust store (specified in the <code>truststore</code> setting). Use to accept self-signed and expired certificates. ALLOW_ALL - Trust all certificates; no trust policy is defined. Any kind of SSL certificate is acceptable, including valid, expired, self-signed, or any other. The <code>truststore</code> setting is not required.
<code>VerifyHostName</code>	Set to <code>"true"</code> to enable hostname verification for SSL communication, <code>"false"</code> to disable hostname verification. Default: <code>true</code> .
<code>truststore</code>	(Used only when <code>sslmode</code> is <code>SPECIFY_SSL_CERT</code>) Truststore file path. To set up the truststore: Get the server's public certificate. If not available, open the VTS URL in a browser and export it from the Security option. Import the certificate and create the truststore. Use the following command. It will output the truststore password. <pre>keytool -import -alias "vts host certificate" -file server.crt -keystore server.truststore</pre> IMPORTANT: Note this password. You need to provide it in the <code>password</code> parameter.
<code>password</code>	(Used only when <code>sslmode</code> is <code>SPECIFY_SSL_CERT</code>) Truststore file password obtained when you imported the VTS certificate and created the truststore.

VTS client authentication

In the `vts{}` section of `bdt.config`, the `client{}` object contains the following settings related to SSL authentication:

<code>sslmode</code>	One of the following values: DEFAULT - Client authentication is disabled. No need to send client identity. ALLOW_ALL - Client authentication is disabled. No need to send client identity. SPECIFY_SSL_CERT - Client authentication is enabled. Create keystore with client certificate and key. Set keystore path in the <code>keystore</code> parameter. Communication succeeds if the VTS server finds a valid certificate set in the keystore.
<code>keystore</code>	Client keystore file path. This assumes a keystore has already been created; for example, using <code>keytool</code>
<code>storepassword</code>	Client keystore file password
<code>keypassword</code>	Client's key password

Using Batch Data Transformation

This chapter tells how to configure Batch Data Transformation policies and run transformations. It contains the following sections:

- [“Running BDT” on page 15](#)
- [“Creating a BDT Policy” on page 19](#)
- [“Using Text Qualifier Characters in Input Files” on page 43](#)
- [“Transforming Databases” on page 44](#)
- [“Filtering Input Data” on page 49](#)
- [“Monitoring and Troubleshooting” on page 51](#)

Running BDT

Overview of running BDT

1. Update the properties in the `bdt.config` file to reflect your environment.
2. Create column transformation rules in the file `bdt.policy` based on your input file and transformation requirements.
3. Change to the `/bin` subdirectory of the BDT installation directory. For example, on Linux:

```
cd /home/bdt/bin
```
4. Run BDT from the command line using either `bdt.sh` or `bdt.bat`. If this is first time you are running BDT, use the `-e` option to set the passwords.

```
./bdt.sh [-e] -t [-c configfilepath] -p policyfilepath
```

Use `-e` the first time you run BDT. After that, use it whenever you want to change the passwords.

Use `-c` to specify the location of `bdt.config`. If `-c` is omitted, the default configuration file `bdt/conf/bdt.config` is used.

See also: [“Example 3: Set BDT passwords in bdt.config file” on page 17](#) and [“Example 3b: Set database passwords in a BDT policy file” on page 18](#).

Output file format

When BDT runs a data transformation (that is, when you run BDT with the `-t` option) it first validates the `bdt.config` and `bdt.policy` files to be sure they are valid. Then it performs the data transformation specified in those files.

BDT stores the transformed data in the output directory specified in `bdt.config`. The output file for each BDT run is marked with a time stamp. The output directory can contain output files from multiple runs of BDT.

If the input file contains records which BDT can not transform, they are stored in the same output directory in `<policy_name-timestamp>.failed`. (Policy name is defined under `name` in a policy file.)

The output file contains fields separated by the delimiter character specified in the policy file. Each line represent a individual record.

If a field value contains a delimiter character, that character is escaped in the output file with a backslash character (`\`). For example:

```
Jon, Smith, 500, "wRui89$ass, 3000
```

is escaped as

```
Jon, Smith, 500\, "wRui89$ass, 3000
```

When using the file BDT output file as input for another transformation, always set the `unescapeInput` flag in the policy file to `true`. (See [“Creating a BDT Policy” on page 19.](#))

BDT command syntax

The Batch Data Transformation utility runs at the command line with the following syntax:

```
bdt [-c <configfilepath>] [-e] [-h | -ld <type> | -ls <type> | -t | -v] [-p <policyfilepath>] [-sv] [-table <tableName>]
```

<code>-c, --configfile <configfilepath></code>	Location of the BDT configuration file. Replace <code><configfilepath></code> with the path to <code>bdt.config</code> . If omitted, the default file <code>bdt/conf/bdt.config</code> is used.
<code>-e, --encryptPassword</code>	Set the VAE library password and VTS password, encrypt them, and store in <code>bdt.config</code> . Use this option the first time you run BDT. You can also use it whenever you want to change the passwords. BDT prompts you to enter the passwords at the console.
<code>-h, --help</code>	Display the BDT command syntax and information about how to use it.
<code>-ld <type></code>	<code>listDestination <type></code> list data destination objects. Object types [tables, columns]
<code>-ls <type></code>	<code>listSource <type></code> list data source objects. Object types [tables, columns]

<code>-p, --policyfile <policyfilepath></code>	Location of the BDT policy file. Replace <code><policyfilepath></code> with the path to <code>bdt.policy</code> .
<code>-sv, --skipvalidation</code>	Run BDT without first checking the <code>bdt.config</code> and <code>bdt.policy</code> files for correctness.  Caution: Use only for testing. Do not use in a production environment.
<code>-t, --transform</code>	Validate <code>bdt.config</code> and <code>bdt.policy</code> , then transform the input file and store the results in the output directory. If this option is omitted, BDT does not perform the data transformation. Running without <code>-t</code> is useful when you only want to set passwords or validate configuration files.
<code>-v, --validate</code>	Validate <code>bdt.config</code> and (optionally) <code>bdt.policy</code> . Use this option when you want to check the files without actually transforming the data. The policy file is validated if the <code>-p</code> option is included in the command. If you are running with <code>-t</code> , you don't need to also include <code>-v</code> . The <code>-t</code> option includes an implicit <code>-v</code> .
<code>-table <tableName></code>	List columns for this table. This option must be accompanied by <code>-ls</code> or <code>-ld</code> option. General syntax: <code>bdt.bat -ls (or -ld) columns -table <table_name> -p <policy file></code>

Example BDT commands

Example 1: Run the BDT utility

Run `bdt.sh` or `bdt.bat` from the `distribution/bin` directory.

Example 2: Display help

Run `./bdt.sh -h` or `./bdt.sh --help`

Example 3: Set BDT passwords in `bdt.config` file

The first time you run BDT, use the `-e` option to store encrypted passwords in the BDT configuration file. Run the following command:

```
./bdt.sh -e [-c configfilepath][-p policyfilepath]
```

This will prompt for the VAE library password and the VTS user password, keystore, truststore and key password. These passwords will be encrypted and stored in the `bdt.config` file specified in the `-c` option. If `-c` is omitted, the default file `bdt/conf/bdt.config` is used.

Example 3b: Set database passwords in a BDT policy file

The `-e` option can also be used to store the database password in a policy file, if the policy file has a database as a source or destination. Database passwords will also be stored in encrypted form.

Run the following command:

```
./bdt.sh -e [-c configfilepath][-p policyfilepath]
```

To change the password at any time, run BDT with the `-e` option again.

Example 4: Validate configuration

If you only want to validate the input files, not perform any other operation, use the `-v` option. You can specify which files to validate by adding `-c` and `-p`.

```
./bdt.sh -v [-c configfilepath -p policyfilepath]
```

`-c` is optional. If not provided, the default configuration file `bdtd/conf/bdtd.config` is validated.

`-p` is optional. If not provided, the policy file is not validated.

To validate `bdtd.config` alone, assuming the file is stored in the expected default location, use `-v` with no other options:

```
./bdt.sh -v
```

Example 5: Transform input file

1. Update properties inside `bdtd.config` file as per your environment.
2. Create `bdtd.policy` based on your input file and transformation requirement. The Samples directory has `bdtd.policy` samples with explanatory comments.
3. Run `./bdt.sh -t [-c configfilepath] -p policyfilepath`

`-c` is optional. If not provided, the default `config` file from the location `BDT/conf/bdtd.config` will be used

This will first validate configuration(`bdtd.config`+`bdtd.policy` validation) and then trigger transformation

The output file will be generated in the output directory specified in `bdtd.config`. Check the output file name with the current timestamp appended.

The same output directory will have a file `<policy_name-timestamp>.failed.` , which records any utility that has failed to transform. (Policy name is defined under `name` in a policy file.)

Example 6: Skip validation

The `-SV` option allows you to trigger transformation without performing any validation, in order to save validation time.

Example 7: Set BDT passwords and transform data

The `-e` option can be used with the `--validate` or `--transform` option. This will first put the encrypted passwords in `bdt.config` and then perform the specified operation: either validate the configuration and policy files or perform data transformation. For example, the following command gets new passwords (`-e`), then transforms the data (`-t`) using the policy specified in the `-p` option:

```
./bdt.sh -e -t -p policyfilepath
```

Example 8: List source tables, columns (for db transformations)

Source connection properties are picked from the policy file source attribute.

Run `./bdt.sh -ls table -p policyfilepath` to list source tables.

Run `./bdt.sh -ls column -table test1 -p policyfilepath` to list the columns of source table `test1`

Example 9: List destination tables, columns (for db transformations)

Destination connection properties are picked from the policy file destination attribute.

Run `./bdt.sh -ld table -p policyfilepath` to list destination tables.

Run `./bdt.sh -ld column -table test1 -p policyfilepath` to list columns of destination table `test1`

Creating a BDT Policy

A BDT policy tells how to perform transformation of the data in the input file. The policy is stored in the file `bdt.policy`.

Each `bdt.policy` file includes the following:

- “Top-level policy attributes”
- “The source/destination attributes”
- “The tables attributes”

Top-level policy attributes

id	A unique identifier for the policy.
name	A unique name for the policy.
source	Defines details of data input. For RDBMS details include connection parameters. For file detail includes file type (CSV_FILE or FIXED_LENGTH_FILE), delimiter, encoding etc. See also “The source/destination attributes” on page 20 .
destination	Defines details of data output. Where to write transformed data. For RDBMS details include connection parameters. For file detail includes file type (CSV_FILE or FIXED_LENGTH_FILE), delimiter, encoding etc. See also “The source/destination attributes” on page 20
tables	List of table to be transformed. See also, “The tables attributes” on page 23
createBadRecordFile	True or false. Set true to create .failed file, otherwise set false.
fpemode	ASCII or UTF. (FPE-only) Set fpemode to ASCII or UTF to define which FF3-encoding mechanism to use. ASCII supports only ascii characters and is faster than UTF. Default is ASCII. Set to UTF when using FPE to encrypt Unicode characters. Note: ASCII encryption mode is separate from ASCII character encoding.

The source/destination attributes

For databases

@type	DB2, ORACLE, MYSQL, SQL_SERVER
connectionurl	Database connection url. For example -jdbc: mysql://localhost:3306/world
username	database username
password	database password. use bdt -e option to add encrypted password
driverclass	jdbc connection driver class, e.g. com.mysql.jdbc.Driver

For CSV files

@type	CSV_FILE
filepath	The filepath relative to the inputDir or outputDir path in the config file
delimiter	The character that is used to divide one column from the next in the input file. The supported delimiters are space (), comma (,), pipe (), slash (/), underscore (_), colon (:), semi-colon (;), and tab.
qualifier	(Optional) Character to enclose fields that contain a delimiter character.

columnCount	Number of columns in the input file. This does not necessarily equal the number of columns that have rules defined for them in this bdt.policy file.
hasHeaderRow	True or false. Default false. If true, the utility will treat the first row as header row. Values from this row will be treated as column names. The same column names should be mentioned in the transformation action.
unescapeInput	True or false. Default: false. If true, delimiter and qualifier characters in input preceded by a backslash (\) are considered as normal characters and part of the input data. If you are using the BDT output file as input to another process, set unescapeInput to true.
encoding	(Semi-optional) Used to set character encoding, for example, to enable IBM's EBCDIC. Input file must use same character encoding. Output and failed record files will be created with same character encoding. Sample: for EBCDIC encoding, set encoding: "ibm500" in policy file. Note: to encrypt ASCII files, you must set encoding: ASCII. Supported encodings: https://docs.oracle.com/javase/7/docs/technotes/guides/intl/encoding.doc.html See "(Semi-optional) Set character encoding" on page 32.

For fixed-length files

@type	FIXED_LENGTH_FILE (See “(Optional) Define fixed-length record format” on page 33 for details.)
filepath	The filepath relative to inputDir or outputDir path in config file
columnCount	The number of columns a row has
encoding	(Semi-optional) Used to set character encoding, for example, to enable IBM’s EBCDIC. Input file must use same character encoding. Output and failed record files will be created with same character encoding. Sample: for EBCDIC encoding, set encoding: "ibm500" in policy file. Supported encodings: https://docs.oracle.com/javase/7/docs/technotes/guides/intl/encoding.doc.html See “(Semi-optional) Set character encoding” on page 32.
columnPositionInfo	Column positioning
recordLength	Record length
lineSeparator	True or false. Is record separated with line separator?
hasHeaderRow	True or false. Default false. If true, the utility will treat the first row as header row. Values from this row will be treated as column names. The same column names should be mentioned in the transformation action.

The tables attributes

source			Source table name. For database only.
destination			Destination table name. For database only.
columns			List of columns to be transformed and transformation operation details Policy rules for transforming one or more columns of data in the input file. For each column where transformation is desired, the <code>bdt.policy</code> file specifies the data transformation action to perform and a set of parameters related to that action. Columns are identified by number using the position parameter. NOTE: The first column is number 0.
	name		Column name
	action		Action to be taken. Supported options: ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY
	config		
		@type	Options: AES_CBC_PAD, AES_CTR, FPE, FF1, TOKENIZE, DETOKENIZE See also: “About Format-Preserving Encryption (FPE)” on page 24
		key	Name of the encryption key
		tweak	(FPE required, FF1 optional) There are two ways of defining tweak: * "tweak":<8-byte value> * "tweak": "auto" Either can be used.
		characterSet	Name of the characterSet that was defined under characterSets in the <code>bdt.config</code> file. Defaults include "latin", "digits", "alphabets", and "alphanumeric". Users can also define their own characterSet in the config file. See also: “About characterSets” on page 13.
subset			Table-specific data filter criteria. filter input data based on these criteria. See also: “Transforming Databases” on page 44
	offset		Start record index. Default to 0.
	limit		Maximum number of records/rows to transform, starting from offset.
	recurrency		Select every Nth record. Default is 1 (process every record).
	filters		Subset-specific filters to be used

		selector	Column name
		operator	Options: "=", "<", ">", "<=", ">=", "!=", "like"
		expression	Expression to evaluate filter on selector using specified operator.
	orderBy		Order by column. E.g. column1. Not supported for file transformation.
	order		ASC (ascending) or DESC (descending) record order. Not supported for file transformation.
create DestinationTable			True or false. Default false. Create destination table if none exists. For DB, the destination table will be created with the schema as source table. For file to DB, datatype of columns in the destination table will be varchar(10000)  Caution: Use only for testing. Do not use in a production environment.

About Format-Preserving Encryption (FPE)

To encrypt/decrypt data using either of the NIST-defined FPE formats — FF3 or FF1 — you will specify the ENCRYPT or DECRYPT policy actions with a `type` value. The value for FF1 is `FF1`. The value for FF3 is `FPE`. Keep in mind that the BDT syntax uses `FPE` as a synonym for `FF3`.

Sample policy

```
{
  "id": "5ec94388-ae95-4c98-8803-b004f83efaa", /* transformation policy id
*/
  "name": "FileTransformation", /* policy name */
  "source": {                                /* data source details */
    "@type": "CSV_FILE", /* source type. supports CSV_FILE,
FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2 */
    "filepath": "input.csv",
    "delimiter": ",", /* source type specific details. */
    "qualifier": "\"",
    "unescapeInput": false,
```

```

        "columnCount": "5",
        "hasHeaderRow": false
    },
    "destination": {
        "@type": "CSV_FILE", /* destination type. supports CSV_FILE,
FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2 */
        "filepath": "output.csv" /* destination type specific details. */
    },
    "tables": [ /* table list to transform. */
        {
            "columns": [ /* list of columns that should be transformed */
                {
                    "name": "COLUMN2", /* column name */
                    "action": "ENCRYPT", /* action. supported- ENCRYPT,
DECRYPT, TOKENIZE, DETOKENIZE, REKEY*/
                    "config": [
                        {
                            "@type": "FPE", /* supported type - AES_CBC_PAD,
AES_CTR, FPE, FF1, TOKENIZE, DETOKENIZE */
                            "key": "KEY-NEW",
                            "tweak": "010ACD5B99F34CF8", /* FPE tweak */
                            "characterSet": "digits" /* charset name */
                        }
                    ]
                }
            ],
            {
                "name": "COLUMN3",
                "action": "ENCRYPT",
                "config": [
                    {
                        "@type": "FPE",
                        "key": "KEY-NEW",
                        "tweak": "010ACD5B99F34CF8",
                        "characterSet": "digits"
                    }
                ]
            }
        ]
    }

```

```
    }  
  ],  
  "subset" : {                                /* table specific data filter  
criteria. filter input data based on this criteria */  
    "limit": 1000,                            /* max number of rows to be  
transformed */  
    "recurrency": 2,                          /* select every nth row for transformation */  
    "filters": [{  
      "selector": "COLUMN1", /* column name */  
      "operator": "!=", /* operator */  
      "expression": "CA" /* expression to evaluate with selector  
column value and operator */  
    }]  
  }  
}  
],  
  "createBadRecordFile": true /* set true to create failed file, else false */  
}
```

Policy actions

For each column of input data, the bdt.policy file can specify one of the following actions:

- ENCRYPT
- DECRYPT
- TOKENIZE
- DETOKENIZE
- REKEY

If you do not specify any of these actions for a column, the contents of the column are copied to the output file without any transformation.

ENCRYPT policy action

The ENCRYPT action requires the following parameters:

type	Encryption mode: AES_CBC_PAD, AES_CTR, FF1, or FPE.
key	Name of the encryption key.
iv	(Required for AES_CTR and AES_CBC_PAD) Initialization vector. Must be 16 bytes.

characterSet	(FPE and FF1 modes only) Name of the characterSet that was defined under characterSets in the bdt.config file. Defaults include "latin", "digits", "alphabets", and "alphanumeric". Users can define their own characterSet in the config file as well. See also: "Edit the bdt.config File" on page 11.
tweak	(FPE required, FF1 optional) Tweak. The size of the tweak must be 8 bytes.



NOTE: Output and input are base-64 encoded for AES_CBC_PAD mode in ENCRYPT, DECRYPT, and REKEY actions.

The following example shows how to define encryption actions for two columns using AES_CBC_PAD and FPE encryption.

```
{
  "name" : "column2",
  "action" : "ENCRYPT",
  "config" : [ {
    "@type" : "AES_CBC_PAD",
    "key" : "c2KeyName",
    "iv": "000102030405060708090A0B0C0D0E0F"
  } ]
}, {
  "name" : "column3",
  "action" : "ENCRYPT",
  "config" : [ {
    "@type" : "FPE",
    "key" : "c3KeyName",
    "characterSet": "digits",
    "tweak": "0102030405060708"
  } ]
}
```

The following example shows how to define encryption actions for 1 column using FF1 encryption.

```
{
  "id": "transformation-id",
  "name": "transformation-name",
  "createBadRecordFile": true,
```



```
"source":{
  "@type":"CSV_FILE",
  "filepath":"input.csv",
  "delimiter":",",
  "columnCount":"12",
  "hasHeaderRow":true
},
"destination":{
  "@type":"CSV_FILE",
  "filepath":"output.csv"
},
"tables":[
  {
    "columns":[
      {
        "name":"latitude",
        "action":"ENCRYPT",
        "config":[
          {
            "@type":"FF1",
            "key":"KEYNAME",
            "tweak":"auto",
            "characterSet":"digits"
          }
        ]
      }
    ]
  }
]
```

DECRYPT policy action

The DECRYPT action requires the same parameters as the ENCRYPT action.

The following example shows how to define decryption actions for two columns using AES_CBC_PAD and FPE decryption.

```
{
  "name" : "column2",
  "action" : "DECRYPT",
  "config" : [ {
    "@type" : "AES_CBC_PAD",
    "key" : "c2KeyName",
    "iv": "000102030405060708090A0B0C0D0E0F"
  } ]
}, {
  "name" : "column3",
  "action" : "DECRYPT",
  "config" : [ {
    "@type" : "FPE",
    "key" : "c3KeyName",
    "characterSet": "digits",
    "tweak": "0102030405060708"
  } ]
}
```

TOKENIZE policy action

The TOKENIZE action requires the following parameters:

type	Encryption mode: Set to "TOKENIZE".
tokenGroup	Name of the token group as defined in VTS.
tokenTemplate	Name of the token template as defined in VTS.

The following sample shows the configuration of a column using tokenization.

```
{
  "name" : "column4",
  "action" : "TOKENIZE",
  "config" : [ {
    "@type" : "TOKENIZE",
    "tokenGroup" : "tokenGroup1",
    "tokenTemplate" : "tokenTemplate1"
  } ]
}
```

DETOKENIZE policy action

The DETOKENIZE action requires the same parameters as in TOKENIZE action. The following sample shows the configuration of a column using detokenization.

```
{
  "name" : "column4",
  "action" : "DETOKENIZE",
  "config" : [ {
    "@type" : "TOKENIZE",
    "tokenGroup" : "tokenGroup1",
    "tokenTemplate" : "tokenTemplate1"
  } ]
}
```

REKEY policy action

BDT can change the encryption key and re-encrypt the data using the new key. This can be done using VTS to tokenize the data, or using VAE to encrypt the data. The same policy can perform both types of rekey.

In a REKEY policy consists of two parts. In fact, REKEY is really just a container for two other actions. First, the data is detokenized or decrypted using the existing key. Then, the data is tokenized or encrypted using the new key.

The following example shows a sample configuration for a column rekey through VTS:

```
{
  "name" : "column6",
  "action" : "REKEY",
  "config" : [ {
    "@type" : "TOKENIZE",
    "tokenGroup" : "group1",
    "tokenTemplate" : "abcdef9876543210",
    "action" : "DETOKENIZE"
  }, {
    "@type" : "TOKENIZE",
    "tokenGroup" : "group2",
    "tokenTemplate" : "abcdef9876543210",
    "action" : "TOKENIZE"
  } ]
}
```

The following example shows a sample configuration for a column rekey through VAE:

```
{
  "name" : "column6",
  "action" : "REKEY",
  "config" : [ {
    "@type" : "FPE",
    "key" : "rekey1",
    "characterSet": "digits",
    "tweak": "0102030405060708",
    "action" : "DECRYPT"
  }, {
    "@type" : "FPE",
    "key" : "rekey2",
    "characterSet": "digits",
    "tweak": "0102030405060708",
    "action" : "ENCRYPT"
  } ]
}
```

As you can see, the two actions within each REKEY action are defined using DETOKENIZE, DECRYPT, TOKENIZE, and ENCRYPT with the same parameters as you would use with each of these actions alone.

(Semi-optional) Set character encoding

Supported encodings are listed in the following table. Note that naming from either column can be used.

<https://docs.oracle.com/javase/7/docs/technotes/guides/intl/encoding.doc.html>

The input file must use same character encoding. Failed record files will be created with the same character encoding. Output file encoding can vary, depending on configurations in the policy file.



NOTE: Encoding is mandatory only for EBCDIC-encoded files.

The following example shows how to set EBCDIC character encoding (Extended Binary Coded Decimal Interchange Code) in the policy file.

```
{
  "id": "transformation-id",
  "name": "transformation-name",
  "createBadRecordFile": true,
  "source": {
    "@type": "CSV_FILE",
    "filepath": "input.csv",
    "delimiter": ",",
    "columnCount": "12",
    "hasHeaderRow": true,
    "encoding": "ibm500"
  },
  "destination": {
    "@type": "CSV_FILE",
    "filepath": "output.csv"
  },
  "tables": [
    {
      "columns": [
```

```
{
  "name": "latitude",
  "action": "ENCRYPT",
  "config": [
    {
      "@type": "FF1",
      "key": "KEYNAME",
      "tweak": "auto",
      "characterSet": "digits"
    }
  ]
}
```

(Optional) Define fixed-length record format

Some systems may require fixed-length record formats. As described by IBM,

“In fixed-length or fixed-format records, each field starts and ends at the same place in every record. A data file that contains data records of equal and constant length might be organized as follows.

Sample file with fixed-length records: aaabbbbccccdddggghhhh

The data file illustrated previously has three records. Each record has a field of three characters followed by a field of four characters, so the total record length is seven characters. The file does not contain any separation between records; delimiters are unnecessary because all fields have the same length. The VARCHAR data types are therefore always the fixed maximum size of the field.”¹

This option is valid for FPE and FF1 (ENCRYPT and DECRYPT), and TOKENIZE actions only. Use the sample policy file `FixedLengthFileTransformation.policy` and the attributes described under [“For fixed-length files” on page 22](#) to define this feature.

1. https://www.ibm.com/support/knowledgecenter/en/SSGU8G_12.1.0/com.ibm.hpl.doc/ids_hpl_132.htm



NOTE: If applying tokenization on fixed-length format records, be sure not to add any prefix or suffix to the tokenized output. Adding such a string will result in failure of detokenization.

The following example defines a fixed-length record format, along with EBCDIC character encoding.

```
{
  "id": "FixedLengthFileSample-5ec94388",
  "name": "FixedLengthFileSample",
  "createBadRecordFile": true,
  "source": {
    "@type": "FIXED_LENGTH_FILE",
    "filepath": "fixed_length.txt",
    "lineSeparator": true,
    "hasHeaderRow": true,
    "columnCount": 7,
    "encoding": "ibm500",
    "recordLength": 59,
    "columnPositions": [
      {
        "column": 0,
        "startIndex": 0,
        "endIndex": 10
      },
      {
        "column": 1,
        "startIndex": 10,
        "endIndex": 20
      },
      {
        "column": 2,
        "startIndex": 20,
        "endIndex": 26
      },
      {
```

```

        "column":3,
        "startIndex":26,
        "endIndex":32
    },
    {
        "column":4,
        "startIndex":32,
        "endIndex":39
    },
    {
        "column":5,
        "startIndex":39,
        "endIndex":48
    },
    {
        "column":6,
        "startIndex":48,
        "endIndex":59
    }
]
},
"destination":{
    "@type":"FIXED_LENGTH_FILE",
    "filepath":"output.txt"
},
"tables":[
    {
        "columns":[
            {
                "name":"latitude",
                "action":"ENCRYPT",
                "config":[
                    {
                        "@type":"FPE",
                        "key":"KEY1",

```



```
        "tweak": "auto",
        "characterSet": "digits"
    }
]
},
{
    "name": "longitude",
    "action": "ENCRYPT",
    "config": [
        {
            "@type": "FPE",
            "key": "KEY1",
            "tweak": "auto",
            "characterSet": "digits"
        }
    ]
}
]
}
```

Example policy

```
{
  "id": "policyId",
  "name": "policyName",
  "source": {
    "@type": "CSV_FILE",
    "filepath": "inputFile",
    "delimiter": ",",
    "qualifier": "",
    "unescapeInput": false,
    "columnCount": 20,
    "hasHeaderRow": false
  },
  "destination": {
    "@type": "CSV_FILE",
    "filepath": "outputFile"
  },
  "fpemode": "ASCII",
  "createBadRecordFile": true,
  "tables": [
    {
      "columns": [
        {
          "name": "Column1",
          "action": "TOKENIZE",
          "config": [
            {
              "@type": "TOKENIZE",
              "tokenTemplate": "demoTemplate",
              "tokenGroup": "tg1"
            }
          ]
        }
      ]
    }
  ],
  {
```

```

        "name": "Column3",
        "action": "DETOKENIZE",
        "config": [
            {
                "@type": "TOKENIZE",
                "tokenTemplate": "demoTemplate",
                "tokenGroup": "tg1"
            }
        ]
    },
    {
        "name": "Column4",
        "action": "ENCRYPT",
        "config": [
            {
                "@type": "FPE",
                "key": "key1",
                "characterSet": "digits",
                "tweak": "AUTO"
            }
        ]
    },
    {
        "name": "Column5",
        "action": "DECRYPT",
        "config": [
            {
                "@type": "FPE",
                "key": "key1",
                "characterSet": "digits",
                "tweak": "AUTO"
            }
        ]
    },
    {

```

```
"name": "Column6",
"action": "ENCRYPT",
"config": [
  {
    "@type": "FF1",
    "key": "key1",
    "characterSet": "digits"
  }
],
{
  "name": "Column7",
  "action": "DECRYPT",
  "config": [
    {
      "@type": "FF1",
      "key": "key1",
      "characterSet": "digits",
      "tweak": "AUTO"
    }
  ]
},
{
  "name": "Column8",
  "action": "REKEY",
  "config": [
    {
      "@type": "FPE",
      "key": "key1",
      "characterSet": "digits",
      "tweak": "1ABD0EAB12F34560",
      "action": "DECRYPT"
    }
  ],
  {
    "@type": "FPE",
```

```
        "key": "key2",
        "characterSet": "digits",
        "tweak": "1ABD0EAB12F34560",
        "action": "ENCRYPT"
    }
]
},
{
    "name": "Column9",
    "action": "REKEY",
    "config": [
        {
            "@type": "AES_CBC_PAD",
            "key": "key1",
            "iv": "1ABD0EAB12F345601ABD0EAB12F34560",
            "action": "DECRYPT"
        },
        {
            "@type": "AES_CBC_PAD",
            "key": "key2",
            "iv": "1ABD0EAB12F345601ABD0EAB12F34560",
            "action": "ENCRYPT"
        }
    ]
},
{
    "name": "Column12",
    "action": "DECRYPT",
    "config": [
        {
            "@type": "AES_CTR",
            "key": "key1",
            "iv": "1ABD0EAB12F345601ABD0EAB12F34560"
        }
    ]
}
```

```

    },
    {
      "name": "Column13",
      "action": "ENCRYPT",
      "config": [
        {
          "@type": "AES_CTR",
          "key": "key1",
          "iv": "1ABD0EAB12F345601ABD0EAB12F34560"
        }
      ]
    },
    {
      "name": "Column14",
      "action": "DECRYPT",
      "config": [
        {
          "@type": "AES_CBC_PAD",
          "key": "key1",
          "iv": "1ABD0EAB12F345601ABD0EAB12F34560"
        }
      ]
    },
    {
      "name": "Column15",
      "action": "ENCRYPT",
      "config": [
        {
          "@type": "AES_CBC_PAD",
          "key": "key1",
          "iv": "1ABD0EAB12F345601ABD0EAB12F34560"
        }
      ]
    }
  ]
}

```



```
}  
]  
}
```

Using Text Qualifier Characters in Input Files

A text qualifier character can be used to mark the start and end of a column field in a file that is input to the BDT utility. This is useful when the field value itself contains a character that would normally act as a field delimiter. Use the qualifier to indicate to BDT that the data following the delimiter is part of the same field, and not the beginning of the next field.

The supported text qualifier characters are double quote ("), single quote('), pipe (|), slash (/), at (@), hash (#), percentage (%), and ampersand (&).

For example, in the following input file, the comma is the delimiter character, but it is also part of the address field. To let BDT know that the text after the comma is also part of the same field, the value must be enclosed with a text qualifier.

Example of data before adding the text qualifier:

```
Firstname, Lastname, Address
James,Brown,1745 E. New St., Apt. 22,Chicago
Scott,Smith,400 South Warren Street,Trenton
```

After adding the text qualifier:

```
James,Brown,"1745 E. New St., Apt. 22,Chicago"
Scott,Smith,"400 South Warren Street,Trenton"
```

In most cases, the input file for BDT is created by exporting data from a database. Databases provide the option to specify a character to be used as a qualifier in exported data.

To add text qualifier characters:

1. When exporting data from the database, specify the qualifier using the technique that is supported by the database.
2. In the policy file, add the qualifier parameter to the top of the file, before the column specifications begin. If the qualifier is a double quote character, escape it in the policy file with a backslash.

Example configuration in policy file, including the double quote character (") as a qualifier:

```
"source":{
  "@type":"CSV_FILE",
  "filepath":"input.csv",
  "delimiter":",",
  "qualifier":"\"",
  "unescapeInput":true,
  "columnCount":"12",
  "hasHeaderRow":true
}
```


Transforming Databases

Overview

BDT can be used to encrypt, decrypt or rekey database table data and move it to another database. Multiple tables can be transformed in single execution of the utility. You can choose table columns and specify what action to be performed on particular column.

Terminology

- **source database:** database where tables need to be transformed
- **destination database:** database where transformed data will be moved
- **source table:** table in source db which needs to be transformed
- **destination table:** table of destination database where transformed data will be moved

Supported databases

(See also the *Vormetric Batch Data Transformation 2.0 Release Notes*.)

- MySQL 5.7.20
- Oracle 11g
- Microsoft SQL Server 2017
- IBM DB2 10.5



NOTE: Download the JDBC connector .jar for the required version of database you are using, and place the .jar files under the bdt/lib directory.

Example 1: Transforming database table columns

To transform database table columns, create a bdt.policy file and add source database connection properties to the policy source attribute. Do the same for destination database. In the tables section of the policy, add an entry for table to transform, specify source and destination table, and the columns to transform. Ensure the destination table has the exact same schema as the source table.

DbToDbTransformation.policy sample

```
{  
  "id": "OracleToSqlServerSample-90643295a90sdf5",
```

```

"name":"OracleToSqlServerSample",
"source":{
  "@type":"ORACLE",
  "connectionurl":"jdbc:oracle:thin:@//localhost:1521/XE",
  "username":"admin",
  "password":"",
  "driverclass":"oracle.jdbc.driver.OracleDriver"
},
"destination":{
  "@type":"SQL_SERVER",
  "connectionurl":"jdbc:sqlserver://localhost;databaseName=db",
  "username":"admin",
  "password":"",
  "driverclass":"com.microsoft.sqlserver.jdbc.SQLServerDriver"
},
"tables":[
  {
    "columns":[
      {
        "name":"ADDRESS",
        "action":"ENCRYPT",
        "config":[
          {
            "@type":"AES_CBC_PAD",
            "key":"KEY-NEW",
            "iv":"1ABD0EAB12F345601ABD0EAB12F34560"
          }
        ]
      }
    ]
  },
  "createDestinationTable":true,
  "sourceTable":"employee",
  "destinationTable":"employee"
}
],

```

```
"createBadRecordFile":true
}
```

Example 2: Transforming database tables to files

BDT supports transforming a database table and copying the data to an output file.

Specify the destination type as CSV_FILE or FIXED_LENGTH_FILE in the policy file.

Specify needed attributes of the input file, such as delimiter, encoding etc.

If more than one table is transformed in single execution, BDT creates a separate output file for each table. The source table name is suffixed in output file.

DBToFileTransformation.policy sample

```
{
  "id": "Db2ToFileSample-90643295a90sdf5",
  "name": "Db2ToFileSample",
  "createBadRecordFile": true,
  "source": {
    "@type": "DB2",
    "connectionurl": "jdbc:db2://localhost:50000/SAMPLE",
    "username": "db2admin",
    "password": "",
    "driverclass": "com.ibm.db2.jcc.DB2Driver"
  },
  "destination": {
    "@type": "CSV_FILE",
    "filepath": "output.csv",
    "delimiter": ",",
  },
  "tables": [
    {
      "columns": [
        {
          "name": "POPULATION",
          "action": "ENCRYPT",
          "config": [
```

```

        {
            "@type": "FPE",
            "key": "KEY-NEW",
            "characterSet": "digits",
            "tweak": "auto"
        }
    ]
}
],
"source": "country"
}
]
}

```

Example 3: Transforming input file to database table

To transform an input file and copy data to a database table, in policy file specify the source type as `@CSV_FILE` or `@FIXED_LENGTH_FILE` and set the destination db connection properties in the policy destination attribute. The destination table schema should have all columns specified by the input file header row. If a header row is not present in the input file, columns are named as `COLUMN0`, `COLUMN1`.. `COLUMNn`.

FileToDBTransformation.policy sample

```

{
  "id": "FileToDBSample-b004f83efaa",
  "name": "FileToDBSample",
  "source": {
    "@type": "CSV_FILE",
    "filepath": "input.csv",
    "delimiter": ",",
    "qualifier": "\"\"",
    "columnCount": 12,
    "hasHeaderRow": true,
    "unescapeInput": true,
    "encoding": "UTF-8"
  },

```

```
"destination":{
  "@type":"MYSQL",
  "connectionurl":"jdbc:mysql://localhost:3306/world",
  "username":"username",
  "password":"",
  "driverclass":"com.mysql.jdbc.Driver"
},
"createBadRecordFile":true,
"tables":[
  {
    "columns":[
      {
        "name":"LATITUDE",
        "action":"ENCRYPT",
        "config":[
          {
            "@type":"FPE",
            "key":"KEY-NEW",
            "characterSet":"digits",
            "tweak":"auto"
          }
        ]
      }
    ]
  },
  "createDestinationTable":true,
  "destinationTable":"REALESTATE"
}
]
```

Filtering Input Data

BDT supports filtering of input data. For example, in a case with one million input rows, you can designate a subset for transformation. To do so, specify subset criteria in a policy file to filter the input records.

`subset` is a table-level element, and is applicable only to that table.

See also: [“The tables attributes” on page 23](#).

Example: Filter input rows from a source file

```
"subset":{
  "offset":"10",
  "limit":1000,
  "recurrency": 2,
  "filters":[
    {
      "selector":"name",
      "operator":"like",
      "expression":"'p.*'"
    }
  ]
}
```

Specify the starting `offset` and the `limit`, which define the number of rows to transform.

The `recurrency` attribute specifies whether to transform rows in a sequence or skip rows. If `recurrency` is set to 2, then every second row in the sequence is transformed and the row in between is skipped.

`filters` specifies the list of conditions to match. The row should satisfy all conditions specified in the list.

- `selector` is the name of the column that the filter should evaluate
- `operators` Options: "=", "<", ">", "<=", ">=", "!=", "like".
- `expression` Used to evaluate the filter on the selector using specified operator. For file transformation if operator is specified as `like`, then specify `regex` expression to match in the column value.

To create a regex expression see:

<https://docs.oracle.com/javase/tutorial/essential/regex/index.html>

Example: Filter database table rows

```
"subset":{
  "offset":"10",
  "limit":1000,
  "recurrency": 1,
  "orderBy":"ID",
  "order":"DESC",
  "filters":[
    {
      "selector":"name",
      "operator":"like",
      "expression":"'p.*'"
    },
    {
      "selector":"salary",
      "operator":"<",
      "expression":"100000"
    }
  ]
}
```

Compared with file transformations, the database transformation `subset` can include two additional attributes:

- `orderBy` Use the name of column which should be used to order records. Records are ordered first, then offset and limit attributes are applied.
- `order` Define ascending (ASC) or descending (DESC) order.

For the `like` operator, use database-specific syntax for the expression to evaluate.

Monitoring and Troubleshooting

Log files

BDT stores its log file in the file `BDT_HOME/log/bdt.log`.

The default log level is `DEBUG` for the log file and `INFO` for the console. These log properties can be changed in the `BDT_HOME/conf/log4j.properties` file.

Thread count and batch size best practices

To best configure thread count and batch size, follow the principles below.

1. Identify the ideal thread count for your environment, depending on your system configuration.
BDT gives optimal performance with 16 threads on four core machines.
Setting thread count too low or too high will slow down the application.
2. Decide on batch size, configured based on available memory, size of individual record, and configured thread count. Setting batch size too high may result in an out-of-memory error.

Use the following calculation to calculate the approximate maximum memory utilization by BDT:

$\text{thread count} * \text{batch size} * \text{record size} = \text{memory utilization}$

Therefore, thread count and batch size will be $\leq$ about 60% of available memory.

Remaining memory is required to run the utility and to maintain transformed batches in the write queue.

For example: If you have 4GB available memory, and individual record size of approximately 50MB, you can set:

Batch size to 50 and thread count 1, utilizing approximately 60% of memory:

$50 * 1 * 50\text{MB} = 2500\text{MB}$

Or

Batch size to 10 and thread count to 3, utilizing $10 * 3 * 100\text{MB} = 3000\text{MB}$.





CipherTrust Batch Data Transformation (BDT)

Version: v2.6.0

30 January 2026

Contents

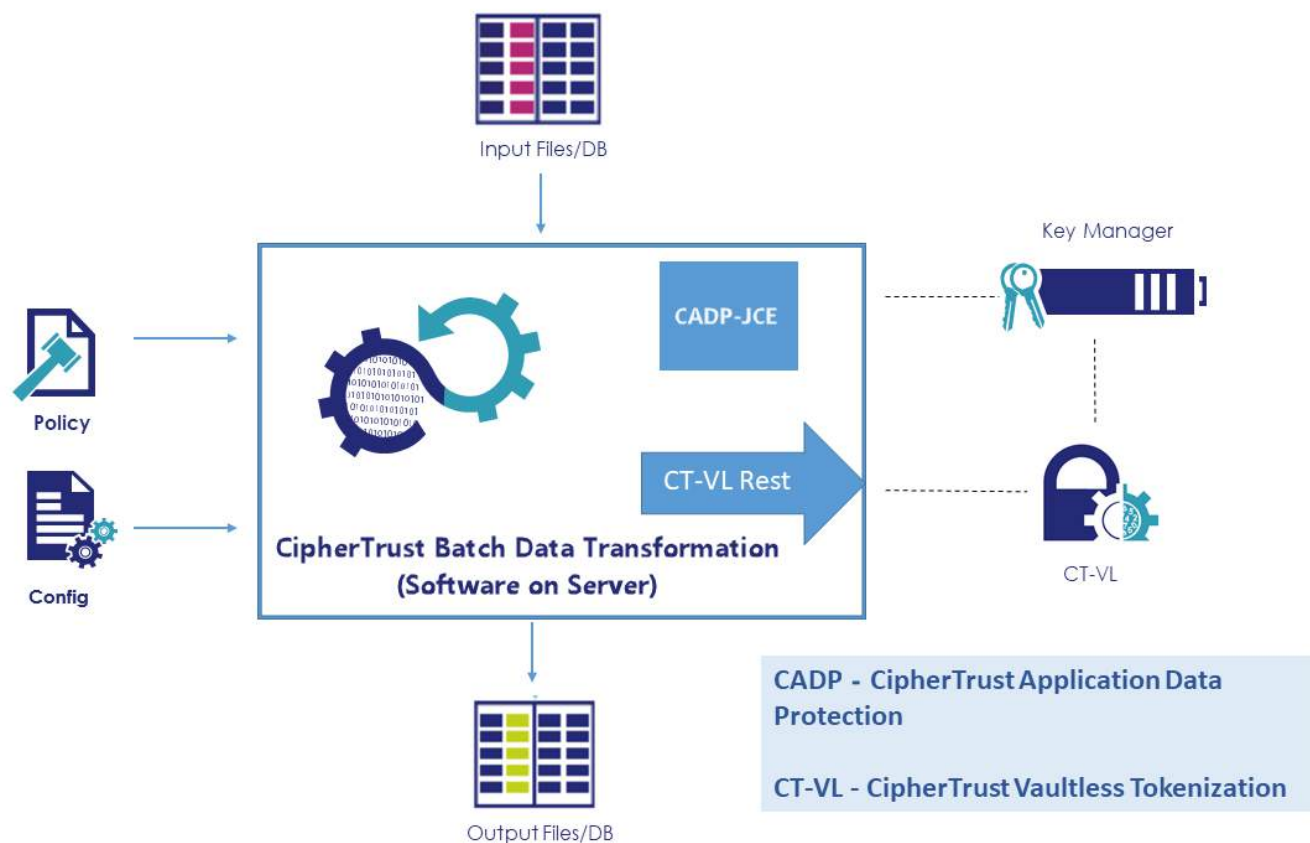
Administration	3
Quick Start	8
BDT Transformation Process	14
Tasks	22
Setting up BDT Policy	23
Setting up BDT Policy Using Local File	24
Setting up Access Credentials (for CM and Database)	24
Performing Encryption Through VAE	25
Restarting Transformation	25
Configure Logging	26
Configuring TLS for use with CipherTrust Vaultless Tokenization (CT-VL)	27
Filtering Input Data	30
Setting up Character Encoding in the Policy	31
Setting up Input Files with Fixed-Length Record Format	32
Using Text Qualifier Characters in Input Files	32
Validating Configuration and Policy Files	33
Performing Initial Data Transformation for DPG Compatibility	34
Storing Output of Crypto Operations in a New Column	36
Using TU Features in BDT	37
Operations	40
Encryption Examples	40
Decryption Example	41
Tokenize Example	42
Detokenize Example	42
Rekey Examples	42
Advanced Topics	43
BDT Command Syntax	44
BDT Config File	45
BDT Properties File	52
BDT Policy File	61
Encryption Key Versioning	78
Configure TLS for use with CipherTrust Vaultless Tokenization (CT-VL)	79
Configure SSL on CipherTrust Manager for NAE Interface	82
FPE/AES/Unicode Cardinality Block-Size Table	87
Samples	95
Sample BDT Policy File	95
Sample BDT Config File	115
Best Practices	120
Thread Count and Batch Sizes	120
Troubleshooting	120
FAQs	123

Administration

CipherTrust Batch Data Transformation (BDT) is a command line utility that is used to transform (encrypt/tokenize) data in files and databases. It is a policy-based tool and can efficiently transform bulk data. It can also be used for rekey operations.

BDT Architecture

The BDT utility works with [CipherTrust Manager \(CM\)](#) for key management, and [CipherTrust Vaultless Tokenization \(CT-VL\)](#) for tokenization.



BDT Policy

The BDT utility's actions are based on a policy. For each action or group of actions that you want to perform with the utility, you need to define a policy.

The BDT policy defines the rules on how to perform a transformation of the data provided by the input files or databases. The policy can be configured in a file locally or on a CipherTrust Manager (CM) instance that is serving as a centralized manager for configuration, allowing for easier reuse and maintenance. Refer to [Setting up BDT Policy](#) for details.

Supported File Formats and Databases

BDT supports the following file formats:

- CSV File
- Fixed Length File

BDT is supported with the following databases. The table below lists the versions tested with.

Database	Tested Version
MySQL	8.0, 8.0.27
Oracle	12c, 19c
IBM DB2	10.5, 11.5.7
SAP HANA	2.0
Microsoft SQL Server	2017, 2019

Supported Transformations

- **Database to database** (DB-to-DB): Encrypt, decrypt, tokenize, detokenize, or rekey the data of a database table and move it to another database. Multiple tables can be transformed in a single execution of the utility. You can choose table columns and specify what action needs to be performed on a particular column.
- **Database to file** (DB-to-File): Encrypt, decrypt, tokenize, detokenize, or rekey the data of a database table and move it to another file. You can choose table columns and specify what action needs to be performed on a particular column.
- **File to database** (File-to-DB): Encrypt, decrypt, tokenize, detokenize, or rekey the data of a file and move it to another database. You can choose file columns and specify what action needs to be performed on a particular column.
- **File to file** (File-to-File): Encrypt, decrypt, tokenize, detokenize, or rekey the data of a file and move it to another file. You can choose file columns and specify what action needs to be performed on a particular column.

Refer to [BDT Transformation Process](#) for details.

Supported Encryption Algorithms

Expand (click **+**) to view details.

FF1

Key Size (in bits)	128 (default) 192

	256
Tweak Data	Tweak data is mandatory. The value must be 16 characters HEX encoded string.
Additional Notes	• FF1 supports only non-versioned AES Keys. • FF1 is supported when symmetric key cache is enabled. • FF1 requires minimum two characters to perform encryption. The maximum data length can be 128000 characters. • While performing crypto operations, the characters in the input data other than those specified in the character set range, are preserved and do not get encrypted. • While performing transformation, the character set range cannot be updated. • While performing decryption, do not modify the character set range, it must be same as encrypt.

FF3

Key Size (in bits)	128 (default) 192 256
Tweak Data	Tweak data is mandatory. The value must be 16 characters HEX encoded string.
Additional Notes	• FF3 supports only non-versioned AES Keys. • FF3 is supported when symmetric key cache is enabled. • FF3 requires minimum two characters to perform encryption. The maximum data length can be 128000 characters. • While performing crypto operations, the characters in the input data other than those specified in the character set range, are preserved and do not get encrypted. • While performing transformation, the character set range cannot be updated. • While performing decryption, do not modify the character set range, it must be same as encrypt.

FPE_AES

Note

The number of characters in the character set range are treated as cardinality for the input data.

IV	When cardinality is y, a x characters IV is used when data size is > x characters. Corresponding value of x is derived using the following formula: <pre>double lg = Math.log10(Math.pow((double)2, (double)</pre> The table with cardinality and corresponding IV value based on the above formula is provided here. The value of each HEX encoded byte in the IV value will be in the range 00 to cardinality-1. For example, when CARD62 is used, the maximum value will be 3D (hex encode of 62-1=61). In the following IV for CARD62, the hex 0A lies in the range 00 to cardinality-1, that is, 00 to 3D: <pre>0102030405060708090A0B0C0D0E0F1000303132333435363</pre>
Key Size (in bits)	128 (default) 192 256
Tweak Algorithm	Specify a hashing algorithm to be applied to specified tweak data. Following are the valid values: • None • SHA1 • SHA256
Tweak Data	FPE_AES uses the tweakable cipher concept to protect against statistical attacks due to potentially small input/output space. If tweak data algorithm is None or absent, the value must be HEX encoded string representing 64-bit long (hence, HEX encoding will consume 16 characters).
Additional Notes	• Default tweak algorithm will be None, if invalid or Null value is provided.

	• FPE_AES supports only non-versioned AES Keys. • FPE_AES is supported when symmetric key cache is enabled. • While performing crypto operations, the characters in the input data, other than those specified in the character set range, are preserved and do not get encrypted. • If any character other than those specified in the character set range, are present in the input data, you must calculate the effective input data length and provide IV accordingly. • FPE_AES requires minimum four characters to perform encryption. • While performing transformation, the character set range cannot be updated. • While performing decryption, do not modify the character set range, it must be same as encrypt.

DESede

Block Size	8 bytes
Supported Modes	ECB CBC
Padding Schemes	PKCS5Padding NoPadding
IV	CBC mode requires 8 characters or 8 HEX encoded characters IV.
Key Size	Supported key sizes are 168 (default) and 112 bits. Each key contains an extra 8 bits of parity. Thus, when you create a key of 112 bits, the actual key size is 128 bits; when you create a key of 168 bits, the actual key size is 192 bits.
Additional Notes	• When using DESede with NoPadding, then data for encryption must be in multiples of 8 bytes. • DESede is supported when symmetric key cache is either enabled or disabled.

AES_CTR

Block Size	16 bytes

Padding Schemes	PKCS5Padding NoPadding
IV	CTR mode requires 16 characters or 16 HEX encoded characters IV.
Key Size (in bits)	128 (default) 192 256
Additional Notes	• AES_CTR is supported when symmetric key cache is enabled. • By default, AES_CTR is with NoPadding.

AES_CBC_PAD

Block Size	16 bytes
Padding Schemes	PKCS5Padding NoPadding
IV	CBC mode requires 16 characters or 16 HEX encoded characters IV.
Key Size (in bits)	128 (default) 192 256
Additional Notes	• AES_CBC_PAD is supported when symmetric key cache is either enabled or disabled. • By default, AES_CBC_PAD is with PKCS5Padding.

Supported Tokenization Algorithms

BDT supports the following tokenization algorithms (supported by CT-VL):

- FF1, FF1-luhn
- FF3, FPE-luhn
- Dates, Random, Random-luhn

Refer to [CipherTrust Vaultless Tokenization \(CT-VL\)](#) for details.

Quick Start

Use CipherTrust Batch Data Transformation (BDT) to transform your data through **encryption** and **tokenization**. This section describes how to run BDT in its simplest form, that is, performing a file-to-file transformation through *encryption*.

BDT supports various [other transformations](#), but the scope of this section is limited to [file encryption](#) (file-to-file

transformation) only.

Prerequisites

- To perform **tokenization**, a compatible version (2.2 or higher) of Vormetric Tokenization Server (now renamed as CipherTrust Vaultless Tokenization (CT-VL)) is up and running. Refer to the CT-VL [Quick Start](#) document for details.
- A CipherTrust Manager version compatible with the installed CT-VL/CADP for Java version is up and running. Refer to the CipherTrust Manager [Getting Started](#) document for details.
- Java 17 must be installed.

Encrypting Files

Commands to encrypt files on Linux and Windows are detailed below. Click the desired tab for details.

Installation

Linux

1. Download the BDT distribution file. You can use `wget` at a terminal prompt.

```
wget https://<path to download site>/bdt-x.x.x.tar.gz
```

2. Create a BDT home directory at a convenient location. `sudo` may be required.

```
cd /usr/local/bin  
sudo mkdir bdt
```

3. Extract the distribution to the BDT home directory.

```
sudo tar -xzvf <filename.tgz> -C /usr/local/bin/bdt
```

4. Add the Java bin directory path to the PATH environment variable. Edit the `.bashrc` file (or equivalent for other shells) for the admin user and add the following lines:

```
export JAVA_HOME=/usr/lib/java/jre  
export PATH=$JAVA_HOME/bin:$PATH
```

5. Verify the installation by ensuring the following directory structure is created in the installation directory.

Directory	Description
bin	Contains executable scripts for validating configuration, testing, and execution.
conf	Contains configuration files such as <code>bdt.config</code>, <code>logging.properties</code>, <code>bdt.properties</code>, and <code>bdt.mv.db</code> (H2 database file). Note: H2 database is upgraded from 1.4.199 to 2.1.212 for the backup of old version file. Refer to Backup using the Script Tool and Restore from a Script for details.
lib	Contains required JAVA library dependencies.
log	Contains log file directory.
samples	Contains sample policy and configuration files.

6. Configure at least the following properties in the BDT properties file:

- `NAE_IP.1= CM_IP`
- `NAE_Port= TCP_PORT`
- `Protocol= tcp`

Windows

1. Download the BDT distribution file.
2. Create a BDT home directory at a convenient location. You can use the File Explorer's **New Folder** option to create a new folder named BDT under the folder C:\Program Files, for example.
3. Extract the distribution to the BDT home directory. Use your favorite file compression/extraction utility (winzip, pkzip, or 7zip etc).
4. Add the Java bin directory path to the PATH environment variable:
 - a. Open the Control Panel.
 - b. Click **System**.
 - c. Click **Advanced System Settings**.
 - d. Click the **Environment Variables** button.
 - e. Under System Variables, select **Path** and then click **Edit**.

Note

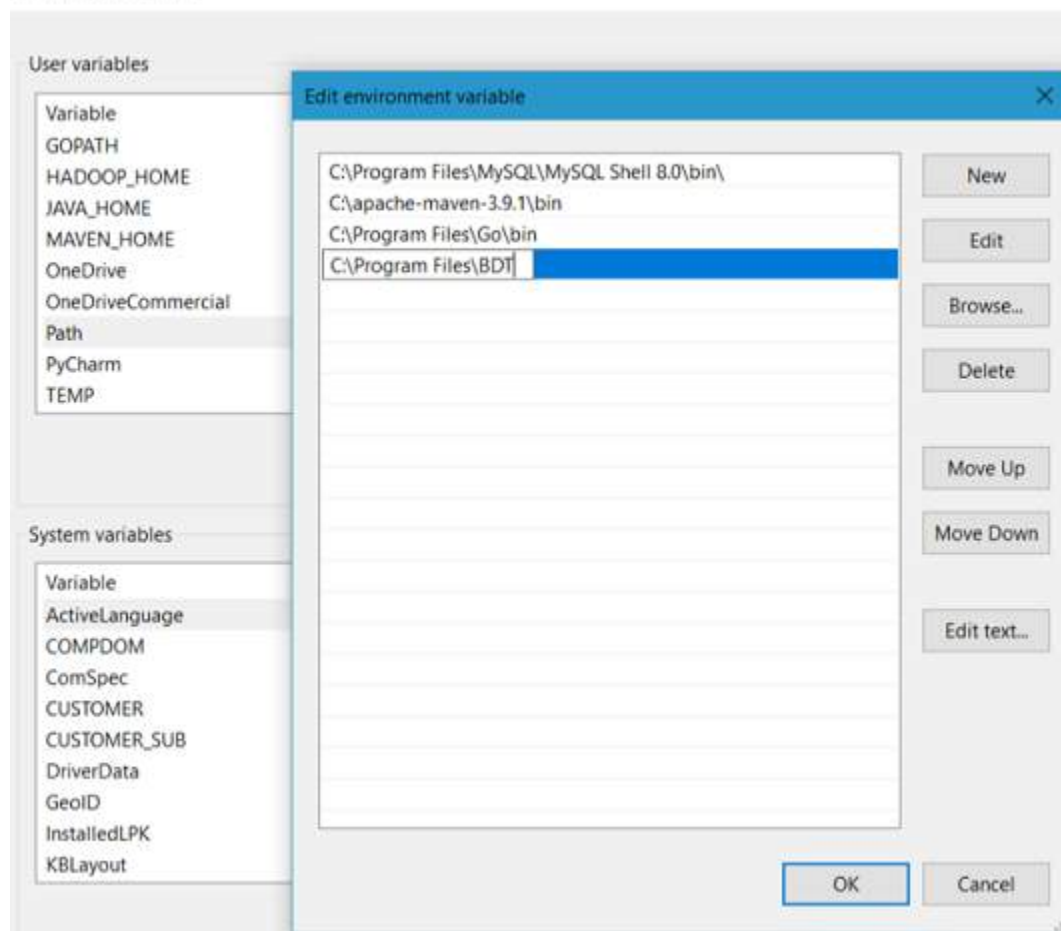
Do not delete any of the existing text here.

- f. Append the following to whatever you already have:

```
;C:\Program Files\BDT
```

- g. Click **OK**.

Environment Variables



5. Verify the installation by ensuring the following directory structure is created in the installation directory.

Directory	Description
bin	Contains executable scripts for validating configuration, testing, and execution.
conf	Contains configuration files such as <code>bdt.config</code> ,

Directory	Description
	logging properties, <code>bdt.properties</code> , and <code>bdt.mv.db</code> (H2 database file). Note: H2 database is upgraded from 1.4.199 to 2.1.212 for the backup of old version file. Refer to Backup using the Script Tool and Restore from a Script for details.
lib	Contains required JAVA library dependencies.
log	Contains log file directory.
samples	Contains sample policy and configuration files.

6. Configure at least the following properties in the BDT properties file:

- `NAE_IP.1= CM_IP`
- `NAE_Port= TCP_PORT`
- `Protocol= tcp`

File-to-File Transformation

Linux

1. Create a user `test_user` and a key `test_key` for this user on the CipherTrust Manager.
2. On the CipherTrust Manager, configure the NAE interface to work with `No TLS`, `allow anonymous logins`.
3. Download and copy the [QuickStartEncryptInput.csv](#) and [QuickStartEncrypt.config](#) files to the `$BDT_HOME/conf/` directory. The `ContactDetails` column of the `QuickStartEncryptInput.csv` file will get encrypted using these steps.
4. Download and copy the [QuickStartEncrypt.policy](#) file to `$BDT_HOME/samples/`.
5. Configure properties of default crypto library. Open command prompt from `$BDT_HOME/bin/` and run the following command:

```
bdt.sh -f
```

Enter values as per the prompt messages and you are all set to run BDT.

6. Run the following command to write encrypted NAE user `test_user` password in `QuickStartEncrypt.config` file:

```
bdt.sh -e -c ../conf/QuickStartEncrypt.config
```

7. Run the following command:

```
bdt.sh -t -c ../conf/QuickStartEncrypt.config -p ../samples/QuickStartEncrypt.policy
```

8. Check the QuickStartEncryptOutput csv file created in \$BDT_HOME/conf/.

Windows

1. Create a user `test_user` and a key `test_key` for this user on the CipherTrust Manager.
2. On the CipherTrust Manager, configure the NAE interface to work with `No TLS, allow anonymous logins`.
3. Download and copy the `QuickStartEncryptInput.csv` and `QuickStartEncrypt.config` files to the `$BDT_HOME/conf/` directory. The `ContactDetails` column of the `QuickStartEncryptInput.csv` file will get encrypted using these steps.
4. Download and copy the `QuickStartEncrypt.policy` file to `$BDT_HOME/samples/`.
5. Configure properties of default crypto library. Open command prompt from `$BDT_HOME/bin/` and run the following command:

```
bdt.bat -f
```

Enter values as per the prompt messages and you are all set to run BDT.

6. Run the following command to write encrypted NAE user `test_user` password in `QuickStartEncrypt.config` file:

```
bdt.bat -e -c ../conf/QuickStartEncrypt.config
```

7. Run the following command:

```
bdt.bat -t -c ../conf/QuickStartEncrypt.config -p ../samples/QuickStartEncrypt.policy
```

8. Check the QuickStartEncryptOutput csv file created in `$BDT_HOME/conf/`.

Tip

Your demo of the file-to-file transformation using *encryption* is complete. Now, you can explore all the supported transformations and the [transformation process](#). Also, you can explore the tasks that you can perform using BDT, advanced topics, samples, best practices, and troubleshooting information. Use the left pane to navigate to the desired sections.

BDT Transformation Process

BDT supports different types of transformations.

Transformation Types

- **Database to database** (DB-to-DB): Encrypt, decrypt, tokenize, detokenize, or rekey the data of a database table and move it to another database. Multiple tables can be transformed in a single execution of the utility. You can choose table columns and specify what action needs to be performed on a particular column.
- **Database to file** (DB-to-File): Encrypt, decrypt, tokenize, detokenize, or rekey the data of a database table and move it to another file. You can choose table columns and specify what action needs to be performed on a particular column.
- **File to database** (File-to-DB): Encrypt, decrypt, tokenize, detokenize, or rekey the data of a file and move it to another database. You can choose file columns and specify what action needs to be performed on a particular column.
- **File to file** (File-to-File): Encrypt, decrypt, tokenize, detokenize, or rekey the data of a file and move it to another file. You can choose file columns and specify what action needs to be performed on a particular column.

Prerequisites

- BDT is installed. Refer to [Installation](#) for instructions on installing BDT on Linux and Windows.
- To perform **tokenization**, a compatible version (2.2 or higher) of Vormetric Tokenization Server (now renamed as CipherTrust Vaultless Tokenization (CT-VL)) is up and running. Refer to the CT-VL [Quick Start](#) document for details.
- A CipherTrust Manager version compatible with the installed CT-VL/CADP for Java version is up and running. Refer to the CipherTrust Manager [Getting Started](#) document for details.
- Java 17 must be installed.

Click the desired tab to view transformation-specific prerequisites.

DB-to-DB

- Download the JDBC connector `.jar` compatible to your database version.

The following table captures the details of database drivers and their versions that have explicitly been tested.

Database	Driver
SQL Server	mssql-jdbc-9.2.1.jre8.jar
MYSQL	mysql-connector-java-8.0.15.jar
Oracle	ojdbc6.jar
SAP HANA	ngdbc-2.4.70.jar
DB2	db2jcc4.jar

- Place the driver `.jar` files in the `bdt/lib` directory.
- Prepare input databases. Refer to [Filtering Input Data](#) for details.

DB-to-File

- Download the JDBC connector `.jar` compatible to your database version.

The following table captures the details of database drivers and their versions that have explicitly been tested.

Database	Driver
SQL Server	mssql-jdbc-9.2.1.jre8.jar
MYSQL	mysql-connector-java-8.0.15.jar
Oracle	ojdbc6.jar
SAP HANA	ngdbc-2.4.70.jar
DB2	db2jcc4.jar

- Place the driver `.jar` files in the `bdt/lib` directory.
- Prepare input databases. Refer to [Filtering Input Data](#) for details.
- For the output file, BDT accepts the output files in the following file formats:
 - CSV File
 - Fixed Length File
- Prepare input databases. Refer to [Filtering Input Data](#) for details.

File-to-DB

Input Data

BDT accepts the input files in the following file formats:

- CSV File
- Fixed Length File

The input files must meet the following data requirements:

- Per-column data size limit: 128K
- The input data file can contain quoted and unquoted values. Both `field1_value` and `field2_value` are recognized as data values. To use quoted values, you must specify the double quote character as a text qualifier.
- Fields must be separated by the delimiter character specified in the policy file.
- If a field value contains the delimiter character, the value must be enclosed by text qualifier characters as specified in the policy file.
- If a field value contains the text qualifier, the entire value must be enclosed in text qualifier characters.
- Another way to deal with field values having delimiter or qualifier characters is to escape those character using the backslash (\) instead of enclosing the field in text qualifier characters. When using this technique, set the `unescapeInput` attribute in the policy file to true. For example:

If the field value has a backslash character, it must also be escaped using an additional backslash character.

- If you are using fixed length file format, you must set up input files accordingly. Refer to [Setting up Input Files with Fixed-Length Record Format](#) for details.
- Prepare input files. Refer to [Filtering Input Data](#) for details.

Output Data

BDT is supported with the following databases. The table below lists the versions tested with.

Database	Tested Version
MySQL	8.0, 8.0.27
Oracle	12c, 19c
IBM DB2	10.5, 11.5.7
SAP HANA	2.0
Microsoft SQL Server	2017, 2019

File-to-File

Input Data

BDT accepts the input files in the following file formats:

- CSV File
- Fixed Length File

The input files must meet the following data requirements:

- Per-column data size limit: 128K
- The input data file can contain quoted and unquoted values. Both `field1_value` and `field2_value` are recognized as data values. To use quoted values, you must specify the double quote character as a text qualifier.
- Fields must be separated by the delimiter character specified in the policy file.
- If a field value contains the delimiter character, the value must be enclosed by text qualifier characters as specified in the policy file.
- If a field value contains the text qualifier, the entire value must be enclosed in text qualifier characters.
- Another way to deal with field values having delimiter or qualifier characters is to escape those character using the backslash (`\`) instead of enclosing the field in text qualifier characters. When using this technique, set the `unescapeInput` attribute in the policy file to true. For example:

If the field value has a backslash character, it must also be escaped using an additional backslash character.

- If you are using fixed length file format, you must set up input files accordingly. Refer to [Setting up Input Files with Fixed-Length Record Format](#) for details.
- Prepare input files. Refer to [Filtering Input Data](#) for details.

Transformation Process

1. Set up BDT Config

Update properties inside the `bdt.config` file as per your environment. Refer to [BDT Config file](#) for the file settings.

If you want to perform encryption using the CipherTrust Manager, then follow the below step, else move to step 3.

2. Set up BDT Properties

Update properties inside the `bdt.properties` file as per your environment. Refer to [BDT Properties File](#) for details.

3. Set up BDT Policy

DB-to-DB

Create `bdt.policy` based on your input DB and transformation requirement. The `Samples` directory has `bdt.policy` samples with explanatory comments. Refer to [Setting up BDT Policy](#) for details.

To transform database table columns:

1. Create a `bdt.policy` file and add source database connection properties to the policy source attribute. Do the same for destination database. Refer to [Listing Source](#) and [Destination](#) tables and columns for details.
2. In the `tables` section of the policy, add an entry for table to transform, specify source and destination table, and the columns to transform.
3. Ensure the destination table has the exact same schema as the source table.
4. Specify the transformation operation for each column of the input data.

Note

If you do not specify any of these actions for a column, the contents of the column are copied to the output file without any transformation.

Listing Source Tables and Columns

Source connection properties are picked from the policy file `source` attribute.

- Run `./bdt.sh -ls table -p policyfilepath` to list source tables.
- Run `./bdt.sh -ls column -table test1 -p policyfilepath` to list the columns of source table `test1`

Listing Destination Tables and Columns

Destination connection properties are picked from the policy file `destination` attribute.

- Run `./bdt.sh -ld table -p policyfilepath` to list destination tables.
- Run `./bdt.sh -ld column -table test1 -p policyfilepath` to list columns of destination table `test1`

Performing Inplace Transformations

You can choose to have BDT create a separate database table with the transformed data, or instead perform an in-place transformation where the source database is itself transformed with new data, and no new database created. Specify either behavior with the `inPlaceUpdate` attribute value in the policy file.

If you specify an in-place transformation (by setting the `inPlaceUpdate` attribute to `true`), where the source and destination are the same, the `destination` attribute is ignored.

Sample DB-to-DB Transformation Policy

Sample `DbToDbTransformation.policy` for reference.

DB-to-File

Create `bdt.policy` based on your input DB and transformation requirement. The `Samples` directory has `bdt.policy` samples with explanatory comments. Refer to [Setting up BDT Policy](#) for details.

BDT supports transforming a database table and copying the data to an output file. To do so:

1. Specify the destination type as `CSV_FILE` or `FIXED_LENGTH_FILE` in the policy file.
2. Specify needed attributes of the input file, such as delimiter, encoding, and so on.
 - If more than one table is transformed in a single execution, BDT creates a separate output file for each table.
 - The source table name is suffixed in the output file.
3. You can specify the [Transformation Operations](#) that needs to be performed.

Note

If you do not specify any of these actions for a column, the contents of the column are copied to the output file without any transformation.

Listing Source Tables and Columns

Source connection properties are picked from the policy file `source` attribute.

- Run `./bdt.sh -ls table -p policyfilepath` to list source tables.
- Run `./bdt.sh -ls column -table test1 -p policyfilepath` to list the columns of source table `test1`

Sample DB-to-File Transformation Policy

Sample `DBToFileTransformation.policy` for reference.

File-to-DB

Create `bdt.policy` based on your input file and transformation requirement. The `Samples` directory has `bdt.policy` samples with explanatory comments. Refer to [Setting up BDT Policy](#) for details.

To transform an input file and copy data to a database table:

1. In the policy file, specify the source type as `@CSV_FILE` or `@FIXED_LENGTH_FILE`. You can also [add text qualifier characters in input files](#) while setting up the BDT policy.
2. Set the destination DB connection properties in the policy destination attribute. The destination table schema should have all columns specified by the input file header row. If a header row is not present in the input file, columns are named as `COLUMN0`, `COLUMN1` . . . `COLUMNn`. Refer to [BDT Policy Attributes](#) for the list of all attributes.
3. You can specify the [Transformation Operations](#) that needs to be performed.

Note

If you do not specify any of these actions for a column, the contents of the column are copied to the output file without any transformation.

Listing Destination Tables and Columns

Destination connection properties are picked from the policy file `destination` attribute.

- Run `./bdt.sh -ld table -p policyfilepath` to list destination tables.
- Run `./bdt.sh -ld column -table test1 -p policyfilepath` to list columns of destination table `test1`

Sample File-to-DB Transformation Policy

Sample `FileToDBTransformation.policy` for reference.

See Also

[Setting up Character Encoding in the Policy](#)

[Validating Configuration and Policy Files](#)

File-to-File

Create `bdt.policy` based on your input file and transformation requirement. The `Samples` directory has `bdt.policy` samples with explanatory comments. Refer to [Setting up BDT Policy](#) for details.

- You can also [add text qualifier characters in input files](#) while setting up BDT policy for file-to-file transformation.
- You can specify the [Transformation Operations](#) that needs to be performed.

Note

If you do not specify any of these actions for a column, the contents of the column are copied to the output file without any transformation.

Sample File-to-File Transformation policy

Refer to [sample File Transformation Policy](#) for reference.

See Also

[Setting up Character Encoding in the Policy](#)

[Validating Configuration and Policy Files](#)

4. Set up Access Credentials (for CM and Database)

You must set up BDT passwords and other access credentials after setting up BDT policy. Refer to [Setting up Access Credentials \(for CM and Database\)](#) for details.

5. Run Transformation**Linux**

Run `./bdt.sh -t [-c configfilepath] -p policyfilepath` for transforming files.

Windows

Run `bdt.bat -t [-c configfilepath] -p policyfilepath` for transforming files.

Note

`-c` is optional. If not provided, the default `config` file from the location `bdt/conf/bdt.config` is used.

- This command first validates configuration (`bdt.config` and `bdt.policy` validation) and then triggers transformation.
- The `transformation_id` is optional. When provided as a value to the `-t` option, the specified ID overrides the ID field value that is set in the policy file. Refer to [Restarting Transformation](#) for details.

See Also

[BDT Command Syntax](#)

6. Verify Output

DB-to-DB

Verify the output in the column mentioned in the policy file.

DB-to-File

- The output file is generated in the output directory specified in `bdt.config`. Check the output file name with the current timestamp appended.
- The same output directory can also contain a file named `<policy_name-timestamp>.failed`, which records any utility that has failed to transform. (The `policy_name` is defined with the `name` attribute in the policy file.)

File-to-DB

Verify the output in the column mentioned in the policy file.

File-to-File

- The output file is generated in the output directory specified in `bdt.config`. Check the output file name with the current timestamp appended.
- The same output directory can also contain a file named `<policy_name-timestamp>.failed`, which records any utility that has failed to transform. (The `policy_name` is defined with the `name` attribute in the policy file.)

Note

BDT does not support the following transformations:

- CSV to Fixed-length
- Database to Fixed-length

Tasks

This section describes BDT tasks:

- [Setting up BDT Policy](#)
 - [Setting up Access Credentials \(for CM and Database\)](#)
 - [Performing Encryption Through VAE](#)
 - [Restarting Transformation](#)
 - [Configure Logging](#)
-

- Filtering Input Data
- Setting up Character Encoding in the Policy
- Setting up Input Files with Fixed-Length Record Format
- Using Text Qualifier Characters in Input Files
- Validating Configuration and Policy Files
- Performing Initial Data Transformation for DPG Compatibility
- Storing Output of Crypto Operations in a New Column
- Using TU Features in BDT
- Operations

Setting up BDT Policy

The BDT policy provides instructions to the utility on how to perform transformation of the data in the input source. The policy is stored in the `bdt.policy` file or on a [CipherTrust Manager \(CM\)](#) instance that serves as a centralized manager for configuration, for easier reuse and maintenance.

See Also

[Sample BDT policy](#)

Using Local File

To configure your transformation policies using a local file:

1. Update the BDT Policy File attributes as applicable.
2. Open the command prompt, run `bdt.sh` or `bdt.bat`, and use `-p` option. This option identifies the local policy file.

For example:

```
./bdt.sh [-e] -t [-c configfilepath] {-p policyfilepath}
```


Using CipherTrust Manager (CM)

Note

CADP-JCE must be installed on your system to set up policies on the CipherTrust Manager for performing tokenization.

Refer to [BDT Policies](#) for details.

Setting up BDT Policy Using Local File

Use the following steps to configure your transformation policies through a local file:

1. Update the [BDT Policy File attributes](#) as applicable.
2. While running BDT from the command line using `bdt.sh` or `bdt.bat`, use `-p` to identify the local policy file.

For example:

```
./bdt.sh [-e] -t [-c configfilepath] {-p policyfilepath}
```

See Also

[Sample BDT policy](#)

Setting up Access Credentials (for CM and Database)

The first time you run BDT, use the `-e` option to store encrypted passwords in the BDT configuration file. Run the following command:

```
./bdt.sh -e [-c configfilepath] [-p policyfilepath]
```

The `-e` option can be used with the `--validate` or `--transform` option. This first puts the encrypted passwords in `bdt.config` and then performs the specified operation:

- Validates the configuration and policy files
- Performs data transformation

For example, the following command gets new passwords (`-e`), then transforms the data (`-t`) using the policy specified in the `-p` option:

```
./bdt.sh -e -t -p policyfilepath
```

Note

The `policyfilepath` option is not needed to be provided for the centralized policy.

Based on the configuration given in the config file, this command prompts for different passwords such as user password, keystore, truststore, and key password, to encrypt and update them in the config file.

These passwords will be encrypted and stored in the `bdt.config` file specified in the `-c` option. If `-c` is omitted, the default file `bdt/conf/bdt.config` is used.

Performing Encryption Through VAE

By default, BDT encryption is configured to use CipherTrust Manager (CM) as its key manager, as described in [Quick Start](#).

You can also configure BDT to use as its cryptographic server Vormetric Application Encryption (VAE) connected to a DSM security manager.

To do so, perform the following steps:

1. Open the `bdt.config` file, and under the `crypto` heading, set the cryptographic server to `vae`.

Sample for vae

```
"crypto": {
  "@type": "vae", /* Specify @type field as "vae" if vae is used as cryptographic
  c server, else skip @type field. */
  "pin": "", /* Key manager passphrase. */
  "libPath": "" /* Path to vae library. */
},
```

2. Follow steps described in the [transformation process](#).

Note

VAE does not support CM as the key manager.

Restarting Transformation

If a transformation run fails (for example, because of a system or process failure), the user can restart BDT with the `-r` option so that the utility resumes processing from the last committed batch. Such a restart is a more efficient and faster way to resume transformation, rather than rerunning from the beginning.

The following requirements must be met to successfully restart a transformation run:

- The destination must be empty at the time of the first run.
- There cannot be any new records in either source file or table.

To restart a BDT transformation at the point of failure, use the `-r` option:

```
bdm -r <transformation_id>
```

Where, by default `transformation_id` is the ID attribute in the policy file. If there are duplicate policy IDs in the internal BDT database, find the proper transformation ID from the failed transformation log file entry.

The `transformation_id` can be explicitly provided with `bdm -t` in the failed run.

```
bdm -t <transformation_id>
```

BDT launches the new transformation job to process the remaining records from the point of the failed transformation. If the number of records in the committed state and the number of actual written records are not identical, BDT cannot restart the transformation. This is a rare case where the system failed just after a record batch write but before writing the commit state.

Note

Do not change the policy file while restarting BDT. Doing so might result in inconsistent data transfers.

Configure Logging

BDT uses the standard `log4j` framework to record the logs, and allows you to configure log levels using `log4j.properties` file at `$BDT_HOME/conf`. Log levels can be configured for log files and console.

Configure Log Level for Log Files and Console

To configure log level for log files and console, you can set the log level in the `log4j.properties` file manually. To configure log level for log files via CLI, use `-f` option (before performing the transformation).

Note

The log file path can be absolute or relative to your application. Do not use the quotes even if the path contains spaces.

Log Levels

Log Level	Description
FATAL	Reserved for internal errors.
ERROR	Only error messages are logged.
WARN	Logs error messages and warnings.
INFO	Logs error messages, warnings, and informational messages.
DEBUG	Logs the diagnostic information.

Note

When you set a log level, all log events with equal or more severe levels are included. Logs with less severe levels are excluded. For example, if `ERROR` is set as the log level, only the `ERROR` and `FATAL` events are included.

Configuring TLS for use with CipherTrust Vaultless Tokenization (CT-VL)

Authentication can be done using server authentication or using client authentication. The end user can do either, both, or none of them.

Users can configure TLS in one of the following ways:

- [Configure SSL using Default Settings](#)
- [Configure SSL using all Certificates](#)
- [Configure SSL using Specified Certificates](#)

Setting up SSL using `Default` Setting

CT-VL Server Authentication

1. Go to the `vtls{}` section of the `bdtd.config` file.
2. Specify the following values for the `server{}` object commands:
 - `sslmode`: **Default**. Indicates trust only a standard valid certificate issued by a Certificate Authority (CA). If the certificate is expired, self-signed, or invalid, communication with the CT-VL server fails. The other `sslmode` values available for CT-VL server authentication are `Allow-All` and `Specify_SSL_Cert`. Refer to [Configuring TLS](#) for details.

-
- `VerifyHostName`: By default, it is set to **true** to enable hostname verification for SSL communication.

CT-VL Client Authentication

1. Go to the `mts{}` section of the `bdt.config` file.
2. Specify the following values for the `client{}` object commands:
 - `sslmode`: **Default**. Indicates client authentication is disabled. No need to send client identity. The other `ssl-mode` values available for CT-VL client authentication are `Allow-All` and `Specify_SSL_Cert`. Refer to [Configuring TLS](#) for details.
 - `Keystore`: **Client keystore file path**. This assumes a keystore has already been created; for example, using `keytool`.
 - `storepassword`: **Client keystore file password**.
 - `keypassword`: **Client's key password**.

Setting up SSL using `Allow-All` Setting

User can opt for server and client authentication by configuring `bdt.config`.

Perform the following steps to set up SSL for secure communication between the BDT utility and the CipherTrust Vaultless Tokenization (CT-VL) using all trust certificates:

CT-VL Server Authentication

1. Go to the `mts{}` section of the `bdt.config` file.
2. Specify the following values for the `server{}` object commands:
 - `sslmode`: Select **Allow-All**. Indicates Trust all certificates; no trust policy is defined. Any kind of SSL certificate is acceptable, including valid, expired, self-signed, or any other. The truststore setting is not required.
 - `VerifyHostName`: By default, it is set to **true** to enable hostname verification for SSL communication.

CT-VL Client Authentication

1. Go to the `mts{}` section of the `bdt.config` file.
2. Specify the following values for the `client{}` object commands:
 - `sslmode`: Select **Allow-All**. Indicates client authentication is disabled and there is no need to send client identity.

When passing `sslmode` as **ALLOW_ALL**, you don't need to configure following 3 params:

- `keystore`: **Client keystore file path**. This assumes a keystore has already been created; for example, using `keytool`.
- `storepassword`: **Client keystore file password**.
- `keypassword`: **Client's key password**.

Setting up SSL using `Specify_SSL_Cert` Setting

Perform the following steps to set up SSL for secure communication between the BDT utility and the CipherTrust Vaultless Tokenization (CT-VL) using valid certificates:

CT-VL Server Authentication

1. Go to the `mts{}` section of the `bdm.config` file.
2. Specify the following values for the `server{}` object commands:
 - `sslmode`: Select **Specify_SSL_Cert**. Indicates trust standard certificates and certificates stored in the provided trust store (specified in the truststore setting). Use to accept self-signed and expired certificates.
 - `VerifyHostName`: By default, it is set to **true** to enable hostname verification for SSL communication. Set to "false" to disable hostname verification.
 - `truststore`: Truststore file path. To set up the truststore:
 - Get the server's public certificate. If not available, open the VTS URL in a browser and export it from the Security option.
 - Import the certificate and create the truststore. Use the following command, it will output the truststore password.

```
keytool -import -alias "mts host certificate" -file server.crt -keystore
server.truststore
```

Important: Note this password. You need to provide it in the password parameter.

- `password`: Truststore file password obtained when you imported the VTS certificate and created the truststore.

CT-VL Client Authentication

1. Go to the `mts{}` section of the `bdm.config` file.
2. Specify the following values for the `client{}` object commands:
 - `sslmode`: **Specify_SSL_Cert** Indicates Client authentication is enabled. Create keystore with client certificate and key. Set keystore path in the keystore parameter. Communication succeeds if the VTS

server finds a valid certificate set in the keystore.

- `Keystore`: **Client keystore file path**. This assumes a keystore has already been created; for example, using `keytool`.
- `storepassword`: **Client keystore file password**.
- `keypassword`: **Client's key password**.

Filtering Input Data

BDT supports filtering of input data. For example, in a case with one million input rows, you can designate a subset for transformation. To do so, specify subset criteria in a policy file to filter the input records.

The element `subset` is a table-level element, and is applicable only to that table. Refer to [BDT Policy Files](#) for more information on Table attributes.

Filter Input Rows from Source Files

The following example shows how to filter input rows from source files:

```
"subset":{
  "offset":"10",
  "limit":1000,
  "recurrency": 2,
  "filters":[
    {
      "selector":"name",
      "operator":"like",
      "expression":"'p.*'"
    }
  ]
}
```

Specify the starting `offset` and the `limit`, which define the number of rows to transform.

The `recurrency` attribute specifies whether to transform rows in a sequence or skip rows. If recurrency is set to 2, then every second row in the sequence is transformed and the row in between is skipped.

`filters` specifies the list of conditions to match. The row should satisfy all conditions specified in the list.

- `selector` is the name of the column that the filter should evaluate.
- `operators` Options: "=", "<", ">", "<=", ">=", "!=", "like".
- `expression` Used to evaluate the filter on the selector using specified operator. For file transformation if `operator` is specified as `like`, then specify `regex expression` to match in the column value.

Note

To create a regex expression, see [Regex Tutorial](#) for details.

Filter Database Table Rows

The following example shows how to filter input database table rows:

```
"subset":{
  "offset":"10",
  "limit":1000,
  "recurrency": 1,
  "orderBy":"ID",
  "order":"DESC",
  "filters":[
    {
      "selector":"name",
      "operator":"like",
      "expression":"'p.*'"
    },
    {
      "selector":"salary",
      "operator":"<",
      "expression":"100000"
    }
  ]
}
```

Compared with file transformations, the database transformation `subset` can include two additional attributes:

- `orderBy`: Use the name of column which should be used to order records. Records are ordered first, then offset and limit attributes are applied.
- `order`: Define ascending (ASC) or descending (DESC) order.

For the `like` operator, use database-specific syntax for the expression to evaluate.

Setting up Character Encoding in the Policy

Note

Character encoding is mandatory only for the Extended Binary Coded Decimal Interchange Code (EBCDIC)-encoded files.

The supported encodings are listed in the linked [table](#) with the following caveats:

- The naming from either columns in the table *Canonical Name for `java.nio` API* and *Canonical Name for `java.io` API and `java.lang` API* can be used.
- The input file must use the same character encoding. Failed record files are created with the same character encoding. Output file encoding can vary, depending on configurations in the policy file.

Example

Example showing how to set Extended Binary Coded Decimal Interchange Code (EBCDIC) character encoding in the policy file.

See Also

BDT Policy File

Setting up Input Files with Fixed-Length Record Format

Some systems may require fixed-length record formats. As described by IBM:

“In fixed-length or fixed-format records, each field starts and ends at the same place in every record. A data file that contains data records of equal and constant length might be organized as follows.

Sample file with fixed-length records: `aaabbbbccccdddddggghhhh`

The data file illustrated previously has three records. Each record has a field of three characters followed by a field of four characters, so the total record length is seven characters. The file does not contain any separation between records; delimiters are unnecessary because all fields have the same length. The VARCHAR data types are therefore always the fixed maximum size of the field.”

Reference: [IBM® Informix® 12.10](#)

This option is valid for FPE and FF1 (ENCRYPT and DECRYPT), and TOKENIZE actions only. Refer to the sample policy file `FixedLengthFiletransformation.policy` in the BDT Sample folder.

Note

If applying tokenization on fixed-length format records, be sure not to add any prefix or suffix to the tokenized output. Adding such a string will result in failure of detokenization.

Example with a fixed-length record format along with EBCDIC character encoding.

Using Text Qualifier Characters in Input Files

A text qualifier character can be used to mark the start and end of a column field in a file that is input to the BDT utility. This is useful when the field value itself contains a character that would normally act as a field delimiter. Use the qualifier to indicate to BDT that the data following the delimiter is part of the same field, and not the beginning of the next field.

Any printable ASCII character can be specified as a text qualifier, except for the backslash (\) character. Also note that the qualifier character cannot be the same as the delimiter character.

For example, in the following input file, the comma is the delimiter character, but it is also part of the address field. To let BDT know that the text after the comma is also part of the same field, the value must be enclosed with a text qualifier.

Example of data before adding the text qualifier:

```
Firstname, Lastname, Address
James,Brown,1745 E. New St., Apt. 22,Chicago
Scott,Smith,400 South Warren Street,Trenton
```

After adding the text qualifier:

```
James,Brown,"1745 E. New St., Apt. 22,Chicago"
Scott,Smith,"400 South Warren Street,Trenton"
```

In most cases, the input file for BDT is created by exporting data from a database. Databases provide the option to specify a character to be used as a qualifier in exported data.

To add text qualifier characters:

1. When exporting data from the database, specify the qualifier using the technique that is supported by the database.
2. In the policy file, add the qualifier parameter to the top of the file, before the column specifications begin. If the qualifier is a double quote character, escape it in the policy file with a backslash.

Example configuration in policy file, including the double quote character (") as a qualifier:

```
"source":{
  "@type":"CSV_FILE",
  "filepath":"input.csv",
  "delimiter":",",
  "qualifier":"\"",
  "unescapeInput":true,
  "columnCount":"12",
  "hasHeaderRow":true
}
```

Validating Configuration and Policy Files

Perform the following steps to validate the BDT config and policy files.

Validating Configuration Files

If the config file is named as `bdtd.config` and assuming the file is stored in the expected default location, then to validate `bdtd.config` alone, use `-v` with no other options:

```
./bdtd.sh -v
```

If your config file is named differently, then to validate config files, use the `-c` option:

```
./bdt.sh -v [-c configfilepath]
```

Note

- `-c` is optional. If not provided, the default configuration file `bdt/conf/bdt.config` is validated.
- Replace `bdt.sh` with `bdt.bat` in the Windows environment wherever using commands with `bdt.sh`.

Validating Policy Files

If you want to only validate the policy files but not perform any other operation, you can specify which files to validate by adding `-p` for local policy file and `-central` for central policy.

For example, to validate the files `configfilepath` and `policyfilepath`, use the following command:

```
./bdt.sh -v [-c configfilepath] [-p <policyfilepath> | -central centralized_policyfile]
```

Note

- `-c` is optional. If not provided, the default configuration file `bdt/conf/bdt.config` is validated.
- `-p` and `-central` are optional. If not provided, the policy file is not validated.
- Replace `bdt.sh` with `bdt.bat` in the Windows environment wherever using commands with `bdt.sh`.

Performing Initial Data Transformation for DPG Compatibility

CipherTrust Batch Data Transformation (BDT) performs the initial, one-time encryption of existing plaintext data to make it compatible with the CipherTrust Data Protection Gateway (DPG). This process uses a BDT policy file to encrypt the data with the same protection policy that DPG will use for ongoing operations.

Note

- Initial encryption is needed only for the plaintext data.
- Initial encryption is supported only through BDT policy file and not from BDT tile on CipherTrust Manager UI.

- Initial encryption is supported only up to DPG version 1.2.0.

Steps for Initial Transformation of Data

- Create protection policy on CipherTrust Manager. Refer to the [Creating Protection Policy](#) for details.
- Create a BDT policy file using the same protection policy configurations defined in the previous step. Refer to the table below to map the attribute of BDT policy with the corresponding protection policy fields.

Protection Policy Fields	BDT Policy Attributes
Algorithm	@type
Key Name	key
IV	iv
Tweak	tweak
Tweak Algorithm	tweakAlgo
Character Set	characterSet
Version	policyVersion

Refer to the table below for algorithm name mappings between CipherTrust Manager and BDT policy file.

Algorithm name on CipherTrust Manager	Algorithm name in BDT Policy
AES/CBC/PKCS5Padding	AES_CBC_PAD
FPE/AES	FPE_AES

Following are the snippets of BDT policy for `FPE_AES` and `AES_CBC_PAD` respectively:

BDT policy configuration for FPE_AES

```
"config": [
  {
    "@type": "FPE_AES",
    "key": "key1",
    "tweak": "010ACD5B99F3C343",
    "characterSet": "alphanumeric",
    "policyVersion": 1 /* Version of protection policy on ${cm} GU
I to be used only for Initial Encryption of DPG. */
```

```
    }
  ]
}
```

BDT policy configuration for AES_CBC_PAD

```
"config" : [
  {
    "@type" : "AES/CBC/PKCS5Padding",
    "key" : "example_key",
    "iv" : "1234567812345678",
    "policyVersion" : 1 /* Version of protection policy on ${cm} G
UI to be used only for Initial Encryption of DPG. */
  }
]
```

- Run the transformation using the configured BDT policy. After the transformation is complete, DPG can process data using the existing protection policy created in the previous steps, or you may choose to create a new one.

Note

- BDT reads the encryption properties and protection policy version information from the policy file.
- A `policyVersion` parameter is used in the policy file to get version information of the protection policy.
- Refer to [BDT Policy File Attributes](#) for the attribute details and [Sample BDT Policy](#) for the sample policy file.

Storing Output of Crypto Operations in a New Column

BDT allows you to store the output of the crypto operations (encrypt/decrypt/rekey) in a new column. To enable this feature, add the `targetColName` parameter to the BDT policy file.

If the `targetColName` parameter is specified, the new column will hold the output of the crypto operations (encrypt/decrypt/rekey).

You can also add the `srcColumnAction` parameter to the BDT policy file to specify the action (preserve/remove/empty) to be performed on the source column.

Refer to [Columns Attributes](#) for details about the possible options regarding the `srcColumnAction` parameter.

Destination Types

Following are the different destination types:

- Destination File
- Destination DB

Destination File

The new column is created with the same name as specified in the `targetColName` parameter. The case sensitivity of the new column is based on the `targetColName` parameter.

If the column name specified in the `targetColName` parameter (irrespective of the case sensitivity) exists anywhere in the input file, the transformation is interrupted and the BDT throws an error as shown below:

```
Column "targetColName" exists in the input file.
```

Destination DB

The target column name in the table will be created as per value of the `caseSensitive` parameter (`true` or `false`) in the BDT policy file.

Following are the possible scenarios and errors:

Scenario	Error
The target column name already exists in the table with a different datatype.	<pre>Column "targetColName" exists in the input file.</pre>
The target column name already exists in the table with same datatype and length.	<pre>Column "targetColName" exists in the input file.</pre>

Refer to [Destination CSV File](#), [Destination Fixed Length File](#), and [Destination DB](#) for details.

Using TU Features in BDT

Supported Algorithms

Supported in TU	Supported in BDT
FPE/AES/CARD10	<pre>"@type": "FPE_AES"</pre> <pre>"characterSet": "digits"</pre>
FPE/AES/CARD62	<pre>"@type": "FPE_AES"</pre>

Supported in TU	Supported in BDT
	"characterSet": "alphanumeric"
AES/CBC/PKCS5Padding	"@type": "AES_CBC_PAD"
DESede/CBC/PKCS5Padding	"@type": "DESede" "Padding": "PKCSPADDING" "mode": "CBC"
DESede/ECB/PKCS5Padding	"@type": "DESede" "Padding": "PKCSPADDING" "mode": "ECB"
DESede/CBC/NoPadding	"@type": "DESede" "Padding": "PKCSPADDING" "mode": "ECB"
DESede/ECB/NoPadding	"@type": "DESede" "Padding": "PKCSPADDING" "mode": "CBC"

Note

- The minimum data length required for the FPE_AES type in BDT is 4.
- For FPE algorithms, BDT supports only UTF-8 encoding.
- BDT does not support the FPE formats.

Example

TU Config

```
<Column>
<Name>CREDITCARD</Name>
<MaxLength>16</MaxLength>
  <Transformation>
    <Type>Encrypt</Type>
    <Key>KEY_NAME</Key>
    <Algorithm>FPE/AES/CARD10</Algorithm>
    <TweakAlgo>SHA1</TweakAlgo>
    <TweakData>12345</TweakData>
    <IVType>Column</IVType>
```

```
<IV>0401030003040604090301030705020505030507040108080102020704020702010304070
400090105020603000002020906070004010200</IV>
<NewName>CREDITCARD_NEW</NewName>
</Transformation>
</Column>
```

BDT Config

```
"columns": [
  {
    "name": "CREDITCARD",
    "targetColName": "CREDITCARD_NEW",
    "srcColumnAction": "empty",
    "action": "ENCRYPT",
    "config": [
      {
        "@type": "FPE_AES",
        "key": "KEY_NAME",
        "iv": "040103000304060409030103070502050503050704010808010202070402
0702010304070400090105020603000002020906070004010200",
        "tweak": "12345",
        "tweakAlgo": "SHA1",
        "characterSet": "digits"
      }
    ]
  }
]
```

Supported Datatypes

The following table lists the datatypes supported by BDT corresponding to the databases supported by TU:

Database (TU)	Datatypes (BDT)
SQL Server	CHAR VARCHAR
DB2	CHAR NUMBER RAWBINARY VARCHAR
Oracle	CHAR NUMBER RAW VARCHAR

Storing Output of Crypto Operations in a New Column

BDT allows you to store the output of the crypto operations (encrypt/decrypt/rekey) in a new column. To enable this feature, add the `targetColName` parameter to the BDT policy file. Click [here](#) for more information.

Operations

- Encryption Examples
- Decryption Example
- Tokenize Example
- Detokenize Example
- Rekey Examples

Encryption Examples

The following example shows how to define encryption actions for two columns using `AES_CBC_PAD` and `FPE` encryption:

```
{
  "name" : "column2",
  "action" : "ENCRYPT",
  "config" : [ {
    "@type" : "AES_CBC_PAD",
    "key" : "c2KeyName",
    "iv" : "000102030405060708090A0B0C0D0E0F"
  } ]
}, {
  "name" : "column3",
  "action" : "ENCRYPT",
  "config" : [ {
    "@type" : "FPE",
    "key" : "c3KeyName",
    "characterSet" : "digits",
    "tweak" : "0102030405060708"
  } ]
}
```

The following example shows how to define encryption actions for one column using `FF1` encryption:

```
{
  "id" : "transformation-id",
  "name" : "transformation-name",
  "createBadRecordFile" : true,
  "source" : {
    "@type" : "CSV_FILE",
    "filepath" : "input.csv",
    "delimiter" : ",",
    "columnCount" : "12",
    "hasHeaderRow" : true
  },
  "destination" : {
    "@type" : "CSV_FILE",
    "filepath" : "output.csv"
  },
}
```

```

"tables": [
  {
    "columns": [
      {
        "name": "latitude",
        "action": "ENCRYPT",
        "config": [
          {
            "@type": "FF1",
            "key": "KEYNAME",
            "tweak": "auto",
            "characterSet": "digits"
          }
        ]
      }
    ]
  }
]

```

The following example shows how to define encryption actions for a column using `DESede` encryption:

```

{
  "name" : "column",
  "action" : "ENCRYPT",
  "config" : [
    {
      "@type" : "DESede",
      "key" : "DESedekey",
      "mode" : "CBC",
      "padding" : "PKCS5Padding",
      "iv": "010ACD5B99F3C343"
    }
  ]
}

```

Note

Output and input are base-64 encoded for `AES_CBC_PAD` mode in `ENCRYPT`, `DECRYPT`, and `REKEY` actions.

Decryption Example

The following example shows how to define decryption actions for two columns using `AES_CBC_PAD` and `FPE` decryption:

```

{
  "name" : "column2",
  "action" : "DECRYPT",
  "config" : [ {
    "@type" : "AES_CBC_PAD",

```

```

        "key" : "c2KeyName",
        "iv": "000102030405060708090A0B0C0D0E0F"
    } ]
}, {
    "name" : "column3",
    "action" : "DECRYPT",
    "config" : [ {
        "@type" : "FPE",
        "key" : "c3KeyName",
        "characterSet": "digits",
        "tweak": "0102030405060708"
    } ]
}

```

Tokenize Example

The following example shows the configuration of a column using tokenization:

```

{
    "name" : "column4",
    "action" : "TOKENIZE",
    "config" : [ {
        "@type" : "TOKENIZE",
        "tokenGroup" : "tokenGroup1",
        "tokenTemplate" : "tokenTemplate1"
    } ]
}

```

Detokenize Example

The following example shows the configuration of a column using detokenization:

```

{
    "name" : "column4",
    "action" : "DETOKENIZE",
    "config" : [ {
        "@type" : "TOKENIZE",
        "tokenGroup" : "tokenGroup1",
        "tokenTemplate" : "tokenTemplate1"
    } ]
}

```

Rekey Examples

BDT can perform key rotation by re-encrypting the data using the new key. Key rotation can be done for both [encryption](#) and [tokenization](#) operations.

A [REKEY](#) policy consists of two parts. In fact, [REKEY](#) is just a container for two other following actions:

1. The data is detokenized or decrypted using the existing key.

2. The data is tokenized or encrypted using the new key.

The two actions within each REKEY action are defined using ENCRYPT, DECRYPT, TOKENIZE, and DETOKENIZE with the same parameters as you would use with each of these actions alone.

To know more about these parameters, refer to [BDT Policy File](#).

The following example shows a sample configuration for a column rekey through CT-VL:

```
{
  "name" : "column6",
  "action" : "REKEY",
  "config" : [ {
    "@type" : "TOKENIZE",
    "tokenGroup" : "group1",
    "tokenTemplate" : "abcedf9876543210",
    "action" : "DETOKENIZE"
  }, {
    "@type" : "TOKENIZE",
    "tokenGroup" : "group2",
    "tokenTemplate" : "abcedf9876543210",
    "action" : "TOKENIZE"
  } ]
}
```

The following example shows a sample configuration for a column rekey through BDT default crypto library:

```
{
  "name" : "column6",
  "action" : "REKEY",
  "config" : [ {
    "@type" : "FPE",
    "key" : "rekey1",
    "characterSet": "digits",
    "tweak": "0102030405060708",
    "action" : "DECRYPT"
  }, {
    "@type" : "FPE",
    "key" : "rekey2",
    "characterSet": "digits",
    "tweak": "0102030405060708",
    "action" : "ENCRYPT"
  } ]
}
```

Advanced Topics

This section contains the following pages:

- [BDT Command Syntax](#)
- [BDT Config File](#)
- [BDT Properties File](#)

- BDT Policy File
- Encryption Key Versioning
- Configure TLS for CipherTrust Vaultless Tokenization (CT-VL)
- Configure SSL on CipherTrust Manager for NAE Interface
- FPE/AES/Unicode Cardinality Block-Size Table

BDT Command Syntax

The CipherTrust Batch Data Transformation utility runs at the command line with the following syntax:

```

bdt [-c <configfilepath>] [-e] [-f] [-h | -ld <type> | -ls <type> | -t [<transfor
mation_id>]
| -v] [-p <policyfilepath> | -central <centralized_policyfile>] [-sv] [-table
<tableName>] [-r <transformation_id>] [-rb <transformation_id>]

```

Command Options

Option	Description
<code>-c, --configfile <configfilepath></code>	Location of the BDT configuration file. Replace <code><configfilepath></code> with the path to <code>bdt.config</code> . If omitted, the default file <code>bdt/conf/bdt.config</code> is used.
<code>-e, --encryptPassword</code>	Sets the CADP-JCE library password and CT-VL password, encrypt them, and store in <code>bdt.config</code> . Use this option the first time you run BDT. You can also use it whenever you want to change the passwords. BDT prompts you to enter the passwords at the console.
<code>-f, --populatePropertyFile</code>	Populates the <code>bdt.properties</code> file. Use this option to configure the minimum required parameters of the default crypto library. It also allows you to configure log file path and log level.
<code>-h, --help</code>	Displays the BDT command syntax and information about how to use it.
<code>-ld <type></code>	Lists destination objects. Object types [tables, columns]
<code>-ls <type></code>	Lists source objects. Object types [tables, columns]
<code>-p, --policyfile <policyfilepath></code>	Location of the BDT policy file. Replace <code><policyfilepath></code> with the path to <code>bdt.policy</code> .
<code>-central <centralized_policyfile></code>	This configuration is applicable if the BDT policy is configured in CM. Provides name of the BDT Policy in CM.

Option	Description
<code>-sv, --skipvalidation</code>	Runs BDT without first checking the <code>bdt.config</code> and <code>bdt.policy</code> files for correctness. It is advisable to run transformation with skip validation option only when policy and configuration are validated beforehand. Caution: Use only for testing. Do not use it in a production environment.
<code>-t, --transform [<transformation_id>]</code>	Validates <code>bdt.config</code> and <code>bdt.policy</code> , then transform the input file and store the results in the output directory. If this option is omitted, BDT does not perform the data transformation. Running without <code>-t</code> is useful when you only want to set passwords or validate configuration files. You can optionally include the transformation ID here. When provided as a value to this option the specified ID overrides the ID field value that is set in the policy file.
<code>-v, --validate</code>	Validates <code>bdt.config</code> and (optionally) <code>bdt.policy</code> . Use this option when you want to check the files without actually transforming the data. The policy file is validated if the <code>-p</code> option is included in the command. If you are running with <code>-t</code> , you do not need to include <code>-v</code> . The <code>-t</code> option includes an implicit <code>-v</code> .
<code>--table <tableName></code>	Lists columns for this table. This option must be accompanied by <code>-ls</code> or <code>-ld</code> option. General syntax: <code>bdt.bat -ls (or -ld) columns --table <tableName> -p <policyfile></code>
<code>-r <transaction_id></code>	Restarts a transformation run at the point of a failed transaction. Only uncommitted records are transformed.
<code>-rb, --rollback<transaction_id></code>	Rolls back a failed row during in-place transformation.

BDT Config File

Refer to the [Sample BDT Config File](#) for details.

Global Config File Attributes

The configuration of the BDT utility is stored in JSON format in the file `bdt.config`. At the top of the file are several global configuration settings, followed by settings that configure the main underlying tools used by BDT:

Attribute	Default Value	Mandatory/Optional	Description
<code>inputDirectory</code>	No default	Mandatory	The path to the directory in which the input file or DB is placed.

Attribute	Default Value	Mandatory/Optional	Description
<code>outputDirectory</code>	No default	Mandatory	The path to the directory in which the output file or DB needs to be placed.
<code>threadCount</code>	No default	Mandatory	The maximum number of running threads required to transform a file.
<code>batchSize</code>	No default	Mandatory	The total number of records in the batch.
<code>dataProtectionConfig</code>	No default	Mandatory (if policy is fetched from Key Manager)	Contains credential information which will be used to get centralized policy.
<code>characterSets</code>	No default	Mandatory	Contains configurable list of charset names and their range. Users can also define their own <code>characterSets</code> in the <code>bdt.config</code> file as shown below: <pre>"characterSets" : [{ "Name of CharacterSets" : ["Range of CharacterSets"] }]</pre>
<code>mts</code>	No default	Mandatory (for tokenization and detokenization)	Contains settings to customize the behavior of the CipherTrust Vaultless Tokenization (CT-VL).
<code>crypto</code>	No default	Mandatory (for encryption and decryption)	Contains settings for the cryptographic provider used in this BDT configuration i.e <code>jce</code> (CADP-JCE).

Data Protection Attributes

BDT has a separate section for 'Data Protection Profile' to add its user information. The `dataProtectionConfig` object contains the following settings:

Attribute	Default Value	Mandatory/Optional	Description
<code>@type</code>	No default	Mandatory	For the <code>dataProtectionConfig</code> , BDT supports two login methods:

Attribute	Default Value	Mandatory/Optional	Description
			password - The user logs in using password. user_certificate - The user logs in using a user certificate.
userName	No default	Optional	(Used only when @type value is password). User name having access to batch data transformation on key manager.
password	No default	Optional	(Used only when @type value is password). User password having access to batch data transformation on key manager. Run <code>bdt -e</code> option to set password.
hostName	No default	Optional	(Used only when @type value is user_certificate). Hostname of the machine where tokenization server is running.
serverConfig	No default	Optional	(Used only when @type value is user_certificate).
clientConfig	No default	Optional	(Used only when @type value is user_certificate).

Below is the sample for @type is set to password:

```
"dataProtectionConfig":
{
  "@type": "password",
  "username": "test_user",
  "password": ""
}
```

Below is the sample for @type is set to user_certificate:

```
"dataProtectionConfig":
{
  "@type": "user_certificate",
  "hostName": "",
  "serverConfig":
  {
```



```

    "truststore": "",
    "password": "",
    "verifyHostname": "true"
  },
  "clientConfig":
  {
    "keystore": "",
    "storePassword": "",
    "keyPassword": ""
  },
}

```

Refer to [Sample BDT Config File](#) for details.

Server Configuration Attributes

Attribute	Default Value	Mandatory/Optional	Description
truststore	No default	Mandatory	Truststore file path, truststore should have server certificate.
password	No default	Mandatory	Truststore file password.
verifyHostname	false	Optional	Set to <code>true</code> to enable hostname verification for SSL communication, and <code>false</code> to disable hostname verification.

Client Configuration Attributes

Attribute	Default Value	Mandatory/Optional	Description
keystore	No default	Mandatory	Keystore file path of the client.
storePassword	No default	Mandatory	Keystore file password of the client.
keyPassword	No default	Mandatory	Key file password, usually same as keystore password.

Transformation Specific Attributes

vts Attributes

CT-VL Attributes

BDT has a separate section for the 'CT-VL Attributes'. The `vts` object contains the following settings:

Attribute	Default Value	Mandatory/Optional	Description
hostName	No default	Mandatory	Hostname of the machine where tokenization server is running.
userName	No default	Mandatory	The CT-VL username.
password	No default	Mandatory	The CT-VL password. Use the <code>bdt -e</code> option to enter encrypted value here. Do not use plaintext.
tokenUrl	No default	Mandatory	The CT-VL tokenize REST URL.
detokenUrl	No default	Mandatory	The CT-VL detokenize REST URL.
sslConfig	No default	Mandatory	Contains the server and client authentication configuration attributes.

Server Authentication Attributes

You must set up SSL for secure communication between the BDT utility and the CT-VL. In the `vts` section of `bdt.config`, the `server` object contains the following settings related to SSL authentication:

Attribute	Default Value	Mandatory/Optional	Description
sslmode	DEFAULT	Optional	One of the following values: DEFAULT - Trust only a standard valid certificate issued by a Certificate Authority (CA). If the certificate is expired, self-signed, or invalid, communication with the VTS server fails. SPECIFY_SSL_CERT - Trust standard certificates and certificates stored in the provided trust store (specified in the <code>truststore</code> setting). Use to accept self-signed and expired certificates. ALLOW_ALL - Trust all certificates; no trust policy is defined. Any kind of SSL certificate is acceptable, including valid, expired, self-signed, or any other. The

Attribute	Default Value	Mandatory/Optional	Description
			truststore setting is not required.
<code>verifyHostname</code>	false	Optional	Set to <code>true</code> to enable hostname verification for SSL communication, and <code>false</code> to disable hostname verification.
<code>truststore</code>	No default	Optional	(Used only when <code>sslmode</code> is <code>SPECIFY_SSL_CERT</code>). Truststore file path. To set up the truststore: 1. Get the server's public certificate. If not available, open the VTS URL in a browser and export it from the Security option. 2. Import the certificate and create the truststore. Use the following command. It will output the truststore password. <pre>keytool -import -alias "vts host certificate" -file server.crt -keystore server.truststore</pre> Important: Note this password. You need to provide it in the password parameter.
<code>password</code>	No default	Optional	(Used only when <code>sslmode</code> is <code>SPECIFY_SSL_CERT</code>). Truststore file password is obtained on importing the CT-VL certificate and creating the truststore.

Client Authentication Attributes

In the `vts` section of `bdt.config`, the `client` object contains the following settings related to SSL authentication:

Attribute	Default Value	Mandatory/Optional	Description
<code>sslmode</code>	DEFAULT	Optional	One of the following

Attribute	Default Value	Mandatory/Optional	Description
			values: <code>DEFAULT</code> - Client authentication is disabled. No need to send client identity. <code>ALLOW_ALL</code> - Client authentication is disabled. No need to send client identity. <code>SPECIFY_SSL_CERT</code> - Client authentication is enabled. Create keystore with client certificate and key. Set keystore path in the keystore parameter. Communication succeeds if the CT-VL server finds a valid certificate set in the keystore.
<code>keystore</code>	No default	Optional	(Used only when <code>sslmode</code> is <code>SPECIFY_SSL_CERT</code>). Client's keystore file path. This assumes a keystore has already been created; for example, using <code>keytool</code> .
<code>storepassword</code>	No default	Optional	(Used only when <code>sslmode</code> is <code>SPECIFY_SSL_CERT</code>). Client's keystore file password.
<code>keypassword</code>	No default	Optional	(Used only when <code>sslmode</code> is <code>SPECIFY_SSL_CERT</code>). Client's key password.

crypto Attributes

Cryptographic Provider Attributes

BDT has a separate section to configure 'Cryptographic Provider'. The `crypto` object contains the following settings:

Attribute	Default Value	Mandatory/Optional	Description
<code>@type</code>	<code>jce</code>	Optional	BDT supports the cryptographic provider <code>jce</code> . If any value is not

Attribute	Default Value	Mandatory/Optional	Description
			specified, BDT will use jce, which is a default crypto provider.
userName	No default	Optional	(Used only when using default crypto provider). Key owner user name.
password	No default	Optional	(Used only when using default crypto provider). Key owner user password.

BDT Properties File

The unified BDT package includes the `bdt.properties` file that is saved at `BDT_HOME/conf/bdt.properties` after installation.

To perform encryption using the default crypto library, it is mandatory to configure the `bdt.properties` file. Use `-f` option to configure the minimum required parameters from the command line using the following command:

```
./bdt.sh -f
```

The BDT configuration parameters are classified as follows:

- Network Configuration Parameters
- Connection Configuration Parameters
- SSL/TLS Configuration Parameters
- Client Key Caching Parameters

Network Configuration Parameters

Parameter	Default Value	Description
NAE_IP.1	No default	The <code>NAE_IP.1</code> parameter specifies the IP address of the Key Manager and multiple IP addresses separated by colons (:) when load balancing is used. For example, <code>192.168.1.10:192.168.1.11:192.168.1.12</code> servers must have the same value for the <code>NAE_Port</code>. For IPv6, the IP address must be

Parameter	Default Value	Description
		specified in curly braces, such as {2002:0dc8:85k3:0000:0000:9a2e:0370:5221}. Combination of IPv4 and IPv6 addresses can be separated by colons (:) provided each IPv6 address must be within curly braces. Refer to Limitations for details.
NAE_Port	9000	The NAE_Port parameter specifies the port of the Key Manager. Note: Both clients and servers must use the same port.
Protocol	tcp	The Protocol parameter is used to communicate between BDT and the Key Manager. Possible settings are: • tcp • ssl The ssl option uses TLSv1.0, TLSv1.1, and TLSv1.2. To establish SSL connections between BDT and Key Manager, at least one of TLSv1.0, TLSv1.1, and TLSv1.2 must be enabled on the servers. Both BDT and the Key Manager must use the same protocol. If the Key Managers are executing SSL requests, and BDT is not sending SSL requests, problems will occur. Note: It is recommended to gradually increase security after confirming connectivity between BDT and the Key Manager. Once a TCP connection is established between BDT and the Key Manager, it is safe to move on to SSL. Initially configuring BDT under the most stringent security constraints can complicate troubleshooting.

Connection Configuration Parameters

Parameter	Default Value	Description
Verify_SSL_Certificate	no	The <code>Verify_SSL_Certificate</code> parameter directs BDT to verify the IP address or hostname against the Subject Common Name (CN) or the Subject Alternative Name (SAN) in the server certificate presented by the Key Manager during authentication. SSL must be configured to use this feature. Possible settings are: • yes: Enables the feature. • no: Disables the feature. The feature is disabled by default.
SSL_Handshake_Timeout	No default	The <code>SSL_Handshake_Timeout</code> parameter allocates time for the SSL handshake. SSL must be configured to use this feature. Set to any positive integer.
Use_Persistent_Connections	yes	The <code>Use_Persistent_Connections</code> parameter enables the persistent connections functionality. Possible settings are: • yes: Enables the feature. BDT establishes persistent connections with the Key Manager. • no: Disables the feature. A new connection is made for each connection request. The connection is closed as soon as BDT receives the server response.
Size_of_Connection_Pool	300	The <code>Size_of_Connection_Pool</code> parameter specifies the total number of client-server connections that the configuration could possibly allow. It does not specify the connections that actually exist at a given moment. Possible setting is: • Any positive integer: Connections in the pool can be

Parameter	Default Value	Description
		active or waiting, TCP or SSL. A connection is created and the pool scales as needed. The pool starts at size 0, and can grow to the value set here. Once the pool is full, new connection requests must wait for an existing connection to close.
Load_Balancing_Algorithm	round-robin	The <code>Load_Balancing_Algorithm</code> parameter is used to determine how BDT selects a Key Manager (server) from a load balancing group. Possible settings are: • round-robin: Directs the connection to the next server in the load balancing group. This is the default. • random: Directs the connection to a randomly selected member of the load balancing group.
Connection_Idle_Timeout	600000ms (10 min)	The <code>Connection_Idle_Timeout</code> parameter specifies the amount of time connections in the connection pool can remain idle before the client closes them. Possible setting is: • Any positive integer: Note: There are two different connection timeout values; one on the Key Manager, and one in the properties file. The value of the timeout in the properties file must be less than what is set on the server. This lets the client control when idle connections are closed. Otherwise, the client can maintain a connection that is closed on the server side, which can lead to error.
Unreachable_Server_Retry_Period	60000ms	The <code>Unreachable_Server_Retry_Period</code> parameter specifies the amount of time the client will spend attempting to establish a

Parameter	Default Value	Description
		connection to a load balancing group. An error is returned after the specified period if no server in the group is reachable. If logging is enabled, error messages are written to the log file. Possible settings are: • -1: This is the infinite retry interval. The client keeps trying to connect to a server until a connection is established. This setting is not compatible with multi-tier load balancing as the load balancer will never switch tiers. • Any positive integer: If multi-tier load balancing is enabled, set this value between 1 and twice the value of the <code>Connection_Retry_Interval</code>.
Maximum_Server_Retry_Period	0	The <code>Maximum_Server_Retry_Period</code> parameter specifies the total amount of time that BDT (client) will spend trying to make connections to any Key Manager (server) on any tier. This value is used when multi-tiered load balancing is enabled. Possible settings are: • -1: BDT will try every server on every tier until any response is received. • 0: The default value is set to 0; there is no overall limit. Setting value to 0 disables this feature. • Any positive integer: BDT will try to make connections for at least the duration set in <code>Maximum_Server_Retry_Period</code> and will return an error if no connection can be made on the tier in use when the try period expires.
Connection_Timeout	1 minute	The <code>Connection_Timeout</code> parameter specifies how long BDT (client) waits for the TCP connection function before timeout.

Parameter	Default Value	Description
		Possible settings are: • 0: Disables this setting. The client uses the operating system's connection timeout. • Any positive integer: Setting this parameter a few hundred ms less than the operating system's connection timeout makes connection attempts to a downed Key Manager (server) fail faster, and failover happens sooner. If a connection cannot be made before the timeout expires, the server is marked as down, and taken out of the rotation. Note: If the client is working with many versions of a key, do not set the <code>Connection_Timeout</code> parameter too low. Otherwise the client connection may close before the operation is complete.
Connection_Read_Timeout	7000ms	The <code>Connection_Read_Timeout</code> parameter controls how long BDT(client) waits when reading data from the Key Manager before determining that it is down. Requests should only timeout if the Key Manager is physically down (e.g. powered off, or not responding because of misconfiguration). Possible settings are: • 0: Disables this setting. The client waits indefinitely until the Key Manager can be reached. Requests remain outstanding until the client's request is successfully satisfied. • Any positive integer: The purpose of this parameter is to control how the client should react when the Key Manager is down. If it should timeout eventually and return an error back to the application, set this parameter to an appropriate number of milliseconds to allow requests to complete in high load and high latency situations.

Parameter	Default Value	Description
Connection_Retry_Interval	60000ms (1 minute)	The <code>Connection_Retry_Interval</code> parameter determines how long BDT (client) waits before trying to reconnect to a disabled Key Manager (server). If one of the Key Managers in a load balanced configuration is not reachable, the client assumes that the server is down, and then waits for the specified time period before trying to connect again. Possible settings are: • 0: This is the infinite retry interval. The disabled server will never be brought back into use. • Any positive integer: If the server or network is under a high load, a connection timeout could occur for a running sever. If your <code>Connection_Retry_Interval</code> is not long enough, another connection attempt will be made to the busy server - adding to its already high load.

SSL/TLS Configuration Parameters

Refer to [Configure SSL on CipherTrust Manager for NAE Interface](#) for instructions on how to configure SSL.

Parameter	Default Value	Description
Client_Cert_Alias	the first certificate in the keystore	The client certificate sent to the Key Manager when client certificate authentication is enabled. If you have multiple client certificates in a keystore, you might want to specify which client certificate is sent to the Key Manager during the SSL handshake. If you do not specify a client certificate in the properties file, the first certificate in the keystore is sent to the Key Manager.
Client_Cert_Passphrase	the keystore password	The passphrase needed to access the client certificate listed in the <code>Client_Cert_Alias</code> .

Parameter	Default Value	Description
		If you specify a value for the <code>Client_Cert_Alias</code> , you should also specify a value for the <code>Client_Cert_Passphrase</code> , otherwise the keystore password is used.
<code>Key_Store_Location</code>	No default	The <code>Key_Store_Location</code> parameter specifies the location of the Java keystore that contains the client certificate. The path can be absolute or relative to your application. Don't use quotes, even if the path contains spaces.
<code>Key_Store_Password</code>	No default	The <code>Key_Store_Password</code> parameter specifies the password to unlock the keystore.

Note

Remember that the properties file is NOT encrypted. Make sure this file has appropriate permissions so that it is readable only by the appropriate user.

Client Key Caching Parameters

Parameter	Default Value	Description
<code>Symmetric_Key_Cache_Enabled</code>	no	The <code>Symmetric_Key_Cache_Enabled</code> parameter determines if the symmetric key caching feature is enabled. Symmetric keys can be cached. Possible settings are: • no: Key caching for symmetric keys is disabled. Crypto operations for symmetric key are performed on the Key Manager. • yes: Key caching for symmetric keys is enabled. Protocol must be set to <code>ssl</code> (and <code>ssl</code> must be configured). • tcp_ok: Key caching for symmetric keys is enabled over both <code>tcp</code> and <code>ssl</code> connections.

Parameter	Default Value	Description
Symmetric_Key_Cache_Expiry	43200s (12 hours)	The <code>Symmetric_Key_Cache_Expiry</code> parameter specifies the minimum amount of time that a key will remain in BDT (client) key cache. Possible settings are: • 0: This is the infinite timeout setting. Keys are never purged from the client cache. • A positive integer: At the end of this interval, the key will be purged from the cache the next time the library is called. The default value is 43200 seconds (12 hours).
Symmetric_Key_Cache_AutoRefresh_Interval	0	The <code>Symmetric_Key_Cache_AutoRefresh_Interval</code> parameter specifies the time after which the cached key becomes eligible for refresh. The actual refresh operation occurs only when a cached key is queried from the cache before the key expires. It can be specified in any time unit; the default is seconds. If the eligible key is not queried from the symmetric cache, it is removed from the cache after its expiry. This parameter is applicable only if the symmetric key cache is enabled. Possible settings are: • 0: Auto refresh feature is disabled. • Any positive integer: The time after which the cached key is eligible for refresh.
Local_Cipher_Cache_Expiry	0	The <code>Local_Cipher_Cache_Expiry</code> parameter determines the minimum amount of time after which the cipher initialized with the key expires and is reinitialized with the cached key. Possible settings are: • -1: This is the infinite timeout setting. Cipher is never purged from

Parameter	Default Value	Description
		the client cache. • 0: The cipher will expire after every operation. • Any positive integer: At the end of this interval, the cipher will be purged from the cache the next time the library is called. Note: The <code>Local_Cipher_Cache_Expiry</code> time should be less than or equal to the <code>Symmetric_Key_Cache_Expiry</code> time and <code>Symmetric_Key_Cache_Enabled</code> parameter should be set as yes or tcp_ok.
Local_Crypto_Provider	SunJCE or IBMJCE (depends on JVM)	The <code>Local_Crypto_Provider</code> parameter specifies the name of the JCE provider that will perform local cryptography if symmetric key caching is enabled. For example, SunJCE provider is the default on Sun JVM.
Key_non_exportable_policy	no	The <code>Key_non_exportable_policy</code> parameter is used to perform the crypto operations remotely when symmetric cache is enabled, and the key is non exportable. By default, this parameter is disabled. Possible settings are: • yes: Enables the feature. • no: Disables the feature.

BDT Policy File

Refer to the [Sample BDT Policy File](#) for details.

Top-level Policy Attributes

BDT Policy File Top-level Policy Attributes

Attribute	Default Value	Mandatory/Optional	Description
id	No default	Mandatory	A unique identifier for the

Attribute	Default Value	Mandatory/Optional	Description
			policy. The length of the policy ID must not exceed 100 characters.
name	No default	Mandatory	A unique name for the policy. The length of the policy name must not exceed 100 characters.
description	String	Optional	Description of the policy.
caseSensitive	false	Optional	True or false. If set to <code>true</code>, all the database objects mentioned in the policy file will be processed in the same case as input. If set to <code>false</code>, all the database objects mentioned in the policy file will be automatically converted to CAPITAL case. Note: Setting <code>caseSensitive</code> parameter to <code>true</code> allows SQL reserved words to be used as database objects in BDT. Refer to Sample BDT Policy File for details.
trimSpaces	false	Optional	True or false. If set to <code>true</code>, it will trim initial and trailing white spaces from the data present in the column to be transformed. If set to <code>false</code>, the flag is disabled, and no processing is done on the data present in the column to be transformed.
enableHexLiteral	false	Optional	Input type: Boolean

Attribute	Default Value	Mandatory/Optional	Description
			If set to <code>true</code> , the ciphertext will be enclosed with hex literal. For example, <code>x'<ciphertext>'</code>
source	No default	Mandatory	Defines details of data input. For databases, such details include connection parameters. For files, such details include file type (CSV_FILE or FIXED_LENGTH_FILE), delimiter, encoding, and so on.
destination	No default	Mandatory (if <code>inPlaceUpdate</code> attribute is set to <code>false</code>)	Defines details of data output, such as where to write transformed data. For databases, such details include connection parameters. If the policy file defines an in-place transformation of data (with <code>inPlaceUpdate</code> attribute set to <code>true</code>), the destination value is ignored if defined. For files, such details include file type (CSV_FILE or FIXED_LENGTH_FILE), delimiter, encoding, and so on.
tables	No default	Mandatory	List of the tables to be transformed.
fpemode	ASCII	Optional	ASCII or UTF. (FPE-only) Set <code>fpemode</code> to define which FF3-encoding mechanism to use. ASCII supports only ASCII characters and is faster than UTF. Default is ASCII. Set to UTF when using FPE to encrypt Unicode characters.

Attribute	Default Value	Mandatory/Optional	Description
			Note: ASCII encryption mode is separate from ASCII character encoding.
createBadRecordFile	false	Optional	True or false. Set to true to create a file with <code>.failed</code> extension, otherwise set to false. Note: It is recommended to delete the <code>BadRecordsFile</code> after being used as it contains sensitive information.
inPlaceUpdate	false	Optional	Set to true to transform data in-place within the database (that is, in-place transformation), rather than the default behavior that creates a new destination table containing the transformed data. If true, the <code>destination</code>, <code>destinationTable</code>, and <code>createDestinationTable</code> attributes are ignored. Note: - For <code>inPlaceUpdate</code> transformation, <code>Primary Key</code> column should be available in the table. If this column is not available, below error message is displayed: <code>"Primary key column not found. Can't perform in-place update."</code> - Ensure to take the backup of the source table before performing <code>inplaceUpdate</code>.

Source and Destination Attributes

For JDBC Connections

Attribute	Default Value	Mandatory/Optional	Description
@type	No default	Mandatory	Specify the database type as one of either DB2, ORACLE, MYSQL, SQL_SERVER, HANA.
connectionurl	No default	Mandatory	Database connection URL. For example: jdbc:mysql://localhost:3306/world.
username	No default	Mandatory	Database username.
password	No default	Mandatory	Database password. Use <code>bdt -e</code> option to add encrypted password.
driverclass	No default	Mandatory	DBC connection driver class. For example: com.mysql.cj.jdbc.Driver.

```

"source" :
{
  "@type" : "HANA",
  "connectionurl" : "jdbc:sap://host:port",
  "username" : "",
  "password" : "",
  "driverclass" : "com.sap.db.jdbc.Driver"
},
"destination" :
{
  "@type" : "HANA",
  "connectionurl" : "jdbc:sap://host:port",
  "username" : "",
  "password" : "",
  "driverclass" : "com.sap.db.jdbc.Driver"
}

```

For CSV Files

Attribute	Default Value	Mandatory/Optional	Description
@type	No default	Mandatory	CSV_FILE.
filepath	No default	Mandatory	The file path relative to the inputDir or outputDir path in the config file.
delimiter	No default	Mandatory	The character that is used to divide one column from the next in the input file.

Attribute	Default Value	Mandatory/Optional	Description
			Any printable ASCII character except for backslash (\) can be used as a delimiter, in addition to space (), tab, and Ctrl-A. Not mandatory in destination if it is same as source. Note: The delimiter and qualifier characters cannot be the same.
qualifier	double opening quote ("), if source is any database	Optional	A character used to enclose fields that contain a delimiter or a qualifier character itself. Any printable ASCII character except a backslash ("\") can be used as a qualifier. To identify which qualifier character is used for the input/output file, either go to the properties of your CSV editor or open the input file in any text editor and check which character is used as a qualifier to enclose that data. Example Data in CSV File asdf,asdf asdf"asdf Data in Text Editor "asdf,asdf" "asdf""asdf" In the above example, (") is the qualifier character. Note • The delimiter and qualifier characters cannot be the same. • If data includes delimiter characters, qualifier characters, or both, it is recommended to specify the qualifier character, otherwise the output may be ambiguous.
columnCount	No default	Mandatory	Number of columns in the input file. This does not necessarily equal the number of columns that have rules defined for them in this <code>bdt.policy</code> file.

Attribute	Default Value	Mandatory/Optional	Description
hasHeaderRow	false	Optional	True or false. Default false. If true, the utility will treat the first row as a header row. Values from first row will be treated as column names. The same column names should be mentioned in the transformation action. If false, the utility will treat all the rows as data to be transformed.
encoding	UTF8	Optional	Used to set character encoding, for example, to enable IBM's EBCDIC. Input file must use same character encoding. Output and failed record files will be created with the same character encoding. Sample: For EBCDIC encoding, set <code>encoding:"ibm500"</code> in the policy file. To encrypt ASCII files, you must set encoding: ASCII. Refer to Supported Encodings for details.

For file-to-file (CSV) transformation, if the delimiter or qualifier is not configured for destination, the delimiter or qualifier configured in the source will be considered.

For Fixed-Length Files

Attribute	Default Value	Mandatory/Optional	Description
@type	No default	Mandatory	FIXED_LENGTH_FILE.
filepath	No default	Mandatory	The file path relative to inputDir or outputDir path in config file.
columnCount	No default	Mandatory	The number of columns a row has.
encoding	No default	Optional	Used to set character encoding, for example, to enable IBM's EBCDIC.

Attribute	Default Value	Mandatory/Optional	Description
			Input file must use same character encoding. Output and failed record files will be created with the same character encoding. Sample: For EBCDIC encoding, set encoding:"<code>ibm500</code>" in the policy file. Refer to Supported Encodings for details.
columnPositionInfo	No default	Mandatory	Column positioning.
recordLength	No default	Mandatory	Record length.
lineSeparator	false	Optional	True or false. Is record separated with line separator?
hasHeaderRow	false	Optional	True or false. Default false. If <i>true</i>, the utility will treat the first row as a header row. Values from this row will be treated as column names. The same column names should be mentioned in the transformation action.

Tables Attributes

Attribute	Default Value	Mandatory/Optional	Description
sourceTable	No default	Mandatory	Source table name. For database only. Refer to Limitations for details.
destinationTable	No default	Mandatory (if <code>inPlaceUpdate</code> attribute is set to <code>false</code>)	Destination table name. For database only. If the policy file defines an in-place transformation of data (with <code>inPlaceUpdate</code> attribute set to <code>true</code>), the destination value is ignored if defined. By

Attribute	Default Value	Mandatory/Optional	Description
			definition, source and destination tables are the same.
sourceSchema	Username specified in the JDBC connections or the default schema name for the databases that support schema (for example, "dbo for MSSQL")	Optional	Database username or schema (for the databases that support schema) where source table belongs to.
destinationSchema	Username specified in the JDBC connections or the default schema name for the databases that support schema (for example, "dbo for MSSQL")	Optional	Database username or schema (for the databases that support schema) where destination table belongs to.
columns	No default	Mandatory	List of the columns to be transformed. Policy rules for transforming one or more columns. For each column where transformation is desired, the <code>bdt.policy</code> file specifies the data transformation action to be performed and a set of parameters related to that action.
subset	No default	Optional	Table-specific data filter criteria. Filter input data based on these criteria.
createDestinationTable	false	Optional	True or false. Create destination table if none exists. If in-place transformation is defined (when <code>inPlaceUpdate</code> attribute is set to <code>true</code>), <code>createDestinationTable</code> is ignored, because no new destination table is created. For File to DB, datatype of columns in the destination table will be <code>varchar(10000)</code>. Note: The

Attribute	Default Value	Mandatory/Optional	Description
			<code>createDestinationTable</code> attribute is not supported for HANA databases. Caution: Use only for testing. Do not use in a production environment. Refer to Limitations for details.

Columns Attributes

Attribute	Default Value	Mandatory/Optional	Description
name	No default	Mandatory	Column name. If <code>hasHeaderRow</code> is set to false, then configure this parameter as "columnN" where N is the position of column. Note: The position of column is starting from 0. For example: If the user wants to transform first column, then the value will be "column0", for second column; the value will be "column1", and so on.
targetColName	No default	Optional	Name of the new column. Refer to Storing Output of Crypto Operations in a New Column for details.
srcColumnAction	preserve (if <code>targetColName</code> is set)	Optional	Following are the options: preserve: The source column remains preserved. remove: The source column is removed. empty: The source column is empty, that is, contains no data. Note: If <code>srcColumnAction</code> is

Attribute	Default Value	Mandatory/Optional	Description
			set and no <code>targetColName</code> is present, BDT throws an error.
<code>targetColLength</code>	No default	Mandatory (if <code>targetColName</code> is set during fixed file transformation)	The column length of <code>targetColName</code> .
<code>action</code>	No default	Mandatory	For each column of input data, the <code>bdt.policy</code> file can specify any of these actions - ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, and REKEY. Refer to Attributes for ENCRYPT/DECRYPT Actions and Attributes for TOKENIZE/DETOKENIZE Actions for details. Visit the following for the examples of each action: • ENCRYPT • DECRYPT • TOKENIZE • DETOKENIZE • REKEY Note: If you do not specify any of these actions for a column, the contents of the column are copied to the output file without any transformation.
<code>config</code>	No default	Mandatory	Configuration for Encryption or Tokenization operations.

Configuration Attributes

ENCRYPT/DECRYPT Actions

Attribute	Default Value	Mandatory/Optional	Description
<code>@type</code>	No default	Mandatory	Options: AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, and DESede (signifying the triple operations of DES of

Attribute	Default Value	Mandatory/Optional	Description
			encrypt-decrypt-encrypt). To encrypt/decrypt data using either of the NIST-defined FPE formats - FF3 or FF1, the user must specify the ENCRYPT or DECRYPT policy actions with @type value. The value for FF1 is FF1, and for FF3 is FPE. Note: The BDT syntax uses FPE as a synonym for FF3.
key	No default	Mandatory	Name of the encryption key.
characterSet	No default	Mandatory (if @type is FPE or FF1 or FPE_AES)	Name of the characterSet that was defined under characterSets in the bdt.config file. Defaults include "latin", "digits", "alphabets", and "alphanumeric". Users can also define their own characterSets in the bdt.config file. Note: characterSets are not applicable (if @type is AES_CBC_PAD or AES_CTR or DESede).
tweak	No default	Mandatory (if @type is FPE or FF1 or FPE_AES)	It uses the tweakable cipher concept to protect against statistical attacks due to potentially small input/output space. There are two ways of defining tweak: <pre>"tweak":<16 characters long HEX encoded string></pre> <pre>"tweak": "auto"</pre>

Attribute	Default Value	Mandatory/Optional	Description
			Either of these ways can be used. Refer to the <code>tweakSource</code> attribute for details. Note: <code>tweak</code> is not applicable (if <code>@type</code> is <code>AES_CBC_PAD</code> or <code>AES_CTR</code> or <code>DESede</code>).
<code>tweakSource</code>	No default	Optional	Specifies a column in the source for the <code>tweak</code>, to allow different tweaks to be used for each row. For example: <code>"tweakSource": "columnName"</code>. <code>tweakSource</code> is not supported when <code>inPlaceUpdate</code> is set to true.
<code>allowSmallInputs</code>	false	Optional	True or false. Default is false. Applicable to FPE, FF1, and FPE_AES. If true, the following scenarios occur: • Data is passed as untransformed if effective data length is less than 2 characters for FPE and FF1, and less than 4 characters for FPE_AES. • Transformation continues if effective data length is greater than 2 characters for FPE and FF1, and greater than 4 characters for FPE_AES. If false, transformation fails if effective data length is less than 2 characters for FPE and FF1, and less than 4 characters for FPE_AES.

Attribute	Default Value	Mandatory/Optional	Description
			Note: • <code>allowSingleCharInputs</code> is not applicable to DPG initial encryption as DPG doesn't support single characters. • To provide backward compatibility, <code>allowSingleCharInputs</code> is also supported, but it is recommended to use <code>allowSmallInputs</code>.
keepleft	No default	Optional	Number of characters to be preserved from left. It is applicable only if @type is FPE or FF1 or FPE_AES.
keepright	No default	Optional	Number of characters to be preserved from right. It is applicable only if @type is FPE or FF1 or FPE_AES.
policyVersion	0	Optional	Specifies the protection policy version information. If policy version > 0, then the version header in hex will be prepended to the ciphertext. If not, then no policy version header will be prepended to the ciphertext. Note: Applicable only for DPG initial encryption.
iv	No default	Mandatory (if @type is AES_CBC_PAD or AES_CTR or DESede with mode as CBC)	Initialization Vector. Refer to supported encryption algorithms for details. Note: • It is recommended to specify random generated IV, and do not reuse any IV.

Attribute	Default Value	Mandatory/Optional	Description
			• IV is not applicable (if @type is FPE or FF1 or DESede with mode as ECB).
ivSource	No default	Optional	Specifies a column in the source for the IV, to allow different IVs to be used for each row. For example: <code>"ivSource": "columnName"</code>. Value to be specified in hexadecimal format. For example: 01A40933B401A409. If value is not valid hexadecimal, then it is treated as an ASCII string. ivSource is not supported when inplaceUpdate is set to true. Note: It is recommended to specify random generated IV, and do not reuse any IV.
inputEncoding	No default	Optional	Specifies how to decode input and create byte array from it. Valid options are BASE2, BASE16, BASE64, UTF8, UTF16LE, UTF16BE, UTF32LE, or UTF32BE. — The inputEncoding attribute is not used by the FPE algorithm; BDT internally uses UTF-8. —BASE2 is supported only with database Blob data type columns.
outputEncoding	No default	Optional	Specifies how to encode output byte array to a string. Valid options are BASE16, BASE64, UTF8,

Attribute	Default Value	Mandatory/Optional	Description
			UTF16LE, UTF16BE, UTF32LE, or UTF32BE. — The outputEncoding attribute is not used by FPE algorithm; BDT internally uses UTF-8.
mode	No default	Mandatory (if @type is DESede)	Specifies the supported algorithm mode, either CBC or ECB. The mode must be specified when using the DESede (that is, the 3DES) algorithm (as specified by the @type attribute). DESede means DES encrypt-decrypt-encrypt, a common synonym for 3DES that summarizes the basic three-step process underlying it. Note: ECB mode is not recommended.
padding	No default	Mandatory (if @type is DESede)	Valid options are PKCS5Padding or NoPadding. Note: padding is supported (if @type is DESede). Refer to Supported Encryption Algorithms for details.

TOKENIZE/DETOKENIZE Actions

Attribute	Default Value	Mandatory/Optional	Description
@type	No default	Mandatory	Valid value is TOKENIZE.
tokenGroup	No Default	Mandatory (if action is TOKENIZE or DETOKENIZE)	Name of the token group as defined in VTS.
tokenTemplate	No Default	Mandatory (if action is TOKENIZE or DETOKENIZE)	Name of the token template as defined in VTS.

Attributes to Transform a Subset of Records

Attribute	Default Value	Mandatory/Optional	Description
offset	0	Optional	Start record index.
limit	No default	Mandatory (if filtering data for transformation)	Maximum number of records/rows to transform, starting from <code>offset</code> .
recurrency	1	Optional	Select every Nth record. Default is 1 (process every record).
orderBy	First column	Optional	Order by column, for example: <code>column1</code> . Not supported for file transformation.
order	ASC	Optional	ASC (ascending) or DESC (descending) record order. Not supported for file transformation.
filters	No default	Mandatory (if filtering data for transformation)	Subset-specific filters to be used.

Attributes to Filter a Subset

Attribute	Default Value	Mandatory/Optional	Description
selector	No default	Mandatory (if filtering data for transformation)	Column name.
operator	No default	Mandatory (if filtering data for transformation)	Options: "=", "<", ">", "<=", ">=", "!=", "like".
expression	No default	Mandatory (if filtering data for transformation)	Expression to evaluate filter on selector using specified operator.

The following is a sample policy file excerpt for table attributes (Subset, Offset, Limit, Filters, Selector, Operator, Expression) meant for filtering input data:

```
"subset":{
  "offset":"10",
  "limit":1000,
  "filters":[
    {
      "selector":"salary",
      "operator":">",
      "expression":"10000"
    },
    {
      "selector":"name",
      "operator":"like",
```

```

    "expression":"'p%'"
  }
]
}

```

Encryption Key Versioning

Encryption key versioning allows developers to simplify their applications by requesting automated key version advances, changing the key material automatically (“rekeying,” or “rotation”), and placing the current version of the key in the header of the encrypted data.

Note

Versioned keys are supported when using Vormetric Data Security Manager (DSM) with Vormetric Application Encryption (VAE). Versioned keys are not supported:

- With DESede encryption.
- When using CipherTrust Application Data Protection (CADP-JCE) with the CipherTrust Manager as a key manager.

BDT detects the key version from the header that is prefixed with cipher text. Configure header version with the `header` table attribute along with with `action` configuration in the policy file. You can specify different header versions for different columns. Valid combinations are shown below:

Supported Header Versions per Encryption Mode

Header	AES_CBC_PAD	AES_CTR	FPE/FF1
v 1.5	Yes	No	No
v 1.5 Base 64	Yes	No	No
v 2.1	Yes	Yes	No
v 2.7	Yes	Yes	No

The following shows policy code for a versioned key:

```

"columns": [
  {
    "name": "COLUMN0",
    "action": "REKEY",
    "config": [
      {
        "@type": "AES_CTR",
        "action": "DECRYPT",
        "key": "bdtVersionKey",
        "iv": "010203040506070809100A0B0C0D0E0F",
        "header": "V2_1"
      }
    ]
  }
]

```

```

    },
    {
      "@type": "AES_CTR",
      "action": "ENCRYPT",
      "key": "bdtVersionKey",
      "iv": "010203040506070809100A0B0C0D0E0F",
      "header": "V2_7"
    }
  ]
}
]

```

Configure TLS for use with CipherTrust Vaultless Tokenization (CT-VL)

Authentication can be done using server authentication or using client authentication. The end user can do either, both, or none of them.

Users can configure TLS in one of the following ways:

- Configure SSL using Default Settings
- Configure SSL using all Certificates
- Configure SSL using Specified Certificates

Setting up SSL using `Default` Setting

CT-VL Server Authentication

1. Go to the `mts{}` section of the `bdtd.config` file.
2. Specify the following values for the `server{}` object commands:
 - `sslmode`: **Default**. Indicates trust only a standard valid certificate issued by a Certificate Authority (CA). If the certificate is expired, self-signed, or invalid, communication with the CT-VL server fails. The other `sslmode` values available for CT-VL server authentication are `Allow-All` and `Specify_SSL_Cert`. Refer to [Configuring TLS](#) for details.
 - `VerifyHostName`: By default, it is set to **true** to enable hostname verification for SSL communication.

CT-VL Client Authentication

1. Go to the `mts{}` section of the `bdtd.config` file.
2. Specify the following values for the `client{}` object commands:
 - `sslmode`: **Default**. Indicates client authentication is disabled. No need to send client identity. The other `sslmode` values available for CT-VL client authentication are `Allow-All` and `Specify_SSL_Cert`.

Refer to [Configuring TLS](#) for details.

- `keystore`: **Client keystore file path**. This assumes a keystore has already been created; for example, using `keytool`.
- `storepassword`: **Client keystore file password**.
- `keypassword`: **Client's key password**.

Setting up SSL using `Allow-All` Setting

User can opt for server and client authentication by configuring `bdt.config`.

Perform the following steps to set up SSL for secure communication between the BDT utility and the CipherTrust Vaultless Tokenization (CT-VL) using all trust certificates:

CT-VL Server Authentication

1. Go to the `mts{}` section of the `bdt.config` file.
2. Specify the following values for the `server{}` object commands:
 - `sslmode`: Select **Allow-All**. Indicates Trust all certificates; no trust policy is defined. Any kind of SSL certificate is acceptable, including valid, expired, self-signed, or any other. The truststore setting is not required.
 - `VerifyHostName`: By default, it is set to **true** to enable hostname verification for SSL communication.

CT-VL Client Authentication

1. Go to the `mts{}` section of the `bdt.config` file.
2. Specify the following values for the `client{}` object commands:
 - `sslmode`: Select **Allow-All**. Indicates client authentication is disabled and there is no need to send client identity.

When passing `sslmode` as **ALLOW_ALL**, you don't need to configure following 3 params:

- `keystore`: **Client keystore file path**. This assumes a keystore has already been created; for example, using `keytool`.
- `storepassword`: **Client keystore file password**.
- `keypassword`: **Client's key password**.

Setting up SSL using `Specify_SSL_Cert` Setting

Perform the following steps to set up SSL for secure communication between the BDT utility and the CipherTrust Vaultless Tokenization (CT-VL) using valid certificates:

CT-VL Server Authentication

1. Go to the `mts{}` section of the `bdm.config` file.
2. Specify the following values for the `server{}` object commands:
 - `sslmode`: Select **Specify_SSL_Cert**. Indicates trust standard certificates and certificates stored in the provided trust store (specified in the truststore setting). Use to accept self-signed and expired certificates.
 - `VerifyHostName`: By default, it is set to **true** to enable hostname verification for SSL communication. Set to "false" to disable hostname verification.
 - `truststore`: Truststore file path. To set up the truststore:
 - Get the server's public certificate. If not available, open the VTS URL in a browser and export it from the Security option.
 - Import the certificate and create the truststore. Use the following command, it will output the truststore password.

```
keytool -import -alias "mts host certificate" -file server.crt -keystore server.truststore
```

Important: Note this password. You need to provide it in the password parameter.

- `password`: Truststore file password obtained when you imported the VTS certificate and created the truststore.

CT-VL Client Authentication

1. Go to the `mts{}` section of the `bdm.config` file.
2. Specify the following values for the `client{}` object commands:
 - `sslmode`: **Specify_SSL_Cert** Indicates Client authentication is enabled. Create keystore with client certificate and key. Set keystore path in the keystore parameter. Communication succeeds if the VTS server finds a valid certificate set in the keystore.
 - `Keystore`: **Client keystore file path**. This assumes a keystore has already been created; for example, using `keytool`.
 - `storepassword`: **Client keystore file password**.

- `keypassword`: Client's key password.

Configure SSL on CipherTrust Manager for NAE Interface

SSL with Server Certificate Authentication

When communicating with the CipherTrust Manager, you must configure both the server and the client to have SSL with server certificate authentication.

Configure the server

1. Create a local Certificate Authority (CA) on the CipherTrust Manager management console.
2. Create a server certificate and sign it with the local CA.
3. Configure the NAE interface.

Configure the client

1. Add the local CA Certificate, downloaded from the CipherTrust Manager management console, to keystore.
2. Update the `bdt.properties` file.

Create Local CA on CipherTrust Manager

1. Log on to the CipherTrust Manager management console as an administrator.
2. Click the **CA** tab on the left.
3. Under Local Certificate Authorities section, click **New Local CA**.
4. On the New Local CA screen, enter or select the details as required (The Common Name parameter is mandatory).
5. Click **Create Local CA**. The local CA created is listed beside the Pending CAs label.
6. Click the local CA beside the Pending CAs label. The local CA with its detail is displayed on screen.
7. Set the Duration for the local CA. You can either self-sign the certificate or upload an external CA to sign the local CA. The CA gets listed in the Local Certificate Authorities section.

Note

Only a local CA can sign certificate on the CipherTrust Manager. If you are using a CA that does not reside on the CipherTrust Manager, you cannot use the Management Console to sign the sever/client certificate.

-
- Click the ellipsis icon corresponding to local CA and then click the download button to download the local CA certificate. Save the certificate in .pem format in the system where BDT is used.

Create a Certificate on CipherTrust Manager

- Log on to the CipherTrust Manager management console as an administrator.
- Click the **CA** tab on the left.
- Navigate to the Local Certificate Authorities section and click on the name of local CA (under the heading Subject) using which you want to generate and sign the certificate.
- Click **Create New Certificate**. The Create New Certificate screen is displayed.
- Enter or select the details as required (Common Name parameter is mandatory).
- Click **New Certificate*.
- Click save private key to download and save the private key with .pem extension.
- From the Certificate Purpose drop-down, select server.
- Click **Issue Certificate**.
- The server certificate is created and gets signed with the local CA. This certificate can be used as the server certificate for the NAE server.
- Click the ellipsis icon corresponding to the server certificate and then click the download button to save the server certificate in .pem format.

Configure Interface on CipherTrust Manager

- Log on to the CipherTrust Manager management console as an administrator.
- Click to expand **Admin Settings** and then click **Interfaces**.
- On the Interface Configurations page, click **Add Interface**.
- On the Configure Interface tab, select the **Interface Type** as **NAE** and click **Next**.
- On the Network Form screen, enter/select the following details :
 - Select the **Allow unregistered clients** check-box.
 - Enter the port.
 - Select the desired **Network Interface** from the available options.
 - Select the **TLS, user must supply password, verify client cert** option from the drop-down list.

- click **Next**.

6. On the Add Certificate tab, enter/select the details.

- In the Username Location in Certificate, enter CN.
- In the Local CA for Automatic Server Certificate Generation field, select **Turn off auto generation from a Local CA**.
- Select Local Trusted CAs.
- If available, select External Trusted CAs.
- Click **Save**.

Note

Restart the application (Settings >> Services >> Restart button) after interface is configured.

Add the Local CA Certificate to Keystore

Run the following command to add the local CA certificate downloaded from CipherTrust Manager to the keystore:

```
keytool -keystore <name_of_the_keystore> -import -alias <alias_name_of_CAcertificate> -file
</certificate_location/LocalCA_certificate_file.pem>
```

Update bdt.properties File

Update the following parameters in the bdt.properties file:

- NAE_Port=Specify the port used by CipherTrust Manager for SSL connection.
- Protocol=Set it to ssl.
- Key_Store_Location=Location of the keystore . For example /tmp/KYLO_utility_keystore/cacerts, where /tmp/KYLO_utility_keystore/ is the keystore path and cacert is the keystore name. For windows machine, the keystore path will be \\tmp\\KYLO_utility_keystore\\cacerts.
- Key_Store_Password=Password of the keystore.

SSL with Client Certificate Authentication

This section describes the procedures to follow when configuring SSL with Client Certificate Authentication. It explains the following processes:

-
- Generating a Client Certificate with Keytool
 - Signing a Certificate and Downloading the Certificate
 - Configuring TLS Option in NAE Interface
 - Adding the Client Certificate to the Java Keystore
 - Updating the Parameters in bdt.properties

Generate Client Certificate with Keytool

1. Open a command prompt window on your client and navigate to the Java security directory (`<Java_Home>\lib\security`).
2. Generate a public/private key pair by executing the following command. In this step, an alias for the key pair is created.

```
keytool -keystore <KeystoreName> -genkey -alias <KeyPairAlias> -keyalg RSA
```

3. The key generation process will then request the following data:
 - A keystore password
 - The distinguished name - This is a series of fields whose values are incorporated into the certificate request. These fields include country name, state or province name, city or locality name, organization name, organizational unit name, and the users first and last name.
 - The key password- The certificate password must be the same as the keystore password. You can simply hit Return/Enter key to set the password. You need not retype the keystore password.
4. Create the certificate by issuing the following command. Reference the key pair alias, created in step 2.

```
keytool -certreq -alias <KeyPairAlias> -file <CertReqFileName> -keystore <KeystoreName>
```

You will now have a certificate in the `<CertReqFileName>` file.

Sign and Download Certificate

This section describes how to sign a certificate with a local CA and then download the certificate. You must download the certificate immediately after it is signed by the CA.

1. Open the certificate request in a text editor.
2. Copy the text of the certificate request. The copied text must include the header (-----BEGIN CERTIFICATE REQUEST-----) and the footer (-----END CERTIFICATE REQUEST-----).

3. Log on to the CipherTrust Manager management console as an administrator.
4. Click the **CA** tab on the left.
5. In the Local Certificate Authorities section, click the **Subject** corresponding to the local CA with which you want to sign the certificate.
6. Click **Upload and Sign CSR**.
7. Paste the text of the certificate in the text field highlighted as Paste external CSR here in PEM format.
8. Select Certificate Purpose as client and specify the life span of the certificate in days in Duration in days field.
9. Click **Issue Certificate**.
10. Click download button against the certificate to be downloaded.
11. Save the certificate in the machine where BDT is installed.

Configure TLS Option in NAE Interface

1. Log on to the CipherTrust Manager management console as an administrator.
2. Click to expand **Admin Settings** and then click **Interfaces**.
3. Click the edit button under column **Action** against the nae interface. The Configure NAE popup window is displayed.
4. In the **Mode** field, select the **TLS, user must supply password, verify client cert** option.
5. Click **Update**.

Note

Restart the application (Settings >> Services >> Restart button) after the TLS option is updated.

Add Client Certificate to Java Keystore

1. Open a command prompt window on your client and navigate to the Java security directory (\\lib\\security).
2. Import the signed client certificate using the following command. Use the key pair alias you used to create the certificate request. When prompted, enter the keystore password.

```
keytool -keystore <KeystoreName> -alias <KeyPairAlias> -import -file <Cert  
FileName.pem>
```

- Verify that the client certificate was properly imported by executing the following command. Reference the key pair alias you used above. The system should display the certificate.

```
keytool -keystore <KeystoreName> -alias <KeyPairAlias> -list -v
```

Note

To enable Client Certificate Authentication, your keystore must have a copy of the CA certificate downloaded from CipherTrust Manager management console.

Update bdt.properties File

Update the following parameters in the bdt.properties file:

- Key_Store_Location=Location and name of keystore that contains a copy of the server's local CA, the client certificate, and the CA that signed the client certificate. For example `/tmp/KYLO_utility_keystore/cacerts`, where `/tmp/KYLO_utility_keystore/` is the keystore path and `cacerts` is the keystore. For windows machine, the keystore path will be `\\tmp\\KYLO_utility_keystore\\cacerts`.
- Key_Store_Password=Password associated with the keystore.
- Client_Cert_Alias=<client certificate alias>.
- Client_Cert_Passphrase=<client certificate password, if used>

FPE/AES/Unicode Cardinality Block-Size Table

This table provides the cardinality size and the corresponding IV/block-size for the FPE/AES/Unicode usage. In FPE/AES/Unicode, the cardinality and IV/block-size is defined in character length.

Cardinality	IV/Block-size
10	56
11	54
12	52
13	50
14	50
15	48
16	48
17	46
18	46

Cardinality	IV/Block-size
19	44
20	44
21	42
22	42
23	42
24	40
25	40
26	40
27	40
28	38
29	38
30	38
31	38
32	38
33	38
34	36
35	36
36	36
37	36
38	36
39	36
40	36
41	34
42	34
43	34
44	34
45	34
46	34
47	34
48	34
49	34
50	34
51	32

Cardinality	IV/Block-size
52	32
53	32
54	32
55	32
56	32
57	32
58	32
59	32
60	32
61	32
62	32
63	32
64	32
65	30
66	30
67	30
68	30
69	30
70	30
71	30
72	30
73	30
74	30
75	30
76	30
77	30
78	30
79	30
80	30
81	30
82	30
83	30
84	30

Cardinality	IV/Block-size
85	28
86	28
87	28
88	28
89	28
90	28
91	28
92	28
93	28
94	28
95	28
96	28
97	28
98	28
99	28
100	28
101	28
102	28
103	28
104	28
105	28
106	28
107	28
108	28
109	28
110	28
111	28
112	28
113	28
114	28
115	28
116	26
117	26

Cardinality	IV/Block-size
118	26
119	26
120	26
121	26
122	26
123	26
124	26
125	26
126	26
127	26
128	26
129	26
130	26
131	26
132	26
133	26
134	26
135	26
136	26
137	26
138	26
139	26
140	26
141	26
142	26
143	26
144	26
145	26
146	26
147	26
148	26
149	26
150	26

Cardinality	IV/Block-size
151	26
152	26
153	26
154	26
155	26
156	26
157	26
158	26
159	26
160	26
161	26
162	26
163	26
164	26
165	26
166	26
167	26
168	24
169	24
170	24
171	24
172	24
173	24
174	24
175	24
176	24
177	24
178	24
179	24
180	24
181	24
182	24
183	24

Cardinality	IV/Block-size
184	24
185	24
186	24
187	24
188	24
189	24
190	24
191	24
192	24
193	24
194	24
195	24
196	24
197	24
198	24
199	24
200	24
201	24
202	24
203	24
204	24
205	24
206	24
207	24
208	24
209	24
210	24
211	24
212	24
213	24
214	24
215	24
216	24

Cardinality	IV/Block-size
217	24
218	24
219	24
220	24
221	24
222	24
223	24
224	24
225	24
226	24
227	24
228	24
229	24
230	24
231	24
232	24
233	24
234	24
235	24
236	24
237	24
238	24
239	24
240	24
241	24
242	24
243	24
244	24
245	24
246	24
247	24
248	24
249	24

Cardinality	IV/Block-size
250	24
251	24
252	24
253	24
254	24
255	24

Samples

This section contains the following topics

- [Sample BDT Policy File](#)
- [Sample BDT Config File](#)

Sample BDT Policy File

Consolidated Policy

```
{
  "id" : "SqlServerSample-90643295a90sdf5",          /* Transformation policy id.
*/
  "name" : "SqlServerSample",                      /* Name of the policy. */
  "description" :                                  /* Description of the polic
y. */
  "caseSensitive" : true,                          /* True or false. Default va
lue is false. If set to "true", all the database objects mentioned in the policy
file will be processed in the same case as input. If set to "false", all the data
base objects mentioned in the policy file will be automatically converted to UPPE
RCASE. */
  "trimSpaces" : true,                            /* True or false. Default va
lue is false. If set to "true", it will trim initial and trailing white spaces fr
om the data present in the column to be transformed. If set to "false", the flag
is disabled, and no processing is done on the data present in the column to be tr
ansformed. */
  "enableHexLiteral" : false,                     /* True or false. Default va
lue is false. If set to "true", the ciphertext will be enclosed with hex literal.
For example, x'<ciphertext>'. */
  "source": {                                     /* Details of the data sourc
e. */
    "@type": "CSV_FILE",                         /* Source type. Supports CS
V_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "input.csv",                     /* The file path relative to
the inputDir or outputDir path in the config file. */
    "delimiter": ",",                            /* The character that is use
d to divide one column from the next in the input file. */
    "qualifier": "\"",                          /* The character to enclose
fields that contain a delimiter character. This is used when source is a file and
```


the delimiter character is itself a part of the data to be transformed. So to tell BDT that this is not a delimiter, user can enclose input data by a qualifier and mention qualifier here in this field. */

```
"unescapeInput": false, /* True or false. Default value is false. If "true", delimiter and qualifier characters in input preceded by a backslash (\) are considered as normal characters and part of the input data. */
```

```
"columnCount": "5", /* Number of columns in the input file. */
```

```
"hasHeaderRow": false /* True or false. Default value is false. If "true", the utility will treat the first row as a header row. Values from this row will be treated as column names. The same column names should be mentioned in the transformation action. If "false", the utility will treat all the rows as data to be transformed. */
```

```
},
"destination": { /* Details of the data destination. */
```

```
"@type": "CSV_FILE", /* Destination type. Supports CSV_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
```

```
"filepath": "output.csv" /* The file path relative to the inputDir or outputDir path in the config file. */
```

```
},
"tables" : [ { /* List of the tables to be transformed. */
```

```
"sourceSchema" : "DEMO", /* Owner/schema name where source table belongs to, otherwise it will use default owner/schema. */
```

```
"destinationSchema" : "DEMOdes", /* Owner/schema name where destination table belongs to, otherwise it will use default owner/schema. */
```

```
"columns" : [ { /* List of the columns to be transformed. */
```

```
"name" : "FirstName", /* Name of the column. */
```

```
"action" : "ENCRYPT", /* Specifies the action to be taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
```

```
"config" : [ { /* Configuration for Encryption or Tokenization operations. */
```

```
"@type" : "FPE", /* Config type. Supports AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
```

```
"key" : "key1", /* Name of the encryption key. */
```

```
"characterSet" : "alphanumeric", /* Name of the charset. */
```

```
"tweak" : "010ACD5B99F3C343", /* Used for column level tweak data. */
```

```
"allowSmallInputs" : false, /* True or false. Default is false. Applicable to FPE, FF1, and FPE_AES only. If true, data is passed as untransformed if effective data length is less than 2 characters for FPE and FF1, and less than 4 characters for FPE_AES. If false, transformation fails if effective data length is less than 2 characters for FPE and FF1, and less than 4 characters for FPE_AES. */
```

```
"keepleft" : 0, /* Number of characters to be preserved from left. It is applicable only if @type is FPE or FF1 or FPE_AES. */
```

```
"keepright" : 0, /* Number of characters to be preserved from right. It is applicable only if @type is FPE or FF1 or FPE_AES. */
```

```
"policyVersion": 1 /* Specifies version information of the protection policy. Applicable only for DPG initial encryption. */
```

```
} ]
```

```
} ,
```

```
{
```

```

        "name" : "LastName",                                /* Name of the column. */
        "action" : "DECRYPT",                                /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
        "config" : [ {                                     /* Configuration for Encrypt
ion or Tokenization operations. */
            "@type" : "AES_CBC_PAD",                        /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
            "key" : "key1",                                  /* Name of the encryption ke
y. */
            "iv" : "01020304050607080102030405060708",    /* Initialization Vector. It
is recommended to specify random generated IV, and do not reuse any IV. */
            "header": ""                                     /* Used only when encryptin
g/decrypting using VAE. */
            "inputEncoding" : 0,                             /* Encoding of Input data.
*/
            "outputEncoding" : 0,                           /* Encoding of output data.
*/
            "policyVersion": 1                               /* Specifies version informa
tion of the protection policy. Applicable only for DPG initial encryption. */
        } ],
    },
    {
        "name" : "GENDER",                                  /* Name of the column. */
        "action" : "ENCRYPT",                                /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
        "config" : [ {                                     /* Configuration for Encrypt
ion or Tokenization operations. */
            "@type" : "DESede",                              /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
            "key" : "key1",                                  /* Name of the encryption ke
y. */
            "iv" : "01020304050607080102030405060708",    /* Initialization Vector. It
is recommended to specify random generated IV, and do not reuse any IV. */
            "ivSource" : "IV_Col",                          /* Specifes a column in the
source for the IV, to allow different IVs to be used for each row. Value to be sp
ecified in hexadecimal format. If value is not valid hexadecimal, then it is trea
ted as an ASCII string. */
            "mode": "CBC",                                   /* Used only when type is DE
Sede. */
            "inputEncoding" : 0,                             /* Encoding of Input data.
*/
            "outputEncoding" : 0,                           /* Encoding of output data.
*/
            "padding": "PKCS5Padding"                       /* Used only when type is DE
Sede. */
        } ],
    },
    {
        "name" : "EmergencyContact",                        /* Name of the column. */
        "targetColName" : " EmergencyContact _new",        /* Name of the new column.
*/
        "srcColumnAction" : "preserve",                     /* Source column remains pre
served. */
        "action" : "ENCRYPT",                                /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
        "config" : [ {                                     /* Configuration for Encrypt
ion or Tokenization operations. */
            "@type" : "FPE_AES",                             /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */

```

```

        "key" : "KEY1",                                /* Name of the encryption ke
y. */
        "characterSet" : "alphanumeric",                /* Name of the charset. */
        "tweak" : "010ACD5B99F3C343",                  /* Used for column level twe
ak data. */
        "tweakAlgo" : "SHA1",                           /* Specifies tweakAlgo. Supp
orts SHA1/SHA256/NONE. */
        "allowSmallInputs" : false,                     /* True or false. Default is
false. Applicable to FPE, FF1, and FPE_AES only. If true, data is passed as untra
nsformed if effective data length is less than 2 characters for FPE and FF1, and
less than 4 characters for FPE_AES. If false, transformation fails if effective d
ata length is less than 2 characters for FPE and FF1, and less than 4 characters
for FPE_AES. */
        "keepleft" : 2,                                /* Number of characters to b
e preserved from left. It is applicable only if @type is FPE or FF1 or FPE_AES.
*/
        "keepright" : 3,                               /* Number of characters to b
e preserved from right. It is applicable only if @type is FPE or FF1 or FPE_AES.
*/
        "policyVersion" : 0                             /* Specifies the protection
policy version information. */
    } ]
},
{
    "name" : "ContactNo",                                /* Name of the column. */
    "action" : "REKEY",                                  /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    "config" : [ {                                       /* Configuration for Encrypt
ion or Tokenization operations. */
        "@type" : "FPE",                                /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
        "key" : "key1",                                /* Name of the encryption ke
y. */
        "characterSet" : "alphanumeric",                /* Name of the charset. */
        "tweakSource" : "Col_Tweak",                   /* Used for column level twe
ak data. */
        "allowSmallInputs" : false,                     /* True or false. Default is
false. Applicable to FPE, FF1, and FPE_AES only. If true, data is passed as untra
nsformed if effective data length is less than 2 characters for FPE and FF1, and
less than 4 characters for FPE_AES. If false, transformation fails if effective d
ata length is less than 2 characters for FPE and FF1, and less than 4 characters
for FPE_AES. */
        "keepleft" : 0,                                /* Number of characters to b
e preserved from left. It is applicable only if @type is FPE or FF1 or FPE_AES.
*/
        "keepright" : 0,                               /* Number of characters to b
e preserved from right. It is applicable only if @type is FPE or FF1 or FPE_AES.
*/
        "policyVersion": 1,                             /* Specifies version informa
tion of the protection policy. Applicable only for DPG initial encryption. */
        "action" : "DECRYPT"                             /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    }, {
        "@type" : "FPE",                                /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
        "key" : "key2",                                /* Name of the encryption ke
y. */
        "characterSet" : "alphanumeric",                /* Name of the charset. */
        "tweakSource" : "Col_Tweak",                   /* Used for column level twe

```

```

ak data. */
    "allowSmallInputs" : false,                /* True or false. Default is
false. Applicable to FPE, FF1, and FPE_AES only. If true, data is passed as untra
nsformed if effective data length is less than 2 characters for FPE and FF1, and
less than 4 characters for FPE_AES. If false, transformation fails if effective d
ata length is less than 2 characters for FPE and FF1, and less than 4 characters
for FPE_AES. */
    "keepleft" : 0,                            /* Number of characters to b
e preserved from left. It is applicable only if @type is FPE or FF1 or FPE_AES.
*/
    "keepright" : 0,                           /* Number of characters to b
e preserved from right. It is applicable only if @type is FPE or FF1 or FPE_AES.
*/
    "policyVersion": 1,                        /* Specifies version informa
tion of the protection policy. Applicable only for DPG initial encryption. */
    "action" : "ENCRYPT"                        /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
} ]
},
{
    "name" : "GENDER",                         /* Name of the column. */
    "action" : "TOKENIZE",                     /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    "config" : [ {                             /* Configuration for Encrypt
ion or Tokenization operations. */
        "@type" : "TOKENIZE",                 /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
        "tokenGroup" : "tokengp",            /* Used only when action is
TOKENIZE or DETOKENIZE. */
        "tokenTemplate" : "tokentemp"        /* Used only when action is
TOKENIZE or DETOKENIZE. */
    } ]
},
{
    "name" : "Address",                       /* Name of the column. */
    "action" : "DETOKENIZE",                  /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    "config" : [ {                             /* Configuration for Encrypt
ion or Tokenization operations. */
        "@type" : "TOKENIZE",                 /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
        "tokenGroup" : "tokengp",            /* Used only when action is
TOKENIZE or DETOKENIZE. */
        "tokenTemplate" : "tokentemp"        /* Used only when action is
TOKENIZE or DETOKENIZE. */
    } ]
},
{
    "name" : "Account",                       /* Name of the column. */
    "action" : "REKEY",                       /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    "config" : [ {                             /* Configuration for Encrypt
ion or Tokenization operations. */
        "@type" : "TOKENIZE",                 /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
        "tokenGroup" : "group1",             /* Used only when action is
TOKENIZE or DETOKENIZE. */
        "tokenTemplate" : "abcdef9876543210", /* Used only when action is
TOKENIZE or DETOKENIZE. */

```

```

        "action" : "DETOKENIZE"                                /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    }, {
        "@type" : "TOKENIZE",                                  /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
        "tokenGroup" : "group2",                               /* Used only when action is
TOKENIZE or DETOKENIZE. */
        "tokenTemplate" : "abcdef9876543210",                 /* Used only when action is
TOKENIZE or DETOKENIZE. */
        "action" : "TOKENIZE"                                  /* Specifies the action to b
e taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    } ]
    },
    "subset" : {                                                /* Table-specific data filte
r criteria. Filter input data based on this criteria. */
        "offset": 0,                                           /* Start record index. */
        "limit":5,                                             /* Maximum number of record
s/rows to transform, starting from offset. */
        "recurrency" : 3,                                       /* Select every Nth record.
Default is 1 (process every record). */
        "orderBy" : "OrderByCol",                               /* Order by column, for exam
ple: column1. Not supported for file transformation. */
        "order" : "ASC",                                         /* ASC (ascending) or DESC
(descending) record order. Not supported for file transformation. */
        "filters" : [{                                          /* Subset-specific filters t
o be used. */
            "selector" : "SelectorCol",                         /* Name of the column. */
            "operator" : ">",                                     /* Specifies the operator to
use. */
            "expression": "34"                                   /* Expression to evaluate fi
lter on selector using specified operator. */
        }]
    },
    "createDestinationTable" : false,                           /* Create destination table
if none exists. */
    "sourceTable" : "demoSource",                               /* Source table name. For da
tabase only. */
    "destinationTable" : "demoDes"                             /* Destination table name. F
or database only. */
    },
    "inPlaceUpdate" : false,                                     /* Set to true to transform
data in-place within the database (that is, in-place transformation), rather than
the default behavior that creates a new destination table containing the transfor
med data. */
    "createBadRecordFile" : true                                /* True or false. Default va
lue is false. Set to "true" to create a ".failed file", otherwise set to "false".
*/
}

```

DPG Migration

```

{
    "id": "FPE_transformation_encryption",                     /* Transformation policy id. */
    "name": "FPE_transformation_encryption",                   /* Name of the policy. */
    "createBadRecordFile": true,                               /* True or false. Set to true to crea
te a file with .failed extension, otherwise set to false. */
    "source": {                                                 /* Details of the data source. */

```

```

    "@type": "CSV_FILE", /* Source type. Supports CSV_FILE, FI
XED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "input.csv", /* The file path relative to the inpu
tDir or outputDir path in the config file. */
    "delimiter": ",", /* The character that is used to divi
de one column from the next in the input file. */
    "qualifier": "\"", /* The character to enclose fields th
at contain a delimiter character. This is used when source is a file and the deli
miter character is itself a part of the data to be transformed. So to tell BDT th
at this is not a delimiter, user can enclose input data by a qualifier and mentio
n qualifier here in this field. */
    "unescapeInput": "true", /* True or false. Default value is fa
lse. If "true", delimiter and qualifier characters in input preceded by a backsla
sh (\) are considered as normal characters and part of the input data. */
    "columnCount": "12", /* Number of columns in the input fil
e. */
    "hasHeaderRow": true /* True or false. Default value is fa
lse. If "true", the utility will treat the first row as a header row. Values from
this row will be treated as column names. The same column names should be mention
ed in the transformation action. If "false", the utility will treat all the rows
as data to be transformed. */
  },
  "destination": { /* Details of the data destination.
*/
    "@type": "CSV_FILE", /* Destination type. Supports CSV_FIL
E, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "output.csv" /* The file path relative to the inpu
tDir or outputDir path in the config file. */
  },
  "tables": [ /* List of the tables to be transform
ed. */
    {
      "columns": [ /* List of the columns to be transfor
med. */
        {
          "name": "latitude", /* Name of the column. */
          "action": "ENCRYPT", /* Specifies the action to be taken.
Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
          "config": [ /* Configuration for Encryption or To
kenization operations. */
            {
              "@type": "FPE", /* Config type. Supports AES_CBC_PAD,
AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
              "key": "bdt_key", /* Name of the encryption key. */
              "tweak": "1ABD0EAB12F34560", /* Used for column level tweak data.
*/
              "characterSet": "digits", /* Name of the charset. */
              "policyVersion": 1 /* Specifies version information of t
he protection policy. Applicable only for DPG initial encryption. */
            }
          ]
        }
      ]
    }
  ]
}

```

Encrypt/Decrypt/Rekey

Encrypt

```
{
  "id": "FPE_transformation_encryption",      /* Transformation policy id. */
  "name": "FPE_transformation_encryption",    /* Name of the policy. */
  "createBadRecordFile": true,                /* True or false. Set to true to crea
  te a file with .failed extension, otherwise set to false. */
  "source": {                                /* Details of the data source. */
    "@type": "CSV_FILE",                     /* Source type. Supports CSV_FILE, FI
  XED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "input.csv",                 /* The file path relative to the inpu
  tDir or outputDir path in the config file. */
    "delimiter": ",",                        /* The character that is used to divi
  de one column from the next in the input file. */
    "qualifier": "\"",                       /* The character to enclose fields th
  at contain a delimiter character. This is used when source is a file and the deli
  miter character is itself a part of the data to be transformed. So to tell BDT th
  at this is not a delimiter, user can enclose input data by a qualifier and mentio
  n qualifier here in this field. */
    "unescapeInput": "true",                 /* True or false. Default value is fa
  lse. If "true", delimiter and qualifier characters in input preceded by a backsla
  sh (\) are considered as normal characters and part of the input data. */
    "columnCount": "12",                     /* Number of columns in the input fil
  e. */
    "hasHeaderRow": true                     /* True or false. Default value is fa
  lse. If "true", the utility will treat the first row as a header row. Values from
  this row will be treated as column names. The same column names should be mention
  ed in the transformation action. If "false", the utility will treat all the rows
  as data to be transformed. */
  },
  "destination": {                            /* Details of the data destination.
  */
    "@type": "CSV_FILE",                     /* Destination type. Supports CSV_FIL
  E, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "output.csv"                 /* The file path relative to the inpu
  tDir or outputDir path in the config file. */
  },
  "tables": [                                 /* List of the tables to be transform
  ed. */
    {
      "columns": [                            /* List of the columns to be transfor
  med. */
        {
          "name": "latitude",                 /* Name of the column. */
          "action": "ENCRYPT",                 /* Specifies the action to be taken.
  Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
          "config": [                         /* Configuration for Encryption or To
  kenization operations. */
            {
              "@type": "FPE",                 /* Config type. Supports AES_CBC_PAD,
  AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
              "key": "bdt_key",               /* Name of the encryption key. */
              "tweak": "1ABD0EAB12F34560",   /* Used for column level tweak data.
  */
              "characterSet": "digits"        /* Name of the charset. */
            }
          ]
        }
      ]
    }
  ]
}
```

```

    ]
  }
]
}

```

Decrypt

```

{
  "id": "FPE_transformation_decryption",          /* Transforma
tion policy id. */
  "name": "FPE_transformation_decryption",        /* Name of th
e policy. */
  "createBadRecordFile": true,                    /* True or fa
lse. Set to true to create a file with .failed extension, otherwise set to false.
*/
  "caseSensitive": false                          /* True or fa
lse. Default value is false. If set to "true", all the database objects mentioned
in the policy file will be processed in the same case as input. If set to "fals
e", all the database objects mentioned in the policy file will be automatically c
onverted to UPPERCASE. */
  "source": {                                     /* Details of
the data source. */
    "@type": "ORACLE",                           /* Source typ
e. Supports CSV_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "connectionurl": "jdbc:oracle:thin:@//localhost:1521/XE", /* Database c
onnection URL. */
    "username": "admin",                          /* Database u
sername. */
    "password": "",                               /* Database p
assword. */
    "driverclass": "oracle.jdbc.driver.OracleDriver" /* DBC connec
tion driver class. */
  },
  "destination": {                               /* Details of
the data destination. */
    "@type": "SQL_SERVER",                        /* Destinati
on type. Supports CSV_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HAN
A. */
    "connectionurl": "jdbc:sqlserver://localhost;databaseName=db", /* Database c
onnection URL. */
    "username": "admin",                          /* Database u
sername. */
    "password": "",                               /* Database p
assword. */
    "driverclass": "com.microsoft.sqlserver.jdbc.SQLServerDriver" /* DBC connec
tion driver class. */
  },
  "tables": [                                     /* List of th
e tables to be transformed. */
    {
      "columns": [                               /* List of th
e columns to be transformed. */
        {
          "name": "latitude",                     /* Name of th
e column. */
          "action": "DECRYPT",                     /* Specifies
the action to be taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY.

```



```

*/
    "config": [                                     /* Configuratio
ion for Encryption or Tokenization operations. */
        {
            "@type": "FPE",                          /* Config typ
e. Supports AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
            "key": "bdt_key",                        /* Name of th
e encryption key. */
            "tweakSource": "col_tweak",              /* Used for c
olumn level tweak data. */
            "characterSet": "digits",                /* Name of th
e charset. */
            "keepleft" : 0,                          /* Number of
characters to be preserved from left. It is applicable only if @type is FPE or FF
1 or FPE_AES. */
            "kepright" : 0,                          /* Number of
characters to be preserved from right. It is applicable only if @type is FPE or F
F1 or FPE_AES. */
        }
    ],
    "subset" : {                                     /* Table-spec
ific data filter criteria. Filter input data based on this criteria. */
        "offset": 0,                                /* Start reco
rd index. */
        "limit":5,                                  /* Maximum nu
mber of records/rows to transform, starting from offset. */
        "recurrency" : 3,                           /* Select eve
ry Nth record. Default is 1 (process every record). */
        "orderBy" : "OrderByCol",                   /* Order by c
olumn, for example: column1. Not supported for file transformation. */
        "order" : "ASC",                            /* ASC (ascen
ding) or DESC (descending) record order. Not supported for file transformation.
*/
        "filters" : [{                             /* Subset-spe
cific filters to be used. */
            "selector" : "SelectorCol",              /* Name of th
e column. */
            "operator" : ">",                        /* Specifies
the operator to use. */
            "expression": "34"                       /* Expression
to evaluate filter on selector using specified operator. */
        }],
        "sourceTable":"employee",                   /* Source tab
le name. For database only.*/
        "destinationTable":"employee"               /* Destinatio
n table name. For database only.*/
    }
}

```

Rekey

```

{
    "id": "rekey_encryption_rekey",                  /* Transformation policy

```

```

id. */
  "name": "rekey_encryption_rekey", /* Name of the policy. */
  "createBadRecordFile": true, /* True or false. Set to
true to create a file with .failed extension, otherwise set to false. */
  "source": { /* Details of the data source. */
    "@type": "CSV_FILE", /* Source type. Supports
CSV_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "input.csv", /* The file path relative
to the inputDir or outputDir path in the config file. */
    "delimiter": ",", /* The character that is
used to divide one column from the next in the input file. */
    "qualifier": "\"\"", /* The character to enclose
fields that contain a delimiter character. This is used when source is a file
and the delimiter character is itself a part of the data to be transformed. So to
tell BDT that this is not a delimiter, user can enclose input data by a qualifier
and mention qualifier here in this field. */
    "unescapeInput": true, /* True or false. Default
value is false. If "true", delimiter and qualifier characters in input preceded by
a backslash (\) are considered as normal characters and part of the input data.
*/
    "columnCount": 4, /* Number of columns in the
input file. */
    "hasHeaderRow": true /* True or false. Default
value is false. If "true", the utility will treat the first row as a header row.
Values from this row will be treated as column names. The same column names should
be mentioned in the transformation action. If "false", the utility will treat all
the rows as data to be transformed. */
  },
  "destination": { /* Details of the data destination. */
    "@type": "CSV_FILE", /* Destination type. Supports
CSV_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "output.csv" /* The file path relative
to the inputDir or outputDir path in the config file. */
  },
  "tables": [ /* List of the tables to
be transformed. */
    {
      "columns": [ /* List of the columns to
be transformed. */
        {
          "name": "name", /* Name of the column. */
          "action": "REKEY", /* Specifies the action to
be taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
          "config": [ /* Configuration for Encryption or Tokenization operations. */
            {
              "@type": "AES_CBC_PAD", /* Config type. Supports
AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
              "key": "bdt_key", /* Name of the encryption
key. */
              "action": "DECRYPT", /* Specifies the action to
be taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
              "iv": "1ABD0EAB12F345601ABD0EAB12F34560" /* Initialization Vector.
It is recommended to specify random generated IV, and do not reuse any IV. */
            },
            {
              "@type": "AES_CTR", /* Config type. Supports

```

```

AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
    "key": "rekeyUsecase",                               /* Name of the encryption
key. */
    "action": "ENCRYPT",                                   /* Specifies the action t
o be taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    "iv": "1ABD0EAB12F345601ABD0EAB12F34560" /* Initialization Vector.
It is recommended to specify random generated IV, and do not reuse any IV. */
  }
}
}
}
]
}
}
}
}

```

Encrypt/Decrypt/Rekey in a New Column For CSV File

```

{
  "id":"FileSample-b004f83efaa",                        /* Transformation policy
id. */
  "name":"FileSample",                                  /* Name of the policy. */
  "createBadRecordFile":true,                           /* True or false. Defaul
t value is false. Set to "true" to create a ".failed file", otherwise set to "fal
se". */
  "caseSensitive":true,                                  /* True or false. Defaul
t value is false. If set to "true", all the database objects mentioned in the pol
icy file will be processed in the same case as input. If set to "false", all the
database objects mentioned in the policy file will be automatically converted to
UPPERCASE. */
  "source":{                                             /* Details of the data so
urce. */
    "@type":"CSV_FILE",                                  /* Source type. Supports
CSV_FILE. */
    "filepath":"input.csv",                              /* The file path relativ
e to the inputDir or outputDir path in the config file. */
    "delimiter":",",                                     /* The character that is
used to divide one column from the next in the input file. */
    "qualifier":"\"",                                     /* The character to enclo
se fields that contain a delimiter character. This is used when source is a file
and the delimiter character is itself a part of the data to be transformed. So t
o tell BDT that this is not a delimiter, user can enclose input data by a qualifi
er and mention qualifier here in this field. */
    "unescapeInput":true,                                /* True or false. Defaul
t value is false. If "true", delimiter and qualifier characters in input precede
d by a backslash (\) are considered as normal characters and part of the input da
ta. */
    "columnCount":"14",                                  /* Number of columns in t
he input file. */
    "hasHeaderRow":true                                  /* True or false. Defaul
t value is false. If "true", the utility will treat the first row as a header ro
w. Values from this row will be treated as column names. The same column names sh
ould be mentioned in the transformation action. If "false", the utility will trea
t all the rows as data to be transformed. */
  },
  "destination":{                                       /* Details of the data de

```

```

destination. */
    "@type":"CSV_FILE",                                /* Destination type. Supports
ports CSV_FILE. */
    "filepath":"output.csv"                            /* The file path relative
to the inputDir or outputDir path in the config file. */
},
    "tables":[                                          /* List of the tables to
be transformed. */
        {
            "columns":[                                /* List of the columns to
be transformed. */
                {
                    "name":"column1",                  /* Name of the column. */
                    "targetColName":"newcolumn1",      /* New column containing
encrypted data. */
                    "srcColumnAction":"preserve",      /* Source column remains
preserved. */
                    "action":"ENCRYPT",                 /* Specifies the action to
be taken. Supports ENCRYPT, DECRYPT, REKEY. */
                    "config":[                          /* Configuration for crypt
to operations. */
                        {
                            "@type":"AES_CBC_PAD",      /* Config type. Supports
AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
                            "key":"bdt-key",           /* Name of the key. */
                            "tweak":"010ACD5B99F3C343", /* Used for column level
tweak data. */
                            "characterSet":"digits",    /* Name of the charset.
*/
                            "iv":"DB1BE0FEC759E2FFE828D8053D955FF9" /* Initialization Vector.
It is recommended to specify random generated IV, and do not reuse any IV. */
                        }
                    ],
                },
            },
            {
                "name":"column2",                      /* Name of the column. */
                "targetColName":"newcolumn2",          /* New column containing
decrypted data. */
                "srcColumnAction":"empty",             /* Source column is emptied.
*/
                "action":"DECRYPT",                    /* Specifies the action to
be taken. Supports ENCRYPT, DECRYPT, REKEY. */
                "config":[                            /* Configuration for crypt
to operations. */
                    {
                        "@type":"AES_CBC_PAD",          /* Config type. Supports
AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
                        "key":"bdt-key",               /* Name of the key. */
                        "tweak":"010ACD5B99F3C343",    /* Used for column level
tweak data. */
                        "characterSet":"digits",        /* Name of the charset.
*/
                        "iv":"DB1BE0FEC759E2FFE828D8053D955FF9" /* Initialization Vector.
It is recommended to specify random generated IV, and do not reuse any IV. */
                    }
                ],
            },
            {
                "name":"column3",                      /* Name of the column. */

```

```

        "targetColName":"newcolumn3",                /* New column containing
rekeyed data. */
        "srcColumnAction":"remove",                  /* Source column is remov
ed. */
        "action":"REKEY",                             /* Specifies the action t
o be taken. Supports ENCRYPT, DECRYPT, REKEY. */
        "config":[                                     /* Configuration for cryp
to operations. */
            {
                "@type":"AES_CBC_PAD",                /* Config type. Supports
AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
                "key":"bdt-key",                      /* Name of the key. */
                "tweak":"010ACD5B99F3C343",          /* Used for column level
tweak data. */
                "characterSet":"digits",              /* Name of the charset.
*/
                "iv":"DB1BE0FEC759E2FFE828D8053D955FF9", /* Initialization Vecto
r. It is recommended to specify random generated IV, and do not reuse any IV. */
                "action":"DECRYPT"                    /* Specifies the action t
o be taken. Supports ENCRYPT, DECRYPT, REKEY. */
            },
            {
                "@type":"AES_CBC_PAD",                /* Config type. Supports
AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
                "key":"bdt-rekey",                    /* Name of the key. */
                "tweak":"010ACD5B99F3C343",          /* Used for column level
tweak data. */
                "characterSet":"digits",              /* Name of the charset.
*/
                "iv":"DB1BE0FEC759E2FFE828D8053D955FF9", /* Initialization Vecto
r. It is recommended to specify random generated IV, and do not reuse any IV. */
                "action":"ENCRYPT"                    /* Specifies the action t
o be taken. Supports ENCRYPT, DECRYPT, REKEY. */
            }
        ]
    }
]
}
]
}
}

```

For Fixed Length File

```

{
    "id":"FixedLengthFileSample-5ec94388",          /* Transformation policy id. */
    "name":"FixedLengthFileSample",                 /* Name of the policy. */
    "createBadRecordFile":true,                     /* True or false. Default value i
s false. Set to "true" to create a ".failed file", otherwise set to "false". */
    "source":{                                       /* Details of the data source. */
        "@type":"FIXED_LENGTH_FILE",                /* Source type. Supports FIXED_LE
NGTH_FILE. */
        "filepath":"input.txt",                     /* The file path relative to the
inputDir or outputDir path in the config file. */
        "lineSeparator":true,                       /* Separate the line. */
        "hasHeaderRow":true,                        /* True or false. Default value i
s false. If "true", the utility will treat the first row as a header row. Values
from this row will be treated as column names. The same column names should be me

```

```

mentioned in the transformation action. If "false", the utility will treat all the
rows as data to be transformed. */
    "columnCount":3,                                /* Number of columns in the input
file. */
    "recordLength":30,                              /* Length of the record. */
    "columnPositions":[                             /* Positions of the column. */
        {
            "column":0,                              /* Index of the column. */
            "startIndex":0,                          /* The start index of the column.
*/
            "endIndex":10                            /* The end index of the column.
*/
        },
        {
            "column":1,                              /* Index of the column. */
            "startIndex":10,                          /* The start index of the column.
*/
            "endIndex":20                            /* The end index of the column.
*/
        },
        {
            "column":2,                              /* Index of the column. */
            "startIndex":20,                          /* The start index of the column.
*/
            "endIndex":30                            /* The end index of the column.
*/
        }
    ],
    "destination":{                                /* Details of the data destination.
*/
        "@type":"FIXED_LENGTH_FILE",                /* Destination type. Supports FIXED_LENGTH_FILE. */
        "filepath":"output.txt"                    /* The file path relative to the
inputDir or outputDir path in the config file. */
    },
    "tables":[                                       /* List of the tables to be transformed.
*/
        {
            "columns":[                             /* List of the columns to be transformed.
*/
                {
                    "name":"column1",                /* Name of the column. */
                    "targetColName":"name1",         /* Name of the target column. */
                    "srcColumnAction":"preserve",    /* Source column remains preserved.
*/
                    "targetColLength":10,            /* The column length of targetColumn.
*/
                    "action":"ENCRYPT",               /* Specifies the action to be taken. Supports ENCRYPT, DECRYPT, REKEY.
*/
                    "config":[                       /* Configuration for crypto operations.
*/
                        {
                            "@type":"FPE",           /* Config type. Supports AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede.
*/
                            "key":"bdt-key",         /* Name of the key. */
                            "tweak":"auto",          /* Used for column level tweak data.
*/
                            "characterSet":"alphanumeric" /* Name of the charset.
*/
                        }
                    ]
                }
            ]
        }
    ]
}

```

```

    }
  ],
  {
    "name": "column2",
    "targetColName": "name2",
    "srcColumnAction": "empty",
    "targetColLength": 10,
    Name. /*
      "action": "DECRYPT",
    en. Supports ENCRYPT, DECRYPT, REKEY. /*
    "config": [
    tions. /*
      {
        "@type": "FPE",
        C_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. /*
        "key": "bdt-key",
        "tweak": "auto",
        ta. /*
        "characterSet": "alphanumeric"
      }
    ],
    {
      "name": "column3",
      "targetColName": "newcolumn3",
      "srcColumnAction": "remove",
      "targetColLength": 10,
      Name. /*
      "action": "REKEY",
    en. Supports ENCRYPT, DECRYPT, REKEY. /*
      "config": [
      tions. /*
        {
          "@type": "FPE",
          C_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. /*
          "key": "bdt-key",
          "tweak": "auto",
          ta. /*
          "characterSet": "alphanumeric",
          "action": "DECRYPT"
        en. Supports ENCRYPT, DECRYPT, REKEY. /*
        },
        {
          "@type": "FPE",
          C_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. /*
          "key": "bdt-key1",
          "tweak": "auto",
          ta. /*
          "characterSet": "alphanumeric",
          "action": "ENCRYPT"
        en. Supports ENCRYPT, DECRYPT, REKEY. /*
        }
      ]
    }
  ]
}

```

For DB

```
{
  "id": "OracleToSqlServerSample-90643295a90sdf5",          /* Transf
ormation policy id. */
  "name": "OracleToSqlServerSample",                        /* Name o
f the policy. */
  "source": {                                               /* Define
s details of data input. */
    "@type": "MYSQL",                                       /* Specif
ies the database type. */
    "connectionurl": "jdbc:mysql://localhost:3306/my_db",   /* Databa
se connection URL. */
    "username": "root",                                     /* Databa
se username. */
    "password": "",                                         /* Databa
se password. */
    "driverclass": "com.mysql.cj.jdbc.Driver"              /* DBC co
nnection driver class. */
  },
  "destination": {                                          /* Define
s details of data output. */
    "@type": "MYSQL",                                       /* Specif
ies the database type. */
    "connectionurl": "jdbc:mysql://localhost:3306/my_db",   /* Databa
se connection URL. */
    "username": "root",                                     /* Databa
se username. */
    "password": "",                                         /* Databa
se password. */
    "driverclass": "com.mysql.cj.jdbc.Driver"              /* DBC co
nnection driver class. */
  },
  "tables": [                                               /* List o
f the tables to be transformed. */
    {
      "columns": [                                          /* List o
f the columns to be transformed. */
        {
          "name": "Age",                                     /* Name o
f the column. */
          "targetColName": "NewAge",                        /* Name o
f the new column. */
          "srcColumnAction": "preserve",                    /* Source
column action. */
          "action": "ENCRYPT",                               /* Specif
ies the action to be taken. Supports ENCRYPT, DECRYPT, REKEY. */
          "config": [                                        /* Config
uration for crypto operations. */
            {
              "@type": "AES_CBC_PAD",                       /* Config
type. Supports AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
              "key": "tes_key",                             /* Name o
f the key. */
              "iv": "1ABD0EAB12F345601ABD0EAB12F34560"     /* Initia
lization Vector. */
            }
          ]
        }
      ]
    }
  ]
}
```



```

    },
    {
        "name": "Name",                                /* Name of
f the column. */
        "targetColName": "NewName",                    /* Name of
f the new column. */
        "srcColumnAction": "remove",                    /* Source
column action. */
        "action": "ENCRYPT",                             /* Specif
ies the action to be taken. Supports ENCRYPT, DECRYPT, REKEY. */
        "config": [                                     /* Config
uration for crypto operations. */
            {
                "@type": "AES_CBC_PAD",                    /* Config
type. Supports AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
                "key": "tes_key",                          /* Name of
f the key. */
                "iv": "1ABD0EAB12F345601ABD0EAB12F34560" /* Initia
lization Vector. */
            }
        ]
    },
    {
        "name": "Sub",                                /* Name of
f the column. */
        "targetColName": "NewSub",                      /* Name of
f the new column. */
        "srcColumnAction": "empty",                      /* Source
column action. */
        "action": "ENCRYPT",                             /* Specif
ies the action to be taken. Supports ENCRYPT, DECRYPT, REKEY. */
        "config": [                                     /* Config
uration for crypto operations. */
            {
                "@type": "AES_CBC_PAD",                    /* Config
type. Supports AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
                "key": "tes_key",                          /* Name of
f the key. */
                "iv": "1ABD0EAB12F345601ABD0EAB12F34560" /* Initia
lization Vector. */
            }
        ]
    },
    {
        "name": "Add",                                /* Name of
f the column. */
        "targetColName": "NewAdd",                      /* Name of
f the new column. */
        "action": "ENCRYPT",                             /* Source
column action. */
        "config": [                                     /* Specif
ies the action to be taken. Supports ENCRYPT, DECRYPT, REKEY. */
            {
                "@type": "AES_CBC_PAD",                    /* Config
type. Supports AES_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
                "key": "tes_key",                          /* Name of
f the key. */
                "iv": "1ABD0EAB12F345601ABD0EAB12F34560" /* Initia
lization Vector. */
            }
        ]
    }
}

```

```

    }
  ]
}
],
"sourceTable": "demo33" /* Source
table name. */
}
],
"inPlaceUpdate": true /* Transf
orm data in-place within the database. */
}

```

Tokenize/Detokenize

Tokenize

```

{
  "id": "Tokenization_transformation_encryption", /* Transformation policy id.
*/
  "name": "Tokenization_transformation_encryption", /* Name of the policy. */
  "createBadRecordFile": true, /* True or false. Set to true
to create a file with .failed extension, otherwise set to false. */
  "source": { /* Details of the data source
e. */
    "@type": "CSV_FILE", /* Source type. Supports CS
V_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "basic_input.csv", /* The file path relative to
the inputDir or outputDir path in the config file. */
    "delimiter": ",", /* The character that is used
to divide one column from the next in the input file. */
    "qualifier": "\"\"", /* The character to enclose f
ields that contain a delimiter character. This is used when source is a file and
the delimiter character is itself a part of the data to be transformed. So to tel
l BDT that this is not a delimiter, user can enclose input data by a qualifier an
d mention qualifier here in this field. */
    "unescapeInput": "true", /* True or false. Default val
ue is false. If "true", delimiter and qualifier characters in input preceded by a
backslash (\) are considered as normal characters and part of the input data. */
    "columnCount": "12", /* Number of columns in the i
nput file. */
    "hasHeaderRow": true /* True or false. Default val
ue is false. If "true", the utility will treat the first row as a header row. Val
ues from this row will be treated as column names. The same column names should b
e mentioned in the transformation action. If "false", the utility will treat all
the rows as data to be transformed. */
  },
  "destination": { /* Details of the data destin
ation. */
    "@type": "CSV_FILE", /* Destination type. Supports
CSV_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "output.csv" /* The file path relative to
the inputDir or outputDir path in the config file. */
  },
  "tables": [ /* List of the tables to be t
ransformed. */
    {
      "columns": [ /* List of the columns to be

```

```

transformed. */
{
    "name": "latitude", /* Name of the column. */
    "action": "TOKENIZE", /* Specifies the action to be
taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
    "config": [ /* Configuration for Encrypti
on or Tokenization operations. */
        {
            "@type": "TOKENIZE", /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
            "key": "test_bdt", /* Name of the encryption ke
y. */
            "tokenGroup": "bdt_token_group", /* Name of the token group as
defined in VTS. */
            "tokenTemplate": "BDT_FPE" /* Name of the token template
as defined in VTS. */
        }
    ]
}
]
}
]
}
}

```

Detokenize

```

{
    "id": "Tokenization_transformation_decryption", /* Transformation policy id.
*/
    "name": "Tokenization_transformation_decryption", /* Name of the policy. */
    "createBadRecordFile": true, /* True or false. Set to true
to create a file with .failed extension, otherwise set to false. */
    "source": { /* Details of the data sourc
e. */
        "@type": "CSV_FILE", /* Source type. Supports CS
V_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
        "filepath": "input.csv", /* The file path relative to
the inputDir or outputDir path in the config file. */
        "delimiter": ",", /* The character that is used
to divide one column from the next in the input file. */
        "qualifier": "\"\"", /* The character to enclose f
ields that contain a delimiter character. This is used when source is a file and
the delimiter character is itself a part of the data to be transformed. So to tel
l BDT that this is not a delimiter, user can enclose input data by a qualifier an
d mention qualifier here in this field. */
        "unescapeInput": "true", /* True or false. Default val
ue is false. If "true", delimiter and qualifier characters in input preceded by a
backslash (\) are considered as normal characters and part of the input data. */
        "columnCount": "12", /* Number of columns in the i
nput file. */
        "hasHeaderRow": true /* True or false. Default val
ue is false. If "true", the utility will treat the first row as a header row. Val
ues from this row will be treated as column names. The same column names should b
e mentioned in the transformation action. If "false", the utility will treat all
the rows as data to be transformed. */
    },
    "destination": { /* Details of the data destin

```

```

ation. */
    "@type": "CSV_FILE",                                /* Destination type. Supports
CSV_FILE, FIXED_LENGTH_FILE, ORACLE, SQL_SERVER, MYSQL, DB2, HANA. */
    "filepath": "output.csv"                            /* The file path relative to
the inputDir or outputDir path in the config file. */
},
    "tables": [                                          /* List of the tables to be t
ransformed. */
    {
        "columns": [                                    /* List of the columns to be
transformed. */
        {
            "name": "latitude",                          /* Name of the column. */
            "action": "DETOKENIZE",                      /* Specifies the action to be
taken. Supports ENCRYPT, DECRYPT, TOKENIZE, DETOKENIZE, REKEY. */
            "config": [                                  /* Configuration for Encrypti
on or Tokenization operations. */
            {
                "@type": "TOKENIZE",                    /* Config type. Supports AE
S_CBC_PAD, AES_CTR, FPE, FF1, FPE_AES, TOKENIZE, DESede. */
                "key": "test_bdt",                      /* Name of the encryption ke
y. */
                "tokenGroup": "bdt_token_group",         /* Name of the token group as
defined in VTS. */
                "tokenTemplate": "BDT_FPE"              /* Name of the token template
as defined in VTS. */
            }
        ]
    }
]
}
]
}
}

```

Sample BDT Config File

Consolidated Config

```

{
    "inputDirectory": "C:\\samples\\resources",          /* The path t
o the directory in which the input file or database is placed. */
    "outputDirectory": "C:\\samples\\resources\\temp",  /* The path t
o the directory in which the output file or database needs to be placed. */
    "threadCount": 4,                                   /* Maximum nu
mber of running threads to transform file. */
    "batchSize": 1000,                                  /* Number of
records processed in batch. */
    "vts": {
        "hostName": "<ip address>",                     /* Hostname o
f a machine where tokenization server is running. */
        "userName": "webadmin",                         /* The CT-VL
username. */
        "password": "",                                 /* The CT-VL
password. Do not put plaintext here, use "bdt -e" option to put encrypted value h
ere. */
    }
}

```

```

    "tokenUrl": "https://<ip address>/vts/rest/v2.0/tokenize", /* The CT-VL
tokenize REST URL. */
    "detokenUrl": "https://<ip address>/vts/rest/v2.0/detokenize", /* The CT-VL
detokenize REST URL. */
    "ssl" : {
        "server": { /* SSL config
uration for server. */
            "sslmode": "DEFAULT", /* SSL mode
(DEFAULT, ALLOW_ALL - allow everything, SPECIFY_SSL_CERT - communicate if server
certificate exists in the specified truststore). */
            "verifyHostname": true, /* Whether t
o do hostname verification */
            "truststore": "", /* Truststor
e file path, truststore should have server certificate. Applicable only for SPECI
FY_SSL_CERT mode. */
            "password": "" /* Truststor
e file password. Applicable only for SPECIFY_SSL_CERT mode. */
        },
        "client": { /* SSL config
uration for client. */
            "sslmode": "DEFAULT", /* SSL mode
(DEFAULT/ALLOW_ALL - do not send client authentication, SPECIFY_SSL_CERT - send c
lient authentication certificate in the specified keystore). */
            "keystore": "", /* Keystore f
ile path. Keystore should have client key and certificate. */
            "storepassword": "", /* Keystore f
ile password. */
            "keypassword": "" /* Key file p
assword, usually same as keystore password. */
        }
    }
}
"crypto": { /* Settings f
or the cryptographic provider used in this BDT configuration. */
    "@type": "jce", /* Two types
of cryptographic providers - one is default jce (CADP-JCE) and other is vae. */
    "username": "nameofuser", /* The name o
f user who owns the key. If user is in a specific domain, use domain||username fo
rmat. For example, thales||joe, where thales is the domain and joe is username.
*/
    "password": "" /* Password f
or the user. */
}
"dataProtectionConfig": { /* Contains c
redential information which will be used to get centralized policy. */
    "@type": "user_certificate", /* BDT suppor
ts two login methods - password and user_certificate. */
    "hostname": "", /* Hostname o
f key manager. */
    "serverConfig": { /* Used only
when @type value is user_certificate. */
        "truststore": "", /* Truststor
e file path, truststore should have server certificate. */
        "password": "", /* Truststor
e file password. */
        "verifyHostname": "true" /* Set to "tr
ue" to enable hostname verification for SSL communication, and "false" to disabl
e hostname verification. */
    },

```

```

        "clientConfig": {                                /* Used only
when @type value is user_certificate. */
            "keystore": "",                                /* Keystore f
ile path of the client. */
            "storePassword": "",                          /* Keystore f
ile password of the client. */
            "keyPassword": ""                            /* Key file p
assword, usually same as keystore password. */
        },
        "characterSets": [                                /* Contains c
onfigurable list of charset names and their range. */
            {
                "latin": ["0020-007E"]                    /* Latin char
acter sets. */
            },
            {
                "digits": ["0030-0039"]                    /* Digits cha
racter sets. */
            },
            {
                "alphabets": ["0041-005A", "0061-007A"]   /* Alphabets
character sets. */
            },
            {
                "alphanumeric": ["0030-0039", "0041-005A", "0061-007A"] /* Alphanumer
ic character sets. */
            }
        ]
    }

```

Encrypt/Decrypt/Rekey

```

{
    "inputDirectory": "C:\\samples\\resources",           /* The path t
o the directory in which the input file or database is placed. */
    "outputDirectory": "C:\\samples\\resources\\temp",    /* The path t
o the directory in which the output file or database needs to be placed. */
    "threadCount": 4,                                     /* Maximum nu
mber of running threads to transform file. */
    "batchSize": 1000,                                    /* Number of
records processed in batch. */
    "crypto": {                                           /* Settings f
or the cryptographic provider used in this BDT configuration. */
        "@type": "jce",                                   /* Two types
of cryptographic providers - one is default jce (CADP-JCE) and other is vae. */
        "username": "nameofuser",                        /* The name o
f user who owns the key. If user is in a specific domain, use domain\\username fo
rmat. For example, thales\\joe, where thales is the domain and joe is username.
*/
        "password": ""                                    /* Password f
or the user. */
    },
    "dataProtectionConfig": {                             /* Contains c
redential information which will be used to get centralized policy. */
        "@type": "user_certificate",                      /* BDT suppor
ts two login methods - password and user_certificate. */
    }
}

```

```

        "hostName": "",                                /* Hostname o
f key manager. */
        "serverConfig": {                             /* Used only
when @type value is user_certificate. */
            "truststore": "",                          /* Truststor
e file path, truststore should have server certificate. */
            "password": "",                            /* Truststor
e file password. */
            "verifyHostName": "true"                  /* Set to "tr
ue" to enable hostname verification for SSL communication, and "false" to disabl
e hostname verification. */
        },
        "clientConfig": {                             /* Used only
when @type value is user_certificate. */
            "keystore": "",                            /* Keystore f
ile path of the client. */
            "storePassword": "",                      /* Keystore f
ile password of the client. */
            "keyPassword": ""                         /* Key file p
assword, usually same as keystore password. */
        },
        "characterSets": [                             /* Contains c
onfigurable list of charset names and their range. */
            {
                "latin": ["0020-007E"]                /* Latin char
acter sets. */
            },
            {
                "digits": ["0030-0039"]               /* Digits cha
racter sets. */
            },
            {
                "alphabets": ["0041-005A", "0061-007A"] /* Alphabets
character sets. */
            },
            {
                "alphanumeric": ["0030-0039", "0041-005A", "0061-007A"] /* Alphanumer
ic character sets. */
            }
        ]
    }
}

```

Tokenize/Detokenize

```

{
    "inputDirectory": "C:\\samples\\resources",        /* The path t
o the directory in which the input file or database is placed. */
    "outputDirectory": "C:\\samples\\resources\\temp", /* The path t
o the directory in which the output file or database needs to be placed. */
    "threadCount": 4,                                /* Maximum nu
mber of running threads to transform file. */
    "batchSize": 1000,                                /* Number of
records processed in batch. */
    "vts": {
        "hostName": "<ip address>",                    /* Hostname o
f a machine where tokenization server is running. */
    }
}

```

```

    "userName": "webadmin", /* The CT-VL
username. */
    "password": "", /* The CT-VL
password. Do not put plaintext here, use "bdt -e" option to put encrypted value h
ere. */
    "tokenUrl": "https://<ip address>/vts/rest/v2.0/tokenize", /* The CT-VL
tokenize REST URL. */
    "detokenUrl": "https://<ip address>/vts/rest/v2.0/detokenize", /* The CT-VL
detokenize REST URL. */
    "ssl" : {
        "server": { /* SSL config
uration for server. */
            "sslmode": "DEFAULT", /* SSL mode
(DEFAULT, ALLOW_ALL - allow everything, SPECIFY_SSL_CERT - communicate if server
certificate exists in the specified truststore). */
            "verifyHostname": true, /* Whether t
o do hostname verification */
            "truststore": "", /* Truststor
e file path, truststore should have server certificate. Applicable only for SPECI
FY_SSL_CERT mode. */
            "password": "" /* Truststor
e file password. Applicable only for SPECIFY_SSL_CERT mode. */
        },
        "client": { /* SSL config
uration for client. */
            "sslmode": "DEFAULT", /* SSL mode
(DEFAULT/ALLOW_ALL - do not send client authentication, SPECIFY_SSL_CERT - send c
lient authentication certificate in the specified keystore). */
            "keystore": "", /* Keystore f
ile path. Keystore should have client key and certificate. */
            "storepassword": "", /* Keystore f
ile password. */
            "keypassword": "" /* Key file p
assword, usually same as keystore password. */
        }
    }
    "dataProtectionConfig": { /* Contains c
redential information which will be used to get centralized policy. */
        "@type": "user_certificate", /* BDT suppor
ts two login methods - password and user_certificate. */
        "hostName": "", /* Hostname o
f key manager. */
        "serverConfig": { /* Used only
when @type value is user_certificate. */
            "truststore": "", /* Truststor
e file path, truststore should have server certificate. */
            "password": "", /* Truststor
e file password. */
            "verifyHostname": "true" /* Set to "tr
ue" to enable hostname verification for SSL communication, and "false" to disabl
e hostname verification. */
        },
        "clientConfig": { /* Used only
when @type value is user_certificate. */
            "keystore": "", /* Keystore f
ile path of the client. */
            "storePassword": "", /* Keystore f
ile password of the client. */

```



```

        "keyPassword": ""
assword, usually same as keystore password. */
    }
}
}

```

Best Practices

This section describes the best practices for:

- [Thread Count and Batch Sizes](#)

Thread Count and Batch Sizes

To best configure thread count and batch size, use the following principles:

1. Identify the ideal thread count for your environment depending on your system configuration. BDT gives optimal performance with 16 threads on four core machines. Setting thread count too low or too high will slow down the application.
2. Decide on batch size, configured based on available memory, size of individual record, and configured thread count. Setting batch size too high may result in an out-of-memory error.
3. Use the following formula to calculate the approximate maximum memory utilization by BDT:

```
thread count * batch size * record size = memory utilization
```

Therefore, thread count and batch size will be less than or equal to about 60% of available memory. The remaining memory is required to run the utility and to maintain transformed batches in the `write` queue.

Example

If you have 4GB available memory and individual record size of approximately 50MB, you can set either:

- Batch size to 50 and thread count to 1, utilizing $50 * 1 * 50\text{MB} = 2500\text{MB}$, approximately 60% of memory.
- Batch size to 10 and thread count to 3, utilizing $10 * 3 * 100\text{MB} = 3000\text{MB}$.

Troubleshooting

Log Files

- BDT stores its logs in the file `BDT_HOME/log/bdt.log`.
- The default log level is `DEBUG` for the log file and `INFO` for the console. These log properties can be changed in the `BDT_HOME/conf/log4j.properties` file.

Note

BDT_home points to your installation directory.

Error and Description

Error / Exception	Description
Value too long for column "PARAMETER_NAME CHARACTER VARYING(100)"	This error occurs if the length of the policy ID or the policy name exceeds 100 characters.
Thread count must be greater than or equal to number of tables.	This error occurs if the number of tables transforming are greater than the thread count.
NAE_IP.1 contains invalid IP addresses in the IngrianNAE.properties	The <code>bdt.properties</code> file is not configured, and the parameter <code>NAE_IP.1</code> is blank. Refer to BDT Properties File for configuring the properties.
Failed to obtain JDBC Connection; nested exception is java.sql.SQLException: Cannot create PoolableConnectionFactory (Access denied for user 'userName'@'xx.xx.xx.xx').	This exception occurs if: - Database user's password is empty. - Database user's password is incorrect.
Driver class not found:	Copy the required database driver to <code>BDT_HOME/lib</code> path.
PreparedStatementCallback; SQL [Insert into MYTESTDB.CUSTOMERYD27 values(?,?)]: Duplicate entry '3' for key 'customeryd27.PRIMARY'; nested exception is java.sql.BatchUpdateException: Duplicate entry '3' for key 'customeryd27.PRIMARY'.	This error occurs when a table contains primary key, <code>createDestinationTable</code> is set to true and destination table already exists. So, the same value for a primary key can not be written.
Loading class 'com.mysql.jdbc.Driver': This is deprecated. The new driver class is <code>com.mysql.cj.jdbc.Driver</code> . The driver is automatically registered via the SPI and manual loading of the driver class is generally unnecessary.	Change the driver class from <code>com.mysql.jdbc.Driver</code> to <code>com.mysql.cj.jdbc.Driver</code> in the BDT policy.
Could not create the destination table: Make sure the source table exists.	If the source table exists, ensure table name is configured correctly in the BDT policy file.
Invalid Object Name:	If <code>caseSensitive</code> flag is enabled in the policy file, the database object names should not be enclosed in double quotes.
Ciphertext version header does not match to policy version for this record:	The value of <code>policyVersion</code> field in the BDT policy file during decryption must be same as the one used during encryption.

Error / Exception	Description
Record parsing failed: The value of <code>columnCount</code> in the BDT policy file and parsed records does not match.	Ensure that all the records in the input file have the same column count as mentioned in the <code>columnCount</code> field of the BDT policy file.
Invalid or missing algorithm: The encryption algorithm used in <code>config@type</code> is not supported when symmetric key cache is disabled.	Refer to supported encryption algorithms for details.
Column <code>targetColName</code> exists in the input file	This error occurs if the column name specified in the <code>targetColName</code> parameter (irrespective of the case sensitivity) exists anywhere in the input file. Refer to Storing Output of Crypto Operations in a New Column for details.
<code>targetColName</code> is not specified, cannot modify the source column	This error occurs if <code>srcColumnAction</code> is specified without <code>targetColName</code> .
**Value of <code>srcColumnAction</code> "entered-value" is invalid **	This error occurs if "entered-value" in <code>srcColumnAction</code> is other than <code>preserve</code> , <code>empty</code> , <code>remove</code> . Refer to BDT Policy File for details.
Exception <code>java.lang.NoSuchMethodError</code> in the "main" thread <pre> org.apache.logging.log4j.spi.LoggerContextFactory .isClassLoaderDependent() Z org.apache.logging.slf4j.Log4jLoggerFactory .getContext(Log4jLoggerFactory.java:55) org.apache.logging.log4j.spi.AbstractLoggerAdapter .getLogger(AbstractLoggerAdapter.java:46) org.apache.logging.slf4j.Log4jLoggerFactory .getLogger(Log4jLoggerFactory.java:33) org.slf4j.LoggerFactory.getLogger(LoggerFactory.java:358) org.slf4j.LoggerFactory.getLogger(LoggerFactory.java:383) com.vormetric.bdt.cli.BDTCli. (BDTCli.java:50) </pre>	If you are using OpenJDK, try reinstalling it. If the issue persists, use Sun JDK.
SQL0668N operation not allowed for reason code "7" on table	This error occurs while performing any operation on destination table after a successful transformation with destination database as DB2. Note: This error is applicable only for DB2. Workaround: Run the following query after the transformation:

Error / Exception	Description
	<code>call sysproc.admin_cmd ('reorg table <schema>.<TableName>')</code>

Limitations

- If a source table contains spaces in its column name, then that source table cannot be transformed.
- Multiple IP addresses are not supported in the `NAE_IP.x` field of `bdt.properties` file when running BDT using the centralized policy `-central` option.
- When `createDestinationTable` is set to `true`:
 - For Oracle databases, only CAPITAL casing is supported for database user names.
 - If multiple tables with the same name but different casing (for example, "testtable" and "TestTable") exist in any source/destination and owner/schema, such tables cannot be transformed.
 - For MSSQL and MYSQL databases, if the parameter `caseSensitive` is set to `false`, then `sourceTable` name in policy should be in the same case as it is created in the database.

In case of casing mismatch, transformation will give the following error:

```
Could not create destination table. Make sure source table exists.
```

- In a multi-threaded environment, the sequence of the output order will be different than the one provided in the input order. To maintain the same sequence in the input and output order, it is recommended to use `threadCount` as 1 in [BDT Config File](#).

FAQs

- **Can I use FPE with BDT? If yes, which FPE algorithms are supported in BDT?**

BDT supports FF1 and FF3 algorithms. To do so, update the BDT config file as shown here:

- For FF3, set `@type` to `FPE`
- For FF1, set `@type` to `FF1`

- **Is there a way to configure BDT to not remove the double quotes from the header row?**

As of now, BDT removes qualifiers from headers and input data. To avoid it, the user can use any other character UTF-8 character as qualifier; for example, `#`, `@`, or `%`. But then the column name must also be changed from `ADRES_ID` to `\ "ADRES_ID\ "`.

```
{
  "id": "policyId",
  "name": "policyName",
  "source": {
    "@type": "CSV_FILE",
    "filepath": "persoonexample.csv",
    "delimiter": ",",
    "qualifier": "#",
    "unescapeInput": false,
    "columnCount": 51,
    "hasHeaderRow": true
  },
  "destination": {
    "@type": "CSV_FILE",
    "filepath": "persoonout.csv"
  },
  "fpemode": "ASCII",
  "createBadRecordFile": true,
  "tables": [
    {
      "columns": [
        {
          "name": "\"ADRES_ID\"",
          "action": "ENCRYPT",
          "config": [
            {
              "@type": "FPE",
              "key": "bdt_key",
              "characterSet": "alphanumeric",
              "tweak": "AUTO"
            }
          ]
        }
      ]
    }
  ]
}
```

- **Can BDT be configured for both encryption and tokenization?**

Yes, BDT can be configured for both encryption and tokenization. For this, the user needs to configure both `vt`s and `crypto` attributes in BDT, refer to [Sample BDT Config File](#) for details.

For a common policy of encryption and tokenization, refer to [Sample BDT Policy File](#).

- **Can I store my encrypted/decrypted/rekeyed data in a new column?**

Yes, BDT allows you to store the output of the crypto operations (encrypt/decrypt/rekey) in a new column. To do so, specify the `targetColName` parameter in the BDT policy file under [Columns Attributes](#).

Refer to [Storing Output of Crypto Operations in a New Column](#) for details.

- **Can I store my encrypted/decrypted/rekeyed data in the same column?**

If you want to store the encrypted/decrypted/rekeyed data in the same column, do not specify the `targetColName` parameter in the BDT policy file, leave `targetColName` column empty, or specify `targetColName` as `null`.