Navigate to Dell PERC 11 configuration utility

Steps

1. Enter the UEFI configuration Utility. See Enter the PERC 11 HII configuration utility.
   The **Device Settings** screen displays a list of NIC ports and the RAID controllers.
2. To enter PERC 11 configuration utility, click the appropriate PERC controllers.
   The **Dashboard view** screen is displayed.

View the HII Configuration utility dashboard

The first screen that is displayed when you access the HII Configuration Utility is the **Dashboard View** screen. The following table provides detailed information about the options available on the **Dashboard View** screen.

Table 8. Dashboard view screen

Dashboard view options	Description
Main menu	Displays the following configuration options: • Configuration Management • Controller Management • Virtual Disk Management • Physical Disk Management • Hardware Components
Help	Provides context sensitive help message.
Properties	Displays the following information about the controller: • Status — displays the status of the controller. • Backplane — displays information about the number of backplanes connected to the controller. • BBU — displays information about the availability of Battery Backup Unit (BBU). • Enclosure — displays information about the number of enclosures connected to the controller. • Physical Disks — displays information about the number of physical disks connected to the controller. • Disk Groups — displays information about the number of disk groups connected to the controller. • Virtual Disks — displays information about the number of virtual disks connected to the controller.
View server profile	Displays HII Spec version supported on the system and also displays the following menu options for controller components: • Controller Management • Hardware Components • Physical Disk Management • Virtual Disk Management
Actions	Displays the following options: • Configure — displays configuration options that are supported by the controller. • Set Factory Defaults — restore factory default values for all controller properties.
Background operations	Displays if virtual disk or physical disk operations are in progress.

Configuration management

Auto Configure RAID 0

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Configuration Management** > **Auto Configure RAID 0**.
3. Select **Confirm** and click **Yes** to continue.
   A RAID 0 Virtual disk is created on all physical disks that are in Ready state.

Create virtual disks

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See, Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Configuration Management** > **Create Virtual Disk**.
   The following list of options are displayed for you to define the virtual disk parameters:

Option	Description
Create Virtual Disk	Allows you to create virtual disk selecting the RAID level, physical disks, and virtual disk parameters
Select RAID level	Allows you to choose the RAID level of your choice
Secure Virtual Disk	If you want to create a secured virtual disk, select **Secure Virtual Disk**. ⓘ **NOTE:** The Secure Virtual Disk option is enabled by default, only if the security key has been configured. Only SED physical disks are listed.
Select Physical Disks From	Allows you to select one of the physical disk capacities: ● **Unconfigured Capacity**: creates a virtual disk on unconfigured physical disks. ● **Free Capacity**: utilizes unused physical disk capacity that is already part of a disk group.
Select Physical Disks	If you want to select the physical disks from which the virtual disks are being created, click **Select Physical Disks**. This option is displayed if you select **Unconfigured Capacity** as your physical disk capacity.
Select Disk Groups	If you want to select the disk groups from which the virtual disks are being created, click **Select Disk Group**. This option is displayed if you select **Free Capacity** as your physical disk capacity.
Configure Virtual Disk Parameters	Allows you to set the virtual disk parameters when creating the virtual disk. For more information, see Configuring virtual disk parameters.

3. Click **Create Virtual Disk**.
   The virtual disk is created successfully.

Configure virtual disk parameters

Steps

1. Create a virtual disk, see Creating the virtual disks.
   The **Configure Virtual Disk Parameters** section is displayed on the **Create Virtual Disk** screen.

2. In the **Configure Virtual Disk Parameters** section, you can set the following virtual disk parameters:

Table 9. Configure virtual disk parameters

Virtual disk parameters	Description
Virtual Disk Name	Allows you to enter the name for the virtual disk ⓘ **NOTE:** Allowed characters are A-Z, a-z, 0-9, underscore (_), and hyphen (-) only.
Virtual Disk Size	Displays the maximum capacity available for the virtual disk
Virtual Disk Size Unit	Displays the virtual disk storage space in megabytes, gigabytes, and terabyte.
Strip Element Size	Allows you to select the strip element size The disk striping involves partitioning each physical disk storage space in stripes of the following sizes: 64 KB, 128 KB, 256 KB, 512 KB, and 1 MB. By default, the strip element size is set to 256 KB.
Read Policy	Displays the controller read policy You can set the read policy to: • No read ahead—specifies that the controller does not use read ahead for the current virtual disk. • Read ahead—specifies that the controller uses read ahead for the current virtual disk. Read ahead capability allows the controller to read sequentially ahead of requested data and store the additional data in the cache memory, anticipating that the data is required soon. By default, the read cache policy is set to read ahead.
Write Policy	Displays the controller write cache policy You can set the write policy to: • Write through—the controller sends a data transfer completion signal to the host when the disk subsystem has received all the data in a transaction. • Write back—the controller sends a data transfer completion signal to the host when the controller cache has received all the data in a transaction. By default, the write policy is set to Write Back.
Disk Cache	Allows you to set the disk cache policy to default, enable, or disable. By default, the disk cache is set to default.
Default Initialization	Displays the virtual disk initialization options. You can set the default initialization to: • No — The virtual disk is not initialized. • Fast — The first 8 MB of the virtual disk is initialized. • Full — The entire virtual disk is initialized. For more information, see Virtual disk initialization. By default, the default initialization is set to No.

Create profile based virtual disk

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Configuration Management** > **Creating Profile Based Virtual Disk**.
   The following list of RAID modes are displayed:
   - Generic RAID 0
   - Generic RAID 1
   - Generic RAID 5
   - Generic RAID 6
   - File Server
   - Web/Generic Server
   - Database
3. Based on the RAID mode selected, one or more the physical disk selection criteria is displayed.
4. From the **Physical Disk Selection Criteria** drop-down box, select a criterion based your requirement.
   The Profile Parameters of the selected option is displayed.
5. Click **Create Virtual Disk**.

6. Select **Confirm** and click **Yes** to continue.
   The virtual disk is created with the parameters of the profile selected.

View disk group properties

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Configuration Management** > **View Disk Group Properties**.
   The list of disk group properties are displayed:

Properties	Descriptions
Capacity Allocation	Displays all the virtual disks associated with the specific disk group. It also provides information about the available free space
Secured	Displays whether the disk group is secured or not

Convert to Non-RAID disk

Prerequisites

To convert a physical disk to non-RAID disk from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Configuration Management** > **Convert to Non-RAID Disk**.
   The list of physical disks appears.
3. Select the physical disk to convert to Non-RAID disk.
4. Click **Ok**.
   A screen appears asking if you are sure you want to perform the operation.
5. Select the **Confirm** option.
6. Click **Yes**.
   The operation is successful.

Delete configurations

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Configuration Management** > **Clear Configuration**.
   A screen is displayed asking if you are sure you want to perform the operation.
3. △ CAUTION: **It is recommended that you back up data stored on the virtual disks and hot spare disks on the controller before deleting the virtual drive.**

   Select **Confirm** and click **Yes** to continue.
   The virtual disks and hot spare disks available on the controller are deleted successfully.

Controller management

Clear controller events

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.

2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Clear Controller Events**.
   A screen is displayed asking if you are sure you want to clear the controller events.
4. Select **Confirm** and click **Yes** to continue.

Save controller events

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Save Controller Events**.
   A screen is displayed asking if you want to replace the existing file name.
4. Select **Confirm** and click **Yes** to continue.

Save debug log

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Save Debug Log**.
   A screen is displayed indicating that the operation is successful.
4. Click **Ok**.

Enable security

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Enable security**, select **Local Key Management**.
4. Click **Ok**.
5. If you want to use the passphrase generated by the controller, click **Suggest Passphrase** and **Confirm** the passphrase by re-entering.
   The operation is successful.
6. Select **I Recorded the Security Settings For Future Reference**, click **Enable Security**.
   A screen is displayed indicating that the security will be enabled on this controller if you proceed.
7. Select **Confirm** and click **Yes** to continue.
   The operation is successful and click **Ok**.

Disable security

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Disable security**.
   A screen is displayed asking if you are sure you want to disable security.
4. Select **Confirm** and click **Yes** to continue.
   The operation is successful and click **Ok**.

Change security settings

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Change Security Settings**, select **Change Current Security Settings**.
4. Click **Ok**.
5. If you want to use the passphrase generated by the controller, click **Suggest Passphrase** and **Confirm** the passphrase by re-entering.
   The operation is successful.
6. Click **Save Security Settings**.
7. Select **Confirm** and click **Yes** to continue.
   The operation is successful and click **Ok**.

Restore factory default settings

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Set Factory Defaults**.
   A screen is displayed asking you to confirm the operation.
3. Select **Confirm** and click **Yes** to continue.

Auto configure behavior

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management > Manage Controller Mode**.
   You can view current Controller Mode.
3. Click **Manage Controller Mode**.
   You can view/change the physical disk settings for the controller, if required. The possible options are:
   - Off and Non-RAID Disk
4. Click **Apply Changes** to save the changes.
5. Select **Confirm** and click **Yes** to continue.

   ⓘ NOTE: This feature is not supported on PERC H355 adapter SAS, PERC H355 front SAS, and PERC H350 adapter SAS

Manage controller profile

About this task

View the details of the profile and choose the desired profile, if supported. To view the properties of the controller profiles:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Manage Controller Profiles**.
   The current profile and profile properties are displayed.

Advanced controller properties

Set the patrol read mode

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Patrol Read**.
   The following options are displayed:
   - Start—Starts patrol read for the selected controller.
   - Suspend—Suspends the ongoing patrol read operation on the controller.
   - Resume—Resumes the suspended patrol read operation.
   - Stop—Stops patrol read for the selected controller.
4. Set the **Mode** to **Auto**, **Manual**, or **Disabled**.
5. Click **Apply Changes**.

Enable physical disk power management

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Physical Disk Power Management**.
   The following list of options is displayed:
   - Time Interval for Spin Down—allows the user to specify the delay time before a disk is spun down.
   - Spin Down Hot Spare—allows you to enable or disable the spin down of hot spare disks.
   - Spin Down Unconfigured Good—spin down of un-configured disks.
4. Select the applicable options and click **Apply Changes**.
   The changes made are saved successfully.

Configure hot spare drives

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Spare**.
   The following list of options are displayed:
   - Persistent Hot Spare—allows you to enable or disable the ability to have same system backplane or storage enclosure disk slots dedicated as hot spare slots.
   - Allow Replace Member with Revertible Hot Spare—allows you to enable or disable the option to copy the data form a hot spare disk to physical disk.
   - Auto Replace Member on Predictive Failure—allows you to enable or disable the option to start a Replace Member operation if a predictive failure error is detected on a physical disk.
4. Select the applicable option and click **Apply Changes**.
   The changes made are saved successfully.

Set task rates

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Task Rates**.

The following options are displayed:

- Background Initialization (BGI) Rate
- Consistency Check Rate
- Rebuild Rate
- Reconstruction Rate

4. You can make the necessary changes and then click **Apply Changes**.
   The task rates operation is completely successfully.

Properties of Enterprise Key Management (EKM)

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Enterprise Key Management**.
   The properties of Enterprise Key Management is displayed.

Controller properties

Auto import foreign configuration

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, set the **Auto Import Foreign Configuration** option to **Enabled** or **Disabled**.
4. Click **Apply Changes**.

Disable auto import

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, set the **Auto Import Foreign Configuration** option to **Disabled**.
4. Click **Apply Changes**.
   The auto import is disabled successfully.

Enable auto import

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, set the **Auto Import Foreign Configuration** option to **Enabled**.
4. Click **Apply Changes**.
   The auto import is enabled successfully.

Select boot mode

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, select boot mode from the **Boot Mode** drop-down box.
   The following lists of boot mode options appear:

Table 10. Boot mode options

Option	Description
Stop on errors	The system stops during boot for errors which require attention from the user to rectify the issue.
Pause on errors	System pauses during boot to show errors but continue boot after it times out. Only critical events with an infinite timeout halt boot and require the user's attention to correct the issue.

ⓘ **NOTE:** In UEFI BIOS mode, errors with timeouts do not appear during boot. It is designed to arise only in legacy BIOS mode.

ⓘ **NOTE:** By default, the boot mode option is set to pause on errors.

4. Click **Apply Changes**.
   The boot mode operation is completed successfully.

Abort the consistency check

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, set the **Abort Consistency Check on Error** option to **Enabled** or **Disabled**.
4. Click **Apply Changes**.
   The option to abort the consistency check operation on a redundant virtual disk is enabled if there is any inconsistency found in the data.

Preboot trace buffer

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, set the **Preboot Trace Buffer** option to **Enabled** or **Disabled**.
4. Click **Apply Changes**.

Clear the cache memory

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Cache and Memory** > **Discard Preserved Cache**.
   The preserved cache is cleared successfully.

Enable boot support

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management**.
3. From the **Select Boot Device** drop-down box, select the primary bootable device.

   In **Select Boot Device**, you will not be able to view 4 K sector drives. To view all the virtual disks created, navigate to the **Virtual Disk Management** screen in HII. For more information, see Virtual disk management.

If no boot device is selected, the first virtual disk will be set as the boot device on the next reboot. A Non-RAID disk is auto-selected as the boot device, if the controller does not have any virtual disks present.

ⓘ NOTE: **Select Boot Device** is only applicable in legacy BIOS mode.

ⓘ NOTE: 4 K sector drives boot support is only available in UEFI mode and managed by the boot loader.

4. Click **Apply Changes**.
   Boot support is enabled for the selected controller.

Virtual disk management

Virtual disk numbering

Virtual disks are numbered in descending order beginning with the highest, ID 239.

View virtual disk properties

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   All the virtual disks associated with the RAID controller are displayed.
3. To view the properties, click on the virtual disk. You can view the following properties of the Virtual disk:

Table 11. Virtual disk properties

Option	Description
Operation	List of operations you can perform on the selected virtual disk. The options are: • Blink • Unblink • Delete Virtual Disk • Reconfigure Virtual Disks • Fast Initialization • Slow Initialization
Name	Indicates the name of the virtual disk.
RAID level	Indicates the RAID level of the virtual disk.
Status	Indicates the status of the virtual disk. The possible options are: • Optimal • Degraded • Offline • Failed
Size	Indicates the size of the virtual disk.

View physical disks associated with a virtual disk

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   All the virtual disks associated with the RAID controller are displayed.
3. Click on a virtual disk.
   The properties of the virtual disk are displayed.

4. Click **View Associated Physical Disks**.
   All the physical disks that are associated with the virtual disk are displayed.
5. From the **Associated Physical Disks** section, select the physical disk.
6. Click **View Physical Disk Properties** to view the physical disk properties.

View physical disks associated with a virtual disk

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   All the virtual disks associated with the RAID controller are displayed.
3. Click on a virtual disk.
   The properties of the virtual disk are displayed.
4. Click **Advanced...**.
   You can view the following additional properties of the virtual disk:

Table 12. Advanced properties of the virtual disk

Option	Description
Logical sector size	Indicates the logical sector size of this virtual disk.
Strip element size	Indicates the strip element size for the virtual disk.
Secured	Indicates whether the virtual disk is secured or not.
Bad blocks	Indicates whether the virtual disk has corrupted blocks.

Configure virtual disk policies

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   All the virtual disks associated with the RAID controller are displayed.
3. Click **Advanced...**.
   You can view the following virtual disk policies:

Table 13. Virtual disk policies

Option	Description
Current write cache	Indicates the current write cache policy for the virtual disk.
Default write cache	Allows selection of the write cache policy for the virtual disk. The possible options are: • Write Through • Write Back • Force Write Back
Read cache policy	Allows selection of the read cache policy for the virtual disk. The possible options are: • No Read Ahead • Read Ahead
Disk cache	Allows selection of the disk cache policy for the virtual disk. The possible options are: • Default (Disk Default) • Enable • Disable

4. Click **Apply Changes**.
   The changes made are saved successfully.

Configure Virtual Disks

When configuring the virtual disks, you should consider the workload intended; RAID 1: for simple boot disk; RAID 5 or 6: for file or web servers (sequential reads/writes of files); RAID 10: for transactional database (small random reads and writes).

Virtual disks configured on hard drives should use the controller default cache setting of Write Back and Read Ahead.

Virtual disks configured on SSDs can use the same controller defaults settings as hard drives. Most users perform a copy of OS files or a data base to the new array. This setting provides optimum performance in this configuration.

Once the copy is complete, the array can be used as it is depending on the number and type of SSDs. It is recommended to enable FastPath by changing the controller's Write cache policy to Write Through and the Read cache policy to No Read Ahead. FastPath is developed to achieve the best random read/write performance from SSDs.

Only IO block sizes smaller than the virtual disk's stripe size are eligible for FastPath. In addition, there should be no background operations (rebuild, initialization) running on the virtual disks. FastPath is disabled if there is active background operation.

ⓘ NOTE: RAID 50, and RAID 60 virtual disks cannot use FastPath.

ⓘ NOTE: The Physical Disk Power Management feature is not applicable to FastPath-capable virtual disks.

Perform expand virtual disk operation

Prerequisites

To enable expand virtual disk feature from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   The list of virtual disks is displayed.
3. Select the virtual disk.
4. From the **Operations** drop-down menu, select **Expand Virtual Disk**.

   ⓘ NOTE: You can view the Expand Virtual Disk feature only if there is free space available in the associated disk group.

5. Click **Go**.
6. To expand virtual disk, enter the percentage of available capacity, and then click **Ok**.
   A screen is displayed asking if you are sure you want to perform the operation.
7. Select the **Confirm** option.
8. Click **Yes**.
   The expand virtual disk operation is completed successfully.

Perform consistency check

Prerequisites

To enable consistency check from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   The list of virtual disks is displayed.
3. Select the virtual disk.

   ⓘ NOTE: Consistency check cannot be run on RAID 0 virtual disks.

4. From the **Operations** drop-down menu, select **Check Consistency**.
5. Click **Go**.

A screen is displayed asking if you are sure you want to perform the operation.

6. Select the **Confirm** option.
7. Click **Yes**.
   The consistency check operation is completed successfully.

Physical disk management

View physical disk properties

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Physical Disk Management**.
   All the physical disks associated with the RAID controller are displayed.
3. To view the properties, click the physical disk.

Table 14. Physical disk properties

Option	Description
Operation	The list of operations you can perform on the selected physical disk. The options are: ● Blink ● Unblink ● Assign global hotspare ● Cryptographic erase ● Convert to non–RAID disk
Device ID	Unique identifier of the physical disk.
Backplane ID	Backplane ID in which the physical disk is located in for PERC H755 adapter, PERC H755 front SAS, PERC H755N front NVMe, PERC H750 adapter SAS, PERC H755 MX adapter, PERC H355 adapter SAS, PERC H355 front SAS, and PERC H350 adapter SAS
Slot number	The drive bay in which the physical disk is located for the corresponding backplane or enclosure to which the controller is connected.
Status	Status of the physical disk.
Size	Size of the physical disk.
Type	Type of the physical disk.
Model	Model of the physical disk.
Serial number	Serial of the physical disk.

4. To view additional properties of the physical disk, click **Advanced....**

Table 15. Advanced physical disk properties

Option	Description
Logical sector size	Logical sector size of the selected physical disk
Physical sector size	Physical sector size of the selected physical disk
SMART status	SMART status of a physical disk
Revision	Firmware version of the physical disk
WWID	Unique identifier used to identify the device
Multipath	Multipath of the controller

Table 15. Advanced physical disk properties (continued)

Option	Description
Physical disk power state	Power condition (On or Power Save) of the physical disk
Disk cache setting	Disk cache setting ⓘ NOTE: Disk cache for SATA Gen3 drives is disabled by default.
Disk protocol	Type of hard disk used
Device speed	Speed of the physical disk
Negotiated link speed	Negotiated link speed of the device
PCIe capable link width	N/A for SAS/SATA drives
PCIe negotiated link width	N/A for SAS/SATA drives
Encryption capable	Encryption capability of the physical disk
Encryption supported	Encryption capability enabled at the controller level
Secured	Security status of the physical disk
Cryptographic erase capable	Cryptographic erase capability of the physical disk

Cryptographic erase

Cryptographic erase is a process to erase all data permanently on an encryption-capable and unconfigured physical disk, and reset the security attributes.

Prerequisites

- The non-RAID and virtual disks associated with the drive are deleted.
- The disks are not hot spares.

About this task

The Cryptographic erase feature is supported only on Instant Secure Erase (ISE) and Self Encrypting Drives (SED) drives.

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Physical Disk Management**.
   The list of physical disks is displayed.
3. Select a physical disk.
4. From the **Operations** drop-down menu, select **Cryptographic Erase**.

   ⓘ NOTE: If the drive installed is ISE or SED capable only then the Cryptographic erase option is displayed.

5. Click **Go**.
   A screen is displayed asking if you are sure you want to perform the operation.
6. Select the **Confirm** option.
7. Click **Yes**.
   The Cryptographic erase operation is completed successfully.

Physical disk erase

Prerequisites

To use the Physical Disk Erase feature from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Physical Disk Management**.
   The list of physical disks is displayed.
3. Select a physical disk.
4. From the **Operations** drop-down menu, select **Physical Disk Erase**.

   ⓘ NOTE: If the drive installed is neither SED or ISE capable, then only the Physical Disk Erase option is displayed.

5. Click **Go**.
   A screen is displayed asking if you are sure you want to perform the operation.
6. Select the **Confirm** option.
7. Click **Yes**.
   The physical disk erase operation is completed successfully.

Assigning a global hot spare

Prerequisites

To assign a global hot spare from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Physical Disk Management**.
   The list of physical disks is displayed.
3. Select the physical disk.
4. From the **Operations** drop-down menu, select **Assign Global Hot Spare**.
5. Click **Go**.
   A screen is displayed asking if you are sure you want to perform the operation.
6. Select the **Confirm** option.
7. Click **Yes**.
   The global hot spare disk is created successfully.

Assigning a dedicated hot spare

Prerequisites

To assign a dedicated hot spare from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Physical Disk Management**.
   The list of physical disks is displayed.
3. Select the physical disk.
4. From the **Operations** drop-down menu, select **Assign Dedicated Hot Spare**.
5. Click **Go**.
   A screen is displayed asking if you are sure you want to perform the operation.
6. Select the **Confirm** option.
7. Click **Yes**.
   The dedicated hot spare disk is created successfully.

Convert to RAID capable

Prerequisites

To convert a non–RAID disk to RAID capable disk from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Physical Disk Management**.
   The list of physical disks appears.
3. Select the physical disk.
4. From the **Operations** drop-down menu, select **Convert to RAID capable**.
5. Click **Go**.
   A screen appears asking if you are sure you want to perform the operation.
6. Select the **Confirm** option.
7. Click **Yes**.
   The operation is successful.

Convert to Non–RAID disk

Prerequisites

To convert a physical disk to non–RAID disk from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Physical Disk Management**.
   The list of physical disks appears.
3. Select the physical disk.
4. From the **Operations** drop-down menu, select **Convert to Non–Raid disk**.
5. Click **Go**.
   A screen appears asking if you are sure you want to perform the operation.
6. Select the **Confirm** option.
7. Click **Yes**.
   The operation is successful.

Hardware components

View battery properties

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Hardware Components** > **Battery Management**.
   The battery and capacity information are displayed.
3. You can view the following properties of the battery:

   Table 16. Battery properties

Field	Description
Type	Displays the type of battery available.
Status	Displays the current status of the battery.

Table 16. Battery properties (continued)

Field	Description
Temperature	Displays the current temperature of the battery and also indicates whether the temperature is normal or high.
Charge	Displays the available charge of the battery in percentage.

4. Displays click **Advanced...**.
   The additional advanced properties of the physical battery are displayed.
5. You can view the following advanced properties of the battery:

Table 17. Advanced battery properties

Field	Description
Status	Displays whether the current status of the battery is learning, degraded, or failed.
Voltage	Displays whether the voltage status of the battery is normal or high.
Current	Displays power consumption of the battery in milliamps (mA).
Full capacity	Displays the maximum charge capacity of the battery.
Remaining capacity	Displays the current charge capacity of the battery.
Expected margin of error	Displays expected margin of error.
Completed discharge cycles	Displays the completed discharge cycles.
Learn mode	Displays the condition of the battery. The learn cycle is a periodic operation that calculates the charge that is remaining in the battery to ensure there is sufficient energy.

View physical disks associated with an enclosure

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Hardware Components** > **Enclosure Management**.
3. From the **Select Enclosure** field, choose the enclosure for which you need to view the physical disks.
   All the physical disks that are associated with the virtual disk are displayed.
4. Click the **Attached Physical Disks** drop-down box.
   All the physical disks that are associated with the selected enclosure are displayed.

Security key management in HII configuration utility

The Dell OpenManage storage management application and the **HII Configuration Utility** of the controller allow security keys to be created and managed as well as create secured virtual disks. The following section describes the menu options specific to security key management and provide detailed instructions to perform the configuration tasks. The contents in the following section apply to the **HII Configuration Utility**. For more information on the management applications, see Applications and User Interfaces supported by PERC 11 .

- The **Controller Management** screen displays controller information and action menus. You can perform the following security-related actions through the controller management menu:
  - **Security Key Management**—Creates or changes the local key management (LKM) security key. Deletes the local key management (LKM) or secure enterprise key manager (SEKM) security key.
- The **Virtual Disk Management** screen displays physical disk information and action menus. You can perform the following security related actions through the virtual disk management menu:
  - **Secure Disk Group**—Secures all virtual disks in disk group.
  - **Create secure virtual disk**—Creates a new virtual disk that is secured with the security key on the controller.

- The **Physical Disk Management** screen displays physical disk information and action menus. You can perform the following security-related actions through the physical disk management menu:
  - **Secure non-RAID disk**—Secures the non-RAID disk with the controller security key.
  - **Cryptographic Erase**—Permanently erases all data on the physical disk and resets the security attributes.

For more information on the Physical Disk Management screen and the Virtual Disk Management screen, see Physical disk management and Virtual disk management.

8

Security key and RAID management

Topics:

Security key implementation

The PERC 11 series of cards support self-encrypting disk (SED) for protection of data against loss or theft of SEDs. Protection is achieved by the use of encryption technology on the drives. There is one security key per controller. You can manage the security key using local key management (LKM) or OpenManage Secure Enterprise Key Manager, also referred as Secure Enterprise Key Manager (SEKM). The LKM key can be escrowed in to a file using Dell OpenManage Storage Management application. The security key is used by the controller to lock and unlock access to encryption-capable physical disks. In order to take advantage of this feature, you must:

1. Have SEDs in your system.
2. Create a security key.

Local Key Management

You can use Local Key Management (LKM) to generate the key ID and the passphrase required to secure the virtual disk. You can secure virtual disks, change security keys, and manage secured foreign configurations using this security mode.

ⓘ **NOTE:** Under LKM, you are prompted for a passphrase when you create the key. This mode is not supported on PERC H355 adapter SAS and PERC H350 adapter SAS.

Create a security key

About this task

ⓘ **NOTE:** There is no passphrase backup option when you create a security key; you need to remember your passphrase.

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Enable Security**.
3. Select the **Security Key Management** mode as **Local Key Management**.
4. Click **Ok**.
5. In the **Security Key Identifier** field, enter an identifier for your security key.

ⓘ NOTE: The Security Key Identifier is a user supplied clear text label used to associate the correct security key with the controller.

6. If you want to use the passphrase generated by the controller, click **Suggest Passphrase**.
   Assigns a passphrase suggested by the controller automatically.
7. In the **Passphrase** field, enter the passphrase.

   ⓘ NOTE: Passphrase is case-sensitive. You must enter minimum 8 or maximum 32 characters. Ensure that the characters contain at least one number, one lower case letter, one upper case letter, and one non-alphanumeric character.

8. In the **Confirm** field, re-enter the passphrase to confirm.

   ⓘ NOTE: If the Passphrase entered in the Passphrase and Confirm fields do not match, then you are prompted with an error message to enter the passphrase again.

9. Select the **I recorded the Security Settings for Future Reference** option.
10. Click **Enable Security**.
    The Security Key is created successfully.

Change Security Settings

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Change Security Settings.**
3. Select security identifier:
   a. To change the **Security key Identifier** enter a new key identifier in **Enter a New Security Key identifier** text box.
   b. To keep existing key identifier, select **Use the existing Security Key Identifier** check box.
4. Enter the existing passphrase.
5. Set passphrase:
   a. To change the security passphrase, enter a new passphrase in the **Enter a New Passphrase** text box. Re-enter the new passphrase to confirm.
   b. To keep the existing passphrase, select **Use the existing passphrase**.
6. Select **I recorded the Security Settings for Future Reference**.
7. Click **Save Security Settings**.
8. Select **Confirm** and then click **Yes**.
   Security settings changed successfully.

Disable security key

About this task

ⓘ NOTE: Disabling Security Key is active if there is a security key present on the controller.

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Disable Security**.
   You are prompted to confirm whether you want to continue.
3. Select the **Confirm** option.
4. Click **Yes**.
   The security key is disabled successfully.

   ⓘ NOTE: All virtual disks must be deleted or removed to disable security.

   ⚠ WARNING: **Any un-configured secured disks in the system will be repurposed.**

Create a secured virtual disk

About this task

To create a secured virtual disk, the controller must have a security key established first. See Create a security key.

ⓘ **NOTE:** Combining SAS and SATA hard drives within a virtual disk is not supported. Also, combining hard drives and olid-state drives (SSDs) within a virtual disk is not supported. Mixing of NVMe drives is not supported.

After the security key is established, perform the following steps:

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Configuration Management** > **Create Virtual Disk**.

   For more information, see Create virtual disks.
3. Select the **Secure Virtual Disk** option.
4. Click **Create Virtual Disk**.
   The secure virtual disk is created successfully.

Secure a non-RAID disk

In HII, secure a non-RAID disk by using the security key of the controller.

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Physical Disk Management**.
   The list of Non-RAID disks is displayed.
3. Select a non-RAID disk.
4. From the **Operations** drop-down menu, select **Secure Non-RAID Disk**.

Secure a pre-existing virtual disk

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   The list of virtual disks is displayed.
3. Select a virtual disk.
4. From the **Operations** drop-down menu, select **Secure Virtual Disk**.

   ⓘ **NOTE:** The virtual disks can be secured only when the virtual disks are in Optimal state.

Import a secured non-RAID disk

If you are inserting a non-RAID disk into a system that has a controller key different from the security key on the drive, the security key from the system in which it was initially secured must be provided in HII.

Prerequisites

ⓘ **NOTE:** The controller must have an existing security key before importing a secured non-RAID disk.

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.

2. Click **Main Menu** > **Configuration Management** > **Manage Foreign Configurations**.
3. Click **Enter Passphrase for Locked Disks**.
   A screen is displayed asking if you are sure you want to perform the operation.
4. Enter **Passphrase** if importing non-RAID disk with a different passphrase.
5. Select the **Confirm** option.
6. Click **Yes**.

   ⓘ NOTE: If **Auto-Configure** for non-RAID Disks is enabled, the disk becomes a non-RAID disk. Else, it is unconfigured.

Import a secured virtual disk

Prerequisites

ⓘ NOTE: The controller must have an existing security key before importing secured foreign virtual disk.

Steps

1. Enter the **Dell PERC 11 Configuration Utility**. See Navigate to Dell PERC 11 configuration utility.
2. Click **Main Menu** > **Configuration Management** > **Manage Foreign Configurations** > **Preview Foreign Configurations**.
3. Click **Import Foreign Configuration**.
   A screen is displayed asking if you are sure you want to perform the operation.
4. Enter **Passphrase** if importing virtual disk with a different passphrase.
5. Select the **Confirm** option.
6. Click **Yes**.
   The foreign configuration is imported successfully.

Dell Technologies OpenManage Secure Enterprise Key Manager

This feature allows the PERC to receive a security key from a remote server instead of saving the key on a local controller. This protects data on secured disks under the PERC if the disks or entire system is stolen. Refer to the www.dell.com/idracmanuals for more information on configuring OpenManage Secure Enterprise Key Manager, as well as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) related configuration.

ⓘ NOTE: Downgrade of PERC firmware to a firmware that does not support enterprise key management while enterprise key manager mode is enabled, is blocked.

ⓘ NOTE: When replacing a controller enabled with enterprise key management, lifecycle controller part replacement will re-configure the new controller to match the existing controller's configuration.

ⓘ NOTE: If key exchange fails during boot, view and correct any connection issues with the key server identified in the iDRAC lifecycle log. Then the system can be cold booted.

Supported controllers for OpenManage Secure Enterprise Key Manager

Enterprise key manager mode is supported on the PERC H755 adapter, PERC H755 front SAS, and PERC H755N front NVMe, and allows the creation of secured virtual disks and non-RAID disks. For more information on supported platforms, see www.dell.com/idracmanuals.

Enterprise key manager mode is not supported on the PERC H755 MX adapter, PERC H355 front SAS, PERC H355 adapter SAS, and PERC H350 adapter SAS.

Manage enterprise key manager mode

iDRAC manages Enterprise key manager features. For instructions on enabling enterprise key manager mode, see www.dell.com/idracmanuals.

NOTE: If preserved cache is present, the controller does not allow OpenManage Secure Enterprise Key Manager (SEKM) mode to be enabled.

NOTE: When enterprise key manager mode is enabled, the controller waits up to two minutes for iDRAC to send keys, after which the PERC continues to boot.

NOTE: Transitioning a controller from Local Key Management (LKM) mode to SEKM mode is supported on firmware starting with version 52.16.1-4074. For more information, see Transition of drives from local key management to enterprise key (with supported fimware for PERC and iDRAC).

NOTE: iDRAC performs rotation of keys. Any attempt to rekey the controller through a different management application is not supported.

Disable enterprise key manager mode

Enterprise key manager mode can be disabled from any supported Applications & User Interfaces supported by PERC 11. For more information, see the management application's user's guide or see Disable security key.

Manage virtual disks in enterprise key manager mode

Virtual disks are managed in the same way in enterprise key manager mode as in local key manager mode. SED capable virtual disks can be secured during or after creation. See Create a secured virtual disk.

Manage non-RAID disks in enterprise key manager mode

Non-RAID disks are managed in the same way in enterprise key manager mode as in local key manager mode. SED capable non-RAID disks can be secured after creation. See Create a secured virtual disk.

Transition of drives from local key management to enterprise key management (with supported firmware for PERC and iDRAC)

PERC enables transition from Local Key Management (LKM) mode to Secure Enterprise Key Manager (SEKM) mode without disabling LKM security first. For instructions on transitioning from LKM mode to SEKM mode, see https://www.dell.com/idracmanuals.

About this task

NOTE: This feature is supported on firmware starting with version 52.16.1-4074.

The transition from LKM to SEKM on the controller fails if the following are true at time of attempt:

- Snapdump is present on PERC.
- Preserved cache is present on PERC.
- RAID level migration is in progress on PERC.
- Online capacity expansion is in progress on PERC.
- Sanitize on a physical disk is in progress.
- LKM key that does not match with the current key of PERC.
- PERC firmware does not support transition.

Transition of drives from local key management to enterprise key management (without supported firmware for PERC and iDRAC)

Local key management drives can be transitioned to an enterprise key management enabled system, but the controller cannot be transitioned from local key management mode to enterprise key manager mode or the reverse without first disabling security on the controller. Perform the following steps to transition from local key management drives to enterprise key management:

Steps

1. Save the current local key management security key.
2. Shut down both systems.
3. Remove the local key management drives and reinsert them to the enterprise key manager enabled system.
4. Power on the enterprise key manager system.
5. Go to HII foreign configuration.
6. Enter the local key management keys for those drives.
7. Import the configuration.

   ⓘ NOTE: Once local key management drives are migrated to enterprise key manager, they cannot be migrated back to local key management mode. The drives have to be cryptographically erased to disable security and then converted back to local key management disks. For more information about performing this action, contact https://www.dell.com/supportassist.

9

Troubleshooting

To get help with your Dell Technologies PowerEdge RAID Controller 11 series, you can contact your Dell Technical Service representative or see https://www.dell.com/support.

Topics:

Single virtual disk performance or latency in hypervisor configurations

Multi-initiator or hypervisor configurations running multiple I/O workloads to a single raid array may experience degraded performance or latency. This is caused by upper layers sending separate I/O workloads for each virtual machine to the storage subsystem which ends up being a random I/O workload to the under lying RAID array. For I/O workload configurations that require lower latency restrictions and higher I/O performance it may be beneficial to run fewer I/O workloads to individual RAID arrays or to use separate RAID arrays and physical disks for each I/O workload. Other considerations are making sure write-back, read ahead cache is enabled for rotational disks or using solid state drives (SSDs) to improve random I/O workload performance.

Performance degradation may also be observed when background operations such as initialization, consistency check, or reconstructions are running on the virtual disk. See your hypervisor storage best practices or performance best practices guides for additional configuration support.

Configured disks removed or not accessible error message

Error Message:

```
Some configured disks have been removed from your system or are no longer
accessible. Check your cables and ensure all disks are present. Press any
key or 'C' to continue.
```

Probable Cause: The message indicates that some configured disks were removed. If the disks were not removed, they are no longer accessible. The cables from the PERC controller to the backplane might be improperly connected.

Corrective Action: Check the cable connections and fix issues if any. Restart the system. If there are no cable problems, press any key or <C> to continue.

Dirty cache data error message

Error Message:

```
The following virtual disks are missing: (x). If you proceed (or load
the configuration utility), these virtual disks will be removed from your
configuration. If you wish to use them at a later time, they will have
to be imported. If you believe these virtual disks should be present,
please power off your system and check your cables to ensure all disks
are present. Press any key to continue, or 'C' to load the configuration
utility. The cache contains dirty data, but some virtual disks are missing
or will go offline, so the cached data cannot be written to disk. If this
is an unexpected error, then please power off your system and check your
cables to ensure all disks are present. If you continue, the data in cache
will be permanently discarded. Press 'X' to acknowledge and permanently
destroy the cached data.
```

Probable Cause: The controller preserves the dirty cache from a virtual disk if the disk becomes offline or is deleted because of missing physical disks. This message indicates that some configured disks were removed. If the disks were not removed, they are no longer accessible. The cables from the PERC controller to the backplane might be improperly connected.

Corrective Action: Check the cable connections and fix any problems. Restart the system. Use the HII configuration utility to import the virtual disk or discard the preserved cache. For the steps to discard the preserved cache, see Clear the cache memory.

Discovery error message

Error Message:

```
A discovery error has occurred, please power cycle the system and all the
enclosures attached to this system.
```

Probable Cause: This message indicates that discovery did not complete within 120 seconds. The cables from the PERC controller to the backplane might be improperly connected.

Corrective Action: Check the cable connections and fix any problems. Restart the system.

Drive Configuration Changes Error Message

Error Message:

```
Entering the configuration utility in this state will result in drive
configuration changes. Press 'Y' to continue loading the configuration
utility or please power off your system and check your cables to ensure all
disks are present and reboot.
```

Probable Cause: The message is displayed after another HII warning indicating there are problems with previously configured disks and you have chosen to accept any changes and continue. The cables from the PERC controller to the backplane might be improperly connected.

Corrective Action: Check the cable connections and fix any problems before restarting the system. If there are no cable problems, press any key or <Y> to continue.

Windows operating system installation errors

Ensure that you perform the following step before installing Windows on 4 KB sector drives:

1. Read and understand the updates to the version of Windows that you have installed. You can find this information in the Microsoft help. For more information, see Microsoft support policy for 4 K sector hard drives in Windows.

Firmware fault state error message

Error Message: `Firmware is in Fault State.`

Corrective Action: Contact Global Technical Support.

Foreign configuration found error message

Error Message: `Foreign configuration(s) found on adapter. Press any key to continue, or 'C' to load the configuration utility or 'F' to import foreign configuration(s) and continue.`

Probable Cause: When a controller firmware detects a physical disk with existing foreign metadata, it flags the physical disk as **foreign** and generates an alert indicating that a foreign disk was detected.

Corrective Action: Press **<F>** at this prompt to import the configuration (if all member disks of the virtual disk are present) without loading the **HII Configuration Utility**. Or press **<C>** to enter the **HII Configuration Utility** and either import or clear the foreign configuration.

Foreign configuration not found in HII error message

Error Message: `The foreign configuration message is present during POST but no foreign configurations are present in the foreign view page in HII configuration utility. All virtual disks are in an optimal state.`

Corrective Action: Ensure all your PDs are present and all VDs are in optimal state. Clear the foreign configuration using **HII configuration utility** or **Dell OpenManage Server Administrator Storage Management**.

△ CAUTION: **The physical disk goes to Ready state when you clear the foreign configuration.**

If you insert a physical disk that was previously a member of a virtual disk in the system, and that disk's previous location has been taken by a replacement disk through a rebuild, you must manually remove the foreign configuration flag of the newly inserted disk.

Degraded state of virtual disks

A redundant virtual disk is in a degraded state when one or more physical disks have failed or are inaccessible. For example, if a RAID 1 virtual disk consists of two physical disks and one of them fails or become inaccessible, the virtual disk become degraded.

To recover a virtual disk from a degraded state, you must replace the failed physical disk and rebuild it. Once the rebuilding process is complete, the virtual disk state changes from degraded to optimal.

Memory errors

Memory errors can corrupt cached data, so the controllers are designed to detect and attempt to recover from the memory errors. Single-bit memory errors can be handled by the controller and do not disrupt normal operation. A notification is sent if the number of single-bit errors exceeds a threshold value.

Multi-bit errors are more serious as they result in corrupted data and data loss. The following are the actions that occur in the case of multi-bit errors:

- If a multi-bit error occurs while accessing data in the cache when the controller is started with dirty cache, the controller discards the cache contents. The controller generates a warning message to the system console to indicate that the cache was discarded and generates an event.
- If a multi-bit error occurs at run-time either in code/data or in the cache, the controller stops.
- The controller logs an event to the controller's internal event log and a message during POST is displayed indicating a multi-bit error has occurred.

ⓘ **NOTE:** In case of a multi-bit error, contact Global Technical Support.

Preserved Cache State

The controller preserves the dirty cache from a virtual disk if the virtual disk goes offline or is deleted because of missing physical disks. This preserved dirty cache is called **pinned cache** and is preserved until you import the virtual disk or discard the cache.

1. Import the virtual disk—Power off the system, re-insert the virtual disk and restore the system power. Use the **HII Configuration Utility** to import the foreign configuration.
2. Discard the preserved cache—See Clear the cache memory.

ⓘ **NOTE:** It is recommended to clear the preserved cache before reboot using any of the virtual disks present on the controller.

Security key errors

Secured foreign import errors

A foreign configuration is a RAID configuration that already exists on a replacement physical disk that you install in a system. A secured foreign configuration is a RAID configuration that was created under a different security key.

There are two scenarios in which a secured foreign import fails:

- **The passphrase authentication fails**—A virtual disk secured with a security key different from the current controller security key cannot be imported without authentication of the original passphrase used to secure them. Supply the correct passphrase to import the secured foreign configuration. If you have lost or forgotten the passphrase, the secured foreign disks remain locked (inaccessible) until the appropriate passphrase is entered or if they are erased.
- **The secured virtual disk is in an offline state after supplying the correct passphrase**—You must check to determine why the virtual disk failed and correct the problem.

Failure to select or configure non Self-Encrypting Disks non-SED

A virtual disk can be either secured or unsecured depending on how it was configured when created. In order to create a secured virtual disk, the controller must have a security key present and must contain SEDs only. In order to select/configure non-SED, you must create an unsecured virtual disk. You can create an unsecured virtual disk even if there is a security key. Select the **Secure VD** option as **No** in the **Create New VD** menu. For steps on how to create an unsecured virtual disk, see Create virtual disks.

Failure to delete security key

A security key is used to lock or unlock access to a security-enabled component. This key is not utilized in the actual encryption of data. If a security key is present, both secured and unsecured virtual disks may exist.

To delete the security key, you must have a previously established security key present on the controller and there cannot be any configured secured disks. If there are configured secured virtual disks, remove or delete them.

Failure of Cryptographic Erase on encryption-capable physical disks

Cryptographic Erase is the process of securely erasing all data permanently on an encryption-capable physical disk and resetting the security attributes. It is used in scenarios such as deleting a foreign configuration in the event of a forgotten or lost passphrase or unlocking a disk that had been previously locked.

You can perform Cryptographic Erase only on encryption-capable disks that are not hot spares and not configured as non-RAID or virtual disks. Ensure that the conditions are met and see Cryptographic Erase.

General issues

PERC card has yellow bang in Windows operating system device manager

Issue: The device is displayed in **Device Manager** but has a yellow bang (exclamation mark).

Corrective Action: Reinstall the driver. For more information on reinstalling drivers, see Driver support for PERC 11 .

PERC card not seen in operating systems

Issue: The device does not appear in the **Device Manager**.

Corrective Action: Turn off the system and reseat the controller.

For more information, see Install and remove a PERC 11 card.

Physical disk issues

Physical disk in failed state

Issue: One of the physical disks in the disk array is in the failed state.

Corrective Action: Update the PERC cards to the latest firmware available on https://www.dell.com/support and replace the drive.

Unable to rebuild a fault tolerant virtual disk

Issue: Cannot rebuild a fault tolerant virtual disk. For more information, see the alert log for virtual disks.

Probable Cause: The replacement disk is too small or not compatible with the virtual disk.

Corrective Action: Replace the failed disk with a compatible good physical disk with equal or greater capacity.

Fatal error or data corruption reported

Issue: Fatal error(s) or data corruption(s) are reported when accessing virtual disks.

Corrective Action: Contact Global Technical Support.

Multiple disks are inaccessible

Issue:	Multiple disks are simultaneously inaccessible.
Probable Cause:	Multiple physical disk errors in a single array typically indicate a failure in cabling or connection and could involve the loss of data.
Corrective Action:	You can recover the virtual disk after multiple physical disks become simultaneously inaccessible. Perform the following steps to recover the virtual disk:

△ CAUTION: **Follow the safety precautions to prevent electrostatic discharge.**

1. Turn off the system, check cable connections, and reseat physical disks.
2. Ensure that all the disks are present in the enclosure.
3. Turn on the system and enter the **HII Configuration Utility**.
4. Import the foreign configuration.
5. Press <F> at the prompt to import the configuration, or press <C> to enter the **HII Configuration Utility** and either import or clear the foreign configuration.

If the virtual disk is redundant and transitioned to **Degraded** state before going **Offline**, a rebuild operation starts automatically after the configuration is imported. If the virtual disk has gone directly to the **Offline** state due to a cable pull or power loss situation, the virtual disk is imported in its **Optimal** state without a rebuild occurring.

ⓘ NOTE: You can use the **HII Configuration Utility** or Dell OpenManage storage management application to perform a manual rebuild of multiple physical disks.

Rebuilding data for a failed physical disk

Issue:	Rebuilding data for a physical disk that is in a failed state.
Probable Cause:	Physical disk is failed or removed.
Corrective Action:	If you have configured hot-spares, the PERC card automatically tries to use one of the hot-spares to rebuild a physical disk that is in a failed state. Manual rebuild is necessary if no hot-spares with enough capacity to rebuild the failed physical disks are available. You must insert a physical disk with enough storage in the subsystem before rebuilding the physical disk.

ⓘ NOTE: You can use the **HII Configuration Utility** or Dell OpenManage storage management application to perform a manual rebuild of an individual physical disk.

Virtual disk fails during rebuild using a global hot spare

Issue:	A virtual disk fails during rebuild while using a global hot spare.
Probable Cause:	One or more disks in the virtual disks fails or is disconnected while the rebuild is in progress.
Corrective Action:	No action is required. The global hot spare reverts to **Hot spare** state and the virtual disk is in **Failed** state.

Dedicated hot spare disk fails during rebuild

Issue:	A hot spare disk fails during rebuild while using a dedicated hot spare.
Probable Cause:	The dedicated hot spare assigned to the virtual disk fails or is disconnected while the rebuild is in progress.
Corrective Action:	If there is a global hot spare available with enough capacity, rebuild will automatically start on the global hot spare. Where there is no hot spare present, you must insert a physical disk with enough capacity into the system before performing a rebuild.

Redundant virtual disk fails during reconstruction

Issue: Multiple disks fails during a reconstruction process on a redundant virtual disk that has a hot spare.

Probable Cause: Multiple physical disks in the virtual disk is failed or the cables are disconnected.

Corrective Action: No action is required. The physical disk to which a reconstruction operation is targeted reverts to **Ready** state, and the virtual disk goes to **Failed** state. If there are any other virtual disks that can be supported by the capacity of the hot spare then the dedicated hot spare is converted to global hot spare, if not the hot spare will revert back to **Ready** state.

Virtual disk fails rebuild using a dedicated hot spare

Issue: A virtual disk fails during rebuild while using a dedicated hot spare.

Probable Cause: One or more disks in the virtual disks fails or is disconnected while the rebuild is in progress.

Corrective Action: No action is required. The dedicated hot spare is in **hot spare** state and converted to global hot spare if there is any other virtual disk that is supported, otherwise the dedicated hot spare reverts to **Ready** state and the virtual drive is in **Failed** state.

Physical disk takes a long time to rebuild

Issue: A physical disk is taking longer than expected to rebuild.

Description: A physical disk takes longer to rebuild when under high I/O stress. There is only one rebuild I/O operation for every five host I/O operations.

Corrective Action: If possible, reduce I/O stress on the physical disk or increase the value of rebuild rate controller parameter.

Drive removal and insertion in the same slot generates a foreign configuration event

Issue: When a drive which is part of a virtual disk is removed and reinserted into the same slot the drive goes through a transient state of being foreign for a short period of time before rebuilding.

Description: This transient state could be reported as an event in management applications as **A foreign configuration was detected on RAID Controller is SL x**, where x is the slot of the RAID controller.

Corrective Action: No action is required on the foreign configuration state of the drive as it is transient and the controller handles the event automatically.

SMART errors

SMART monitors the internal performance of all motors, heads, and physical disk electronics and detects predictable physical disk failures.

ⓘ NOTE: For information about where to find reports of SMART errors that could indicate hardware failure, see the Dell OpenManage storage management documentation at www.dell.com/openmanagemanuals.

Smart error detected on a non-RAID disk

Issue: A SMART error is detected on a non-RAID disk.

Corrective Action: Perform the following steps:

1. Back up your data.

2. Replace the affected physical disk with a new physical disk of equal or higher capacity.
3. Restore from the backup.

Smart error detected on a physical disk in a non-redundant virtual disk

Issue: A SMART error is detected on a physical disk in a non-redundant virtual disk.

Corrective Action: Perform the following steps:

1. Back up your data.
2. Use **Replace Member** to replace the disk manually.

   NOTE: For more information about the **Replace Member** feature, see Configure hot spare drives.
3. Replace the affected physical disk with a new physical disk of equal or higher capacity.
4. Restore from the backup.

Smart error detected on a physical disk in a redundant virtual disk

Issue: A SMART error is detected on a physical disk in a redundant virtual disk.

Corrective Action: Perform the following steps:

1. Back up your data.
2. Force the physical disk offline.

   NOTE: If a hot spare is present, the rebuild starts with the hot spare after the disk is forced offline.
3. Replace the disk with a new physical disk of equal or higher capacity.
4. Perform the **Replace Member** operation.

   NOTE: The **Replace Member** operation allows you to copy data from a source physical disk of a virtual disk to a target physical disk that is not a part of the virtual disk. For more information about the **Replace Member** feature, see the topic Configure hot spare drives.

Replace member errors

NOTE: For more information about the **Replace Member** features, see Configure hot spare drives.

Source disk fails during replace member operation

Issue: The source disk fails during the **Replace Member** operation and the **Replace Member** operation stops due to the source physical disk error.

Probable Cause: Physical disk failure or physical disk is removed or disconnected.

Corrective Action: No action required. If the virtual disk can tolerate disk failure, and the source data is available from other disks in the virtual disk, the rebuild begins automatically on the target disk, using the data from the other disks. if the virtual disk cannot tolerate the failure, the virtual disk goes to offline state and the replace member operation is stopped.

Target disk fails during replace member operation

Issue: The target disk failure reported during the **Replace Member** operation, and the **Replace Member** operation stops.