About this task

CAUTION: **Ensure that only the appropriate devices are selected for deployment. After deploying a deployment template on a repurpose and bare-metal device, it might not be possible to revert the device to its original configuration.**

Steps

1. From the list of deployment templates on the **Configuration** > **Templates** page, select the check box corresponding to the IOA template you want to deploy, and click **Deploy Template**.
2. In the **Deploy Template: <template_name>** dialog box, under **Target**:
   a. Click **Select**, and then select device(s) in the **Job Target** dialog box. See Selecting target devices and device groups.
   b. Click **OK**.
3. In the **Host Names** dialog box, you can change the **Host name** of the target IOA device. Click **Next**.
4. In the **Advanced Options** dialog box, select **Preview Mode** to simulate the deployment or select **Continue On Warning** to deploy the template and ignore the warnings encountered. Click **Next**.
5. In the **Schedule** section, run the job immediately or schedule for a later time. See Schedule job field definitions on page 192.
6. Click **Finish**. Review the warning message and click **YES**.
   A Device Configuration job is created under Jobs. See Using jobs for device control on page 136.

Clone deployment templates

About this task

Steps

1. From the **OpenManage Enterprise** menu, under **Configuration**, click **Templates**.
   A list of available deployment templates is displayed.
2. Select the check box corresponding to the template you want to clone.
3. Click **Clone**.
4. Enter the name of new deployment template, and then click **Finish**.
   The cloned deployment template is created and displayed in the list of deployment templates.

Auto deployment of configuration on yet-to-be-discovered servers or chassis

Existing deployment templates in the OpenManage Enterprise can be assigned to the servers and chassis which are awaiting discovery. These deployment templates are automatically deployed on the respective devices when they are discovered and onboarded.

To access the **Auto Deploy** page, click **OpenManage Enterprise** > **Configuration** > **Auto Deploy**.

The auto deploy targets and their respective **Identifier** (service tag or node IDs), **template name**, **template type**, **status**, and **Boot to Network ISO status** (for servers) are displayed.

The **Auto Deploy** target list can be customized using the **Advanced Filters** fields available on the top of the list.

Section on the right side of the Auto Deploy page shows the **Created On** and **Created By** details of the selected auto deployment target. When multiple items are selected, details of the last selected item is displayed in the section.

Once an auto-deployment target is discovered, its entry from the Auto-Deploy page is automatically deleted and moved to the All Device page. Also, a profile is created on the Profiles page which contains the configuration settings of the device.

The following actions can be performed on the Auto Deploy page:

- **Create** templates for auto deployment. See Create auto deployment targets on page 98
- **Delete** templates that are not needed. SeeDelete auto deployment targets on page 99
- **Export** the auto deployment templates to different formats. See Export auto deployment target details to different formats on page 99

NOTE:

- Only administrators can perform the create, delete, and export tasks on the auto-deployment templates. The device managers can only 'export' the auto-deployment templates. For more information, see Role and scope-based access control in OpenManage Enterprise on page 18.

Create auto deployment targets

About this task

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope-based access control in OpenManage Enterprise on page 18

To create auto deployment targets :

Steps

1. Click **OpenManage Enterprise** > **Configuration** > **Auto Deploy** > **Create**
   The Auto Deploy Template wizard is displayed.
2. On the **Template Information** page, select the deployment template type (Server or Chassis).
3. From the **Select Template** drop-down menu, select an appropriate template. If the selected template has identity attributes which are not associated with any virtual identity pool, the following message is displayed: *The selected template has identity attributes, but it has not been associated with a virtual identity pool. Deploying this template will not change virtual network addresses on the target devices.*
4. Click Next.
   The **Target Information** page is displayed.
5. On the **Target Information** page, target devices can be selected in one of the following methods:
   - **Enter Manually** : Enter the Service Tag or node IDs to identify the target devices. The identifiers can be entered in any order, however, identifiers must be comma separated. Click Validate to verify the accuracy of the values. It is mandatory to validate the identifiers.
   - **Import CSV**: Click **Import CSV** to browse the folders and select the respective .csv file with the target device details. A summary of the number of successfully imported and invalid entries is displayed. For a more detailed view of the import result, click **View details**.

     The entries in the CSV file must have the following format: The identifiers must be listed in the first column, one per row, starting from the second row. For a template CSV file, click **Download sample CSV file**.
6. Click **Next**.
7. On the **Target Group information** page, specify a subgroup under the **Static group** if available. For more information about grouping of devices, see Organize devices into groups on page 58. The target devices would be placed under the specified target group on their discovery
8. Click **Next**.
9. If the target device is a server, on the **Boot to Network ISO** page :
   - Select the **Boot to Network ISO** check box.
   - Select **CIFS** or **NFS**.
   - Enter the **ISO Path** of location where the ISO image file is stored. Use tool tips to enter the correct syntax.
   - Enter **Share IP Address**, **Workgroup**, **Username**, and **password**.
   - Select the **Time to Attach ISO** dropdown menu options to set the number of hours the network ISO file will remain mapped to the target device(s). By default, this value is set as four hours.
   - Click **Next**.
10. On the **Virtual Identities** page, click **Reserve identities**.
    The assigned virtual identities of the NIC cards of the selected target device are displayed. To view all the assigned identities of the identity pool of the selected target device, click **View all NIC details**.
11. In the **Target Attributes** section, the non-virtual identity attributes specific to each of the selected target devices, such as the location attributes and IP address, can be changed before deploying the deployment template. When the template is deployed, these changed target attributes are implemented on only the specific devices. To change the device-specific, non-virtual identity attributes:
    a. Select a target device from the list displaying the previously-selected target devices.
    b. Expand the attribute categories and then select or clear the attributes that must be included or excluded during template deployment on the target device.

c. Click **Next**.

12. Click **Finish**.
    An alert message *Deploying a template can cause data loss and can cause a restart of the device. Are you sure you want to deploy the template?* is displayed.
13. Click **Yes**.
    A new Auto Deploy target is created and listed on the **Auto Deploy** page.

Delete auto deployment targets

About this task

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18

NOTE: If a template that is associated with auto deployment targets is deleted from the **OpenManage Enterprise** > **Configuration** > **Templates** page, the associated auto deploy entries would also get deleted irrespective of their current state.

To remove the auto deployment targets from the **Auto Deploy** list.

Steps

1. Go to the Auto Deploy page by clicking **OpenManage Enterprise** > **Configuration** > **Auto Deploy**.
2. Select the auto deploy targets from the list.
3. **Delete**, and then click **Yes** to confirm.
   The auto deploy targets that are selected for deletion are removed from the Auto Deploy page.

Export auto deployment target details to different formats

Steps

1. Go to the Auto Deploy page by clicking **OpenManage Enterprise** > **Configuration** > **Auto Deploy**.
2. Select the auto deploy target from the list and click **Export**.
3. In the **Export All** dialog box, select format as either HTML, or CSV, or PDF. Click **Finish.**
   A job is created and the auto deploy target data is exported in the selected format.

Overview of stateless deployment

To deploy a device deployment template with virtual identity attributes on target devices, do the following:

1. **Create a device template**—Click **Create Template** task under the **Deploy** tab to create a deployment template. You can select to create the template from either a configuration file or a reference device.
2. **Create an identity pool**—Click the **Create** task under the **Identity Pools** tab to create a pool of one or more virtual identity types.
3. **Assign virtual identities to a device template**—Select a deployment template from the **Templates** pane, and click **Edit Network** to assign an identity pool to the deployment template. You can also select the Tagged and Untagged network, and assign the minimum and maximum bandwidth to the ports.
4. **Deploying the deployment template on target devices**—Use the **Deploy Template** task under the **Deploy** tab to deploy the deployment template and virtual identities on the target devices.

Manage identity pools—Stateless deployment

The I/O interfaces of a server, such as NICs or HBAs, have unique identity attributes that are assigned by the manufacturer of the interfaces. These unique identity attributes are collectively known as the I/O identity of a server. The I/O identities uniquely identify a server on a network and also determine how the server communicates with a network resource using a specific protocol. Using OpenManage Enterprise, you can automatically generate and assign virtual identity attributes to the I/O interfaces of a server.

Servers deployed by using a device deployment template that contains virtual I/O identities are known as 'stateless.' Stateless deployments enable you to create a server environment that is dynamic and flexible. For example, deploying a server with virtual I/O identities in a boot-from-SAN environment enables you to quickly do the following:

- Replace a failing or failed server by moving the I/O identity of the server to another spare server.
- Deploy additional servers to increase the computing capability during high workload.

The **OpenManage Enteprise** > **Configuration** > **Identity Pools**page allows you to create, edit, delete, or export virtual I/O pools.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. Role and scope-based access control in OpenManage Enterprise on page 18
- Scope based restrictions don't apply to identity pools, therefore, all identify pools can viewed and used by all user types. However, once the identities are assigned by a device manager, then only those identities can be viewed and used by that device manager.

Create Identity Pool - Pool Information

Identity pools are used for template-based deployment on servers to virtualize the network identity for the following:

- Ethernet
- iSCSI
- Fibre Channel over Ethernet (FCoE)
- Fibre Channel (FC)

You can create a maximum of 5000 identity pools in each of these categories.

The server deployment process fetches the next available identity from the pool and uses while providing a server from the template description. You can then migrate the profile from one server to another without losing access to the network or storage resources in your environment.

You can edit the number of entries in the pool. However, you cannot reduce the number of entries less than those assigned or reserved. You can also delete the entries that are not assigned or reserved.

NOTE: Edit Identity Pool fails when the identities range overlaps. The swapping is not allowed, if you have identity pools configured for Ethernet, FCoE, and iSCSI and you try editing and swapping the starting address which is overlapping with the existing range. To swap the starting MAC address, you must move it out of the conflicting range one section at a time.

Pool Name	Enter a name of the identity pool. The pool name can have a maximum length of 255 characters.
Description	Enter a description for the identity pool. The maximum length of the description is 255 characters.

Actions

Next	Displays the **Ethernet** tab.
Finish	Saves the changes and displays the **Identity Pools** page.
Cancel	Closes the **Create Identity Pool** wizard without saving the changes.

Identity pools

An identity pool is a collection of one or more virtual identity types that are required for network communication. An identity pool can contain a combination of any of the following virtual identity types:

- Ethernet identities

  The Identities which are defined by the Media Access Control (MAC) address. MAC addresses are required for Ethernet (LAN) communications.

- iSCSI identities

  The Identities which are defined by the iSCSI Qualified Name (IQN). IQN identities are required to support boot-from-SAN by using the iSCSI protocol.

- Fibre Channel (FC) identities

  The Identities which are defined by the World Wide Node Name (WWNN) and World Wide Port Name (WWPN). A WWNN identity is assigned to a node (device) in an FC fabric and may be shared by some or all ports of a device. A WWPN identity is assigned to each port in an FC fabric and is unique to each port. WWNN and WWPN identities are required to support boot-from-SAN and for data access using FC and Fibre Channel over Ethernet (FCoE) protocols.

- Fibre Channel over Ethernet (FCoE) identities

  Identities that provide a unique virtual identity for FCoE operations. These identities are defined by both MAC address and the FC addresses (that is WWNN and WWPN). WWNN and WWPN identities are required to support boot-from-SAN and for data access using FC and Fibre Channel over Ethernet (FCoE) protocols.

OpenManage Enterprise uses the identity pools to automatically assign virtual identities to the device deployment template that is used for deploying a server.

NOTE:

- For the identities that belong to an existing identity pool but were deployed outside of OpenManage Enterprise, a new Configuration Inventory job must be initiated to identify and designate them as 'assigned' in the appliance.
- The virtual identities which are already assigned, will not be used for a new deployment unless these identities are cleared.

Create identity pools

You can create an identity pool that contains one or more virtual identity types. Common pool created by the administrator can be used by all the device managers. Also, administrator can see all the identities under which are being used. Device managers an see all the identity pools and perform all the operations on it (as specified by RBAC), however under Usage the device managers can only see the identities that are associated to the devices under their scope.

About this task

To create a pool of virtual identity types:

Steps

1. On the **Configuration** page, click **Identity Pools**.
2. Click **Create**.
3. In the **Create Identity Pool** dialog box, under **Pool Information**:
   a. Enter a unique name for the identity pool and an appropriate description.
   b. Click **Next**.
4. In the **Ethernet** section:
   a. Select the **Include ethernet virtual MAC addresses** check box to include the MAC addresses.
   b. Enter a starting MAC address and specify the number of virtual MAC identities to be created.
5. In the **iSCSI** section:
   a. Select the **Include iSCSI MAC addresses** check box to include iSCSI MAC addresses.
   b. Enter the starting MAC address and specify the number of iSCSI MAC addresses to be created.
   c. Select **Configure iSCSI Initiator**, and then enter the IQN prefix.
   d. Select **Enable iSCSI Initiator IP Pool**, and then enter the network details.

NOTE: The iSCSI Initiator IP Pool does not support IPv6 addresses.

6. In the **FCoE** section:
   a. Select the **Include FCoE Identity** check box to include FCoE identities.
   b. Enter the starting MAC address and specify the number of FCoE identities to be created.

   NOTE: The WWPN and WWNN addresses are generated by prefixing 0x2001 and 0x2000 respectively to the MAC addresses.

7. In the **Fibre Channel** section:
   a. Select the **Include FC Identity** check box to include FC identities.
   b. Enter the postfix octets (six octets) and the number of WWPN and WWNN addresses to be created.

   NOTE: The WWPN and WWNN addresses are generated by prefixing the provided postfix with 0x2001 and 0x2000 respectively.

Results

The identity pool is created and is listed under the **Identity Pools** tab.

Create Identity Pool - Fibre Channel

You can add Fibre Channel (FC) addresses to the identity pool. The FC comprises of WWPN/WWNN addresses.

Include FC Identity	Select the check box to add FC addresses to the identity pool.
Postfix (6 octets)	Enter the postfix in one of the following formats: • `AA:BB:CC:DD:EE:FF` • `AA-BB-CC-DD-EE-FF` • `AABB.CCDD.EEFF` The length of the postfix can be a maximum of 50 characters. This option is displayed only if the **Include FC Identity** check box is selected.
Number of WWPN/WWNN Addresses	Select the number of WWPN or WWNN address. The address can be between 1 and 5000. This option is displayed only if the **Include FC Identity** check box is selected.

Actions

Previous	Displays the **FCoE** tab.
Finish	Saves the changes and displays the **Configuration** page.
Cancel	Closes the **Create Identity Pool** wizard without saving the changes.

Create Identity Pool - iSCSI

You can configure the required number of iSCSI MAC addresses in the iSCSI tab.

NOTE: The iSCSI attributes are applied only when the DHCP option for iSCSI Initiator is disabled in the source template.

Include virtual iSCSI MAC Addresses	Select the check box to add the iSCSI MAC addresses to the identity pool.
Starting virtual MAC Address	Enter the starting MAC address of the identity pool in one of the following formats: • `AA:BB:CC:DD:EE:FF`

- AA-BB-CC-DD-EE-FF
- AABB.CCDD.EEFF

The maximum length of a MAC address is 50 characters. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.

Number of iSCSI MAC addresses Enter the number of iSCSI MAC addresses. The MAC address can be between 1 and 5000. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.

Configure iSCSI Initiator Select the check box to configure the iSCSI initiator. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.

IQN Prefix Enter the IQN prefix of iSCSI identity pool. The length of the IQN prefix is a maximum of 200 characters. The system generates the pool of IQN addresses automatically by appending the generated number to the prefix. For example: `<IQN Prefix>.<number>`

This option is displayed only if the **Configure iSCSI Initiator** check box is selected.

NOTE: The IQN configured with identity pools is not deployed on the target system if the boot mode is "BIOS".

NOTE: If the iSCSI initiator name is displayed in a separate line in the **Identity Pools** > **Usage** > **iSCSI IQN** field, then, it indicates that the iSCSI IQN is enabled only on that NIC partition.

Enable iSCSI Initiator IP Pool Select the check box to configure a pool of iSCSI initiator identities. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.

IP Address Range Enter the IP address range for the iSCSI initiator pool in one of the following formats:

- A.B.C.D - W.X.Y.Z
- A.B.C.D/E

Subnet mask Select the subnet mask address of the iSCSI pool from the drop-down.

Gateway Enter the gateway address of the iSCSI pool.

Primary DNS Server Enter the primary DNS server address.

Secondary DNS Server Enter the secondary DNS server address.

NOTE: The **IP Address Range**, **Gateway**, **Primary DNS Server**, and **Secondary DNS Server** must be valid IPv4 addresses.

Actions

Previous Displays the **Ethernet** tab.

Next Displays the **FCoE** tab.

Finish Saves the changes and displays the **Configuration** page.

Cancel Closes the **Create Identity Pool** wizard without saving the changes.

Create Identity Pool - Fibre channel over Ethernet

You can add the required number of Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) MAC addresses to the identity pool. The World Wide Port Name (WWPN)/World Wide Node Name (WWNN) values are generated from these MAC addresses.

Include FCoE Identity Select the check box to include the FCoE MAC addresses to the identity pool.

FIP MAC Address Enter the starting FCoE Initialization Protocol (FIP) MAC address of the identity pool in one of the following formats:

- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

The maximum length of a MAC address is 50 characters. This option is displayed only if the **Include FCoE Identity** check box is selected.

The WWPN/WWNN values are generated from the MAC address.

Number of FCoE Identities Select the required number of FCoE identities. The identities can be between 1 and 5000.

Actions

Previous Displays the **iSCSI** tab.

Next Displays the **Fibre Channel** tab.

Finish Saves the changes and displays the **Identity Pools** page.

Cancel Closes the **Create Identity Pool** wizard without saving the changes.

Create Identity Pool - Ethernet

In the **Ethernet** tab, you can add the required number of MAC addresses to the identity pool.

Include ethernet virtual MAC addresses Select the check box to add the virtual MAC addresses to the identity pool.

Starting virtual MAC Address Enter the starting virtual MAC address in one of the following formats:

- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

The maximum length of a MAC address is 50 characters. This option is displayed only if the **Include ethernet virtual MAC addresses** check box is selected.

Number of virtual MAC Identities Select the number of virtual MAC identities. The identities can be 1 to 50. This option is displayed only if the **Include ethernet virtual MAC addresses** check box is selected.

Actions

Previous Displays the **Pool Information** tab.

Next Displays the **iSCSI** tab.

Finish Saves the changes and displays the **Identity Pools** page.

Cancel Closes the **Create Identity Pool** wizard without saving the changes.

View definitions of identity pools

About this task

To view the definitions of an identity pool:

Steps

1. On the **Configuration** page, click **Identity Pools**.
2. Select an identity pool, and then click **Summary**.
   The various identity definitions of the identity pool are listed.
3. To view the usage of these identity definitions, click the **Usage** tab and select the **View By** filter option.

Edit identity pools

You can edit an identity pool to add ranges that you had not specified earlier, add an identity type, or delete identity type ranges.

About this task

To edit the definitions of an identity pool:

Steps

1. On the **Configuration** page, click **Identity Pools**.
2. Select the identity pool, and then click **Edit**.
   The **Edit Identity Pool** dialog box is displayed.
3. Make the changes to the definitions in the appropriate sections, and then click **Finish**.

Results

The identity pool is now modified.

Delete identity pools

You cannot delete an identity pool if the identities are reserved or assigned to a deployment template.

About this task

To delete an identity pool:

Steps

1. On the **Configuration** page, click **Identity Pools**.
2. Select the identity pool, and then click **Delete**.
3. Click **Yes**.

Results

The identity pool is deleted and the reserved identities associated with one or more deployment templates are removed.

Define networks

On the VLANs page, you can enter information of the networks that are currently configured in your environment which the devices can access.

Prerequisites

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope-based access control in OpenManage Enterprise on page 18.

Steps

1. Select **Configuration** > **VLANs** > **Define**.
2. In the **Define Network** dialog box, enter a name and an appropriate description.
3. Enter the VLAN ID, and then select the network type.
   You can select a network type only for MX7000 chassis. For more information about the network types, see Network types on page 106.
4. Click **Finish**.

Results

The network currently configured in your environment is now defined and resources can access the network.

NOTE: Scope-based restrictions don't apply to VLANs as these are common resource pools. Once a VLAN is defined by the administrator, it is available to all the device managers for use.

Network types

NOTE: You can select a network type for MX7000 chassis only.

Table 14. Network types

Network types	Description
General Purpose (Bronze)	Used for low priority data traffic.
General Purpose (Silver)	Used for standard or default priority data traffic
General Purpose (Gold)	Used for high priority data traffic
General Purpose (Platinum)	Used for extremely high priority data traffic
Cluster Interconnect	Used for cluster heartbeat VLANs
Hypervisor Management	Used for hypervisor management connections such as the ESXi management VLAN
Storage - iSCSI	Used for iSCSI VLANs
Storage - FCoE	Used for FCoE VLANs
Storage - Data Replication	Used for VLANs supporting storage data replication such as for VMware Virtual Storage Area Network (VSAN)
VM Migration	Used for VLANs supporting vMotion and similar technologies
VMWare FT Logging	Used for VLANs supporting VMware Fault Tolerance

Edit or delete a configured network

Steps

1. Go to the VLANs page by clicking **Configuration** > **VLANs**.
2. Select a network from the list, and then click **Edit** in the right pane to change the name, description, VLAN ID, or the network type.

   NOTE: VLAN configuration on M1000e and FX2 chassis is not supported in an IPv6 infra, as the IPv6 addressing is not supported by M I/O Aggregator (IOA) and FN I/O modules.

NOTE: The changed VLAN name and IDs are not updated on the target MX7000 chassis after a stateless deployment task is run.

3. To delete the network, select the network and click **Delete**.
4. Click **Yes**.

Export VLAN definitions

The network definitions available in OpenManage Enterprise can downloaded either as a CSV or as a JASON file.

Steps

1. To download as a CSV file :
   a. Click **Configuration** > **VLANs** > **Export** and select **Export All as CSV**.
2. To download as a JSON file :
   a. Click **Configuration** > **VLANs** > **Export** and select **Export All as JSON**.

Import network definitions

The following options are available to import the network definitions:

Steps

1. **Import VLAN definitions from a file**
   To import VLAN definitions from a file:
   a. Click **Configuration** > **VLANs**.
   b. Click **Import** and select **Import from File**.
   c. Navigate to the file location and select an existing .json or .csv file containing the VLAN definitions, and click **Open**.

   NOTE:
   - Invalid entries or content type in the files are flagged and are not imported.
   - VLAN definitions in the .csv and .json file(s) must be entered in the following formats:

   Table 15. VLAN definition format for CSV file

Name	Description	VLANMin	VLANMax	Type
VLAN1	VLAN with single ID	1	1	1
VLAN2 (Range)	VLAN with an ID range	2	10	2

   and

   Table 16. VLAN definition format for JSON files

```
[{"Name":"VLAN1","Description":"VLAN with single ID
","VlanMinimum":1,"VlanMaximum":1,"Type":1},
{"Name":"VLAN2 (Range)","Description":"VLAN with an ID Range
","VlanMinimum":2,"VlanMaximum":10,"Type":2}]
```

   d. Click **Finish**. A job named **ImportVLANDefinitionsTask** is created to import the networks from the selected file.
2. **Import VLAN definitions from a chassis**
   To import VLAN definitions from an existing MX7000 chassis:

   NOTE: OpenManage Enterprise-Modular version 1.2 must be already installed in the MX7000.

a. Click **Configuration** > **VLANs**.
b. Click **Import** and select **Import VLANs from Chassis**.
c. On the **Job Target** screen, select the chassis from where the VLAN definitions need to be imported and click **OK**. A job with name **ImportVLANDefinitionsTask** is created to import the networks from the selected chassis.

Results

Upon completion of the job, refresh the **Configuration** > **VLANs** page to view the successfully imported VLAN definitions.

To view the execution details of the job and for status of each network that was imported from the chassis, go to the **Jobs** page by clicking **Monitor** > **Jobs**, select the job, and click **View Details**.

12

Manage Profiles

A 'Profile' is a specific instance of an existing deployment template that is customized with attributes unique to an individual device. Profiles can be created either implicitly during a template's deployment/auto-deployment or from the existing templates by the user. A Profile consists of target-specific attribute values along with the BootToISO choices, and iDRAC management IP details of the target device. It could also contain any network bandwidth and VLAN allocations for server NIC ports as applicable. Profiles are linked to the source template from which they are created.

On the **Configuration** > **Profiles** page all the profiles that are in the logged in user's scope are displayed. For example, an administrator can see and manage all profiles, however, a device manager with limited scope can see and use only the profiles that they create and own.

The following details of the listed profiles are displayed:

Table 17. Manage Profiles - Field definitions

Field Name	Description
Modified	A 'modified' symbol ⚠ is displayed to notify any modification or change to the associated profile or template attributes after the initial assigning. If the modified profile is redeployed on the device, the symbol disappears.
Profile Name	Name of the profile
Template Name	Name of the linked source template
Target	Service tag or IP Address of the device on which the profile is assigned. If the profile is not assigned to any device, then target is blank.
Target Type	The device type (server or chassis) on which the profile is assigned
Chassis	Chassis name of the chassis if the target server is discovered as part of a chassis
Profile State	Profile State will be displayed as 'Assigned to Device' if the profile is assigned, 'Unassigned' for unassigned profiles, and 'Deployed' for the deployed profiles.
Last Action Status	Displays a profile's last action status such as Aborted, Cancelled, Completed, Failed, New, Not Run, Paused, Queued, Running, Scheduled, Starting, Stopped, Completed with Errors.

Advanced Filters can be used to customize the Profile list.

On the right side — Description, Last deployed Time, Last Modified Time, Created On, and Created By are displayed for the selected profile. Click View Identities to view the NIC configuration and virtual identities that are tagged to the profile.

Depending on the various profile states, the following actions can be performed on the **Configuration** > **Profiles** page as mentioned below:

ⓘ **NOTE:** Create and Delete operations are not listed as part of the table.

Table 18. Profile states and possible operations

Profile State	Edit	Assign Target	Unassign Target	Re-Deploy	Migrate
Unassigned Profile	Yes	Yes	No	No	No
Assigned to device	Yes	No	Yes	No	No

Table 18. Profile states and possible operations (continued)

Profile State	Edit	Assign Target	Unassign Target	Re-Deploy	Migrate
Deployed	Yes	No	Yes	Yes	Yes

- Create profiles and pre-reserve virtual identities. See, Create profiles on page 110
- View profile details. See, View Profile details on page 111
- Edit profile attributes and settings. See, Edit a profile on page 111
- Assign a profile to a device or service tag (through auto-deploy). See, Assign a Profile on page 112
- Unassign a profile from a device or service tag. See, Unassign profiles on page 113
- Redeploy profile changes to the associated target device. See, Redeploy profiles on page 113
- Migrate profile from one target (device or service tag) to another.
- Delete profiles. See, Delete Profiles on page 114
- Export and then download profile(s) data to HTML, CSV or PDF. See, Export Profile(s) data as HTML, CSV, or PDF on page 115

Topics:

Create profiles

Profiles can be created using the existing deployment templates for deployment on existing target devices or can be reserved for auto-deployment on the yet-to-be-discovered devices.

Prerequisites

NOTE: Only users with OpenManage Enterprise Administrator or Device Manager privileges are allowed to perform the Profile Management tasks. See Role and scope-based access control in OpenManage Enterprise on page 18.

About this task

To create a profile from an existing deployment template:

Steps

1. Go to the Profiles page by clicking **Configuration** > **Profiles**.
2. Click **Create** to activate the Create Profiles wizard.
3. In the Template section, select the **Template Type** as either Server or Chassis and then select a deployment template in the **Select Template** drop down list. Click **Next**.
4. In the **Details** page, modify the **Name Prefix** and provide a description in the **Description** box if needed. In the **Profile Count** box, enter the number of profiles. Click **Next**.
5. Optionally, in the **Boot to Network ISO** page, select the **Boot to Network ISO** check box and specify the full ISO path, the file share location, and choose a **Time to Attach ISO** option to set the number of hours the network ISO file will remain mapped to the target device(s).
6. Click **Finish**.

Results

Profiles are created based on the deployment template name and the count provided. These profiles are listed on the Profiles page.

View Profile details

To just view the details of an existing profile without editing:

Steps

1. Select a profile from the list of profiles on the **Configurations** > **Profiles** page.
2. Click **View** to activate the View Profile Wizard.
3. On the **Details** page of the wizard, Source Template, Name, Description, and Target information are displayed.
4. Click **Next**. On the **Boot to Network ISO** page, the ISO image file path, the share location of the ISO image file, and the Time to Attach ISO value are displayed if the profile was initially set with that preference.

Profiles — view network

To view the network bandwidth and VLAN allocations for the NIC ports associated to a profile:

Steps

1. Select a profile on the **Configuration** > **Profiles** page.
2. Click **View** > **View Network** to activate the View Network wizard.
3. The **Bandwidth** section displays the following bandwidth settings of the partitioned NICs: NIC identifier, Port, Partition, Min Bandwidth (%), and Max Bandwidth (%). Click **Next**
4. The **VLANs** section displays the following VLAN details of the profiles: NIC teaming, NIC identifier, Port, Team, Untagged Network, and Tagged Network.
5. Click **Finish** to close the View Network wizard.

Edit a profile

An existing profile can be edited on the **Configurations** > **Profiles** page. The changes in the profile do not affect the associated target system automatically. For the changes to take effect, the modified profile must be redeployed on the target device.

Prerequisites

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope-based access control in OpenManage Enterprise on page 18

About this task

To rename, edit network, or edit the attributes of an existing profile, select the profile on the Profiles page and click **Edit**. The following edit options can be selected:

Steps

1. Select **Rename** and in the Rename Profile wizard edit the profile name in the **Name** box.
2. Select **Edit Profile** to activate the Edit Profile wizard and edit the following:
   a. On the **Details** page, you can edit the **Name** and **Description**. Click **Next**.
   b. On the Boot to Network ISO page, select the **Boot to Network ISO** check box to specify the full ISO path and the share location and do the following:
      - Select **Share Type** as either CIFS or NFS.
      - In the **ISO Path** box, enter the full ISO path. Use the tool tips to enter the correct syntax.
      - Provide details in the **Share IP Address**, **Username**, and **Password** boxes.

- Select the **Time to Attach ISO** dropdown menu options to set the number of hours the network ISO file will remain mapped to the target device. By default, this value is set as four hours.
- Click **Next**.

c. On the **iDRAC Management IP** page, select from one of the following :
   - Don't change IP settings.
   - Set as DHCP
   - Set static IP and provide the relevant Management IP, Subnet Mask, and Gateway details.

d. On the **Target Attributes** page, you can select and edit the BIOS, System, NIC, iDRAC, and virtual identity attributes of the profile.

e. Click **Finish** to save the changes.

Assign a Profile

From the **Configuration** > **Profiles** page, an unassigned profile can be either deployed on an existing server or can be reserved for auto deployment on a yet-to-be discovered server.

About this task

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope-based access control in OpenManage Enterprise on page 18.
- The existing attributes, if any, of the target server would be overwritten when a profile is deployed on it.
- Only the devices that are not associated with any profiles are available for deployment or auto deployment.

Steps

1. To **Deploy a profile**:
   a. Select an unassigned profile on the **Configuration** > **Profiles** page, click **Assign** > **Deploy** to activate the Deploy Profile wizard.
   b. The **Details** page displays the source template, profile name and description. Click **Next**.
   c. On the **Target** page:
      - Click **Select** and from the list of devices, select a target device.

        NOTE: Devices that are already assigned a profile will be greyed out and not selectable in the target list.
      - If a reboot is required after the deployment, select the **Do not forcefully reboot the host OS if the graceful reboot fails** check box.
      - Click **Next**.

   d. (Optional) On the **Boot to Network ISO** page, select the **Boot to Network ISO** check box and provide the relevant ISO path, share location details, and the Time to Attach ISO value. Click **Next**.
   e. On the **iDRAC Management IP** page, select from one of the following options and provide further relevant details.
      - Don't change IP settings
      - Set as DHCP
      - Set static IP

   f. On the **Target Attributes** page, the attributes are displayed under the BIOS, System, NIC, and iDRAC sections. You can select, unselect, or edit the attributes before deployment.
   g. On the **Virtual Identities** page, click **Reserve identities**. The assigned virtual identities of the NIC cards of the selected target device are displayed. To view all the assigned identities of the identity pool of the selected target device, click **View all NIC details**.
   h. On the **Schedule** page, you can choose **Run Now** to immediately deploy the profile, or choose **Enable Schedule** and select an appropriate Date and Time for the profile deployment.
   i. Click **Finish**.

   NOTE: If identities are already assigned outside of the appliance, then a new deployment will not use those identities unless they are cleared. For more information, see Identity pools on page 101

2. To **Autodeploy a profile**:

   NOTE: For modular devices, the strict checking of the VLAN definitions is enabled by default.

a. Select an unassigned profile on the **Configuration** > **Profiles** page, click **Assign** > **Auto Deploy** to activate the Auto Deploy wizard.
b. The Details page displays the Source Template, Name, and Description (if any) of the profile. Click **Next**.
c. On the **Target** page, specify the service tag or node id of the yet-to-be discovered device in the **Identifier** box. Click **Next**.
d. (Optional) On the Boot to Network ISO page, select the **Boot to Network ISO** check box to specify the full ISO path and the share location:
   - Select **Share Type** as either CIFS or NFS.
   - In the **ISO Path** box, enter the full ISO path. Use tool tips to enter the correct syntax.
   - Provide details in the **Share IP Address**, **Username**, **Password** boxes.
   - Select the **Time to Attach ISO** dropdown menu options to set the number of hours the network ISO file will remain mapped to the target device(s). By default, this value is set as four hours.
e. Click **Finish**.

Unassign profiles

Using **Configuration** > **Profiles** > **Unassign**, the deployed or auto-deployed profiles can be disassociated from their respective targets. .

About this task

To unassign profiles:

Steps

1. Select the profiles from the Profiles list on the **Configuration** > **Profile** page.
2. Click **Unassign**.
3. Click **Finish** on the Confirmation dialog box.

Results

The selected profiles are unassigned and the identities from their respective targets are removed.

NOTE: For the deployed target devices, unassigning the profiles will revert them to their factory-assigned identities.

Redeploy profiles

For the attribute changes of an already deployed profile to take affect on the associated target device, it must be redeployed. For modular devices, VLAN definitions can be configured during redeployment, however the strict checking to match the VLAN attributes is disabled.

About this task

NOTE: VLAN attribute changes fail on the target MX7000 sleds during profile redeployment if the VLAN attributes were not initially deployed on the MX7000 sleds during template deployment using the 'Propagate VLAN settings immediately' option.

To redeploy profile(s):

Steps

1. On the **Configuration** > **Profiles** page, select the profile(s) that are 'Deployed' and/or 'Modified' (⚠) and click **Re-deploy** .
2. On the Re-deploy wizard's Attribute Deploy Options page choose one of the following attribute deploy options and click **Next**:
   - **Modified attributes only**: To redeploy only the modified attributes on the target device.
   - **All Attributes**: To redeploy all the attributes, along with any modified attributes, on the target device.
3. On the Schedule page, choose from one of the following options:

- **Run Now** to implement the changes immediately.
- **Enable Schedule** and select a date and time to schedule the redeployment.

4. Click **Finish** to proceed.

Results

When a profile is redeployed, a **Redeploy Profiles** job is executed. The status of the job can viewed on the **Monitor** > **Jobs** page.

Migrate a Profile

A deployed or an autodeployed profile can be migrated from it's existing target device or service tag to a another identical target device or service tag.

About this task

When a migration is successful, the profile target assignment reflects the new target. If the migration is from a target device to a yet-to-be-seen service tag, then the profile's state is changed to "Assigned."

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 18.
- Migrate profile will move settings defined by the profile (including deployed virtual identities) from source to the target.
- You can force the migration of a profile even if the source device cannot be contacted. In this case, the user must ensure that there are no virtual identity conflicts.
- True target specific attributes are not reclaimed from the 'source' server as part of migration. Due to this, same inventory details can be present on two servers post migration.

To Migrate a profile:

Steps

1. On the **Configuration** > **Profiles page**, select a profile and click **Migrate** to activate the Migrate Profile wizard.
2. On the Selection page:
   a. From the **Select source profile** drop down, select the profile that you want to migrate
   b. Click **Select Target** and from the Job target dialog box, select a target device and click **Ok**.
   c. If needed, select the 'Force the migration even if the source device cannot be contacted' check box.

      NOTE: You must ensure that there are no virtual identity conflicts.

   d. Click **Next**.
3. On the Schedule page select from one of the following:
   a. Select **Update Now** to migrate the profile settings immediately to the target.
   b. Select a **Date** and **Time** to schedule the migration.
4. Click **Finish**.

Results

A job is created to migrate profile's settings to the new target device. You can view the status of the job on the **Monitor** > **Jobs** page.

Delete Profiles

The existing 'unassigned' profile(s) can be deleted from the **Configuration** > **Profiles** page:

About this task

NOTE:

- An assigned or deployed profile can be deleted from the Profile portal only if it is unassigned.
- Deleting of an unassigned profile that had identities reserved, returns those identities to the Identity pool they came from. It is recommended to wait for 10 minutes to use these reclaimed identities for future reservations and deployments.

To delete the unassigned profiles:

Steps

1. Select the unassigned profiles on the Profiles page.
2. Click **Delete** and confirm by clicking **Yes** when prompted.

Export Profile(s) data as HTML, CSV, or PDF

To export the profile(s) data as a HTML, CSV, or PDF file.

Steps

1. On the **Configuration** > **Profiles** page, select the profile(s).
2. Click **Export** and in the Export Selected dialog box choose from HTML, CSV, or PDF.
3. Click **Finish.** The profile(s) data is downloaded in the selected format.

13

Managing the device configuration compliance

By selecting **OpenManage Enterprise** > **Configuration** > **Configuration Compliance**, you can create configuration-compliance baselines by using the built-in or user-created compliance templates. You can create a compliance template from an existing deployment template, reference device, or by importing from a file. To use this feature, you must have the Enterprise level license of OpenManage Enterprise and iDRAC for servers. For Chassis Management Controller, no license is required. User's only with certain privileges are permitted to use this feature. See Role and scope-based access control in OpenManage Enterprise on page 18.

After a configuration baseline is created by using a compliance template, the summary of compliance level of each baseline is listed in a table. Each device associated with the baseline has its own status, however, the highest severity status is considered as the status of the baseline. For more information about Rollup Health status, see the *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* white paper on the support site.

NOTE: A baseline with multiple devices can sometimes show up as non-complaint permanently as few of the attribute values are not necessarily same across all the targets. For example, the Boot Control attributes such as the iSCSI Target IQN, LUN ID, FCoE Target WWPN and so on that are not same across all targets and can cause a permanent non-compliance of the baseline.

The Overall Compliance Summary report displays the following fields:

- **COMPLIANCE**: The Rollup compliance level of devices attached to a configuration compliance baseline. The status of the device with least compliance (say, critical) is indicated as the status of the whole baseline.
- **NAME**: Name of the configuration compliance baseline.
- **TEMPLATE**: The name of the compliance template used by the baseline.
- **LAST RUN TIME**: The most recent date and time when the compliance baseline was run.

To view the configuration compliance report of a baseline, select the corresponding check box, and then click **View Report** in the right pane.

Use the query builder feature to generate device level compliance to the selected baseline. See Select a query criteria on page 61.

OpenManage Enterprise provides a built-in report to view the list of monitored devices and their compliance to the configuration compliance baseline. Select **OpenManage Enterprise** > **Monitor** > **Reports** > **Devices per Template Compliance Baseline**, and then click **Run**. See Run reports on page 148.

Related tasks

Create a configuration compliance baseline on page 119
Edit a configuration compliance baseline on page 120
Remove a configuration compliance baseline on page 123
Manage compliance templates on page 117
Select a query criteria on page 61

Topics:

Manage compliance templates

Use compliance template to create compliance baselines and then periodically check the configuration compliance status of devices that are associated with the baseline. See Managing the device configuration compliance on page 116.

You can create compliance templates by using deployment template, reference device, importing from a file. See Manage compliance templates on page 117.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope-based access control in OpenManage Enterprise on page 18.

By selecting **Configuration** > **Configuration Compliance** > **Template Management**, you can view the list of compliance templates based on the scope-based access that you have in OpenManage Enterprise. For example, an administrator can view and manage all the compliance templates, however, device managers can only view and manage the templates that they create and own. On this page:

- You can create compliance template by:
  - Using a deployment template. See Create a compliance template from deployment template on page 117.
  - Using a reference device. See Create a compliance template from reference device on page 118.
  - Importing from a template file. See Create a compliance template by importing from a file on page 118.
- Edit a compliance template. See Edit a compliance template on page 119.
- Clone a compliance template. See Clone a compliance template on page 118.
- Export report about a compliance template. On the **Compliance Templates** page, select the corresponding check box, and then click **Export**. See Export all or selected data on page 71.
- Delete a compliance template. On the **Compliance Templates** page, select the corresponding check box, and then click **Delete**.

Configuration compliance is scalable to a maximum of 6,000 devices. To efficiently manage large-scale configuration compliance activity do the following:

- Disable the default Configuration Inventory task that is triggered automatically and run it manually when needed.
- Create compliance baselines with lesser number of devices. For example, 6,000 devices must be categorized into four separate baselines with 1,500 devices each.
- All the baselines should not be checked for compliance at the same time.

NOTE: When you edit a compliance template, configuration compliance is automatically triggered on all the baselines that it is associated with. If there is a use case of frequent template edits the above scale environment is unsupported, and it is recommended that you associate a maximum of 100 devices per baseline for optimal performance.

Related information

Managing the device configuration compliance on page 116
Edit a configuration compliance baseline on page 120
Remove a configuration compliance baseline on page 123
Create a compliance template from deployment template on page 117
Edit a compliance template on page 119

Create a compliance template from deployment template

Prerequisites

About this task

Steps

1. Click **Configuration** > **Configuration Compliance** > **Template Management** > **Create** > **From Deploy Template**.

2. In the **Clone Deployment Template** dialog box, from the **Template** drop-down menu, select a deployment template that must be used as the reference for the new template.
3. Enter a name and description for the compliance template.
4. Click **Finish**.
   A compliance template is created and listed in the list of compliance templates.

Related tasks

Manage compliance templates on page 117
Clone a compliance template on page 118

Create a compliance template from reference device

Prerequisites

About this task

To use the configuration properties of a device as a template for creating configuration baseline, the device must be already onboarded. See Onboarding devices on page 47.

Steps

1. Click **Configuration** > **Configuration Compliance** > **Template Management** > **Create** > **From Reference Device**.
2. In the **Create Compliance Template** dialog box, enter a name and description for the compliance template.
3. Select the options to create the compliance template by cloning properties of either a server or chassis.
4. Click **Next**.
5. In the **Reference Device** section, select the device that must be used as the 'reference' for creating the compliance template. See Select target devices and device groups on page 143.
   a. If you select a server as the reference, select the server configuration properties that must be cloned.
6. Click **Finish**.
   A template creation job is created and run. The newly-created compliance template is listed on the **Compliance Templates** page.

Create a compliance template by importing from a file

Prerequisites

About this task

Steps

1. Click **Configuration** > **Configuration Compliance** > **Template Management** > **Create** > **Import from File**.
2. In the **Import Compliance Template** dialog box, enter a name for the compliance template.
3. Select either the server or chassis template type, and then click **Select a file** to browse through to the file and select.
4. Click **Finish**.
   The compliance template is created and listed.

Clone a compliance template

About this task

Steps

1. Click **Configuration** > **Configuration Compliance** > **Template Management**.

2. Select the compliance template to be cloned, and then click **Clone**.
3. In the **Clone Template** dialog box, enter the name of new compliance template.
4. Click **Finish**.
   The new compliance template is created and listed under **Compliance Templates**.

Related information

Create a compliance template from deployment template on page 117
Edit a compliance template on page 119

Edit a compliance template

About this task

The compliance templates can be edited on the **Configuration Compliance** > **Compliance Templates** page. When editing, selecting or deselecting the template attributes does not change the template-stored attributes and all attributes will still be part of the template if it is exported. It does affect what is deployed.

NOTE:

- Editing a compliance template that is already associated with other baseline(s), will automatically trigger a configuration compliance for all devices across all the baselines that use the template.
- Editing a compliance template that is linked to multiple baselines having large number of devices may result in a session timeout as the configuration compliance check for all the associated devices may take several minutes. A session timeout does not indicate that the changes made to the compliance template had any issue.
- When editing a compliance template on large-scale systems consisting of 1,000 or configuration inventory of a maximum of 6,000 managed devices, ensure that there are no other configuration inventory or compliance operations running at the same time. Additionally, **disable** the default system generated Configuration Inventory job on the **Monitor** > **Jobs** page (set source to System generated).
- It is recommended that you associate a maximum of 1500 devices per baseline for optimal performance.
- If there is a use case of frequent template edits, it is recommended that you associate a maximum of 100 devices per baseline for optimal performance.

Steps

1. On the **Compliance Templates** page, select the corresponding check box, and then click **Edit**.
2. On the **Template Details** page, the configuration properties of the compliance template is listed.
3. Expand the property you want to edit, and then enter or select data in the fields.
   a. To enable the property, select the check box, if not already enabled.
4. Click **Save** or **Discard** to implement or to reject the changes.
   The compliance template is edited and the updated information is saved.

Related tasks

Manage compliance templates on page 117
Clone a compliance template on page 118

Create a configuration compliance baseline

A configuration compliance baseline is a list of devices associated to a compliance template. A device in OpenManage Enterprise can assigned to 10 baselines. You can check the compliance of a maximum 250 devices at a time. .

About this task

To view the list of baselines, click **OpenManage Enterprise** > **Configuration** > **Configuration Compliance**.

The list of compliance baselines available to you depends on your role and scope based access privileges in OpenManage Enteprise. For example, an administrator can view and manage all the compliance baselines, however, a device manager can only

view and manage the compliance baselines created and owned by that device manager. Also, the target devices available to the device managers are restricted by the devices / device groups that are in their respective scope.

You can create a configuration compliance baseline by:

- Using an existing deployment template. See Managing the device configuration compliance on page 116.
- Using a template captured from a support device. See Create a compliance template from reference device on page 118.
- Using a template imported from a file. See Create a compliance template by importing from a file on page 118.

When you select a template for creating a baseline, the attributes associated with the templates are also selected. However, you can edit the baseline properties. See Edit a configuration compliance baseline on page 120.

CAUTION: **If a compliance template used for a baseline is already associated with another baseline, editing the template properties changes the baseline compliance levels of devices already associated. Read through the Error and Event message displayed and act accordingly. For more information about error and event messages, see the *Error and Event Message Reference Guide* available on the support site.**

NOTE: Before creating configuration compliance baseline, ensure that you have created the appropriate compliance template.

Steps

1. Select **Configuration** > **Configuration Compliance** > **Create Baseline**.
2. In the **Create Compliance Baseline** dialog box:
   - In the **Baseline Information** section:
   a. From the **Template** drop-down menu, select a compliance template. For more information about templates, see Managing the device configuration compliance on page 116.
   b. Enter a compliance baseline name and description.
   c. Click **Next**.
   - In the **Target** section:
   a. Select devices or device groups. Only compatible devices are displayed. See Select target devices and device groups on page 143.

   NOTE: Only compatible devices are listed. If you select a group, the devices that are not compatible with the compliance template, or the devices that do not support the configuration compliance baseline feature, are exclusively identified to help you select effectively.

3. Click **Finish**.
   A compliance baseline is created and listed. A compliance comparison is initiated when the baseline is created or updated. The overall compliance level of the baseline is indicated in the **COMPLIANCE** column. For information about the fields in the list, see Managing the device configuration compliance on page 116.

   NOTE: Whenever a configuration baseline is created, a configuration inventory job is automatically created and run by the appliance to collect the inventory of the devices associated with the baseline for which the inventory data is unavailable. This newly-created Configuration inventory job has the same name as the baseline for which the inventory is collected. Also, on the Configuration Compliance page a progress bar indicating the progress of Inventory job appears alongside the respective baseline.

Related information

Managing the device configuration compliance on page 116
Remove a configuration compliance baseline on page 123

Edit a configuration compliance baseline

About this task

You can edit the devices, name, and other properties associated with a configuration baseline. For field descriptions displayed in the list, see Managing the device configuration compliance on page 116.

CAUTION: **If a compliance template used for a baseline is already associated with another baseline, editing the template properties changes the baseline compliance levels of devices already associated. See Edit a compliance template on page 119. Read through the Error and Event message displayed and act accordingly. For more**

information about error and event messages, see the *Error and Event Message Reference Guide* available on the support site.

Steps

1. Select **Configuration** > **Configuration Compliance**.
2. From the list of configuration compliance baselines, select the corresponding check box, and then click **Edit**.
3. In the **Edit Compliance Baseline** dialog box, update the information. See Create a configuration compliance baseline on page 119.

   NOTE: Whenever a configuration baseline is edited, a configuration inventory job is automatically triggered to collect the inventory of the devices associated with the baseline for which the inventory data is unavailable. This newly-created configuration inventory job has the same name as the baseline for which the inventory is collected. Also, on the Configuration Compliance page a progress bar indicating the progress of inventory job appears alongside the respective baseline.

Related tasks

Manage compliance templates on page 117
Select a query criteria on page 61

Related information

Managing the device configuration compliance on page 116
Remove a configuration compliance baseline on page 123

Delete configuration compliance baselines

You can delete the configuration compliance baselines on the **Configuration** > **Configuration Compliance** page and delink the devices from the associated baselines.

Prerequisites

NOTE: To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18

About this task

To delete the configuration compliance baselines:

Steps

1. Select the baseline(s) from the baselines listed on the Configuration Compliance page.
2. Click **Delete** and click **Yes** on the Confirmation prompt.

Results

The deleted configuration baselines are removed from the Configuration Compliance page.

Refresh compliance of the configuration compliance baselines

About this task

The compliance status check of a compliance baseline is triggered automatically if changes are made to either the attributes of the baseline reference template or if there is any change to the configuration inventory of any of the baseline-associated devices.

The compliance status of a configuration compliance baseline is a roll-up compliance level of the devices attached to that configuration compliance baseline. The status of the device with least compliance (say, critical) is indicated as the status of the whole baseline.

The overall compliance summary of all the configuration baselines is represented on a donut chart located above the Baseline grid. The Compliance Last Run Date and Time is displayed below the chart.

Compliance status check on large baselines may take several minutes, however, you can click **Refresh Compliance** to get an overall compliance summary of the devices on an as-needed basis while the large baseline compliance jobs are running.

NOTE: When the Configuration Compliance is in 'Running' status, initiating new jobs that impact baselines, such as editing of a compliance template or baseline, is not allowed.

To initiate a refresh of the overall compliance summary of all baselines do the following:

Steps

1. Click **Configuration** > **Configuration Compliance**, the Configuration Compliance page is displayed.
2. Click **Refresh Compliance.**

Results

The compliance refresh job (Load Summary of Compliance) is initiated and the overall compliance summary at that moment is displayed and the Compliance Last Run Time is updated.

Remediate noncompliant devices

On the Compliance Report page of a baseline, you can remediate the devices that do not match the associated baseline by changing the attribute values to match with the associated baseline attributes.

About this task

The Compliance Report page displays the following fields for the target devices that are associated with the compliance template baseline:

- **COMPLIANCE**: The status of the device with least compliance (for example, critical) is indicated as the status of the device.
- **DEVICE NAME**: The Name of the target device associated with the baseline.
- **IP ADDRESS**: The IP address of the target device.
- **TYPE**: Type of the target device associated.
- **MODEL**: Model name of the target device.
- **SERVICE TAG**: The service tag of the target device.
- **LAST RUN TIME**: The most recent date and time when the compliance baseline was run.

You can use the Advanced Filters to quickly see non-compliant devices. Also, the Select All and sorting support can be used on Configuration compliance results. To undo the filters, click **Clear Filters**.

To view the drifted attributes of a noncompliant target device, select the device and click **View Report**. The **Compliance Report** of the respective target device lists the attribute names with the expected and current values of the attributes.

To remediate one or more noncompliant devices:

Steps

1. Select **Configuration** > **Configuration Compliance**.
2. From the list of configuration compliance baselines, select the corresponding check box, and then click **View Report**.
3. From the list of noncompliant devices, select one or more devices, and then click **Make Compliant**.
4. Schedule the configuration changes to run immediately or later, and then click **Finish**.

   To apply the configuration changes after the next server reboot, you can select the **Stage configuration changes to device(s) on next reboot** option.

Results

A new configuration inventory task is run, and the compliance status of the baseline is updated on the **Compliance** page.

Export the Compliance Baseline report

A complete or partial list of the devices associated with a compliance template baseline can be exported to a CSV file.

About this task

On Compliance Report page of a configuration baseline

Steps

1. Click **Export All** to export details of all the devices in the compliance baseline. Or,
2. Click **Export Selected** after selecting the individual devices from the report.

Remove a configuration compliance baseline

About this task

You can remove the configuration compliance level of devices associated with a configuration baseline. For field descriptions displayed in the list, see Managing the device configuration compliance on page 116.

CAUTION: **When you delete a compliance baseline, or delete device(s) from a compliance baseline:**

- **The compliance data of the baseline and/or device(s) is deleted from the OpenManage Enterprise data.**
- **If a device is removed, its configuration inventory is no longer retrieved, and the already retrieved information is also deleted, unless the inventory is associated with an Inventory job.**

A compliance template used as a compliance baseline cannot be deleted if associated with a device. Appropriate messages are displayed in such cases. Read through the error and event message displayed and act accordingly. For more information about error and event messages, see the *Error and Event Message Reference Guide* available on the support site.

Steps

1. Click **Configuration** > **Configuration Compliance**.
2. From the list of configuration compliance baselines, select the corresponding check box, and then click **Delete**.
3. When prompted whether or not you want to delete, click **YES**.
   The compliance baseline is deleted and the **Overall Compliance Summary** table of baselines is updated.

Related tasks

Create a configuration compliance baseline on page 119
Select a query criteria on page 61
Manage compliance templates on page 117
Edit a configuration compliance baseline on page 120

Related information

Managing the device configuration compliance on page 116

14

Monitor and Manage device alerts

By selecting **OpenManage Enterprise** > **Alerts**, you can view and manage alerts generated by the devices in the management system environment. The Alerts page has the following tabs displayed:

- **Alert log**: You can view and manage all alerts generated on the target devices.
- **Alert Policies**: You can create alert policies to send alerts generated on target devices to destinations such as email, mobile, syslog server and so on.
- **Alert Definitions**: You can view alerts that are generated for errors or informational purposes.

NOTE:

- To manage and monitor device alerts on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope-based access control in OpenManage Enterprise on page 18.
- Alert policies and alert logs are governed by the scope based access that you have in OpenManage Enterprise. For example, an administrator can view and manage all the alert policies, however, device managers can only view and manage the default alert policies and the policies that they create and own. Also, the device managers can only view the alerts for the devices that are in their scope.
- Currently, only the SNMPv1 and SNMPv2 alerts are received by OpenManage Enterprise from the following PowerEdge servers— MX840c and MX5016s.
- OpenManage Enterprise provides a built-in report to view the list of devices monitored by OpenManage Enterprise and the alerts generated for each device. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Alert Counts per Device Report**. Click **Run**. See Run reports on page 148

Related concepts

View alert logs on page 124

Topics:

View alert logs

The **Alerts Log** page displays the list of alert logs for events occurring in the devices. From OpenManage Enterprise, click **Alerts** > **Alert Log**. The **Alerts Log** page is displayed.

By default, only the unacknowledged alerts are displayed. You can customize the list of the alerts using either the **Advanced Filters**, located on the top left hand side of the alert list, or by changing the **Alert Display Settings** in the **Application Settings** page. See Customize the alert display on page 176. You can view the alerts details as follows:

- **Acknowledge**: If the alert has been acknowledged a tick mark appears under **ACKNOWLEDGE**. Click between the square bracket under **ACKNOWLEDGE** to acknowledge or unacknowledge an alert.
- **Time**: The time at which the alert was generated.
- **Source name**: Operating system host name of the device that generated the alert. Click on the source name to view and configure the properties of the device.

  NOTE: Alerts cannot be filtered based on the IP address (source name) if the alert is generated from an undiscovered device or in case of an internal alert.
- **Category**: The category indicates the type of alert. For example, system health and audit.
- **Message ID**: The ID of the generated alert.
- **Message**: The generated alert.

- The box on the right provides additional information such as the detailed description and recommended action for a selected alert

NOTE: In multi-chassis management (MCM) environment, if several alerts occur at once in the lead chassis, the processing of the alerts may be delayed.

Select an alert to view the additional information such as the detailed description and recommended action on the right side of the Alerts Log page. You can also perform the following tasks on the Alerts Log page:

- Acknowledge alerts
- Unacknowledge alerts
- Ignore alerts
- Export alerts
- Delete alerts
- Archived alerts

Related information

Monitor and Manage device alerts on page 124

Manage alert logs

After alert logs have been generated and displayed on the **Alert Log** page, you can acknowledge, unacknowledge, ignore, export, delete, and archive them.

Acknowledge alerts

After you view an alert and understand its contents, you can acknowledge that you have read through the alert message. Acknowledging an alert prevents storing the same event in the system. For example, if a device is noisy and is generating the same event multiple times, you can ignore further recording of the alert by acknowledging the events that are received from the device. And, no events of the same type are recorded further.

To acknowledge an alert, on the **Alert Log** page, select the check box corresponding to the alert, and then click **Acknowledge**.

A tick mark is displayed in the **ACKNOWLEDGE** column. Once an alert is acknowledged, the **Last Updated By** field, located in the alert-detail section, is populated.

Unacknowledge alerts

You can unacknowledge alert logs that are acknowledged. Unacknowledging an alert implies that all events from any device are recorded even when the same event recurs frequently. By default, all alerts are unacknowledged.

To unacknowledge alerts, select the check box corresponding to the alerts, and then click the **Unacknowledge** button. Else, you can click the tick mark corresponding to each alert to unacknowledge.

NOTE: The **Last Updated By** field in the alert-detail section would retain the username of the user who had last acknowledged the alert.

Ignore alerts

Ignoring an alert creates an alert policy, which is enabled, and discards all future occurrences of that alert. Select the check box corresponding to the alert, and then click **Ignore** . A message is displayed that a job is being created to ignore the selected alert. The total number of alerts displayed in the header row of OpenManage Enterprise is decremented.

Export alerts

You can export alert logs in .csv format to a network share or local drive on your system.

To export alert logs, on the **Alert Log** page, select the alert logs that you want to export and click **Export** > **Export Selected**. You can export all alert logs by clicking **Export** > **Export All.** The alert logs are exported in .csv format.

Delete alerts

You can delete an alert to permanently remove that occurrence of the alert from the console.

Select the check box corresponding to the alert, and then click **Delete**. A message is displayed prompting you to confirm the deletion process. Click **YES** to delete the alert. The total number of alerts displayed in the header row of OpenManage Enterprise is decremented.

View archived alerts

A maximum of 50,000 alerts can be generated and viewed within OpenManage Enterprise. When 95% of the 50,000 limit (47,500) is reached, OpenManage Enterprise generates an internal message indicating that, when the count reaches 50,000, OpenManage Enterprise will automatically purge 10% (5000) of the archived alerts. The table lists different scenarios involving the alert purging.

Table 19. Alert purging

Workflow	Description	Result
Purge Task	Runs after every 30 minutes on the console.	If the alerts have reached its maximum capacity (that is, 50,000), check and generate the purge archives.
Purge Alert Warning	Generates an internal purge alert warning.	If the alerts have exceeded more than 95% (that is, 475000), generates an internal purge alert to purge 10% of the alerts .
Purge Alerts	Alerts purged from the alert log.	If the number of alerts have exceeded more than 100% then 10% of the old alerts are purged to return to 90% (that is 45,000).
Download Purge Alerts	Download the purged alerts.	Archives of the recent five purged alerts can be downloaded from the Archive Alerts.

Download archived alerts

Archived alerts are the oldest 10% of the alerts (5000 nos) that are purged when the alerts exceed 50,000 in number. These oldest 5000 alerts are removed from the table and stored in a .csv file, and then archived. To download the archived alert file:

1. Click **Archived Alerts**.

   In the **Archived Alerts** dialog box, the last five purged archived alerts are displayed. File size, name, and archived date are indicated.

2. Select the check box corresponding to the alert file and click **Finish**. The .CSV file is downloaded to the location you selected.

NOTE: To download archived alerts, you must have necessary privileges. See Role and scope-based access control in OpenManage Enterprise on page 18.

Alert policies

This topic explains the concept of alert policies and how they can be useful. For instructions on creating, editing, enabling, disabling, and deleting alert policies, see *Configuring and managing alert policies*.

Alert policies enable you to configure and send specific alerts for specific devices or components to a specific destination such as email, mobile, syslog server and so on. Alerts help you to monitor and manage devices effectively.

Use alert policies to perform the following functions:

- Automatically trigger actions based on the input from an alert.
- Send an alert to an email address.
- Send an alert to a phone through an SMS or notification.

- Send an alert through an SNMP trap.
- Send an alert to a syslog server.
- Perform device power control actions such as turning on or turning off a device when an alert of a predefined category is generated.
- Run a remote script.

To view, create, edit, enable, disable, and delete alert policies, click **Alerts** > **Alert Policies**.

Related tasks

Configure and manage alert policies on page 127

Configure and manage alert policies

This topic provides instructions on how to create, edit, enable, disable, and delete alert policies.

Prerequisites

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope-based access control in OpenManage Enterprise on page 18.

Related information

Alert policies on page 126
Forward audit logs to remote Syslog servers on page 128

Create an alert policy

You can create alert policies and enable them to send alerts to email address, phone, SNMP traps, and perform device control actions such as turning on or off a device, power cycling, and graceful shutdown when an alert of a predefined category is generated.

Prerequisites

Steps

On the **Alerts** > **Alerts Policies** page, click **Create**, and do the following:

1. Enter a name and description for the alert policy and click **Next**. The **Enable Policy** check-box is selected by default.
2. Select the alert category by selecting any or all the built-in and imported third-party Management Information Base (MIB) categories.

   You can expand each category to view and select the sub categories. To know more about categories and subcategories, see Alert definitions on page 131.
3. Select the devices or groups for which an alert is required and click **Next**. An alert can be applied for:
   - A device or devices.
   - A group or groups of devices.
   - A specified undiscovered device by entering its IP address or hostname.
   - Any undiscovered device.

     NOTE: The Remote Script Execution and Power Action tasks cannot be performed on the undiscovered devices..

     NOTE: Alerts of SNMPv1, SNMPv2, and SNMPv3 protocols sent by such undiscovered (foreign) devices are recognized by OpenManage Enterprise.
4. (Optional) Specify the duration for when the alert policy is applicable by selecting the required values for **Date Range**, **Time Interval** and **Days**, and then click **Next**.
5. Select the severity of the alert and click **Next**.

   To select all the severity categories, select the **All** check box.
6. Select one or more alert actions and click **Next**. The available options are:

- Email—Select Email to send an email to a designated recipient by specifying information for each field and use tokens if required for the subject and message. See Token substitution in remote scripts and alert policy on page 194

  NOTE: Emails for multiple alerts of the same category, message ID and content are triggered only once every 2 minutes to avoid repeated or redundant alert messages in the inbox.
- SNMP Trap Forwarding (Enable)—Click Enable to view the SNMP Configuration window where you can configure the SNMP settings for the alert. See Configure SMTP, SNMP, and Syslog alerts on page 129.
- Syslog (Enable)—Click Enable to view the Syslog Configuration window where you can configure the system log settings for the alert. See Configure SMTP, SNMP, and Syslog alerts on page 129.
- Select the Ignore check box to ignore the alert message and not activate the alert policy.
- Send an SMS to specified phone number.
- Power Control—Select Power Control check box to view the actions where you can turn on, turn off, power cycle, or gracefully shutdown a device. To shut down an operating system before performing power control actions, select the **Shut down OS First** check box.
- Remote Script Execution (Enable)—Click Enable to view the Remote Command Setting window where you can add and run remote commands on remote nodes. For more information about adding remote commands, see Execute remote commands and scripts on page 130.

  From the drop-down menu, select the script that you want to run when this alert policy is run. You can set up running the remote command also as described in Managing OpenManage Enterprise appliance settings on page 156.
- Send a notification to the mobile phone registered with OpenManage Enterprise. See OpenManage Mobile settings on page 185.

7. Review the details of the created alert policy in the Summary tab and click **Finish**.
   The alert policy is successfully created and listed in the **Alert Policies** section.

Manage alert policies

After alert policies have been created on the **Alert Policies** page, you can edit, enable, disable, and delete them. In addition, OME provides built-in alert policies that trigger associated actions when the alert is received. You cannot edit or delete the built-in alert policies, however, you can only enable or disable them.

To view the created alert policies, click **Alerts** > **Alerts Policies**.

To select all the alert policies, select the check box to the left of **Enabled.** Select one or more check boxes next to the alert policy to perform the following actions:

- **Edit an alert policy**: Select an alert policy and click **Edit** to edit the required information in the Configure and manage alert policies on page 127 dialog box.

  NOTE: Only one alert policy can be edited at a time.

  NOTE: The Time Interval check box is disabled by default for alert policies on OpenManage Enterprise versions before version 3.3.1. After upgrading, enable the Time Interval and update the fields to reactivate the policies.
- **Enable alert policies**: Select the alert policy and click **Enable**. A check mark appears under the **Enabled** column when an alert policy is enabled. The **Enable** button of an alert policy that is already enabled appears grayed-out.
- **Disable alert policies**: Select the alert policy and click **Disable**. The alert policy is disabled and the tick mark in the **ENABLED** column is removed.

  You can also disable an alert policy while creating the alert policy by clearing the **Enable Policy** check box in the Name and Description section.
- **Delete alert policies**: Select the alert policy and click **Delete**.

  You can delete multiple alert policies at a time by selecting the respective check boxes. To select or clear all the check boxes, select the check box in the header row next to **ENABLED**.

Forward audit logs to remote Syslog servers

To monitor all the audit logs of OpenManage Enterprise from Syslog servers, you can create an alert policy. All the audit logs such as user login attempts, creation of alert policies, and running different jobs can be forwarded to Syslog servers.

About this task

To create an alert policy to forward audit logs to Syslog servers:

Steps

1. Select **Alerts** > **Alert Policies** > **Create**.
2. In the **Create Alert Policy** dialog box, in the **Name and Description** section, enter a name and description of the alert policy.
   a. The **Enable Policy** check box is selected by default to indicate that the alert policy will be enabled once it is created. To disable the alert policy, clear the check box. For more information about enabling alert policies at a later time, see Configure and manage alert policies on page 127.
   b. Click **Next**.
3. In the **Category** section, expand **Application** and select the categories and subcategories of the appliance logs. Click **Next**.
4. In the **Target** section, the **Select Devices** option is selected by default. Click **Select Devices** and select devices from the left pane. Click **Next**.

   NOTE: Selecting target devices or groups is not applicable while forwarding the audit logs to the Syslog server.

5. (Optional) By default, the alert policies are always active. To limit activity, in the **Date and Time** section, select the 'from' and 'to' dates, and then select the time frame.
   a. Select the check boxes corresponding to the days on which the alert policies must be run.
   b. Click **Next**.
6. In the **Severity** section, select the severity level of the alerts for which this policy must be activated.
   a. To select all the severity categories, select the **All** check box.
   b. Click **Next**.
7. In the **Actions** section, select **Syslog**.

   If Syslog servers are not configured in OpenManage Enterprise, click **Enable** and enter the destination IP address or the hostname of Syslog servers. For more information about configuring Syslog servers, see Configure SMTP, SNMP, and Syslog alerts on page 129.
8. Click **Next**.
9. In the **Summary** section, details of the alert policy you defined are displayed. Carefully read through the information.
10. Click **Finish**.

Results

The alert policy is successfully created and listed in the **Alert Policies** section.

Related tasks

Configure and manage alert policies on page 127
Monitor audit logs on page 133

Configure SMTP, SNMP, and Syslog alerts

By clicking **OpenManage Enterprise** > **Application Settings** > **Alerts**, you can configure the email (SMTP) address that receives system alerts, SNMP alert forwarding destinations, and Syslog forwarding properties. To manage these settings, you must have the OpenManage Enterprise administrator level credentials.

To configure and authenticate the SMTP server that manages the email communication between the users and OpenManage Enterprise:

1. Expand **Email Configuration**.
2. Enter the SMTP server network address that sends email messages.
3. To authenticate the SMTP server, select the **Enable Authentication** check box and enter the username and password.
4. By default, the SMTP port number to be accessed is 25. Edit if necessary.
5. Select the **Use SSL** check box to secure your SMTP transaction.
6. To test if the SMTP server is working properly, click on the **Send Test Email** check box and enter an **Email Recipient**.
7. Click **Apply**.
8. To reset the settings to default attributes, click **Discard**.

To configure the SNMP alert forwarding configuration:

1. Expand **SNMP Alert Forwarding Configuration**.
2. Select the **ENABLED** check box to enable the respective SNMP traps to send alerts in case of predefined events.
3. In the **DESTINATION ADDRESS** box, enter the IP address of the destination device that must receive the alert.

NOTE: Entering of the console IP is disallowed to avoid duplication of alerts.

4. From the **SNMP VERSION** menu select the SNMP version type as SNMPv1, SNMPv2, or SNMPv3 and fill the following fields:
   a. In the COMMUNITY STRING box, enter the SNMP community string of the device that must receive the alert.
   b. Edit the PORT NUMBER if needed. Default port number for SNMP traps=162. See Supported protocols and ports in OpenManage Enterprise on page 34.
   c. If SNMPv3 is selected, provide the following additional details:
      i. USERNAME: Provide a username.
      ii. AUTHENTICATION TYPE : From the drop down list select SHA, MD_5, or None.
      iii. AUTHENTICATION PASSPHRASE: Provide an authentication passphrase having a minimum of eight characters.
      iv. PRIVACY TYPE: From the drop down list select DES, AES_128, or None.
      v. PRIVACY PASSPHRASE: Provide a privacy passphrase containing a minimum of eight characters.
5. To test an SNMP message, click the **Send** button of the corresponding trap.
6. Click **Apply**. To reset the settings to default attributes, click **Discard**.

To update the Syslog forwarding configuration:

1. Expand **Syslog Forwarding Configuration**.
2. Select the check box to enable the Syslog feature on the respective server in the **SERVER** column.
3. In the **DESTINATION ADDRESS/HOST NAME** box, enter the IP address of the device that receives the Syslog messages.
4. Default port number by using UDP=514. Edit if necessary by entering or selecting from the box. See Supported protocols and ports in OpenManage Enterprise on page 34.
5. Click **Apply**.
6. To reset the settings to default attributes, click **Discard**.

Execute remote commands and scripts

About this task

When you get an SNMP trap, you can run a script on OpenManage Enterprise. This sets up a policy that opens a ticket on your third party ticketing system for alert management. You can create and store only up to **four** remote commands.

NOTE: The use of the following special characters as RACADM and IPMI CLI parameters is not supported: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, *****, and **'**.

Steps

1. Click **Application Settings** > **Script Execution**.
2. In the **Remote Command Setting** section, do the following:
   a. To add a remote command, click **Create**.
   b. In the **Command Name** box, enter the command name.
   c. Select any one of the following command type:
      i. Script
      ii. RACADM
      iii. IPMI Tool
   d. If you select **Script**, do the following:
      i. In the **IP Address** box, enter the IP address.
      ii. Select the authentication method: **Password** or **SSH Key**.
      iii. Enter the **user name** and **password** or the **SSH Key**.
      iv. In the **Command** box, type the commands.
         - Up to 100 commands can be typed with each command required to be on a new line.
         - Token substitution in scripts is possible. See Token substitution in remote scripts and alert policy on page 194
      v. Click **Finish**.
   e. If you select **RACADM**, do the following:
      i. In the **Command Name** box, enter the command name.
      ii. In the **Command** box, type the commands. Up to 100 commands can be typed with each command required to be on a new line.
      iii. Click **Finish**

f. If you select **IPMI Tool**, do the following:
   i. In the **Command Name** box, enter the command name.
   ii. In the **Command** box, type the commands. Up to 100 commands can be typed with each command required to be on a new line.
   iii. Click **Finish**

3. To edit a remote command setting, select the command, and then click **Edit**.
4. To delete a remote command setting, select the command, and then click **Delete**.

Automatic refresh of MX7000 chassis on insertion and removal sleds

OpenManage Enterprise can almost instantly reflect the addition or removal of sleds after a standalone or a lead MX7000 chassis is discovered or onboarded.

When a standalone or a lead MX7000 chassis is discovered or onboarded by using OpenManage Enterprise (versions 3.4 and later), an alert policy is created simultaneously on the the MX7000 chassis. For more information on discovering and onboarding devices in OpenManage Enterprise, see Create a device discovery job on page 46 and Onboarding devices on page 47.

The automatically-created alert policy on the MX7000 OpenManage Enterprise-Modular appliance triggers a chassis inventory refresh job, named **Refresh Inventory of Chassis** in OpenManage Enterprise every time a sled is inserted, removed, or replaced in the MX7000 chassis.

Post completion of the chassis- inventory-refresh job, the sled-related changes to the MX7000 are displayed on the All Devices page.

The following prerequisites must be met while onboarding the MX7000 chassis for a successful creation of the automatic alert policy :

- OpenManage Enterprise-Modular version 1.2 must be already installed in the MX7000.
- MX7000 chassis should be onboarded with the options **'Enable trap reception from discovered iDRAC servers and MX7000 chassis'** and **'Set Community String for trap destination from Application Settings'**.
- The OpenManage Enterprise appliance IP should get successfully registered as one of the four available alert destinations in the newly-onboarded MX7000. If all the alert destinations in the MX7000 are already configured at the time of onboarding, then the automatic alert policy creation will fail.

NOTE:

- The alert policy on MX7000 is only specific to the sleds and are not applicable to the other components of the chassis, such as the IOMs.
- MX7000 alert preferences can be set in OpenManage Enterprise to either receive all the alerts or only the chassis-category alerts from the MX7000 chassis. For more information, see Manage Console preferences on page 173.
- Some delay is to be expected between the actual action on the sleds and the triggering of the chassis inventory refreshing on OpenManage Enterprise.
- The automatically created alert policy is deleted if the MX7000 chassis is deleted from the device inventory of OpenManage Enterprise.
- The All Devices page will list the **Managed State** for a successfully onboarded MX7000 chassis with automatic alert forwarding policy as 'Managed with Alerts'. For more information on onboarding, refer Onboarding devices on page 47

Alert definitions

By clicking **OpenManage Enterprise** > **Alerts** > **Alert Definitions**, you can view alerts that are generated for errors or informational purposes. These messages are:

- Called as Event and Error messages.
- Displayed on the Graphical User Interface (GUI), and Command Line Interface (CLI) for RACADM and WS-Man.
- Saved in the log files for information purpose only.
- Numbered and clearly defined to enable you implement corrective and preventive actions effectively.

An Error and Event message has:

- **MESSAGE ID**: Messages are classified based on components such as BIOS, power source (PSU), storage (STR), log data (LOG), and Chassis Management Controller (CMC).

- **MESSAGE**: The actual cause of an event. Events are triggered for information purpose only, or when there is an error in performing tasks.
- **CATEGORY**: Class to which the error message belongs to. For information about categories, see the *Event and Error Message Reference Guide for Dell EMC PowerEdge Servers* available on the support site.
- **Recommended Action**: Resolution to the error by using GUI, RACADM, or WS-Man commands. Where necessary, you are recommended to refer to documents on the support site or TechCenter for more information.
- **Detailed Description**: More information about an issue for easy and fast resolution.

You can view more information about an alert by using filters such as message ID, message text, category, and Subcategory. To view the alert definitions:

1. From the **OpenManage Enterprise** menu, under **Alerts**, click **Alert Definitions**.

   Under **Alert Definitions**, a list of all the standard alert messages is displayed.

2. To quickly search for an error message, click **Advanced Filters**.

The right pane displays Error and Event Message information of the message ID you selected in the table.

15

Monitor audit logs

About this task

OpenManage Enterprise > **Monitor** > **Audit logs** page lists the log data to help you or the Dell EMC Support teams in troubleshooting and analysis. An audit log is recorded when:

- A group is assigned or access permission is changed.
- User role is modified.
- Actions that were performed on the devices monitored by OpenManage Enterprise.

The audit log files can be exported to the CSV file format. See Export all or selected data on page 71.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18.
- Scope-based restrictions are not applicable to the Audit logs.

Steps

1. To view the audit logs, select **Monitor** > **Audit Logs**.
   The audit logs that OpenManage Enterprise stores and displays about the tasks performed by using the appliance are displayed. For example, user login attempts, creation of alert policies, and running different jobs.
2. To sort data in any of the columns, click the column title.
3. To quickly search for information about an audit log, click **Advanced Filters**.
   The following fields are displayed that act as filters to quickly search for data.
4. Enter or select data in the following fields:
   - **Severity**: Select the severity level of a log data. The available options are info, warning, and critical.
     - Critical: Any unusual action happened. Immediate attention is needed.
     - Warning: The event is significant, but does not need immediate attention.
     - Info: Any action performed with success.
   - **Start Time** and **End Time**: To view audit logs of a specified period.
   - **User**: To view audit logs from a specific user. For example, admin, system, device manager, and viewer.
   - **Source Address**: To view audit logs from a specific system. For example, the system where you have logged in to the OpenManage Enterprise.
   - **Category**: To view audit logs of audit or configuration type.
     - Audit: Generated when a user logs in or out of the OpenManage Enterprise appliance.
     - Configuration: Generated when any action is performed on a target device.
   - **Description Contains**: Enter the text or phrase contained in the log data that you are searching for. All logs with the selected text are displayed. For example, if you enter `warningSizeLimit`, all the logs with this text are displayed.
   - **Message ID**: Enter the message ID. If the search criteria matches, only the items with the matching message ID are displayed.
5. To remove the filter, click **Clear All Filters**.
6. To export an audit log or all the audit logs, select **Export** > **Export Selected**, or **Export** > **Export All Audit Logs** respectively. For more information about exporting the audit logs, see Export all or selected data on page 71.
7. To get all the latest console logs and create an archive that is available for download, click **Troubleshoot** > **Create Console Log Archive**.
8. To download the console log archives, click **Troubleshoot** > **Download Archived Console Logs**.
9. To download the FSD dat file, click **Troubleshoot** > **Download FSD dat file**. This option is only available if the Field Service Debug (FSD) mode is enabled in the TUI (Text User Interface). For more information, see Configure OpenManage Enterprise by using Text User Interface on page 29, Field service debug workflow on page 194 and Unblock the FSD capability on page 195.

   NOTE: If the DAT file is downloaded as DAT.txt, you must rename it to DAT.ini.

10. To upload the signed .dat file and SSH public key, click **Troubleshoot** > **Upload of signed .dat file, SSH public key.** This option is only available if the Field Service Debug (FSD) mode is enabled in the TUI (Text User Interface). For more information, see Configure OpenManage Enterprise by using Text User Interface on page 29, Field service debug workflow on page 194 and Unblock the FSD capability on page 195.

Results

NOTE:

- Currently, for any M1000e chassis discovered with chassis firmware version of 5.1x and earlier, the date in the TIMESTAMP column under Hardware Logs is displayed as JAN 12, 2013. However, for all chassis versions of VRTX and FX2 chassis, the correct date is displayed.
- The file will not be immediately ready for download especially in cases where there is a large set of logs being collected. The collection process happens in the background, and a file save prompt is displayed when the operation is completed.

Related information

Forward audit logs to remote Syslog servers on page 128

Topics:

- Forward audit logs to remote Syslog servers

Forward audit logs to remote Syslog servers

To monitor all the audit logs of OpenManage Enterprise from Syslog servers, you can create an alert policy. All the audit logs such as user login attempts, creation of alert policies, and running different jobs can be forwarded to Syslog servers.

About this task

To create an alert policy to forward audit logs to Syslog servers:

Steps

1. Select **Alerts** > **Alert Policies** > **Create**.
2. In the **Create Alert Policy** dialog box, in the **Name and Description** section, enter a name and description of the alert policy.
   a. The **Enable Policy** check box is selected by default to indicate that the alert policy will be enabled once it is created. To disable the alert policy, clear the check box. For more information about enabling alert policies at a later time, see Configure and manage alert policies on page 127.
   b. Click **Next**.
3. In the **Category** section, expand **Application** and select the categories and subcategories of the appliance logs. Click **Next**.
4. In the **Target** section, the **Select Devices** option is selected by default. Click **Select Devices** and select devices from the left pane. Click **Next**.

   NOTE: Selecting target devices or groups is not applicable while forwarding the audit logs to the Syslog server.

5. (Optional) By default, the alert policies are always active. To limit activity, in the **Date and Time** section, select the 'from' and 'to' dates, and then select the time frame.
   a. Select the check boxes corresponding to the days on which the alert policies must be run.
   b. Click **Next**.
6. In the **Severity** section, select the severity level of the alerts for which this policy must be activated.
   a. To select all the severity categories, select the **All** check box.
   b. Click **Next**.
7. In the **Actions** section, select **Syslog**.
   If Syslog servers are not configured in OpenManage Enterprise, click **Enable** and enter the destination IP address or the hostname of Syslog servers. For more information about configuring Syslog servers, see Configure SMTP, SNMP, and Syslog alerts on page 129.
8. Click **Next**.

9. In the **Summary** section, details of the alert policy you defined are displayed. Carefully read through the information.
10. Click **Finish**.

Results

The alert policy is successfully created and listed in the **Alert Policies** section.

Related tasks

Configure and manage alert policies on page 127
Monitor audit logs on page 133

16

Using jobs for device control

A job is a set of instructions for performing a task on one or more devices. The jobs include discovery, firmware update, inventory refresh for devices, warranty, and so on. You can view the status and details of jobs that are initiated in the devices and its components, on the **Jobs** page. OpenManage Enterprise has many internal maintenance jobs which are triggered on a set schedule automatically by the appliance. For more information on the 'default' jobs and their schedule, see OpenManage Enterprise default jobs and schedule on page 138.

Prerequisites:

To create and manage jobs such as blink, power control, managing firmware baselines, managing configuration compliance baseline, and so on, where the device selection task is involved.

- You must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- Each job type is limited to devices that you must have:
  - permissions to access.
  - ability to complete the required action.

To create and manage jobs, select **OpenManage Enterprise** > **Monitor** > **Jobs**. You can perform the following tasks on the **Jobs** page:

- View list of jobs currently running, failed, and successfully completed.
- Create jobs to blink device LEDs, control the device power, and run remote command on devices. See Create a Remote command job for managing devices on page 142, Creating jobs for managing power devices, and Creating job to blink device LEDs. You can perform similar actions on a server on the device details page. See View and configure individual devices on page 72.
- Manage jobs such as run, stop, enable, disable or delete jobs.

To view more information about a job, select the check box corresponding to a job, and then click **View Details** in the right pane. See Viewing job information.

Topics:

View job lists

From OpenManage Enterprise, click **Monitor** > **Jobs** to view the list of existing jobs. Information about jobs are provided in the following columns:

- **Job Status**: Provides the execution status of a job.

  See Jobs status and Jobs type description on page 137.

- **State**: Provides the state of a job. The available options are Enabled or Disabled.
- **Job Name**: Name of a job.
- **Job Type**: Provides the type of a job.

  See Jobs status and Jobs type description on page 137.

- **Description**: Detail description of a job.
- **Last Run**: Last run period of a job.

Jobs can also be filtered by entering or selecting the values in the **Advanced Filters** section. The following additional information can be provided to filter the alerts:

- **Last run start date:**Jobs last run start date.
- **Last run end date**: Jobs last run end date.
- **Source**: The available options are All, User Generated (Default), and System.

To view more information about a job, select a job and click **View Details** in the right pane. See View an individual job information on page 141.

OpenManage Enterprise provides a built-in report to view the list of scheduled jobs. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Scheduled Jobs Report**. Click **Run**. See Run reports on page 148.

NOTE: On the **Discovery and Inventory Schedules** pages, the status of a scheduled job is identified by **Queued** in the **STATUS** column. However, the same status is indicated as **Scheduled** on the **Jobs** page.

Jobs status and Jobs type description

Table 20. Job status and description

Job Status	Description
Scheduled	Job is scheduled for run at a later date or time.
Queued	Jobs that are waiting to be executed.
Starting	
Running	Job is triggered using **Run Now**
Completed	Job has run.
Failed	Job run was unsuccessful.
New	Job is created but not run.
Completed with errors	Job run was partially successful and was completed with errors.
Aborted	Job run was paused by the user.
Paused	Job run was stopped by the user.
Stopped	Job run was interrupted by the user.
Canceled	
Not run	Job is either Queued or Scheduled and is yet to run.

A job can belong to any one of the following types:

Table 21. Job Types and description

Job Type	Description
Health	Checks the health status of the devices. See Device health statuses on page 42.
Inventory	Creates inventory report of the devices. See Managing device inventory on page 77.
Device Config	Creates device configuration compliance baseline. See Managing the device configuration compliance on page 116.
Report_Task	Creates reports about devices by using built-in or customized data fields. See Reports on page 147.
Warranty	Generate data about devices' warranty status. See Manage the device warranty on page 145.
Onboarding_Task	Onboards the discovered devices. See Onboarding devices on page 47.
Discovery	Discovers devices. See Discovering devices for monitoring or management on page 43.
Console Update Execution Task	Console Upgrade Job is being tracked using this task, This task helps to identify if the upgrade is completed or failed

Table 21. Job Types and description (continued)

Job Type	Description
Backup	
Chassis Profiles	
Debug Logs	Collects Debug logs of the application monitoring tasks, events, and the task execution history.
Device Action	Creates actions on devices such as Turn LED On, Turn LED Off, IPMI CLI, RACADM CLI, and so on.
Diagnostic_Task	Download/Run of Diagnostic/TSR or Services (SupportAssist) tasks are related to Diagnostic task. See Run and download Diagnostic reports.
Import VLAN Definition	Import of VLAN definitions from excel or from MSM.
OpenID Connect Provider	Configuration on OpenID connection. See OpenManage Enterprise login using OpenID Connect providers.
PluginDownload_Task	Plugin Download task is being tracked and this task helps to identify wether the downloading of Plugins RPM are completed and ready for installation. See Check and update the version of the OpenManage Enterprise and the available plugins.
Post_Upgrade_Task	PostUpgrade task is been tracked to set the appliance settings peformed in N-1 or N-2 Version also runs the discovery task which were created in Previous Version to make sure all devices are being listed.
Report_Task	Report Task is being tracked when user runs the report (for Canned as well for Custom).
Restore	
Settings Update	Settings Update task is being tracked when user applies a new setting under Application Settings tab.
Software Rollback	Rollback is task being tracked when user performs Rollback operation on a target device.
Update	Update task is being tracked when user performs the Firmware or Driver Update on the target devices.
Upgrade_Bundle_Download_Task	Upgrade bundle download task is being tracked and this task helps to identify wether the downloading of OMEnterprise RPM are completed and ready for installation

OpenManage Enterprise default jobs and schedule

OpenManage Enterprise has many internal maintenance jobs which are triggered automatically by the appliance on a set schedule.

Table 22. The following table lists the OpenManage Enterprise Default job names and their schedule.

Job Name	Cron Expression	Cron Expression Description	Example
Configuration Inventory	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021
Default Console Update Task	0 0 12 ? * MON *	At 12:00:00pm, on every Monday, every month	• Mon May 24 12:00:00 UTC 2021 • Mon May 31 12:00:00 UTC 2021
Default Inventory Task	0 0 5 * * ? *	At 05:00:00am every day	• Tue May 18 05:00:00 UTC 2021

Table 22. The following table lists the OpenManage Enterprise Default job names and their schedule. (continued)

Job Name	Cron Expression	Cron Expression Description	Example
			• Wed May 19 05:00:00 UTC 2021
Device Config Purge Task for cleanup	0 0/1 * * * ? *	At second :00, every minute starting at minute :00, of every hour	• Mon May 17 18:39:00 UTC 2021 • Mon May 17 18:40:00 UTC 2021
File Purge Task for Share Utilization	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021
File Purge Task for Single DUP Files	0 0 0/4 1/1 * ? *	At second :00, at minute :00, every 4 hours starting at 00am, every day starting on the 1st, every month	• Mon May 17 20:00:00 UTC 2021 • Tue May 18 00:00:00 UTC 2021 • Tue May 18 04:00:00 UTC 2021 • Tue May 18 04:00:00 UTC 2021
Global Health Task	0 0 0/1 1/1 * ? *	At second :00, at minute :00, every hour starting at 00am, every day starting on the 1st, every month	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021
Internal Sync Task	0 0/5 * 1/1 * ? *	At second :00, every 5 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 18:45:00 UTC 2021 • Mon May 17 18:50:00 UTC 2021
Metrics Purge Task	0 0 * ? * *	At second :00 of minute :00 of every hour	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 21:00:00 UTC 2021
Metrics Task	0 0/15 * 1/1 * ? *	At second :00, every 15 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 18:45:00 UTC 2021 • Mon May 17 19:00:00 UTC 2021
Mobile Subscription Task	0 0/2 * 1/1 * ? *	At second :00, every 2 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 18:54:00 UTC 2021 • Mon May 17 18:56:00 UTC 2021
Node Initiated Discovery Task	0 0/10 * 1/1 * ? *	At second :00, every 10 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 19:10:00 UTC 2021
Password Rotation Task	0 0 0/6 1/1 * ? *	At second :00, at minute :00, every 6 hours starting at 00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 06:00:00 UTC 2021 • Tue May 18 12:00:00 UTC 2021

Table 22. The following table lists the OpenManage Enterprise Default job names and their schedule. (continued)

Job Name	Cron Expression	Cron Expression Description	Example
Periodic Metrics Registration	0 0 3 * * ?	At 03:00:00am every day	• Tue May 18 03:00:00 UTC 2021 • Wed May 19 03:00:00 UTC 2021
Purge On Demand Health Task for Table: Task	0 0 0/5 1/1 * ? *	At second :00, at minute :00, every 5 hours starting at 00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 05:00:00 UTC 2021 • Tue May 18 10:00:00 UTC 2021
Purge Task Table :Event_Archive	0 0 18/12 ? * * *	At second :00, at minute :00, every 12 hours starting at 18pm, of every day	• Tue May 18 18:00:00 UTC 2021 • Wed May 19 18:00:00 UTC 2021 • Thu May 20 18:00:00 UTC 2021
Purge Task Table :Group_Audit	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
Purge Task Table :Task	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
Purge Task Table :announced_target	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
Purge Task for Table: Core Application Log	0 0 0/5 1/1 * ? *	At second :00, at minute :00, every 5 hours starting at 00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 05:00:00 UTC 2021
Purge Task for Table: Event	0 0/30 * 1/1 * ? *	At second :00, every 30 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 19:30:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 20:30:00 UTC 2021
Purge Task for Table: Infrastructure Device	0 0/30 * 1/1 * ? *	At second :00, every 30 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 19:30:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 20:30:00 UTC 2021