

- **Remote Console:** Click **Launch iDRAC** to start the iDRAC application. Click **Launch Virtual Console** to start the virtual console. Click the **Refresh Preview** symbol to refresh the **Overview** page.
- **Server Subsystem:** Displays health status of other components of the device such as PSU, fan, CPU, and battery.
 - ① **NOTE:** The time taken to collect subsystem data of sensor components discovered using IPMI depends on network connectivity, target server, and target firmware. If you experience timeouts while collecting the sensor data, reboot the target server.
- The **Last Updated** section indicates the last time when the device inventory status was updated. Click the **Refresh** button to update the status. An Inventory job is started and the status is updated on the page.
- By using **Power Control**, turn on, turn off, power cycle, and gracefully shut down a device.
- By using **Troubleshoot**:
 - Run and download the Diagnostics report. See *Run and download Diagnostic reports* on page 74.
 - Reset iDRAC.
 - Extract and download the Services (SupportAssist) report. See *Extract and download Services (SupportAssist) reports* on page 74.
- Refresh the device status.
- Refresh the device inventory.
- Export the device inventory that is collected by clicking **Refresh Inventory**. See *Export all or selected data* on page 71.
- Run a remote RACADM, and IPMI command on the device. See *Run remote RACADM and IPMI commands on individual devices* on page 75.

OpenManage Enterprise provides a built-in report to get an overview of devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise > Monitor > Reports > Devices Overview Report**. Click **Run**. See *Run reports* on page 148.



Device hardware information

OpenManage Enterprise provides a built-in report about the components and their compliance with the firmware compliance baseline. Click **OpenManage Enterprise > Monitor > Reports > Firmware Compliance per Component Report**. Click **Run**. See *Run reports* on page 148.


- **Device Card Information**—Information about cards used in the device.
- **Installed Software**—List of firmware and software installed on different components in the device.
- **Processor**—Processor information such as sockets, family, speed, cores, and model.
- **RAID Controller Information**—PERC and RAID controller used on the storage devices. The rollup status is equal to the status of the RAID that has high severity. 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 Dell TechCenter.
- **NIC Information**—Information about NICs used in the device.
- **Memory Information**—Data about DIMMs used in the device.
- **Array Disk**: Information about the drives installed on the device. OpenManage Enterprise provides a built-in report about the HDDs or virtual drives available on the devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise > Monitor > Reports > Physical Disk Report**. Click **Run**. See *Run reports* on page 148.
- **Storage Controller**: Storage controller installed on the device. Click the plus symbol to view individual controller data.
- **Power Supply Information**: Information about the PSUs installed on the device.
- **Operating System**—OS installed on the device.
- **Licenses**—Health status of different licenses installed on the device.
- **Storage Enclosure**—Storage enclosure status and EMM version.
- **Virtual Flash**—List of virtual flash drives and its technical specification.
- **FRU**—List of Field Replaceable Units (FRUs) that can be replaced by you or the field technicians. OpenManage Enterprise provides a built-in report about the Field Replacable Units (FRUs) installed on the devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise > Monitor > Reports > FRU Report**. Click **Run**. See *Run reports* on page 148.
- **Device Management Info**—IP address information of the iDRAC installed only in case of a server device.
- **Guest Information**—Displays the guest devices monitored by OpenManage Enterprise. UUID is the Universally Unique Identifier of the device. The **GUEST STATE** column indicates the working status of the guest device.

Run and download Diagnostic reports

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](#)
-  **NOTE:** Ensure to enable SMBv1 in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See [Manage Console preferences on page 173](#) and [Generic naming convention for Dell EMC PowerEdge servers on page 197](#) for more information.

Steps

1. On the **<Device name>** page, from the **Troubleshoot** drop-down menu, select **Run Diagnostics**.
2. In the **RemoteDiagnostic Type** dialog box, from the **Remote Diagnostic Type** drop-down menu, select one of the following to generate a report.
 - **Express:** In the least possible time.
 - **Extended:** At nominal speed.
 - **Long Run:** At a slow pace.
-  **NOTE:** See the *Remotely Running Automated Diagnostics Using WS-Man and RACADM Commands* technical white paper at https://en.community.dell.com/techcenter/extras/m/white_papers/20438187.
3. To generate the Diagnostics report now, select **Run Now**.
4. Click **OK**. When prompted, click **YES**.



 **WARNING:** Running a Diagnostics report automatically restarts the server.

A job is created and displayed on the **Jobs** page. To view information about the job, click **View Details** in the right pane. See [View job lists on page 136](#). The job status is also displayed in the **Recent Activity** section. After the job is successfully run, the status of the job is indicated as **Diagnostic Completed**, and the **Download** link is displayed in the **Recent Activity** section.

5. To download the report, click the **Download** link, and then download the **<Servicetag-jobid>.TXT** Diagnostics report file.
 - Else, click **Troubleshoot > Download Diagnostics Report**, and then download the file.
6. In the **Download RemoteDiagnostics Files** dialog box, click the .TXT file link, and then download the report.
7. Click **OK**.

Extract and download Services (SupportAssist) reports

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](#)
-  **NOTE:** Ensure to enable SMBv1 in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See [Manage Console preferences on page 173](#) and [Generic naming convention for Dell EMC PowerEdge servers on page 197](#) for more information.

Steps

1. On the **<Device name>** page, from the **Troubleshoot** drop-down menu, select **Extract SupportAssist Report**.
2. In the **Extract SupportAssist Report** dialog box:
 - a. Enter the file name where the SupportAssist report must be saved.
 - b. Select the check boxes corresponding to the log types whose SupportAssist report must be extracted.
3. Click **OK**.

A job is created and displayed on the **Jobs** page. To view information about the job, click **View Details** in the right pane. See [View job lists on page 136](#). The job status is also displayed in the **Recent Activity** section. After the job is successfully

run, the status of the job is indicated as **Diagnostic Completed**, and the **Download** link is displayed in the **Recent Activity** section.

4. To download the report, click the **Download** link, and then download the <Service Tag>.<Time>.TXT SupportAssist report file.
 - Else, click **Troubleshoot > Download SupportAssist Report**.
5. In the **Download SupportAssist Files** dialog box, click the .TXT file link, and then download the report. Each link represents the log type you selected.
6. Click **OK**.

Managing individual device hardware logs

NOTE: The hardware logs are available for YX4X servers, MX7000 chassis and sleds. See *Generic naming convention for Dell EMC PowerEdge servers* on page 197 for more information.

- On the <Device name> page, click **Hardware logs**. All the event and error messages generated for the device is listed. For field descriptions, see *Monitor audit logs* on page 133.
- For a chassis, the real-time data about the hardware logs are retrieved from the chassis.
- To add a comment, click **Add Comment**.
- In the dialog box, type the comment, and then click **Save**. The comment is saved and identified by a symbol in the **COMMENT** column.
- To export selected log data to a .CSV file, select the corresponding check boxes, and then click **Export > Export Selected**.
- To export all logs on a page, click **Export > Export Current Page**.

Run remote-RACADM and IPMI-commands on individual devices

About this task

RACADM and IPMI commands can be sent to a device's iDRAC from the 'Device name' page to remotely manage the respective device.

NOTE:

- The RACADM CLI only allows for one command at a time.
- The use of the following special characters as RACADM and IPMI CLI parameters is not supported: [, ; , |, \$, >, <, &, ' ,] , .. , * , and ' .

Steps

1. Select the check box corresponding to the device and click **View Details**.
2. On the <device name> page, click **Remote Command Line**, and then select **RACADM CLI** or **IPMI CLI**.

NOTE: The RACADM CLI tab is not displayed for the following servers because the corresponding task is not available in the device pack — MX740c, MX840c, and MX5016S.
3. In the **Send Remote Command** dialog box, type the command. Upto 100 commands can be entered with each command required to be on a new line. To display the results in the same dialog box, select the **Open results after sending** check box.

NOTE: Enter an IPMI command in the following syntax: -I lanplus <command> . To end the command enter 'Exit.'
4. Click **Send**.

A job is created and displayed in the dialog box. The job is also listed on the Job Details. See *View job lists* on page 136.
5. Click **Finish**.

The **Recent Alerts** section displays the job completion status.

Start Management application iDRAC of a device

Steps

1. Select the check box corresponding to the device.

The device working status, name, type, IP, and Service Tag are displayed.

2. In the right pane, click **Launch Management Application**.

The iDRAC login page is displayed. Log in by using the iDRAC credentials.

For more information about using iDRAC, visit Dell.com/idracmanuals.

 **NOTE:** You can also start the management application by clicking the IP address in the Device list. See [Devices list](#) on page 65.

Start the Virtual Console

About this task

The **Virtual Console** link works on the iDRAC Enterprise license of YX4X servers. On the YX2X and YX3X servers, the link works on the 2.52.52.52 and later versions of iDRAC Enterprise license. If the link is clicked when the current plugin type for virtual console is Active X, a message indicates prompting you to update the console to HTML 5 for better user experience. See [Create a job to change the virtual console plugin type](#) on page 143 and [Generic naming convention for Dell EMC PowerEdge servers](#) on page 197 for more information.

Steps

1. Select the check box corresponding to the device.
The device working status, name, type, IP, and Service Tag are displayed.
2. In the right pane, click **Launch Virtual Console**.
The remote console page on the server is displayed.

Refresh device inventory of a single device

About this task

By default, the inventory of software and hardware components in devices or device groups is automatically collected after every 24 hours (say, 12:00 a.m. everyday). However, to collect the inventory report of a single device at any moment:

Steps

1. Select the check box corresponding to the device on the All Devices page (**OpenManage Enterprise > Devices**) and click **View Details** on the right pane. The device's Overview page is displayed.
2. Click **Refresh Inventory** to initiate an Inventory job.
The status of the inventory job can be viewed on the Inventory page (**OpenManage Enterprise > Monitor > Inventory**). Select the Inventory job and click on **View Details** to view the collected inventory of selected device. For more information about viewing the refreshed inventory data, see [View and configure individual devices](#) on page 72. To download a device inventory, see [Export the single device inventory](#) on page 71.

Related information

[Organize devices into groups](#) on page 58

Managing device inventory

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 clicking **OpenManage Enterprise > Monitor > Inventory**, you can generate a device inventory report to better manage your data center, reduce maintenance, maintain minimum stock, and reduce operational costs. By using the Inventory Schedules feature in OpenManage Enterprise, you can schedule jobs to run at predefined time, and then generate reports. You can schedule inventory jobs on the 12th generation and later PowerEdge servers, networking devices, PowerEdge chassis, EqualLogic arrays, Compellent Arrays, and PowerVault devices.

On this page, you can create, edit, run, stop, or delete inventory schedules. A list of existing inventory schedule jobs is displayed.

- **NAME:** The inventory schedule name.
- **SCHEDULE:** Indicates if the job is scheduled to run now or later.
- **LAST RUN:** Indicates the time the job was last run.
- **STATUS:** Indicates if the job is running, completed, or failed.

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.

To preview a job information, click the row corresponding to the job. The right pane displays the job data and the target groups associated with the inventory task. To view information about the job, click **View Details**. The **Job Details** page displays more information. See [View an individual job information](#) on page 141.

Related tasks

- Run an inventory job now on page 78
- Stop an inventory job on page 78
- Delete an inventory job on page 79
- Create an inventory job on page 77

Topics:

- Create an inventory job
- Run an inventory job now
- Stop an inventory job
- Delete an inventory job
- Edit an inventory schedule job

Create an inventory job

The following steps describes how you can initiate the inventory collection on the discovered groups.

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.
 - Inventory collection on chassis storage sleds is not supported in OpenManage Enterprise if they are managed via chassis device management.

Steps

1. To initiate the Inventory wizard, do one of the following:

- a. On the All Devices page (**OpenManage Enterprise > Devices**), select a group on the left pane and from **Inventory** drop-down menu click **Run Inventory on Group**.
 - b. On the Inventory page (**OpenManage Enterprise > Monitor > Inventory**), click **Create**.
 2. In the **Inventory** dialog box, a default inventory job name is populated in **Inventory Job Name**. To change, enter an inventory job name.
 3. From the **Select Groups** drop-down menu, select the device groups on which the inventory must be run.
If you have initiated the Inventory job from the All Devices page after selecting a group, then Select Groups will be prepopulated with the selected group name. For information about device groups, see *Organize devices into groups* on page 58.
 4. In the **Scheduling** section, run the job immediately or schedule for a later point of time.
See *Schedule job field definitions* on page 192.
 5. The following **Additional Options** can be selected while running the inventory job:
 - Select the **Collect configuration inventory** check box to generate an inventory of the configuration compliance baseline.
 - Select the **Collect driver inventory** check box to collect driver inventory information from the Windows server. Also, to install the Inventory Collector and Dell System Update on the Windows server if these components are not available on the server.
- NOTE:**
- 'Collect driver inventory' applies only to devices discovered as 64-bit Windows servers.
 - Inventory collection of Windows-based devices is supported only using OpenSSH. Other SSH implementations on Windows, like the CygWin SSH, are not supported.
- For information about configuration compliance baselines, see *Managing the device configuration compliance* on page 116.
6. Click **Finish**.
 7. The job is created and listed in the queue.
An inventory job is created displayed in the list of inventory jobs. The **SCHEDULE** column specifies whether the job is Scheduled or Not Scheduled. See *Run an inventory job now* on page 78.

Related information

Managing device inventory on page 77

Run an inventory job now

About this task

NOTE: You cannot rerun a job that is already running.

Steps

1. In the list of existing inventory schedule jobs, select the check box corresponding to the inventory job you want to run immediately.
2. Click **Run Now**.

The job starts immediately and a message is displayed in the lower-right corner.

Related information

Managing device inventory on page 77

Stop an inventory job

About this task

You can stop the job only if running. Inventory jobs that are completed or failed cannot be stopped. To stop a job:

Steps

1. In the list of existing inventory schedule jobs, select the check box corresponding to the inventory schedule job you want to stop.
2. Click **Stop**.
The job is stopped and a message is displayed in the lower-right corner.

Related information

Managing device inventory on page 77

Delete an inventory job

About this task

 **NOTE:** You cannot delete a job if it is running.

Steps

1. In the list of existing inventory schedule jobs, select the check box corresponding to the inventory job you want to delete.
2. Click **Delete**.
The job is deleted and a message is displayed in the lower-right corner.

Related information

Managing device inventory on page 77

Edit an inventory schedule job

Steps

1. Click **Edit**.
2. In the **Inventory Schedule** dialog box, edit the inventory job name in **Inventory Job Name**. See [Create an inventory job on page 77](#).
The inventory schedule job is updated and displayed in the table.





Manage the device firmware and drivers

On the **OpenManage Enterprise > Configuration > Firmware/Driver Compliance** page, you can manage firmware of all the 'managed' devices that are discovered out-of-band using iDRAC. Additionally, you can update drivers of the 64-bit Windows-based servers that are discovered and managed in-band using the SSH protocol.

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.
- To perform Windows driver update, ensure that the Windows servers are discovered in-band using the supported protocol. To update both drivers and firmware, you must additionally discover the servers out-of-band using iDRAC.
- The device firmware or driver version, if earlier than baseline version, is not automatically updated and the user must initiate the update.
- It is recommended that the firmware and driver updation is done during the maintenance windows to prevent the devices or environment going offline during business hours.
- To manage a device's firmware and/or driver, the Onboarding status of the system should be either 'Managed' or 'Managed with Alerts'. See *Onboarding devices* on page 47
- Currently, the catalog contains drivers for only the 64-bit Windows-based devices.

By using the Firmware/driver feature, you can:

- Use a firmware and driver catalog from Dell.com either directly or after saving it on a network path. See *Add a catalog by using Dell.com* on page 81 or *Creating a firmware catalog by using local network*.
- Create a firmware and driver baseline by using the available catalogs. These baselines serve as benchmarks to compare the firmware and driver version on the devices against the version in the catalog. See *Creating the firmware baseline*.
- Run a compliance report to check if the devices associated with the baseline comply to the baseline firmware and driver versions. See *Checking firmware compliance*. The **COMPLIANCE** column displays:
 - **OK**  — if the target device's firmware and/or driver version is same as the baseline.
 - **Upgrade** — if the target device's has one or more versions earlier than the baseline's firmware or driver version. See *Updating the device firmware version*
 - **Critical**  — If the component's current firmware/driver version is lower than the baseline version and if the importance assigned is either Recommended or Urgent.
 - **Warning**  — If the component's current version is lower than the baseline version and the importance assigned is Optional.
 - **Downgrade**  — if the device firmware and/or driver is later than the baseline version.
 - Export the compliance report for statistical and analytical purposes.
 - Update device firmware and/or driver version by using the baseline. See *Update the device firmware and drivers by using baselines* on page 68 .

NOTE:

- When a firmware/driver baseline with many devices is checked for compliance, the warning alerts CDEV9000 on the Alerts page is logged for only one random non-compliant device from that baseline.
- The firmware or driver compliance status of network switches, modular IOAs, and Dell storage devices is displayed as **Unknown** as these are not updatable using the Dell catalog. It is recommended to perform individual firmware or driver updates for these devices using their respective individual Update package. To perform individual firmware or driver updates, select a device on the All Devices page, and click **View Details > Firmware/Drivers** and select the individual package option. For more information about the list of unsupported devices, refer *Firmware/driver compliance baseline reports— devices with 'Unknown' compliance status* on page 197 .

You can update firmware version of a device also on the:

- All Devices page. See *Updating the device firmware version*.

- **Device Details page.** In the Devices List, click the device name or IP address to view device configuration data, and then edit. See [View and configure individual devices on page 72](#).

NOTE: Updating a device using the Individual Package workflow only supports executable (EXE) based Dell Update Packages. When updating an FX2 CMC, the executable DUP must be installed via one of the sleds in the chassis.

The summary of all the baselines is displayed in the working pane, and the compliance of a selected baseline is displayed in the right pane by using a Donut chart. A Donut chart and list of items in the baseline changes based on the baseline you select from the Baseline list. See [Donut chart](#).

Topics:

- Manage firmware and driver Catalogs
- Create a firmware/driver baseline
- Delete configuration compliance baselines
- Edit a baseline
- Check the compliance of a device firmware and driver

Manage firmware and driver Catalogs

Catalogs are bundles of firmware and drivers based on device types. All the available catalogs (update packages) are validated and posted to Dell.com. You can use the catalog directly from the online repository or it can be downloaded to a network share.

Using these catalogs, you can create firmware/driver baselines for the discovered devices and check their compliance. This reduces the extra effort of administrators and device managers and also reduces the overall updating and maintenance time.

Administrator users can view and access all the catalogs in OpenManage Enterprise, however, device managers can only view and manage catalogs that they created and own. See, [Role and scope-based access control in OpenManage Enterprise on page 18](#).

For field definitions on the Catalog Management page, see [Catalog Management field definitions on page 196](#). The sources of catalog that you can currently access are:

NOTE:

- Firmware catalog management using Dell.com or a local network path is limited to only the Enterprise Server Catalog.
- OpenManage Enterprise supports UI internationalization, however, it is recommended that the functional content such as the file names and catalog content are entered only in English.
- Catalogs with base location pointing to 'Downloads.dell.com' can be used without the Dell Update Packages (DUPs) while importing catalog OpenManage Enterprise from a network share. During the firmware upgrade process, the DUPs will be downloaded directly from <https://downloads.dell.com>.

- **Latest component versions on Dell.com:** Lists the latest firmware and driver (64-bit Windows) versions of devices. For example, iDRAC, BIOS, PSU, and HDDs that are rigorously tested and released and posted to Dell.com. See [Creating a firmware catalog by using Dell.com](#).
- **Network Path:** Location where the firmware and driver catalogs are downloaded by the Dell Repository Manager (DRM) and saved on a network share. See [Creating a firmware catalog by using local network](#).

Add a catalog by using Dell.com

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](#).
- Ensure to enable SMBv1 in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See [Manage Console preferences on page 173](#) and [Generic naming convention for Dell EMC PowerEdge servers on page 197](#) for more information.
- OpenManage Enterprise supports UI internationalization, however, it is recommended that the functional content such as the file names and catalog content are entered only in English.

Steps

1. On the **Catalog Management** page, click **Add**.
2. In the **Add Update Catalog** dialog box:
 - a. In the **Name** box, enter a firmware catalog name.
 - b. For the **Catalog Source**, select the option **Latest component versions on Dell.com**.
 - c. In the **Update Catalog** box, select either **Manually** or **Automatically**.
 - d. If **Automatically** is selected in the **Update Catalog** box, **Update Frequency** need to be selected as either **Daily** or **Weekly** followed by time in the 12-hour format with AM/PM.
 - e. Click **Finish**.

The **Finish** button appears only after you have entered all the fields in the dialog box

A new firmware catalog is created and listed in the Catalog table on the **Catalog Management** page.
3. To go back to the **Firmware/Driver Compliance** page, click **Return to Firmware/Driver Compliance**.

Add a catalog to the local network

About this task


Catalog containing the firmware and drivers (64-bit Windows) can be downloaded using the Dell Repository Manager (DRM) and saved on a network share.

NOTE:

- For local network shares using Windows 2019 or later, the catalog must be generated using DRM version 3.3.2 and later.
- OpenManage Enterprise supports UI internationalization, however, it is recommended that the functional content such as the file names and catalog content are entered only in English.

Steps

1. On the **Catalog Management** page, click **Add**.
 2. In the **Add Update Catalog** dialog box:
 - a. In the **Name** box, enter a catalog name.
 - b. For the Catalog Source, select the option **Network Path**.
The **Share Type** drop-down menu is displayed.
 - c. Select one of the following:



NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See [Manage Console preferences on page 173](#) and [Generic naming convention for Dell EMC PowerEdge servers on page 197](#) for more information.
- NFS
 - i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
 - ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `nfsshare\catalog.xml`
 - CIFS
 - i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
 - ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `Firmware\m630sa\catalog.xml`
 - iii. In the **Domain** box, enter the domain name of the device.
 - iv. In the **User Name** box, enter the user name of the device where the catalog is stored.
 - v. In the **Password** box, enter the password of the device to access the share. Type the username and password of the shared folder where the catalog.xml file is stored.
 - HTTP
 - i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
 - ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `compute/catalog.xml`.

- **HTTPS**

- In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
- In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: *compute/catalog.xml*.
- In the **User Name** box, enter the user name of the device where the catalog is stored.
- In the **Password** box, enter the password of the device where the catalog is stored.
- Select the **Certificate Check** check box.

The authenticity of the device where the catalog file is stored is validated and a Security Certificate is generated and displayed in the **Certificate Information** dialog box.

- After you have entered the **Share Address** and the **Catalog File Path**, the **Test now** link is displayed. To validate a connection to the catalog click **Test now**. If the connection to the catalog is established, a *Connection Successful* message is displayed. If connection to the share address or the catalog file path is not established, *Connection to path failed* error message is displayed. This is an optional step.
 - In the **Update Catalog** box, select either **Manually** or **Automatically**. If the **Update Catalog** is selected as **Automatically**, select either **Daily** or **Weekly** as the update frequency and enter time in the 12-hour format.
- Click **Finish**. The **Finish** button appears only after you have entered all the fields in the dialog box. A new firmware catalog is created and listed in the Catalog table on the **Catalog Management** page.
 - To go back to the **Firmware/Driver Compliance** page, click **Return to Firmware/Driver Compliance**.


Related tasks

Delete a catalog on page 84

SSL Certificate Information

The catalog files for firmware and driver updates can be downloaded from the Dell support site, Dell EMC Repository Manager (Repository Manager), or a web site within your organization network.

If you choose to download the catalog file from the web site within your organization network, you can accept or decline the SSL certificate. You can view details of the SSL certificate in the **Certificate Information** window. The information comprises the validity period, issuing authority and the name of the entity to which the certificate is issued.

 **NOTE:** The **Certificate Information** window is displayed only if you create the catalog from the **Create Baseline** wizard.

Actions

Accept	Accepts the SSL certificate and allows you to access the web site.
Cancel	Closes the Certificate Information window without accepting the SSL certificate.

Update a catalog

The existing firmware and driver catalogs can be updated from the Dell.com site (base location).

About this task

To update a catalog:

Steps

- On the Catalog Management page, select a catalog.
- Click the **Check for update** button that is located in the right pane of the **Catalog Management** page.
- Click **YES**.
If the selected catalog was an online catalog, it is replaced by the most up-to-date version that is maintained at the Dell.com site. For the local network catalogs, all the latest firmware and drivers available in the base location are considered for computing the baseline compliance.

Edit a catalog

About this task

- NOTE:** OpenManage Enterprise supports UI internationalization, however, it is recommended that the functional content such as the file names and catalog content are entered only in English.

Steps

1. On the **Catalog Management** page, select a catalog.
The catalog details are displayed in the **<catalog name>** right pane.
2. Click **Edit** in the right pane.
3. In the **Edit Update Catalog** wizard, edit the properties.
The properties that you cannot edit are grayed-out. For field definitions, see *Add a catalog by using Dell.com* on page 81 and *Add a catalog to the local network* on page 82.
4. Enter the **Share Address** and the **Catalog File Path**, the **Test now** link is displayed. To validate a connection to the catalog click **Test now**. If the connection to the catalog is established, a **Connection Successful** message is displayed. If connection to the share address or the catalog file path is not established, **Connection to path failed** error message is displayed. This is an optional step.
5. In the **Update Catalog** box, select either **Manually** or **Automatically**.
If the **Update Catalog** is selected as **Automatically**, select either **Daily** or **Weekly** as the update frequency and enter time in the 12-hour format.
6. Click **Finish**.
A job is created and run immediately. The job status is indicated in the **REPOSITORY LOCATION** column of the **Catalog Management** page.

Delete a catalog

Steps

1. On the **Catalog Management** page, select the catalogs, and then click **Delete**.
The catalogs are deleted from the list.
 2. To go back to the **Firmware/Driver Compliance** page, click **Return to Firmware/Driver Compliance**.
- NOTE:** Catalogs cannot be deleted if linked to a baseline.

Related information

Add a catalog to the local network on page 82

Create a firmware/driver baseline

A baseline is a set of devices or group of devices that are associated with a firmware/driver catalog. A baseline is created for compliance evaluation of the firmware and drivers for the devices in that baseline against the versions specified in the catalog. To create a baseline:

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.
 - Device manager user can only view and manage the firmware/driver baselines that the respective device manager created and owns. Also, while creating baselines, the target groups or devices (capable of firmware update) that are only in the device manager's scope are displayed.

- A non-compliant device with a firmware and/or driver version earlier than the catalog version, is not automatically updated. You must update the firmware version. It is recommended to update device firmware during maintenance windows to prevent the devices or environment going offline during business hours.

Steps


- Under **Firmware**, click **Create Baseline**.
- In the **Create Update Baseline** dialog box:
 - In the **Baseline Information** section:
 - From the **Catalog** drop-down menu, select a catalog.
 - To add a catalog to this list, click **Add**. See *Managing firmware Catalogs*.
 - In the **Baseline Name** box, enter a name for the baseline, and then enter the baseline description.
 - Click **Next**.
 - In the **Target** section:
 - To select the target device(s):
 - Select **Select Devices**, and then click the **Select Devices** button.
 - In the **Select Devices** dialog box, all the devices monitored by OpenManage Enterprise, IOMs, and devices under static or query group are displayed in respective groups.
 - In the left pane, click the category name. Devices in that category are displayed in the working pane.
 - Select the check box corresponding to the device(s). The selected devices are listed under the **Selected Devices** tab.
 - To select the target device group(s):
 - Select **Select Groups**, and then click the **Select Groups** button.
 - In the **Select Groups** dialog box, all the devices monitored by OpenManage Enterprise, IOMs, and devices under static or query group are displayed in respective categories.
 - In the left pane, click the category name. Devices in that category are displayed in the working pane.
 - Select the check box corresponding to the group(s). The selected groups are listed under the **Selected Groups** tab.
- Click **Finish**.
A message is displayed that a job is created for creating the baseline.

In the Baseline table, data about the device and baseline job is displayed. For field definitions, see *Firmware baseline field definitions* on page 192.

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

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

Results

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

Edit a baseline

The baselines on the **Configurations > Firmware/Driver Compliance** page can be edited as follows:

Steps

1. Select a baseline, and then click **Edit** in the right pane.
2. Modify data as described in [Creating the firmware baseline](#).
The updated information is displayed in the Baseline list.
3. To go back to the **Firmware/Driver Compliance** page, click **Return to Firmware/Driver Compliance**.

Check the compliance of a device firmware and driver

On the **Configuration > Firmware/Driver Compliance** page, you can check for the compliance of the firmware and drivers of baseline devices against the associated catalog, view the report, and update the firmware and drivers of non-compliant devices.


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.
- The firmware and drivers (64-bit Windows) for the non-compliant devices in the baseline are not automatically updated and must be updated by the user. It is recommended to update device firmware and drivers during the maintenance windows to prevent the devices or environment going offline during business hours.
- To collect the inventory information, the Inventory Collector and Dell System Update must be available on the Windows server. If these components are not available on the server, then initiate an inventory job and select **Collect driver inventory**. The discovery job also collects driver inventory information, but only the inventory job installs the necessary components on the server. To collect the driver inventory information, create or edit an inventory job and select the **Collect driver inventory** check box. For more information, see [Create an inventory job](#) on page 77 and [Edit an inventory schedule job](#) on page 79.

Steps


1. Select the check box corresponding to the baseline(s), and click **Check Compliance**.
The baseline compliance job is run.

 **NOTE:** If the devices are not associated to a catalog, the compliance is not verified. A job is created only for the devices that are associated and listed in the Compliance table. To associate a device to a catalog, see [Creating the firmware baseline](#).

In the Baseline table, data about the device and baseline job is displayed. For field definitions, see [Firmware baseline field definitions](#) on page 192.

2. To view the Compliance report and to upgrade the firmware and driver version of device(s), click **View Report** in the right pane.


See [Viewing device firmware compliance report](#).

 **NOTE:** Rollback is not supported for drivers.




View the baseline compliance report

About this task



On the **Configuration > Firmware/Driver Compliance** page, the compliance status of the baselines is indicated. A Donut chart provides a summary of baselines' compliance to their respective catalogs. When more than one device is associated with a baseline, the status of the least compliant device to the baseline is indicated as the compliance level of that baseline. For

example, the compliance level of a baseline with only one device with compliance as 'critical', is indicated as 'critical'  even if most of the devices are compliant.

You can view the firmware and driver compliance of individual devices associated with a baseline and choose to either upgrade or downgrade the firmware and/or driver version on that device. To view the baseline compliance report:

- Select the check box corresponding to the baseline and click **View Report** in the right pane.
- On the **Compliance Report** page the list of devices associated with the baseline and their compliance level is displayed. By default, the devices in **Critical** and **Warning** statuses are displayed.
-  **NOTE:** If each device has its own status, the highest severity status is considered as the status of the group. 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 Dell TechCenter.
- **COMPLIANCE:** Indicates the compliance level of a device to the baseline. For more information about symbols used for device firmware/driver compliance levels, see *Manage the device firmware and drivers* on page 80.
- **TYPE:** Type of device for which the compliance report is generated.
- **DEVICE NAME/COMPONENTS:** By default, the Service Tag of the device is displayed.
 1. To view information about components in the device, click the > symbol.
A list of components and their compliance to the catalog is displayed.
 -  **NOTE:** For all the devices (except the MX7000 chassis) which are fully in compliance with the associate firmware baseline, the > symbol is not displayed.
 2. Select one or more check boxes corresponding to the devices whose firmware compliance status is 'Critical' and requires an update.
 3. Click **Make Compliant**. See *Update the device firmware version by using the baseline compliance report*.
- **SERVICE TAG:** Click to view complete information about the device on the <device name> page. For more information about tasks you can complete on this page, see *View and configure individual devices* on page 72.
- **REBOOT REQ:** Indicates if the device must be restarted after updating the firmware.
- **Info** : Symbol corresponding to every device component is linked to the support site page from where the firmware/driver can be updated. Click to open the corresponding Driver Details page on the support site.
- **CURRENT VERSION:** Indicates the current firmware version of the device.
- **BASELINE VERSION:** Indicates the corresponding firmware and driver version of the device available in the associated catalog.
- To export the compliance report to an Excel file, select the check boxes corresponding to the device, and then select from **Export**.
- To go back to the **Firmware** page, click **Return to Firmware**.
- To sort data based on a column, click the column title.
- To search for a device in the table, click **Advanced Filters**, and select or enter data in the filter boxes. See *Advanced Filters* in *OpenManage Enterprise Graphical User Interface overview* on page 38.

Update firmware and/or drivers using the baseline compliance report

After you run a firmware or driver compliance report, if the firmware or driver version on the device is earlier than the version on the catalog, the Compliance Report page indicates the device firmware or driver status as Upgrade ( or ).

About this task

The firmware and driver version of the associated baseline devices is not automatically updated, hence, the user must initiate the update. It is recommended to update the device firmware and/or driver during the maintenance windows to prevent the devices or environment going offline during business hours.

Device managers can run firmware/driver update only on the devices which are in their scope.

- i** **NOTE:** Inventory collection and the firmware update on chassis storage sleds is not supported in OpenManage Enterprise if they are managed via chassis device management.

Prerequisites:

- 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.
- You must create an inbound firewall rule to allow communication with port 22.
- If HTTP and HTTPS shares were configured using the proxy settings, ensure that these local URLs are included in the proxy-exception list before initiating any update tasks.
- Only one update task can be initiated on the target machine at a given time.

i **NOTE:**

- The Reset iDRAC function is not supported for the devices under an MCM chassis that are in a 'Proxied' onboarding state and for updating only the drivers of the devices. For more information about onboarding states, see *Onboarding devices* on page 47.
- The firmware or driver compliance status of network switches, modular IOAs, and Dell storage devices is displayed as Unknown as these are not updatable using the Dell catalog. It is recommended to perform individual firmware or driver updates for these devices using their respective individual Update package. To perform individual firmware or driver updates, select a device on the All Devices page, and click **View Details > Firmware/Drivers** and select the individual package option. For more information about the list of unsupported devices, refer *Firmware/driver compliance baseline reports — devices with 'Unknown' compliance status* on page 197

If the multi-chassis management (MCM) group is managed using OpenManage Enterprise-Modular versions lower than 1.30.00, you must consider the following before updating the firmware and/or drivers of MX7000 chassis and sleds :

- Chassis and sled firmware updates must be undertaken separately.
- The lead chassis must be updated separately as the final step after updating all the member chassis.
- Firmware can be updated for only up to 9 member chassis at a time.
- Firmware update is supported on a maximum of 43 sleds at a time irrespective of onboarding state (Managed or Proxied).

The driver updates are available only on devices discovered as 64-bit Windows servers. Before updating the drivers, do the following:

- Be aware that the rollback of the driver updates is not supported.
- To perform Windows driver update, ensure that the Windows servers are discovered in-band using the supported OpenSSH protocol. To update both drivers and firmware, you must additionally discover the servers' out-of-band using iDRAC.
- Driver updates on third party SSH hosted on Windows, such as the CygwinSSH, are not supported.
- To collect the inventory information, the Inventory Collector and Dell System Update must be available on the Windows server. If these components are not available on the server, then initiate an inventory job and select **Collect driver inventory**. The discovery job also collects driver inventory information, but only the inventory job installs the necessary components on the server. To collect the driver inventory information, create or edit an inventory job and select the **Collect driver inventory** check box. For more information, see *Create an inventory job* on page 77 and *Edit an inventory schedule job* on page 79.

To update a device firmware and/or driver by using the baseline compliance report:

Steps

1. On the **Configuration > Firmware/Driver Compliance** page, select the check box corresponding to the baseline to which the device is attached, and then click **View Report** in the right pane.
On the **Compliance Report** page, the list of devices associated with the baseline and their compliance level is displayed. For field descriptions, see *View the baseline compliance report* on page 86.
2. Select the check box corresponding to the device whose firmware or driver must be updated. You can select more than one device with similar properties.
3. Click **Make Compliant**.
4. In the **Make Devices Complaint** dialog box, you can do the following:
 - Under **Schedule Update**, click **Additional Information** to view the important information and select one of the following:
 - a. **Update Now:** To apply the firmware/driver updates immediately.
 - b. **Schedule Later:** Select to specify a date and time when the firmware and/or driver version must be updated. This mode is recommended if you do not want to disturb your current tasks.

- Under **Server Options** select one of the following reboot options :
 - a. To reboot the server immediately after the firmware/driver update, choose **Reboot server immediately** and from the dropdown menu select one of the following options:
 - i. **Graceful Reboot without Forced Shutdown**
 - ii. **Graceful Reboot with Forced Shutdown**
 - iii. **PowerCycle** for a hard reset of the device.
 - b. Select **Stage for next server reboot** to trigger the firmware/driver update when the next server reboot happens.

i **NOTE:** If the firmware/driver update jobs are created with the 'Stage for next server reboot' option, then the inventory and baseline check must be executed manually after the package is installed in the remote device.
- **Clear Job Queue:** Select to delete all jobs (scheduled, completed, and failed) on the target device, before the update job is initiated.

i **NOTE:** This function is not supported for updating the drivers.
- **Reset iDRAC:** Select to initiate a reboot of the iDRAC before the update job is initiated.

i **NOTE:** This function is not supported for updating the drivers.

5. Click **Update**.

Results

A firmware/driver update job is created to update the device's firmware and/or driver. You can view the status of the job on the **Monitor > Jobs** page.

Manage device deployment templates

Device deployment template in OpenManage Enterprise allows you to set the configuration properties such as BIOS, boot, network properties, and so on of servers and chassis.

The deployment template is a consolidation of system configuration settings referred to as attributes. The deployment template allows for multiple servers or chassis to be configured quickly and automatically without the risk of human error.

Templates enable you to optimize data center resources and reduce the cycle time in creating clones and deployments. Templates also enhance your business-critical operations in converged infrastructure that uses software-defined infrastructures.

You can either use the predefined deployment templates or import the deployment templates from a reference device or an existing template file. To view the list of existing templates, from the OpenManage Enterprise menu, click **Configuration > Templates**.

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.

A device manager can view and perform tasks on the default templates and only the custom templates that are owned by that device manager.

Topics:

- Create a Deployment template from a reference device
- Create a deployment template by importing a template file
- View a deployment template information
- Edit a server deployment template
- Edit a chassis deployment template
- Edit IOA deployment template
- Edit network properties of a deployment template
- Deploy device deployment templates
- Deploy IOA deployment templates
- Clone deployment templates
- Auto deployment of configuration on yet-to-be-discovered servers or chassis
- Create auto deployment targets
- Delete auto deployment targets
- Export auto deployment target details to different formats
- Overview of stateless deployment
- Define networks
- Edit or delete a configured network
- Export VLAN definitions
- Import network definitions

Create a Deployment template from a reference device

Prerequisites

You can create or edit a deployment template by using a reference device or by importing from an existing deployment template.



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.


- Ensure to enable SMBv1 in the **SMB Settings** before you begin any tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See *Manage Console preferences* on page 173 and *Generic naming convention for Dell EMC PowerEdge servers* on page 197.
- With HTTPS-enabled internal shares, Deployment template creation fails on MX7000 sleds that are discovered using the Complete Chassis Discovery (CCD).
- With SMBv2-enabled CIFS share, Deployment template creation fails for the FX2, VRTX, and M1000e chassis.


About this task


To create a Deployment template using a reference device:

Steps

1. From the **OpenManage Enterprise** menu, click **Configuration > Templates > Create Template**, and then select **From Reference Device**.
2. In the **Create Template** dialog box:
 - a. In the **Template Information** section, enter a name for the deployment template and description for the template.
 - b. Select the Deployment template type:
 - **Clone Reference Server**: Enables you to clone the configuration of an existing server.
 - **Clone Reference Chassis**: Enables you to clone the configuration of an existing chassis.
 - **Clone Reference IOA**: Enables you to clone the configuration of an existing M I/O aggregator.


 **NOTE:** The attributes in the IOA template are uneditable. Only the **name** and **description** of an IOA template can be edited.
 - c. Click **Next**.
 - d. In the **Reference Device** section, click **Select Device** to select the device whose configuration properties must be used for creating the new deployment template. For more information about selecting devices, see *Selecting target devices and device groups*.

 **NOTE:** You can select only one device as a reference device.

 **NOTE:** Only the IOA templates that were extracted at the time of chassis discovery are available for cloning. See *Create customized device discovery job protocol for servers –Additional settings for discovery protocols* on page 52
 - e. In the **Configuration Elements** section, select the check boxes corresponding to the device elements that must be cloned. For creating a deployment template by using server as the device, you can select to clone the server properties such as iDRAC, BIOS, Lifecycle Controller, and Event Filters. By default, all elements are selected.
 - f. Click **Finish**.
After successful creation, the job is displayed in the list. A deployment template creation job is started and the status is displayed in the **STATUS** column.
The job information is also displayed on the **Monitor > Jobs** page. To view additional details of the job, select the job and click **View Details** in the working pane. On the **Job Details** page, the execution details of the job are displayed. In the **Results** pane, click **View Details** to view detailed information of the job execution.

Create a deployment template by importing a template file

Prerequisites

-  **NOTE:** Ensure to enable SMBv1 in the **SMB Settings** before you begin any tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See *Manage Console preferences* on page 173 and *Generic naming convention for Dell EMC PowerEdge servers* on page 197 for more information.

About this task

Steps

1. From the **OpenManage Enterprise** menu, click **Configuration > Templates > Create Template**, and then select **Import from File**.

2. In the **Import Template** dialog box:
 - a. Enter a name for the new deployment template.
 - b. Click **Select a File**, and then select a template file.
 - c. Select either **Server**, **Chassis**, or **IOA** to indicate the template type.
3. Click **Finish**.
The properties of an existing template file is imported and a new deployment template is created.

Example

- To view information about a deployment template, select the check box, and then click **View Details** in the right pane. On the **Template Details** page, you can deploy or edit a deployment template. See *Deploy device deployment templates* on page 95 and *Create a Deployment template from a reference device* on page 90.
- To edit a deployment template:
 1. Select the corresponding check box, and then click **Edit**.
 2. In the **Edit Template** dialog box, edit the deployment template name, and then click **Finish**. Updated information is displayed in the list of deployment templates.

View a deployment template information

A list of predefined, user-created, or cloned device deployment templates is displayed under **Configuration > Templates**.

Steps

1. In the list of deployment templates, select the check box corresponding to the required device template.
2. In the working pane, click **View Details**.
On the **Template Details** page, the deployment template name, description, the reference device from which the deployment template was created, and the last updated date by the OpenManage Enterprise user information is displayed.
3. Right-click an element to expand all or collapse all the child elements in the **Configuration Details** section to display all the attributes that are used for creating the deployment template. You can also expand individual child elements specific to a parent element. For example, if you selected that iDRAC and BIOS elements must be used for cloning on the target device, attributes related only to such elements are displayed.

Edit a server deployment template

Prerequisites

Built-in deployment templates cannot be edited. Only the user-created deployment templates that are identified as 'Custom' can be edited. You can edit the attributes of a deployment template irrespective of whether you created it by using a reference template file or a reference device. When editing a template, selecting or deselecting 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.

Steps

1. On the **Configuration > Templates** page, select the required custom template check box, and then click **Edit**.
2. In the **Edit Template** dialog box:
 - a. In the **Template Information** section, edit the deployment template name and description. The template type cannot be edited.
 - b. Click **Next**.
 - c. In the **Edit Components** section, the deployment template attributes are displayed in:
 - The **Guided view** — This view of attributes displays only common attributes, grouped together by function. Attributes from the following categories are shown:
 - i. In the **BIOS Settings** section, select any one of the following:
 - **Manually**: Enables you to manually define the following BIOS properties:
 - **System profile**: From the drop-down menu, select to specify the type of performance optimization to be achieved in the system profile.
 - **User accessible USB ports**: From the drop-down menu, select to specify the ports that the user can access.
 - By default, the use of logical processor and in-band manageability are enabled.

- **Optimize based on workload:** From the Select workload profile drop-down menu, select to specify the type of workload performance optimization you want achieve on the profile.
 - ii. Click **Boot** and define the boot mode:
 - If you select BIOS as the boot mode, do the following:
 - To retry the boot sequence, select the **Enabled** check box.
 - Drag the items to set the boot sequence and hard drive sequence.
 - If you select UEFI as the boot mode, drag the items to set the UEFI boot sequence. If required, select the check box to enable the Secureboot feature.
 - iii. Click **Networking**. All the networks associated with the deployment template are displayed under **Network Interfaces**.
 - To associate an optional identity pool to the deployment template, select from the **Identity pool** drop-down menu. The networks associated with the selected identity pool is displayed. If the deployment template is edited in the Advanced view, the Identity pool selection is disabled for this deployment template.
 - To view the network properties, expand the network.
 - To edit the properties, click the corresponding pen symbol.
 - Select the protocol to be used for booting. Select only if the protocol is supported by your network.
 - Select the Untagged and Tagged network to be associated to the network
 - The partition, max, and min bandwidth are displayed from the deployment template (profile) we created earlier.
 - Click **Finish**. The network settings of the deployment template is saved.
 - The **Advanced view** — This view lists all the deployment template attributes that can be changed (including those shown in the Guided view). This view allows you to specify not only attribute values (like the Guided view), but also whether or not each attribute gets included when the deployment template is deployed to a target device.

Attributes are grouped together functionally for display. Vendor-specific attributes are grouped under Other Attributes. Each individual attribute is displayed with a check box preceding its name. The check box indicates whether or not the attribute will be included when the deployment template is deployed to a target device. Because of attribute dependencies, if you change the setting for whether or not a particular attribute gets deployed, it could cause unexpected results on the target device, or cause deployment to fail. Each group also has a check box to the left of its name. The icon in group check boxes has one of three values:

 - i. Checked — Indicates that all of the attributes in the group are selected for deployment.
 - ii. Hyphen — Indicates some (but not all) of the attributes are selected for deployment.
 - iii. Clear — Indicates that none of the attributes in the group are selected for deployment
- NOTE:**
- Using this option requires care and a good knowledge of attributes and attribute dependencies as various attributes depend on the value in another attribute to determine their behavior.
 - You can click on the group icons to toggle the deployment setting for all the attributes in the group.
 - The attributes with secure information, such as passwords, are hidden and would appear as 'empty' when initially loaded and the changes to these secure attribute values are masked.
 - A deployment template's associated Identity pool cannot be changed if a profile is already associated to it.
3. Click **Next**.
In the **Summary** section, the attributes you edited by using the Guided and Advanced mode are displayed.
 4. This section is read-only. Read through the settings and click **Finish**.
The updated template attributes are saved to the deployment template.

Edit a chassis deployment template

Editing chassis deployment templates is possible with OpenManage Enterprise. When editing a template, selecting or deselecting 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.

About this task

NOTE:

- To edit chassis deployment templates you must have the privileges of an Administrator or a Device Manager. For more details, see [Role and scope-based access control in OpenManage Enterprise](#) on page 18.

- User passwords can't be set on the MX7000 chassis and the Chassis Management Controller (CMC) deployment templates.

To edit a chassis deployment template:

Steps

1. Select **OpenManage Enterprise > Configuration > Templates** to get the list of deployment templates.
2. Select the check box corresponding to the required chassis template, and click **Edit**. Ensure that the deployment template is identified as "Custom".
3. Edit the **Template Name** and **Description** in the **Template Information** section. You cannot edit the **Template Type**.
4. Click **Next**.
5. In the **Edit Components** section under **Advanced View**, you can select or unselect the attributes to include or exclude in the deployment template.
6. Click **Next**.
7. You can review the changes to the attributes under **Summary**. A circle appears next to the changed attributes.
8. Click **Finish** to save the changes to the chassis deployment template.

Edit IOA deployment template

The attributes in the IOA deployment template are uneditable. Only the **name** and **description** of an IOA deployment template can be edited.

About this task

NOTE:

IOA template attributes must not be edited outside of the appliance, as the template will be considered as a corrupt file during deployment.

Edit network properties of a deployment template

On the **Configuration > Templates** page, you can edit the network configuration for the deployment templates that contains applicable NIC attributes.

About this task

After selecting a deployment template, click **Edit Network** to activate the Edit Network wizard and do the following:

- #### NOTE:
- VLAN settings on in-scope 'proxied' MX7000 sleds is allowed for a device manager, even if the MX7000 chassis is out of scope.

Steps

1. Click **IO Pool Assignment** and from the **Identity Pool** list, select an identity pool for the deployment template. Click **Next**.
2. In the **Bandwidth** section, edit the **Minimum Bandwidth (%)** and the **Maximum Bandwidth (%)** of the associated NICs and click **Next**.

- #### NOTE:
- Bandwidth settings are only applicable to the partitioned NICs.


3. In the **VLANs** section (applicable only for the modular systems):
 - a. Select an appropriate **NIC Teaming** option.
 - b. Select the **Propagate VLAN settings immediately** check box, to propagate the changed VLAN settings on the associated modular-system servers immediately without the need for a server reboot. Click **View Details** to view the devices that would be affected.

NOTE:

- **Propagate VLAN settings immediately** is implemented only if the deployment template has been already deployed.

- Before propagating the VLAN settings, ensure that the network profiles are already created for the modular system servers in the fabric.
- If the **Propagate VLAN settings immediately** check box is selected, then a job named **VLAN Propagation** is created to apply the changes. Status of the job can be checked on the **Monitor > Jobs** page.

- c. Select the **Use strict checking** check box to match the VLANs with like characteristics. If unselected, only VLAN name and QoS are used for matching.

 **NOTE:** This option applies only to the modular-system sleds.

- d. Make changes to the **Untagged Network** and **Tagged Network** attributes of the associated NICs as required.

4. Click **Finish** to apply the changes.

Deploy device deployment templates

You can deploy a deployment template that includes a set of configuration attributes to specific devices. Deploying a device deployment template on the devices ensures that the devices are uniformly configured.

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.
- If a device manager is deploying templates, then only the target group(s) and devices that are in that device manager's scope and which are capable of deployment are displayed.

Before you begin deploying a device deployment template, ensure that:

- You have either created a device deployment template or cloned a sample deployment template. See *Create a Deployment template from a reference device* on page 90.
- The target devices meet the requirements that are specified in *Minimum system requirements for deploying OpenManage Enterprise* on page 23.
- The OpenManage Enterprise Advanced license is installed on the target devices.

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.

 **NOTE:** During deployment of an MX7000 chassis template:

- The target device can only be the lead MX7000 chassis.
- If an MX7000 chassis is removed from group, it has to be rediscovered in OpenManage Enterprise.
- Users on the MX7000 chassis are replaced by the users who are configured in the template.
- Imported Active Directory settings are replaced with the values in chassis profile.

Steps

1. From the list of deployment templates on the **Configuration > Templates** page, select the check box corresponding to the deployment template you want to deploy, and then 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. During deployment of the device deployment template, the configuration changes might require a forceful reboot of the server. If you do not wish to reboot the server, select the **Do not forcefully reboot the host OS** option. A graceful reboot of the server is attempted when the **Do not forcefully reboot the host OS** option is selected. If the reboot fails, you must rerun the template deployment task.
 - c. Select the **Use strict checking** check box to match the VLANs with like characteristics. If unselected, only VLAN name and QoS are used for matching.

NOTE: This option is displayed only if the selected target devices are modular system sleds.

- d. Click **Next**.
3. If the target device is a server, in the **Boot to Network ISO** section:
 - a. Select the **Boot to Network ISO** check box.
 - b. Select either **CIFS** or **NFS** as the share type, and then enter information in the fields such as ISO image file path and share location where the ISO image file is stored. Use the tool tips to enter the correct syntax.
 - c. 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.
 - d. Click **Next**.
4. In the **iDRAC Management IP** section, change the target device IP settings if required, and then click **Next**.

NOTE:

 - Template deployment fails if DHCP settings are assigned during template deployment to a target device that was originally discovered using a static IP.
 - If the IP setting is not configured on the discovered MX7000 sled, the Boot to Network ISO operation is not run during the template deployment.
5. 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**.
6. In the **Virtual Identities** section, 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**.

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
7. In the **Schedule** section, run the job immediately or schedule for a later time. See [Schedule job field definitions](#) on page 192.
8. Click **Finish**. Review the warning message and click **YES**.

A Device Configuration job is created. See [Using jobs for device control](#) on page 136.

Deploy IOA deployment templates

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.


Before you begin deploying an IOA deployment template, ensure that:

- You have created an IOA deployment template for deployment. See [Create a Deployment template from a reference device](#) on page 90.
- The target devices meet the requirements that are specified in [Minimum system requirements for deploying OpenManage Enterprise](#) on page 23.
- Firmware version of the target device is the same as the IOA deployment template.
- Only the following cross template deployments are supported:

Table 13. Supported cross template deployments

IOA Deployment template mode	Supported IOA template modes of target
Standalone	Standalone, PMUX
PMUX (Programmable MUX)	PMUX, Standalone
VLT	VLT

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. See *Delete 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 Enterprise > 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 identity 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 can 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)	<p>Enter the postfix in one of the following formats:</p> <ul style="list-style-type: none">• AA:BB:CC:DD:EE:FF• AA-BB-CC-DD-EE-FF• AABB.CCDD.EEFF <p>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.</p>
Number of WWPN/WWNN Addresses	<p>Select the number of WWPN or WWNN address. The address can be between 1 and 5000.</p> <p>This option is displayed only if the Include FC Identity check box is selected.</p>

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	<p>Enter the starting MAC address of the identity pool in one of the following formats:</p> <ul style="list-style-type: none">• 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	<p>Enter the starting FCoE Initialization Protocol (FIP) MAC address of the identity pool in one of the following formats:</p> <ul style="list-style-type: none"> • AA:BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF <p>The maximum length of a MAC address is 50 characters. This option is displayed only if the Include FCoE Identity check box is selected.</p> <p>The WWPN/WWNN values are generated from the MAC address.</p>
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	<p>Enter the starting virtual MAC address in one of the following formats:</p> <ul style="list-style-type: none"> • AA:BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF <p>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.</p>
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 be downloaded either as a CSV or as a JSON 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**.


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](#)
- [View Profile details](#)
- [Profiles — view network](#)
- [Edit a profile](#)
- [Assign a Profile](#)
- [Unassign profiles](#)
- [Redeploy profiles](#)
- [Migrate a Profile](#)
- [Delete Profiles](#)
- [Export Profile\(s\) data as HTML, CSV, or PDF](#)

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.