

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 view Dashboard data pertaining to selected devices or groups, select from the **Device Groups** drop-down menu.

NOTE: The health status of a device or group is indicated by appropriate symbols. The health status of a group is the health of a device in a group that has the most critical health status. For example, among many devices in a group, if the health of a server is Warning then the group health is also 'Warning'. The rollup status is equal to the status of the device 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* technical white paper on the Dell TechCenter.

Groups can have a parent and child group. A group cannot have its parent groups as its own child group. By default, OpenManage Enterprise is supplied with the following built-in groups.

System Groups: Default groups created by OpenManage Enterprise. You cannot edit or delete a System Group, but can view based on user privileges. Examples of System Groups:

- **HCI Appliances:** Hyper-converged devices such as VxRAIL and Dell EMC XC series devices
- **Hypervisor Systems:** Hyper-V servers and VMware ESXi servers
- **Modular Systems:** PowerEdge Chassis, PowerEdge FX2, PowerEdge 1000e chassis, PowerEdge MX7000 chassis and PowerEdge VRTX chassis.

NOTE: An MX7000 chassis can be a lead, stand-alone, or member chassis. If an MX7000 chassis is a lead chassis and has a member chassis, the latter is discovered by using the IP of its lead chassis. An MX7000 chassis is identified by using one of the following syntaxes:

- **MCM group**—Indicates the Multi-Chassis Management (MCM) group that has more than one chassis identified by the following syntax: `Group_<MCM group name>_<Lead_Chassis_Svctag>` where:
 - `<MCM group name>`: Name of the MCM group
 - `<Lead_Chassis_Svctag>`: The Service Tag of the lead chassis. The chassis, sleds, and network IOMs form this group.
- **Stand-alone Chassis group**—Identified by using the `<Chassis_Svctag>` syntax. The chassis, sleds, and network IOMs form this group.

- **Network Devices:** Dell Force10 networking switches and Fibre Channel switches
- **Servers:** Dell iDRAC servers, Linux servers, Non-Dell servers, OEM servers, and Windows servers
- **Storage Devices:** Dell Compellent storage Arrays, PowerVault MD storage arrays, and PowerVault ME storage arrays
- **Discovery Groups:** Groups that map to the range of a discovery task. Cannot be edited or deleted because the group is controlled by the discovery job where the include/exclude condition is applied. See [Discovering devices for monitoring or management](#) on page 43.

NOTE: To expand all the subgroups in a group, right-click the group, and then click **Expand All**.

Custom Groups: Created by the administrators for specific requirements. For example, servers that host email services are grouped. Users can view, edit, and delete based on user privileges and group types.

- **Static Groups:** Manually created by the user by adding specific devices to a group. These groups change only when a user manually changes the devices in the group or a sub-group. The items in the group remain static until the parent group is edited or the child device is deleted.
- **Query Group:** Groups that are dynamically defined by matching user-specified criteria. Devices in the group change based on the result of devices that are discovered by using criteria. For example, a query is run to discover servers that are assigned to the Finance department. However, the Query Groups have a flat structure without any hierarchy.

NOTE: Static and Query groups:

- Cannot have more than one parent group. Meaning, a group cannot be added as a sub-group under its parent group.
- When changes are made to a Static group (devices are added or deleted) or a Query group (when a query is updated), the firmware/driver compliance of the devices associated with these groups is not automatically refreshed. It is recommended that the user initiates a firmware and/or driver compliance for the newly added/deleted devices in such instances.

NOTE: Creating more number of Custom (Query) groups in the device group hierarchy impacts the overall performance of OpenManage Enterprise. For optimized performance, OpenManage Enterprise captures the health-rollup status after every 10 seconds—having more number of Dynamic groups affects this performance.

On the **All Devices** page, in the left pane, you can create child groups under the parent Static and Query group. See [Create a Static device group on page 60](#) and [Create a Query device group on page 61](#).

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 delete the child group of a Static or Query group:

1. Right-click the Static or Query group, and then click **Delete**.
2. When prompted, click **YES**. The group is deleted, and the list under the group is updated.

Plugin Groups: Plugin groups are created when plugins such as Services, Power Manager Plugin are installed. Plugins, when installed, have their own system groups and some plugins such as the Power Manager plugin allow user created Custom groups under them.

Related tasks

[Delete devices from OpenManage Enterprise on page 67](#)

[Refresh device inventory of a single device on page 76](#)

[Refresh the device health of a device group on page 69](#)

Create a custom group (Static or Query)

On the **OpenManage Enterprise > Devices**(All Devices page), you can create static or query groups using the Create Custom Group wizard.

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](#)

Steps

1. To activate the Create Custom Group wizard, you can do the following:
 - On the **OpenManage Enterprise > Devices** left pane CUSTOM GROUPS, right click or click on the three dot vertical menu and click **Create Custom Group**.
 - From the All Device page, **Group Actions** drop-down menu, click **Create Custom Group**.
2. On the Create Custom Group wizard, select from one of the following custom group:
 - a. **Static Group**.
 - b. **Query Group**
3. Click **Create**.
Depending on your selection (static or query), either the Create Static Group Wizard or the Create Query Group Wizard is activated.

Results

Once a group (static or query) is created, it is listed under the CUSTOM GROUP, Static or Query groups.

Create a Static device group

On the All Devices page (**OpenManage Enterprise > Devices**) you can create static groups using the Create Static Group wizard. The devices in a static group remain static until the devices in the group are added or deleted.


About this task

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. To activate the Create Static Group wizard, do one of the following:
 - Under CUSTOM GROUPS, **Static Groups** either right click or click the three vertical dots menu, and then click **Create New Static Group**.

- Click **Group Actions > Create Custom Group > Static Group**.
2. In the **Create Static Group Wizard** dialog box, enter a Name and Description (optional) for the group, and then select a parent group under which the new static group must be created.

 **NOTE:** The static or dynamic group names and server configuration related names in OpenManage Enterprise must be unique (not case-sensitive). For example, *name1* and *Name1* cannot be used at the same time.
 3. Click **Next**.
 4. From the Group Member Selection dialog box, select the devices that must be included in the static group.
 5. Click **Finish**.


Results

The static group is created and listed under the parent group in the left pane. The child groups are indented from its parent group.

Create a Query device group

Query groups are dynamic groups whose devices are defined by matching some user-specified criteria. Devices in the group change based on the result of devices that are discovered by using the query criteria. On the All Devices page (**OpenManage Enterprise > Devices**), You can create query groups using the Create Query Group wizard.

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

Steps

1. To activate the Create Query Group wizard, you can do one of the following:
 - Under Custom Groups, either right click on **Query Groups** or click the three dots vertical menu next to the Query Groups, and then click **Create New Query Group**.
 - Click **Group Actions > Create Custom Group > Query Group**.
2. In the **Create Query Group Wizard** dialog box, enter a **Name** and **Description**(optional) for the group.
3. Click **Next**.
4. In the **Query Criteria Selection** dialog box, from the **Select existing query to copy** drop-down menu, select a query, and then select the other filter criteria. See Select a query criteria on page 61.
5. Click **Finish**.
The query group is created and listed under the Query group section in the left pane.

Select a query criteria

About this task

Define filters while creating query criteria for:

- Generating customized reports. See Creating reports on page 150.
- Creating Query-based device groups under the CUSTOM GROUPS. See Create a Query device group on page 61.

Define the query criteria by using two options:

- **Select existing query to copy:** By default, OpenManage Enterprise provides a list of built-in query templates that you can copy and build your own query criteria. A maximum of 6 criteria (filters) can be used while defining a query. To add filters, you must select from the **Select Type** drop-down menu.
- **Select type:** Build a query criteria from scratch by using attributes listed in this drop-down menu. Items in the menu depend on the devices monitored by OpenManage Enterprise. When a query type is selected, only appropriate operators such as =, >, <, and null are displayed based on the query type. This method is recommended for defining query criteria in building customized reports.

NOTE: When evaluating a query with multiple conditions, the order of evaluation is same as SQL. To specify a particular order for the evaluation of the conditions, add or remove parenthesis when defining the query.

- NOTE:** When selected, the filters of an existing query criteria is copied only virtually to build a new query criteria. The default filters associated with an existing query criteria is not changed. The definition (filters) of a built-in query criteria is used as a starting point for building a customized query criteria. For example:
1. *Query1* is a built-in query criteria that has the following predefined filter: `Task Enabled=Yes`.
 2. Copy the filter properties of *Query1*, create *Query2*, and then customize the query criteria by adding another filter: `Task Enabled=Yes AND (Task Type=Discovery)`.
 3. Later, open *Query1*. Its filter criteria still remains as `Task Enabled=Yes`.

Steps

1. In the **Query Criteria Selection** dialog box, select from the drop-down menu based on whether you want to create a query criteria for Query groups or for report generation.
2. Add or remove a filter by clicking the plus or dustbin symbol respectively.
3. Click **Finish**.
A query criteria is generated and saved in the list of existing queries. An audit log entry is made and displayed in the Audit logs list. See *Monitor audit logs* on page 133.

Related information

Managing the device configuration compliance on page 116

Edit a configuration compliance baseline on page 120

Remove a configuration compliance baseline on page 123

Edit a static group

On the All Devices page (**OpenManage Enterprise > Devices**) the existing static groups can be renamed, repositioned, and the devices in the static group can be added or deleted using the Edit Static Group wizard.

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.
 - Removal of groups from hierarchical static groups, does not affect any tasks that are scheduled on them. Any scheduled tasks, such as Blink device, Power Control, and Remote Command Change Virtual console will continue to run on the groups even when the groups are removed from the hierarchy.

Steps

1. Right-click on the static group or click on the three vertical dots menu next to the static group, and then click **Edit** to activate the Edit Static Group wizard.
2. In the Edit Static Group Wizard, you can edit the Name, Description, and Parent Group.
3. Click **Next**.
4. In the Group Member Selection screen, you can check or uncheck the devices to include or exclude them from the static group.
5. Click **Finish**.

Results

The changes made to the static group are implemented.

Edit a query group

On the All Devices page (**OpenManage Enterprise > All Devices**), the existing query group can be renamed, repositioned, and the query criteria based on which the devices are included in the query group can be edited using the Edit Query Group wizard.

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.

Steps

1. Under **CUSTOM GROUPS**, right-click on the query group or click on the three vertical dots menu next to the query group and then click **Edit**.
2. In the Edit Query Group wizard, make changes to the Name, Description as needed.
3. Click **Next**.
4. In the Query Criteria Selection dialog box, from the **Select existing query to copy** drop-down menu, select a query, and then select the other filter criteria.
5. Click **Finish**.

Results

The changes made to the query group are implemented.

Rename a static or query group

To rename a static or query group on the All Devices page (**OpenManage Enterprise > Devices**):

Steps

1. Under **CUSTOM GROUPS**, right-click a static or query group or click on the three dots next to the group you want to rename, and then click **Rename**. Or, select a group and then click **Group Actions > Rename Group**.
2. In the **Rename Group** dialog box, enter a new name for the group.
3. Click **Finish**
The updated name is listed in the left pane.

Delete a static or query device group

On the All Devices page (**OpenManage Enterprise > Devices**), you can delete an existing static or query group as follows:

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.

About this task

NOTE: This procedure is applicable only for deleting a static or query group, however the devices in the group would not be deleted from the All Devices page. To remove devices from OpenManage Enterprise, see *Delete devices from OpenManage Enterprise* on page 67.

Steps

1. Under **CUSTOM GROUPS**, right-click the static or query group or click on the three dots vertical menu next to the group and then click **Delete**. OR, Select the group you want to delete, and then from the **Group Actions** drop-down menu and click **Delete Group**.
2. When prompted, click **Yes**.

Results

The group is deleted from the CUSTOM GROUPS.

Clone a static or query group

The existing static or query groups can be cloned and added to the CUSTOM GROUPS.

Prerequisites

i 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. Right-click on the static or query group or click on the tree dots vertical menu next to the static or query group, and then click **Clone**.
2. In the **Clone Group** dialog box, enter a Name and description for the group. Additionally for static group, select a parent group under which the cloned Static must be created.
3. Click **Finish**.
The cloned group is created and listed under the parent group in the left pane.

Add devices to a new group

You can create a new group and add devices to it from the device list table available on the All Devices page.

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.

Steps

1. From the **OpenManage Enterprise** menu, click **Devices**.
All Devices page is displayed.
2. In the devices list, select the check box corresponding to the device(s), and then click **Group Actions > Add To New Group**.
 - a. In the **Add Devices to New Group Wizard** dialog box, enter the **Name**, **Description**(optional), and select the **Parent Group** under which the new child group will be created. For more information about groups, see *Device Groups*.
 - b. To add more devices to the group, click **Next**. Else, go to step 3.
3. In the **Group Member Selection** dialog box, select more devices from the **Add Devices** list.
After you select devices under the **All Devices** tab, the selected devices are listed under **All Selected Devices**.
4. Click **Finish**.
A new group is created and the devices are added to the selected group.

i NOTE: For creating groups or adding devices to a group, you must follow the parent-child relationship of groups. See *Device Groups*.

Add devices to existing group

You can add devices to an existing group from the device list table available on the All Devices page.

Prerequisites

i 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. From the **OpenManage Enterprise** menu, click **Devices**.

All Devices page is displayed.

2. In devices list, select the check box corresponding to the device(s), and then click **Group Actions > Add To Existing Group**.
3. In the **Add Selected Devices to Existing Group** dialog box, enter or select data. For more information about groups, see [Device Groups](#).
4. Click **Finish**.

The devices are added to the selected existing group.



NOTE: For creating groups or adding devices to a group, you must follow the parent-child relationship of groups. See [Device Groups](#).

Refresh health on group

The following steps describe how you can refresh the health and online status of a selected group.

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.
- For the in-band devices discovered using the ESXi and Linux operating systems, the Health State () is displayed as Unknown ().

Steps

1. Go to the All Devices page by clicking **OpenManage Enterprise > Devices**.
2. On the left pane, select the group on which you want to refresh the health.
After selection of the group, the devices' list will list the selected group's devices.
3. Click the **Refresh Health** drop-down menu and then click **Refresh Health on Group**. The Health wizard is displayed.
4. In the Health wizard, **Job Name** displays the appliance-generated job name for the refresh-health task. If needed, you can change the job name.
5. The **Select Group** drop down will show the group that you had selected.
6. From the Scheduling drop down, you can select one of the following options:
 - a. **Run Now**— To immediately run the Refresh Health on the selected group.
 - b. **Run Later**— You can select Run Later and then select the Date and Time when the Refresh Health job on the group will run.
 - c. **Run on Schedule**— You can select this option then choose the Daily or Weekly and select a time if you want to refresh the health on the group on Daily or Weekly basis at a particular time.

Results

A job to refresh the health and online status of the group is created. You can view the job details on the Jobs page (**OpenManage Enterprise > Monitor > Jobs**).

Devices list

The list of devices displays the device properties such as IP address and Service Tag. You can select a maximum of 25 devices per page and navigate the pages to select more devices and perform tasks. For more information about the tasks you can perform on the All Devices page, see [All Devices page — device list actions](#) on page 66.

NOTE: By default, the Devices list displays all the devices considered while forming the Donut chart. To view a list of devices that belong to a specific health status, click the corresponding color band in the Donut chart, or click the health status symbol. Devices that belong only to the selected category are listed.

- **Health State** indicates the working state of the device. The health statuses—Normal, Critical, and Warning—are identified by respective color symbols. See [Device health statuses](#) on page 42
- **Power State** indicates if the device is turned on or off

- **Connection State** indicates connection status of the discovered devices to OpenManage Enterprise as: Connected, Disconnected, or Disconnected (Authentication failure)
- **Name** indicates device name.
- **IP Address** indicates the IP address of the iDRAC installed on the device
- **Identifier** indicates the service tag of the device
- **Model** indicates the model number
- **Type** indicates the type of device—Server, Chassis, Dell Storage, and Networking switch
- **Chassis Name** indicates chassis name
- **Slot Name** indicates the slot name for the chassis devices
- **Managed State** column indicates if the device is monitored, managed, or is proxied. See *Discovering devices for monitoring or management* on page 43.

To filter data in the table, click **Advanced Filters** or the Filter symbol. To export data to HTML, CSV, or PDF file format, click the Export symbol in the upper-right corner.

- ① **NOTE:** 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.
- ① **NOTE:** The working pane displays the Donut chart of the selected device group. By using the Donut chart, you can view the list of devices that belongs to other health statuses in that group. To view devices of other health status, click the corresponding color band on the Donut chart. The data in the table changes. For more information about using the Donut chart, see *Donut chart*.

All Devices page — device list actions

On the All Devices page (**OpenManage Enterprise > Devices**) devices list, you can perform various device actions.

The action buttons are context sensitive to both the group selection from the tree on the left and also for the devices selected in the grid. So if the action is group related, for example group actions such as 'Run Inventory on Group' group and 'Refresh Health on Group' — will default to the selected group. All device actions will default to the selected devices. However, few actions such as Discovery are always applicable without any selection. Also, the type of actions available per device depend on the type of device selected.

- ① **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.
- From **Group Actions** drop-down, you can:
 - Create custom device groups. See *Create a custom group (Static or Query)* on page 60.
 - Create static groups. See *Create a Static device group* on page 60.
 - Create query groups. See *Create a Query device group* on page 61
 - Edit static or query groups. See *Edit a static group* on page 62 and *Edit a query group* on page 63.
 - Clone groups. See *Clone a static or query group* on page 64.
 - Rename group. See *Rename a static or query group* on page 63.
 - Delete groups. See *Delete a static or query device group* on page 63.
 - Add device(s) to a new group. See *Add devices to a new group* on page 64.
 - Add device(s) to an existing group. See *Add devices to existing group* on page 64.
- From **Discovery** drop-down, you can:
 - Discover and onboard devices. See *Discovering devices for monitoring or management* on page 43 and *Onboarding devices* on page 47.
 - Exclude devices. See *Exclude devices from OpenManage Enterprise* on page 67.
 - Edit Exclude ranges. See *Global exclusion of ranges* on page 51.
- From **Inventory** drop-down, you can:
 - Run inventory on a device group. See *Create and run an inventory job*.
 - Run inventory on devices. See *Run inventory on devices* on page 68.
- From **Refresh Health** drop-down, you can:
 - Refresh health on group. See *Refresh health on group* on page 65.
 - Refresh health on devices. See *Refresh health on devices* on page 70.
- From **More Actions** drop-down, you can:
 - Turn LED on. See *Create a job to turn device LEDs* on page 141.
 - Turn LED off. See *Create a job to turn device LEDs* on page 141.

- Power on the device(s). See [Create a job for managing power devices on page 142](#).
- Power off the device(s). See [Create a job for managing power devices on page 142](#).
- Graceful shutdown of the device(s). See [Create a job for managing power devices on page 142](#).
- Power Cycle a system (Cold Boot). See [Create a job for managing power devices on page 142](#).
- System reset (Warm Boot). See [Create a job for managing power devices on page 142](#).
- Perform IPMI CLI remote command on a device. See [Run remote-RACADM and IPMI-commands on individual devices on page 75](#).
- Perform RACADM CLI remote command on a device. See [Run remote-RACADM and IPMI-commands on individual devices on page 75](#).
- Delete device(s) from OpenManage Enterprise. See [Delete devices from OpenManage Enterprise on page 67](#).
- Export data on all the devices. See [Export all or selected data on page 71](#).
- Export data on the selected devices. See [Export all or selected data on page 71](#).

Delete devices from OpenManage Enterprise

The following steps describe how to delete and offboard the discovered devices in OpenManage Enterprise.

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](#).
- A device on which a profile is assigned cannot be deleted unless the profile is unassigned from it. For more information, see [Unassign profiles on page 113](#).
- A device can be deleted even when tasks are running on it. Any tasks initiated on a device fails if the device is deleted before the completion of the tasks.

To delete the discovered devices:

Steps

1. Go to the All Devices page by clicking **OpenManage Enterprise > Devices**.
2. From the devices list, select the check boxes corresponding to the devices that you want to delete.
3. Click the **More Actions** drop-down menu and click **Delete Devices**.
4. At the prompt indicating that the devices will be deleted and offboarded from OpenManage Enterprise, click **YES**.

Results

The selected devices are entirely removed from OpenManage Enterprise. After device deletion, all onboarding information corresponding to the deleted devices is removed. The user credential information is automatically deleted if it is not shared with other devices. If OpenManage Enterprise was set as a trap destination on the device that is deleted, then you must remove OpenManage Enterprise console IP as a trap destination from the device.

Related information

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

Exclude devices from OpenManage Enterprise

Devices are discovered and grouped in OpenManage Enterprise for efficient handling of repeated tasks such as firmware updates, configuration updates, inventory generation, and alert monitoring. However, you can also exclude the devices from all OpenManage Enterprise discovery, monitoring, and management activities. The following steps describe how to exclude the already discovered devices from OpenManage Enterprise.

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

Steps

1. Go to the All Devices page by clicking **OpenManage Enterprise > Devices**.
2. In the left pane, select the system group or the custom group whose device must be excluded.
3. In the devices list, select the check box corresponding to the device(s), and then from **Discovery** drop-down menu and click **Exclude Devices**.
4. At the prompt indicating that the devices will be entirely removed and added to the Global-Exclusion list, click **YES**.

Results

The devices are excluded, added to the global exclusion list, and not anymore monitored by OpenManage Enterprise.

NOTE: To remove the device from global exclusion and to make OpenManage Enterprise monitor the device again, you must remove the devices from the global exclusion range, and then rediscover.

Run inventory on devices

The following steps describe how you can initiate inventory collection on the discovered devices.

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](#)

Steps

1. Go to the All Devices page by clicking **OpenManage Enterprise > Devices**.
2. From the devices' list, select the check box corresponding to the devices.
3. From the **Inventory** drop down, click **Run Inventory on Devices**.

Results

An Inventory job is created for the selected devices' inventory collection. You can view the status of this job on the Inventory page (**OpenManage Enterprise > Monitor > Inventory**).

Update the device firmware and drivers by using baselines

About this task

You can update the firmware and/or driver version of device(s) on the All Devices page or from the Firmware/Driver Compliance page (see [Update firmware and/or drivers using the baseline compliance report on page 87](#)). Updating using the All Devices page is recommended when updating firmware and/driver of a single device.

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](#).
- Driver updates are applicable only for devices associated with 64-bit Windows versions.
- Driver updates on the devices cannot be rolled back.
- If the firmware update is done using 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.
- If the device is not associated with any baseline, the **Baseline** drop-down menu is not populated. To associate a device to a baseline, see [Creating the firmware baseline](#).
- If you select multiple devices, only the devices that are associated with the selected baseline are listed in the table.

Steps

1. From the All Devices page **Devices** list, select the device(s) and click **More Actions > Update**.

NOTE: When you select device(s), ensure that they are associated with one or more firmware baselines. Else, the devices are not displayed in the compliance report, and therefore cannot be updated.

2. In the **Device Update** dialog box:

- a. In the **Select Update Source** section select one of the following:
 - From the **Baseline** drop-down menu, select the baseline. A list of devices that are associated with the selected baseline is displayed. The compliance level of each device is displayed in the 'compliance' column. Based on the compliance level, you can update the firmware and/or driver version. For information about the field description on this page, see [Viewing device firmware compliance report](#).
 - i. Select the check boxes corresponding to the devices that must be updated.
 - ii. Click **Next**.
 - You can update the firmware and/or drivers by using Individual Update package also. Click **Individual Package**, and then complete the on-screen instructions. Click **Next**.
- b. In the **Schedule** section:
 - 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:** To specify a date and a 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. If this option is selected, then the inventory and baseline check must be executed manually after the package is installed in the remote device.

3. Click **Finish**.

Results

A firmware/driver update job is created and listed in the Jobs list. See [Using jobs for device control](#) on page 136.

Refresh the device health of a device group

By default, the health of all the devices and device groups is refreshed automatically by the appliance on an hourly basis, however, you can also refresh the health of device(s) and/or device group(s) at any moment. The following steps describe how to refresh health and online status on the selected device group on the All Devices page.

Steps

1. In the left pane, select the group to which the device belongs to.
Devices associated to the group are listed.
2. Select the check box corresponding to the device(s), and then click **Refresh Health on Group**.
A job is created and listed in the Jobs list and identified as **New** in the JOB STATUS column.

Results

The latest working status of selected device(s) is collected and displayed on the Dashboard and other relevant sections of OpenManage Enterprise. To download a device inventory, see [Export the single device inventory](#) on page 71.

Related information



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

Refresh health on devices

By default, the health of all the devices and device groups is refreshed automatically by the appliance on an hourly basis, however, you can also refresh the health of device(s) and/or device group(s) at any moment. The following steps describe how to refresh health and online status on the selected devices on the All Devices page.

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.
- For the in-band devices discovered using the ESXi and Linux operating systems, the Health State () is displayed as Unknown () .

Steps

1. Go to the All Devices page by clicking **OpenManage Enterprise > Devices**.
2. Select the devices from the Devices list on which you want to refresh the health.
3. Click the **Refresh Health** drop-down menu and then click **Refresh Health on Devices**.

Results

A Health task is initiated for the selected devices. You can view the status of the health task on the Jobs page (**OpenManage > Monitor > Jobs**).

Roll back an individual device's firmware version

About this task


You can roll back the firmware version of a device that is later than the firmware version of the baseline it is associated with. This feature is available only when you view and configure properties of an individual device. See [View and configure individual devices](#) on page 72. You can upgrade or roll back the firmware version of an individual device. You can roll back the firmware version of only one device at a time.


NOTE:

- Rollback is applicable only for firmware. Device drivers once updated, can't be rolled back to previous version.
- Rollback is only for devices that are updated from the OME console (it is applicable to both baseline and for single DUP update).
- If any of the installed iDRACs are not in 'ready' state, a firmware update job may indicate failure even though the firmware is successfully applied. Review the iDRAC that is not in the ready state, and then press F1 to continue during the server boot.

Any device firmware that is updated by using the iDRAC GUI is not listed here and cannot be updated. For information about creating baseline, see [Create a firmware/driver baseline](#) on page 84.

Steps

1. In the left pane, select the group, and then click the device name in the list.
2. On the **<device name>** page, click **Firmware/Drivers**.
3. From the **Baseline** drop-down menu, select the baseline to which the device belongs to.
All the devices that are associated with the selected baseline are listed. For information about field description in the table, see [View the baseline compliance report](#) on page 86.
4. Select the check box corresponding to the device whose firmware version must be rolled back which is identified by .
5. Click **Rollback Firmware**.
6. In the **Rollback Firmware** dialog box, the following information is displayed:
 - **COMPONENT NAME:** Component on the device whose firmware version is later than the baseline version.
 - **CURRENT VERSION:** Current version of the component.
 - **ROLLBACK VERSION:** Suggested firmware version to which the component can be downgraded.


- **ROLLBACK SOURCE:** Click **Browse** to select a source from where the firmware version can be downloaded.
7. Click **Finish**. The firmware version is rolled back.
-  **NOTE:** Currently, the Rollback feature tracks only the version number from which the firmware is rolled back. Rollback does not consider the firmware version that is installed by using the Rollback feature (by rolling back the version).

Export the single device inventory

About this task

You can export inventory data of only one device at a time to only the .csv format.

Steps

1. In the left pane, select the device group. A list of devices in the group is displayed in the Devices list. A Donut chart indicates the device status in the working pane. See [Donut chart](#). A table lists the properties of devices selected. See [Device list](#).
 2. In the devices list, select the check box corresponding to the device, and then click **Export Inventory**.
 3. In the **Save As** dialog box, save to a known location.
-  **NOTE:** When exported to .csv format, some of the data displayed on the GUI is not enumerated with a descriptive string.

Performing more actions on chassis and servers

By using the **More Actions** drop-down menu, you can perform the following actions on the All Devices page. Select the device(s) and click any one of the following:

- **Turn LED On:** Turn on the LED of the device to identify the device among a group of devices in a data center.
- **Turn LED Off:** Turn off the LED of the device.
- **Power On:** Turn on the device(s).
- **Power Off:** Turn off the device (s).
- **Graceful Shutdown:** Click to shut down the target system.
- **Power Cycle System (Cold Boot):** Click to power off and then restart the system.
- **System Reset (Warm Boot):** Click to shut down and then reboot the operating system by forcefully turning off the target system.
- **Proxied:** Displayed only for the MX7000 chassis. Indicates that the device is discovered through an MX7000 lead chassis in case of Multi-Chassis Management (MCM).
- **IPMI CLI:** Click to run an IMPI command. See [Create a Remote command job for managing devices on page 142](#).
- **RACADM CLI:** Click to run a RACADM command. See [Create a Remote command job for managing devices on page 142](#).
- **Update Firmware:** See [Update the device firmware and drivers by using baselines on page 68](#).
- **Onboarding:** See [Onboarding devices on page 47](#).
- **Export All and Exported Selected:** See [Export all or selected data on page 71](#).

Hardware information displayed for MX7000 chassis

- **Chassis Power Supplies**—Information about the Power Supply Units (PSUs) used in the sleds and other components.
- **Chassis Slots**—Information about the slots available in the chassis and components, if any, installed in slots.
- **Chassis Controller**—The Chassis Management Controller (CMC) and its version.
- **Fans**—Information about the fans used in the chassis and its working status.
- **Temperature**—Temperature status and threshold values of chassis.
- **FRU**—Components or Field Replaceable Units (FRUs) that can be installed in the chassis.

Export all or selected data

About this task

You can export data:

- About the devices you view in a device group and perform strategic and statistical analysis.
- About a maximum of 1000 devices.
- Related to system alerts, reports, audit logs, group inventory, device list, warranty information, OpenManage Enterprise Services, and so on.
- Into the following file formats: HTML, CSV, and PDF.

NOTE:

- Avoid exporting 'wide' tables that have column(s) with long strings or with too many columns to PDF. Due to a limitation in the PDFMaker library, the right-most section of such exported data is truncated or cut off.
- A single device inventory can be exported only into a .csv format. See [Export the single device inventory on page 71](#)
- Only in case of reports, you can export only selected reports at a time and not all the reports. See [Export selected reports on page 151](#).

Steps

1. To export data, select **Export All** or **Export Selected**.
A job is created and the data is exported to the selected location.
2. Download the data and perform strategic and statistical analysis, if necessary.
The data is opened or saved successfully based on your selection.

NOTE: If you export data in the .csv format, you must have the administrator-level credentials to open the file.

View and configure individual devices

In the **Device list**, click the device name or IP address to view device configuration data, and then edit device configuration as described in this section.

NOTE: Some device actions are not available for sleds in a 'Proxied' Managed State. See, [Supported and unsupported actions on 'Proxied' sleds on page 192](#).

By clicking **OpenManage Enterprise > Devices > selecting a device in the device list > View Details**, you can:

- View information about the health and power status, device IP, and Service Tag.
 - View general information about the device and perform device control and troubleshooting tasks.
 - View device information such as RAID, PSU, OS, NIC, memory, processor, and storage enclosure. OpenManage Enterprise provides a built-in report to get an overview about the NIC, BIOS, Physical Disk and Virtual Disk used on the devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise > Monitor > Reports**.
 - Update or roll back firmware versions of components in a device that are associated with a firmware baseline. See [Manage the device firmware and drivers on page 80](#).
- 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.
- Acknowledge, export, delete, or ignore the alerts pertaining to a device. See [Managing device alerts](#).
 - View and export hardware log data of a device. See [Managing individual device hardware logs on page 75](#).
 - View and manage the configuration inventory of the device for the purposes of configuration compliance. A compliance comparison is initiated when the configuration inventory is run against the devices.
 - View the compliance level of a device against the configuration compliance baseline it is associated with. See [Managing the device configuration compliance on page 116](#).

Device Overview

- On the **<device name>** page, under **Overview**, the health, power status, and Service Tag of the device is displayed. Click the IP address to open the iDRAC login page. See the *iDRAC User's Guide* available on the Dell support site.
 - **Information:** Device information such as Service Tag, DIMM slots, iDRAC DNS name, processors, chassis, operating system, and data center name. Multiple management IP addresses correlated to the device are listed and can be clicked to activate the respective interfaces.
 - **Recent Alerts:** The recent alerts generated for the device.
 - **Recent Activity:** A list of recent jobs run on the device. Click **View All** to view all the jobs. See [Using jobs for device control on page 136](#).

- **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.
 - 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.

- 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**.
- 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.
- 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

- Select the check box corresponding to the device and click **View Details**.
- 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.
- 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.'
- 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.
- Click **Finish**.
The **Recent Alerts** section displays the job completion status.

Start Management application iDRAC of a device


Steps

- 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
 - 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*.
 - iii. In the **User Name** box, enter the user name of the device where the catalog is stored.
 - iv. In the **Password** box, enter the password of the device where the catalog is stored.
 - v. 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.

- d. 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.
 - e. 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.
3. 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.
 4. 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

1. On the Catalog Management page, select a catalog.
2. Click the **Check for update** button that is located in the right pane of the **Catalog Management** page.
3. 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


1. Under **Firmware**, click **Create Baseline**.
2. In the **Create Update Baseline** dialog box:
 - a. In the **Baseline Information** section:
 - i. From the **Catalog** drop-down menu, select a catalog.
 - ii. To add a catalog to this list, click **Add**. See [Managing firmware Catalogs](#).
 - iii. In the **Baseline Name** box, enter a name for the baseline, and then enter the baseline description.
 - iv. Click **Next**.
 - b. In the **Target** section:
 - To select the target device(s):
 - i. Select **Select Devices**, and then click the **Select Devices** button.
 - ii. 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.
 - iii. In the left pane, click the category name. Devices in that category are displayed in the working pane.
 - iv. 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):
 - i. Select **Select Groups**, and then click the **Select Groups** button.
 - ii. 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.
 - iii. In the left pane, click the category name. Devices in that category are displayed in the working pane.
 - iv. Select the check box corresponding to the group(s). The selected groups are listed under the **Selected Groups** tab.
3. 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

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

Results

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

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.

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.

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.

 **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.

 **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.

 **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