

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

Unassign profiles

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

About this task


To unassign profiles:

Steps

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

Results

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

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

Redeploy profiles


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

About this task

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

To redeploy profile(s):

Steps

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

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

4. Click **Finish** to proceed.

Results

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

Migrate a Profile

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

About this task

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


NOTE:

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

To Migrate a profile:

Steps

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

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

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

Results

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

Delete Profiles

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

About this task

 NOTE:

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

To delete the unassigned profiles:

Steps

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

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

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

Steps

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

Managing the device configuration compliance

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

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

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

The Overall Compliance Summary report displays the following fields:

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

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

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

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

Related tasks

Create a configuration compliance baseline on page 119

Edit a configuration compliance baseline on page 120

Remove a configuration compliance baseline on page 123

Manage compliance templates on page 117

Select a query criteria on page 61

Topics:

- Manage compliance templates
- Create a configuration compliance baseline
- Edit a configuration compliance baseline
- Delete configuration compliance baselines
- Refresh compliance of the configuration compliance baselines
- Remediate noncompliant devices
- Remove a configuration compliance baseline

Manage compliance templates

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

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

NOTE:

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

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

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

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

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



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

Related information

[Managing the device configuration compliance on page 116](#)

[Edit a configuration compliance baseline on page 120](#)

[Remove a configuration compliance baseline on page 123](#)

[Create a compliance template from deployment template on page 117](#)

[Edit a compliance template on page 119](#)

Create a compliance template from deployment template

Prerequisites

About this task

Steps

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

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

Related tasks

Manage compliance templates on page 117

Clone a compliance template on page 118

Create a compliance template from reference device

Prerequisites

About this task

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

Steps

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

Create a compliance template by importing from a file

Prerequisites

About this task

Steps

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

Clone a compliance template

About this task

Steps

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

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

Related information

Create a compliance template from deployment template on page 117

Edit a compliance template on page 119

Edit a compliance template

About this task

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

NOTE:

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

Steps

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

Related tasks

Manage compliance templates on page 117

Clone a compliance template on page 118

Create a configuration compliance baseline

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

About this task

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


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


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

You can create a configuration compliance baseline by:

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


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

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


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

Steps

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

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

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

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

Related information


[Managing the device configuration compliance on page 116](#)

[Remove a configuration compliance baseline on page 123](#)

Edit a configuration compliance baseline

About this task

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

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

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

Steps

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

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

Related tasks

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

Related information

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

Delete configuration compliance baselines

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

Prerequisites

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

About this task

To delete the configuration compliance baselines:

Steps

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

Results

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

Refresh compliance of the configuration compliance baselines

About this task

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

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

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

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

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

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

Steps

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

Results

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

Remediate noncompliant devices

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

About this task

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

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

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

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

To remediate one or more noncompliant devices:

Steps

1. Select **Configuration > Configuration Compliance**.
2. From the list of configuration compliance baselines, select the corresponding check box, and then click **View Report**.
3. From the list of noncompliant devices, select one or more devices, and then click **Make Compliant**.
4. Schedule the configuration changes to run immediately or later, and then click **Finish**.
To apply the configuration changes after the next server reboot, you can select the **Stage configuration changes to device(s) on next reboot** option.

Results

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

Export the Compliance Baseline report

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

About this task

On Compliance Report page of a configuration baseline


Steps

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

Remove a configuration compliance baseline

About this task

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

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

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

Steps

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

Related tasks

Create a configuration compliance baseline on page 119

Select a query criteria on page 61

Manage compliance templates on page 117

Edit a configuration compliance baseline on page 120

Related information

Managing the device configuration compliance on page 116

Monitor and Manage device alerts

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

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

NOTE:

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

Related concepts

View alert logs on page 124

Topics:


- [View alert logs](#)
- [Alert policies](#)
- [Alert definitions](#)

View alert logs

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

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

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

 NOTE: Alerts cannot be filtered based on the IP address (source name) if the alert is generated from an undiscovered device or in case of an internal alert.

- **Category:** The category indicates the type of alert. For example, system health and audit.
- **Message ID:** The ID of the generated alert.
- **Message:** The generated alert.

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

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

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

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

Related information

Monitor and Manage device alerts on page 124

Manage alert logs

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

Acknowledge alerts

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

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

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

Unacknowledge alerts

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

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

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

Ignore alerts

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

Export alerts

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

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

Delete alerts

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

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

View archived alerts

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

Table 19. Alert purging

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


Download archived alerts

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

1. Click **Archived Alerts**.

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

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

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

Alert policies

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

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

Use alert policies to perform the following functions:

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

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

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

Related tasks

Configure and manage alert policies on page 127

Configure and manage alert policies

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

Prerequisites



NOTE:

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

Related information

Alert policies on page 126

Forward audit logs to remote Syslog servers on page 128

Create an alert policy

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

Prerequisites

Steps

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

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

You can expand each category to view and select the sub categories. To know more about categories and subcategories, see *Alert definitions* on page 131.

3. Select the devices or groups for which an alert is required and click **Next**. An alert can be applied for:

- A device or devices.
- A group or groups of devices.
- A specified undiscovered device by entering its IP address or hostname.
- Any undiscovered device.




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



NOTE: Alerts of SNMPv1, SNMPv2, and SNMPv3 protocols sent by such undiscovered (foreign) devices are recognized by OpenManage Enterprise.

4. (Optional) Specify the duration for when the alert policy is applicable by selecting the required values for **Date Range**, **Time Interval** and **Days**, and then click **Next**.
5. Select the severity of the alert and click **Next**.
To select all the severity categories, select the **All** check box.
6. Select one or more alert actions and click **Next**. The available options are:

- Email—Select Email to send an email to a designated recipient by specifying information for each field and use tokens if required for the subject and message. See [Token substitution in remote scripts and alert policy](#) on page 194
 -  **NOTE:** Emails for multiple alerts of the same category, message ID and content are triggered only once every 2 minutes to avoid repeated or redundant alert messages in the inbox.
 - SNMP Trap Forwarding (Enable)—Click Enable to view the SNMP Configuration window where you can configure the SNMP settings for the alert. See [Configure SMTP, SNMP, and Syslog alerts](#) on page 129.
 - Syslog (Enable)—Click Enable to view the Syslog Configuration window where you can configure the system log settings for the alert. See [Configure SMTP, SNMP, and Syslog alerts](#) on page 129.
 - Select the Ignore check box to ignore the alert message and not activate the alert policy.
 - Send an SMS to specified phone number.
 - Power Control—Select Power Control check box to view the actions where you can turn on, turn off, power cycle, or gracefully shutdown a device. To shut down an operating system before performing power control actions, select the **Shut down OS First** check box.
 - Remote Script Execution (Enable)—Click Enable to view the Remote Command Setting window where you can add and run remote commands on remote nodes. For more information about adding remote commands, see [Execute remote commands and scripts](#) on page 130.
From the drop-down menu, select the script that you want to run when this alert policy is run. You can set up running the remote command also as described in [Managing OpenManage Enterprise appliance settings](#) on page 156.
 - Send a notification to the mobile phone registered with OpenManage Enterprise. See [OpenManage Mobile settings](#) on page 185.
7. Review the details of the created alert policy in the Summary tab and click **Finish**.
The alert policy is successfully created and listed in the **Alert Policies** section.

Manage alert policies


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

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

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

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

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

 **NOTE:** The Time Interval check box is disabled by default for alert policies on OpenManage Enterprise versions before version 3.3.1. After upgrading, enable the Time Interval and update the fields to reactivate the policies.

- **Enable alert policies:** Select the alert policy and click **Enable**. A check mark appears under the **Enabled** column when an alert policy is enabled. The **Enable** button of an alert policy that is already enabled appears grayed-out.
- **Disable alert policies:** Select the alert policy and click **Disable**. The alert policy is disabled and the tick mark in the **ENABLED** column is removed.

You can also disable an alert policy while creating the alert policy by clearing the **Enable Policy** check box in the Name and Description section.

- **Delete alert policies:** Select the alert policy and click **Delete**.

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

Forward audit logs to remote Syslog servers


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

About this task

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

Steps

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

 **NOTE:** Selecting target devices or groups is not applicable while forwarding the audit logs to the Syslog server.
5. (Optional) By default, the alert policies are always active. To limit activity, in the **Date and Time** section, select the 'from' and 'to' dates, and then select the time frame.
 - a. Select the check boxes corresponding to the days on which the alert policies must be run.
 - b. Click **Next**.
6. In the **Severity** section, select the severity level of the alerts for which this policy must be activated.
 - a. To select all the severity categories, select the **All** check box.
 - b. Click **Next**.
7. In the **Actions** section, select **Syslog**.

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

Results

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

Related tasks

[Configure and manage alert policies on page 127](#)

[Monitor audit logs on page 133](#)

Configure SMTP, SNMP, and Syslog alerts

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

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

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

To configure the SNMP alert forwarding configuration:

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

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

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

To update the Syslog forwarding configuration:

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

Execute remote commands and scripts

About this task

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

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

Steps

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

- f. If you select **IPMI Tool**, do the following:
 - i. In the **Command Name** box, enter the command name.
 - ii. In the **Command** box, type the commands. Up to 100 commands can be typed with each command required to be on a new line.
 - iii. Click **Finish**
3. To edit a remote command setting, select the command, and then click **Edit**.
4. To delete a remote command setting, select the command, and then click **Delete**.

Automatic refresh of MX7000 chassis on insertion and removal sleds

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

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

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

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

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

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

NOTE:

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

Alert definitions

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

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

An Error and Event message has:

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

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

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

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

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

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

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

Monitor audit logs

About this task

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

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


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

NOTE:

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

Steps

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

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

10. To upload the signed .dat file and SSH public key, click **Troubleshoot > Upload of signed .dat file, SSH public key**.

This option is only available if the Field Service Debug (FSD) mode is enabled in the TUI (Text User Interface). For more information, see *Configure OpenManage Enterprise by using Text User Interface* on page 29, *Field service debug workflow* on page 194 and *Unblock the FSD capability* on page 195.

Results

NOTE:

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

Related information

Forward audit logs to remote Syslog servers on page 128

Topics:

- Forward audit logs to remote Syslog servers

Forward audit logs to remote Syslog servers

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

About this task

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

Steps

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

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

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

If Syslog servers are not configured in OpenManage Enterprise, click **Enable** and enter the destination IP address or the hostname of Syslog servers. For more information about configuring Syslog servers, see *Configure SMTP, SNMP, and Syslog alerts* on page 129.
8. Click **Next**.

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

Results

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

Related tasks

Configure and manage alert policies on page 127

Monitor audit logs on page 133

Using jobs for device control

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

Prerequisites:

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

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

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

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

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

Topics:

- View job lists
- View an individual job information
- Create a job to turn device LEDs
- Create a job for managing power devices
- Create a Remote command job for managing devices
- Create a job to change the virtual console plugin type
- Select target devices and device groups
- Manage jobs

View job lists

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

- **Job Status:** Provides the execution status of a job.
See *Jobs status and Jobs type description* on page 137.
- **State:** Provides the state of a job. The available options are Enabled or Disabled.
- **Job Name:** Name of a job.
- **Job Type:** Provides the type of a job.
See *Jobs status and Jobs type description* on page 137.
- **Description:** Detail description of a job.
- **Last Run:** Last run period of a job.

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

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

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

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

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

Jobs status and Jobs type description

Table 20. Job status and description

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

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

Table 21. Job Types and description

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

Table 21. Job Types and description (continued)

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

OpenManage Enterprise default jobs and schedule

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

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

Job Name	Cron Expression	Cron Expression Description	Example
Configuration Inventory	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021
Default Console Update Task	0 0 12 ? * MON *	At 12:00:00pm, on every Monday, every month	<ul style="list-style-type: none"> Mon May 24 12:00:00 UTC 2021 Mon May 31 12:00:00 UTC 2021
Default Inventory Task	0 0 5 * * ? *	At 05:00:00am every day	<ul style="list-style-type: none"> Tue May 18 05:00:00 UTC 2021

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

Job Name	Cron Expression	Cron Expression Description	Example
			<ul style="list-style-type: none"> Wed May 19 05:00:00 UTC 2021
Device Config Purge Task for cleanup	0 0/1 * * * ? *	At second :00, every minute starting at minute :00, of every hour	<ul style="list-style-type: none"> Mon May 17 18:39:00 UTC 2021 Mon May 17 18:40:00 UTC 2021
File Purge Task for Share Utilization	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021
File Purge Task for Single DUP Files	0 0 0/4 1/1 * ? *	At second :00, at minute :00, every 4 hours starting at 00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 20:00:00 UTC 2021 Tue May 18 00:00:00 UTC 2021 Tue May 18 04:00:00 UTC 2021 Tue May 18 04:00:00 UTC 2021
Global Health Task	0 0 0/1 1/1 * ? *	At second :00, at minute :00, every hour starting at 00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 19:00:00 UTC 2021 Mon May 17 20:00:00 UTC 2021
Internal Sync Task	0 0/5 * 1/1 * ? *	At second :00, every 5 minutes starting at minute :00, every hour, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 18:45:00 UTC 2021 Mon May 17 18:50:00 UTC 2021
Metrics Purge Task	0 0 * ? * *	At second :00 of minute :00 of every hour	<ul style="list-style-type: none"> Mon May 17 19:00:00 UTC 2021 Mon May 17 20:00:00 UTC 2021 Mon May 17 21:00:00 UTC 2021
Metrics Task	0 0/15 * 1/1 * ? *	At second :00, every 15 minutes starting at minute :00, every hour, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 18:45:00 UTC 2021 Mon May 17 19:00:00 UTC 2021
Mobile Subscription Task	0 0/2 * 1/1 * ? *	At second :00, every 2 minutes starting at minute :00, every hour, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 18:54:00 UTC 2021 Mon May 17 18:56:00 UTC 2021
Node Initiated Discovery Task	0 0/10 * 1/1 * ? *	At second :00, every 10 minutes starting at minute :00, every hour, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 19:00:00 UTC 2021 Mon May 17 19:10:00 UTC 2021
Password Rotation Task	0 0 0/6 1/1 * ? *	At second :00, at minute :00, every 6 hours starting at 00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Tue May 18 06:00:00 UTC 2021 Tue May 18 12:00:00 UTC 2021

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

Job Name	Cron Expression	Cron Expression Description	Example
Periodic Metrics Registration	0 0 3 * * ?	At 03:00:00am every day	<ul style="list-style-type: none"> Tue May 18 03:00:00 UTC 2021 Wed May 19 03:00:00 UTC 2021
Purge On Demand Health Task for Table: Task	0 0 0/5 1/1 * ? *	At second :00, at minute :00, every 5 hours starting at 00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Tue May 18 05:00:00 UTC 2021 Tue May 18 10:00:00 UTC 2021
Purge Task Table :Event_Archive	0 0 18/12 ? * * *	At second :00, at minute :00, every 12 hours starting at 18pm, of every day	<ul style="list-style-type: none"> Tue May 18 18:00:00 UTC 2021 Wed May 19 18:00:00 UTC 2021 Thu May 20 18:00:00 UTC 2021
Purge Task Table :Group_Audit	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021 Thu May 20 00:00:00 UTC 2021
Purge Task Table :Task	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021 Thu May 20 00:00:00 UTC 2021
Purge Task Table :announced_target	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021 Thu May 20 00:00:00 UTC 2021
Purge Task for Table: Core Application Log	0 0 0/5 1/1 * ? *	At second :00, at minute :00, every 5 hours starting at 00am, every day starting on the 1st, every month	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Tue May 18 05:00:00 UTC 2021
Purge Task for Table: Event	0 0/30 * 1/1 * ? *	At second :00, every 30 minutes starting at minute :00, every hour, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 19:30:00 UTC 2021 Mon May 17 20:00:00 UTC 2021 Mon May 17 20:30:00 UTC 2021
Purge Task for Table: Infrastructure Device	0 0/30 * 1/1 * ? *	At second :00, every 30 minutes starting at minute :00, every hour, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 19:30:00 UTC 2021 Mon May 17 20:00:00 UTC 2021 Mon May 17 20:30:00 UTC 2021

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

Job Name	Cron Expression	Cron Expression Description	Example
Subscription poller task	0 0/30 * 1/1 * ? *	At second :00, every 30 minutes starting at minute :00, every hour, every day starting on the 1st, every month	<ul style="list-style-type: none"> Mon May 17 19:30:00 UTC 2021 Mon May 17 20:00:00 UTC 2021 Mon May 17 20:30:00 UTC 2021

View an individual job information

Steps

1. On the **Jobs** page, select the check box corresponding to the job.
2. In the right pane, click **View Details**.
On the **Job Details** page, the job information is displayed.
3. Click **Restart Job** if the status of a job is any one of the following: Stopped, Failed, or New.
A message indicates that the job has started running.

The **Execution History** section lists the information about when the job was successfully run. The **Execution Details** section lists the devices on which the job was run and the time taken to run a job.

NOTE: If a configuration remediation task is stopped, the overall task status is indicated as 'Stopped', but the task continues to run. However, the status is indicating as Running in the **Execution History** section.

4. To export data to an Excel file, select the corresponding or all check boxes, and then click **Export**. See [Export all or selected data](#) on page 71.

Create a job to turn device LEDs

The following steps describe how you can blink the LEDs of the specified devices using the Blink Devices 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. The Blink Devices wizard can be activate in the following ways:
 - a. From the Jobs page (**OpenManage Enterprise > Monitor > Jobs**) click **Create**, and then select **Blink Devices**.
 - b. From the All Devices page (**OpenManage Enterprise > Devices**), select the devices and click the **More Actions** drop down and then either click **Turn LED On** or **Turn LED Off**.
2. In the **Blink Devices Wizard** dialog box:
 - a. In the **Options** section:
 - i. In the **Job Name** box, enter a job name.
 - ii. From the **Blink LED Duration** drop-down menu, select options to blink the LED for a set duration, turn on, or to turn off.
 - iii. Click **Next**.
 - b. In the **Target** section, select the target devices or target groups and click **Next**. See [Select target devices and device groups](#) on page 143.
 - c. In the **Schedule** drop down select **Run Now**, or **Run Later**, or **Run on Schedule**. See [Schedule job field definitions](#) on page 192.
3. Click **Finish**.
A Blink LED job is created and listed in the Jobs page (**OpenManage Enterprise > Monitor > Jobs**) **JOB STATUS** column.

Create a job for managing power devices

About this task

 **NOTE:** Power control actions can be performed only on devices that are discovered and managed using iDRAC (out-of-band).

Steps

1. Click **Create**, and then select **Power Control Devices**.
2. In the **Power Control Devices Wizard** dialog box:
 - a. In the **Options** section:
 - i. Enter the job name in **Job Name**.
 - ii. From the **Power Options** drop-down menu, select any one of the tasks: **Power on**, **Power off**, or **Power cycle**.
 - iii. Click **Next**.
 - b. In the **Target** section, select the target devices and click **Next**. See [Select target devices and device groups on page 143](#).
 - c. In the **Schedule** section, run the job immediately or schedule for a later point of time. See [Schedule job field definitions on page 192](#).
3. Click **Finish**.
The job is created and listed in the Jobs list and identified by an appropriate status in the **JOB STATUS** column.
4. If the job is scheduled for a later point of time, but you want to run the job immediately:
 - On the Jobs page, select the check box corresponding to the Scheduled job.
 - Click **Run Now**. The job is run and the status is updated.
 - To view the job data, click **View Details** in the right pane. See [View an individual job information on page 141](#).


Create a Remote command job for managing devices

About this task

Using the Command Line Job wizard, you can create remote command jobs to manage the target devices remotely.

Steps

1. Click **Create**, and then select **Remote Command on Devices**.
2. In the **Command Line Job Wizard** dialog box, in the **Options** section:
 - a. Enter the job name in **Job Name**.
 - b. From the Interface drop-down menu, select one of the interfaces depending on the target devices you want to manage:
 - **IPMI CLI** — for iDRACs and non-Dell servers.
 - **RACADM CLI** — for iDRACs discovered using the WSMAN protocol.
 - **SSH CLI** — for Linux servers discovered using the SSH protocol.
 - c. In the **Arguments** box, enter the command. Up to 100 commands can be typed with each command required to be on a new line.

 **NOTE:** The commands in the Arguments box are run one at a time.
 - d. Click **Next**.
A green tick mark next to **Options** indicates that the necessary data is provided.
3. In the **Target** section, select the target devices and click **Next**. See [Select target devices and device groups on page 143](#).
4. In the **Schedule** section, run the job immediately or schedule for a later time. See [Schedule job field definitions on page 192](#).
5. Click **Finish**.
The job is created and listed in the Jobs list and identified by an appropriate status in the **JOB STATUS** column.
6. If the job is scheduled for a later point, but you want to run the job immediately:
 - On the Jobs page, select the check box corresponding to the Scheduled job.
 - Click **Run Now**. The job is run and the status is updated.

- To view the job data, click **View Details** in the right pane. See [View an individual job information on page 141](#).

Create a job to change the virtual console plugin type

About this task

You can change the virtual console plugin type to HTML5 on multiple devices. Updating to HTML5 can lead to a better browser experience. To update do the following:


Steps

1. Click **OpenManage Enterprise > Monitor > Jobs**
2. Click **Create**, and then select **Change Virtual Console Plugin on Devices**.
3. In the **Change Virtual Console Plugin Wizard** dialog box, in the **Options** section:
 - a. Enter the job name in **Job Name**. By default, the plugin type is displayed as HTML5.
 - b. Click **Next**.
4. In the **Job Target** section, select the target devices and click **Next**. See [Select target devices and device groups on page 143](#).
 - a. Click **Next**.
5. In the **Schedule** section, run the job immediately or schedule for a later point of time. See [Schedule job field definitions on page 192](#).
6. Click **Finish**.
The job is created and listed in the Jobs list and identified by an appropriate status in the **JOB STATUS** column.
7. If the job is scheduled for a later point of time, but you want to run the job immediately:
 - On the Jobs page, select the check box corresponding to the Scheduled job.
 - Click **Run Now**. The job is run and the status is updated.
 - To view the job data, click **View Details** in the right pane. See [View an individual job information on page 141](#).

Select target devices and device groups

About this task

By default, **Select Devices** is selected to indicate that the job can be run on the devices. You can run a job on device groups also by selecting **Select Groups**.

 **NOTE:** The device groups and devices displayed are governed by the scope-based operational access that the user has to the devices. For more information, see [Role and scope-based access control in OpenManage Enterprise on page 18](#).


Steps

1. Click **Select Devices**.
In the **Job Target** dialog box, the left pane lists the devices monitored by OpenManage Enterprise. In the working pane, list of devices associated with each group, and device details are displayed. For field descriptions, see [Devices list on page 65](#). For information about device groups, see [Organize devices into groups on page 58](#).
2. Select the check box corresponding to a device and click **OK**.
The selected devices are displayed in the **All Selected Devices** section of the selected group.

Manage jobs

After jobs have been created and displayed on the **Jobs** page, you can manage them as follows.

- **Run jobs:** Select the check box corresponding to a job, and then click **Run Now** to execute the task on the targeted devices. You can run a job when it is in enabled status.
- **Enable jobs:** Select the check box corresponding to a job, and then click **Enable**.
- **Disable jobs:** Select the check box corresponding to a job, and then click **Disable**.

 NOTE: Only the 'Scheduled' jobs can be disabled from running. Jobs which are active and in their 'Running' state cannot be disabled midway.

- **Stop jobs:** Select the check box corresponding to a job, and then click **Stop**. You can stop a job when it is in running status.
- **Delete:** Select the check box corresponding to a job, and then click **Delete**.

Manage the device warranty




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 > Warranty**, you can view the warranty statuses of all the devices that are monitored by OpenManage Enterprise that are in your scope. For example, an administrator with access to all device groups will see warranty details of all the devices, however, device managers will see warranty details for only the devices that are in their respective scope.

You can also export selected or all data to an Excel sheet for the statistical and analytical purposes. The Warranty page displays the following details:

- **STATUS** of the warranty

NOTE: Warranty status is determined by the settings that the Administrator selects. See [Manage warranty settings](#) on page 178.

-  means **critical**, indicating the warranty has expired.
-  means **warning**, indicating the warranty is approaching expiration.
-  means **normal**, indicating the warranty is active.

- **SERVICE TAG**

- **DEVICE MODEL**

- **DEVICE TYPE**

- **WARRANTY TYPE:**

- Initial: The warranty provided with the purchase of OpenManage Enterprise.
- Extended: The warranty is extended because the initial warranty duration is expired.

- **SERVICE LEVEL DESCRIPTION:** Indicates the Service Level Agreement (SLA) associated with the device warranty.

- **DAYS REMAINING:** Number of days left for the warranty to expire. You can set the days before which you get an alert. See [Manage warranty settings](#) on page 178.

OpenManage Enterprise provides a built-in report about the warranties that expire in the next 30 days. Click **OpenManage Enterprise > Monitor > Reports > Warranties Expiring in Next 30 days**. Click **Run**. See [Run reports](#) on page 148.

To filter data displayed in the table, click **Advanced Filters**. See about advanced filters section in [OpenManage Enterprise Graphical User Interface overview](#) on page 38.

Warranty status of all the discovered devices is collected automatically once a week by a built-in Warranty job. You can also manually initiate the Warranty job by clicking **Refresh Warranty** in the upper-right corner.

To export all or selected warranty data, click **Export**. See [Export all or selected data](#) on page 71.

Related tasks


[View and renew device warranty](#) on page 145

Topics:



- [View and renew device warranty](#)

View and renew device warranty

Click **OpenManage Enterprise > Monitor > Warranty** to get a list of warranty statuses of all the devices monitored by OpenManage Enterprise, along with their Service Tag, model name, device type, associated warranty, and service level information. For field descriptions, see [Manage the device warranty](#) on page 145.

 **NOTE:** Warranty details can be retrieved from external site over IPv4 only. If you have a pure IPv6 setup, consider enabling IPv4 before initiating any warranty-related tasks.

To view the warranty information and to renew the warranty of a device:

- Select the check box corresponding to the device. In the right pane, warranty status and other important details of the device such as the service level code, service provider, the warranty start date, the warranty end date, and so on are displayed.
- Expired warranties can be renewed by clicking **Dell Warranty Renewal for Device**, which redirects you to the Dell EMC support site allowing you to manage your device warranty.
- Click **Refresh Warranty** in the upper right-hand corner to refresh the Warranty table. Warranty statuses automatically change from critical  to normal  for all the devices whose warranties are renewed. A new Device Warranty alert log, with the total number of expired warranties in the console, is generated each time **Refresh Warranty** is clicked. For information on Alert logs, see [View the alert logs](#).
- To sort data in the table based on a column, click the column title.
- Click on the **Advanced Filters** button to customize.

Related information

[Manage the device warranty on page 145](#)

Reports

By clicking **OpenManage Enterprise > Monitor > Reports**, you can build customized reports to view device details at depth. Reports enables you to view data about the devices, jobs, alerts, and other elements of your data center. Reports are built-in, and user-defined. You can edit or delete only the user-defined reports. Definitions and criteria used for a built-in report cannot be edited or deleted. A preview about the report you select from the Reports list is displayed in the right pane.

The reports and the data displayed on the Reports page depend on the scope based user privileges that you have in OpenManage Enterprise. For example, device managers have access to only the reports that they have created in addition to the built-in reports. Also, the report generated by a user would contain data from only the devices that are in the scope for that user. For example, reports generated by administrator and 'unrestricted' device managers will contain data on all the device groups, however, the reports generated by device managers who have a restricted scope would have data pertaining to only the devices and/or device groups that are in their scope.

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.

Table 23. The role-based access privileges for managing reports on OpenManage Enterprise

User Role...	Report tasks permitted...
Administrators and Device Managers	Run, create, edit, copy, email, download, and export
Viewers	Run, email, export, view, and download

Advantages of the Reports feature:

- Build a report criteria by using up to 20 filters
- You can filter data and arrange by column names of your choice
- Reports can be viewed, downloaded, and sent in an email message
- Send reports to up to 20-30 recipients at a time
- If you feel that report generation is taking time, you can stop the process
- The reports generated are automatically translated to the language which is set while installing OpenManage Enterprise
- An audit log entry is made whenever you generate, edit, delete, or copy a report definition

Currently, the following built-in reports can be generated to extract information about the following:

- Device category: Asset, FRU, firmware, firmware/driver compliance, scheduled jobs, Alert summary, hard drive, modular enclosure, NIC, virtual drive, warranty, and license.
- Alerts category: Weekly alerts

Related tasks

Run reports on page 148

Run and email reports on page 148

Edit reports on page 149

Delete reports on page 149

Topics:

- Run reports
- Run and email reports
- Edit reports
- Copy reports
- Delete reports
- Creating reports
- Export selected reports

Run reports

From the Reports page (**OpenManage Enterprise > Monitor > Reports**), you can run, view and download the built-in reports or the reports that you have created.

About this task

When you run a report, the first 20 rows are displayed and paginated results can be paged through. To view all the rows at one time, download the report. To edit this value, see *Export all or selected data* on page 71. Data displayed in the output cannot be sorted because it is defined in the query used to build a report. To sort data, edit the report query or export it to an Excel sheet. It is recommended to not run more than five (5) reports at a time because reporting consumes system resources. However, this value of five reports depends on the devices discovered, fields used, and number of tables joined to generate report. A Reports job is created and run when a report generation is requested. For role-based privileges to generate reports, see *Creating reports* on page 150.

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.
- Reports generated by device managers will only have data pertaining to the devices that are in their scope.
- It is not recommended to frequently run a report because it consumes processing and data resources.
- For a report whose category is 'Device', the first columns by default are Device name, Device model, and Device Service Tag. You may exclude columns while customizing your report.

To run a report, select the report and click **Run**. On the **<report name> Reports** page, the report is tabulated by using the fields that are defined for creating the report.

To download a report:

1. Click **Download**.
2. In the **Download Report** dialog box, select the output file type, and click **Finish**. The selected output file is displayed. Currently, you can export a report to XML, PDF, Excel, and CSV file formats. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

To email a report:

1. Click **Email**.
2. In the **Email Report** dialog box, select the file format, type the receiver's email address, and then click **Finish**. The report is emailed. You can email reports to 20-30 recipients at a time.
3. If the email address is not configured, click **Go to SMTP Settings**. For more information about setting SMTP properties, see *Set SNMP Credentials* on page 177.

NOTE:

If you are downloading or running a report that is already generated, and another user tries to delete that report at the same time, both the tasks are successfully completed.

Related information

Reports on page 147

Run and email reports

You can run the report and email it to 20-30 recipients at a time.

Prerequisites

NOTE:

Email operation may fail with large reports, if the message size exceeds the fixed message size set on the SMTP server. In such instances, consider resetting the SMTP server's message size limit and retry.

Steps

1. Select the report and click **Run and Email**.
2. In the **Email Report** dialog box:

- a. From the **Format** drop-down menu, select one of the file format in which the report must be generated — HTML, CSV, PDF, or MS-Excel.
- b. In the **To** box, enter the email address of the recipient. If the email address is not configured, click **Go to SMTP Settings**. For more information about setting SMTP properties, see *Set SNMP Credentials* on page 177.
- c. Click **Finish**.
The report is emailed and recorded in the Audit logs.


Related information

Reports on page 147

Edit reports

Only user-created reports can be edited.

Steps

1. Select the report and click **Edit**.
 2. In the **Report Definition** dialog box, edit the settings. See *Creating reports*.
 3. Click **Save**.
The updated information is saved. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.
-  **NOTE:** While editing a customized-report, if the category is changed, the associated fields are also removed.

Related information

Reports on page 147

Copy reports

About this task

Only user-created reports can be copied.

Steps


1. Select the report, click **More Actions**, and then click **Copy**.
2. In the **Copy Report Definition** dialog box, enter a new name for the copied report.
3. Click **Save**.
The updated information is saved. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Delete reports

About this task

Only user-created reports can be deleted. If a report definition is deleted, the associated report history is deleted, and any running report using that report definition is also stopped.

Steps

1. From the **OpenManage Enterprise** menu, under **Monitor**, select **Reports**.
A list of devices available reports is displayed.
2. Select the report, click **More Actions**, and then click **Delete**.
 **NOTE:** If you are downloading or running a report that is already generated, and another user tries to delete that report at the same time, both the tasks are successfully completed.
3. In the **Delete Report Definition** dialog box, when prompted whether or not the report must be deleted, click **Yes**.

The report is deleted from the list of reports and the table is updated. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Related information

Reports on page 147

Creating reports

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 reports generated by device managers will only have data pertaining to the device groups which are in their scope.
- Some tables contain device-type-specific data which will effectively lock the report to that device type. Mixing columns from multiple device specific tables of different types (for example servers and chassis) will result in an invalid report with no results.

About this task

While built-in reports have default definitions (filter criteria) for generating reports, you can customize the criteria to create your own definitions, and then generate customized reports. The fields or columns that you want to display in your report depends on the category you select. You can select only one category at a time. The arrangement of columns in a report can be altered by dragging and placing. Also:

- Report names must be unique
- Report definition must have at least one field and one category
- For reports having Device and Alert as categories, device name or device group must be one of the mandatory fields

By default, **Devices** is selected as the category, and device name, device Service Tag, and device model columns are displayed in the working pane. If you select any other category while editing a report criteria, a message is displayed indicating that the default fields will be removed. Every category has predefined properties that can be used as column titles where the data is filtered by using the criteria you define. Example category types:

- Jobs: Task name, task type, task status, and task internal.
- Groups: Group status, group description, group membership type, group name, and group type.
- Alerts: Alert status, alert severity, catalog name, alert type, alert sub-category, and device information.
- Devices: Alert, alert catalog, chassis fan, device software, and so on. These criteria have further classification based on which data can be filtered and reports generated.

Table 24. The role-based access privileges for generating reports on OpenManage Enterprise

User Role...	Report tasks permitted...
Administrators and Device Managers	Run, create, edit, copy, email, download, and export
Viewers	Run, email, export, view, and download

Steps

1. Click **Reports > Create**.
2. In the **Report Definition** dialog box:
 - a. Type the name and description of the new report to be defined.
 - b. Click **Next**.
3. In the **Report Builder** section:
 - a. From the **Category** drop-down menu, select the report category.
 - If you select Device as the category, select the device group also.
 - If necessary, edit the filter criteria. See [Select a query criteria on page 61](#).
 - b. Under the **Select Columns** section, select the check boxes of the fields that must appear as the report columns.

Selected field names are displayed in the **Column Order** section.

c. You can customize the report by

- Using the **Sort by** and **Direction** boxes.
- Dragging the fields either up or down in the **Column Order** section.

4. Click **Finish**.

The report is generated and listed in the list of reports. You can export report for analytical purposes. See [Export all or selected data](#) on page 71. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Results

Select query criteria when creating reports

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 20 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 query criteria from scratch 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.

Export selected reports

About this task

Steps

1. Select the check boxes corresponding to the reports to be exported, click **More Actions**, and then click **Export Selected**.
Currently, you cannot export all the reports at a time.
2. In the **Export Selected Reports** dialog box, select any one of the following file formats in which the report must be exported — HTML, CSV, or PDF.

3. Click **Finish**.

In the dialog box, open or save the file to a known location for analysis and statistical purposes.

70

Managing MIB files

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.

Third party tools in your data center may generate alerts that are vital for your operations. Such alerts are stored in the Management Information Base (MIB) files defined and understood by respective vendor tools. However, OpenManage Enterprise enables you to manage such MIBs also so that the non-Dell EMC MIBs can be imported, parsed, and used by OpenManage Enterprise for device management. OpenManage Enterprise supports SMI1 and SMI2. OpenManage Enterprise provides built-in MIB files that can be used for Dell EMC devices. These are read-only MIBs and cannot be edited.

NOTE: Only valid MIBs with traps are handled by OpenManage Enterprise.

You manage MIBs by:

- Import MIB files on page 153
- Remove MIB files on page 155
- Resolve MIB types on page 155

By clicking **OpenManage Enterprise > Monitor > MIB**, you can manage the MIB files that are used by OpenManage Enterprise and other System Management tools in the data center. A table lists the available MIB files with the following properties. Click the column heading to sort data.

Table 25. Role-based access for MIB files in OpenManage Enterprise

OpenManage Enterprise features	Role-based access control for MIB files		
	Admin	Device Manager	Viewer
View traps or MIBs	Y	Y	Y
Import MIB, Edit traps.	Y	N	N
Remove MIB	Y	N	N
Edit traps	Y	N	N

To download the built-in MIB files from OpenManage Enterprise, click **Download MIB**. The files are saved to the specified folder.

Topics:

- Import MIB files
- Edit MIB traps
- Remove MIB files
- Resolve MIB types
- Download an OpenManage Enterprise MIB file

Import MIB files

Ideal process flow of MIB import: **User uploads a MIB to OpenManage Enterprise > OpenManage Enterprise parses the MIB > OpenManage Enterprise searches the database for any already available similar traps > OpenManage Enterprise displays MIB file data.** The maximum file size of MIB that can be imported is 3 MB. The OpenManage Enterprise Audit log history records every import and removal of MIBs.

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
- Only one MIB file can be imported at a time.

About this task

Steps

1. Click **MIB > Import MIB**.
2. In the **Import MIB** dialog box, in the **Upload MIB Files** section, click **Choose File** to select a MIB file.
If the MIB has import statements that are resolved by external MIBs, a message is displayed.
 - a. Click **Resolve Types**. Resolve the MIB types. See *Remove MIB files* on page 155.
 - b. Click **Finish**. If the MIB file is Dell EMC owned, a message indicates that the MIB is shipped with the product and cannot be modified.
3. Click **Next**.
4. In the **View Traps** section, a list of MIB files is displayed with the following information:
 - Alert category of the trap. You can edit the category to align with the OpenManage Enterprise category definitions. See *Edit MIB traps* on page 154.
 - Trap name is read-only. Defined by the third-party device.
 - Severity levels of an alert: Critical, Warning, Information, and Normal.
 - Alert message associated with an alert.
 - Trap OID is read-only and unique.
 - 'New' indicates that the trap is imported for the first time by OpenManage Enterprise. Already imported traps are indicated as 'Imported'. 'Overwrite' indicates the traps whose definition is rewritten because of an import operation.

To edit the default alert categories or severity level of a MIB file, see *Edit MIB traps* on page 154. To delete MIB files, select the corresponding check boxes, and then click **Delete Trap**. The MIB files are deleted and the list of MIB files is updated.
5. Click **Finish**. The MIB files are parsed, imported to OpenManage Enterprise, and then listed under the **MIN** tab.

Results

- ① **NOTE:** If you import a MIB, and then import it again, the MIB status is shown as **IMPORTED**. However, if you re-import a MIB file that is deleted, the trap status is indicated as **NEW**.
- ① **NOTE:** Traps that are already imported to OpenManage Enterprise cannot be imported.
- ① **NOTE:** MIB files shipped by default with OpenManage Enterprise cannot be imported.
- ① **NOTE:** Events that are generated after the trap is imported will be formatted and displayed according to the new definition.

Edit MIB traps

About this task

Steps

1. Select the report and click **Edit**.
2. In the **Edit MIB Traps** dialog box:
 - a. Select or type data in the fields:
 - Select the new alert category to be assigned to the alert. By default, OpenManage Enterprise displays few built-in alert categories.
 - Type the alert component.
 - The trap name is read-only because it is generated by the third-party tool.
 - Select the severity to be assigned to the alert. By default, OpenManage Enterprise displays few built-in alert categories.