

Table 6. Text User Interface options (continued)

Options	Descriptions
	Enterprise appliance be restarted when this message is displayed.

Configure OpenManage Enterprise

About this task

If you are logging in to OpenManage Enterprise for the first time, the **Welcome to OpenManage Enterprise** page is displayed, which allows setting of time (either manually or using NTP time synchronization) and proxy configurations.

Steps

- To configure the time manually do the following in the **Time Configuration** section:
 - Use the **Timezone** drop down menu to select an appropriate Timezone.
 - In the **Date** box, enter or select a date.
 - In the **Time** box, fill the time.
 - Click **Apply** to save the settings.
- If you want to use the NTP Server for time synchronization, do the following in the **Time Configuration** section:

NOTE: When the NTP Server settings are updated, the currently logged in users are automatically logged out from their OpenManage Enterprise sessions.

 - Select the **Use NTP** check box.
 - Enter the IP address or hostname in **Primary NTP Server Address** and **Secondary NTP Server Address** (optional) for time synchronization
- If you want to set proxy server for external communication, In the Proxy Configuration section do the following:
 - Select the **Enable HTTP Proxy Settings** check box.
 - Enter the **Proxy Address**.
 - Enter the **Port number** for the proxy server.
 - If the proxy server requires credentials to log in, select the **Enable Proxy Authentication** check box and enter the user name and password.
 - Select the **Ignore Certificate Validation** check box if the configured proxy intercepts SSL traffic and does not use a trusted third-party certificate. Using this option will ignore the built-in certificate checks used for the warranty and catalog synchronization.
- Click **Apply** to save the settings.

Results

- NOTE:** For information about supported browsers, see the *OpenManage Enterprise Support Matrix* available on the support site.

Recommended scalability and performance settings for optimal usage of OpenManage Enterprise

The following table lists the performance parameters of the supported features in OpenManage Enterprise. To ensure an optimal performance of OpenManage Enterprise, Dell EMC recommends to run the tasks at the specified frequency on the maximum number of devices that are recommended per task.

Table 7. Scalability and performance considerations of OpenManage Enterprise

Tasks	Recommended frequency of running the tasks	Tasks whether precanned?	Maximum devices that are recommended per task.
Discovery	Once a day for environment with frequent network changes.	No	10,000/task
Inventory	OpenManage Enterprise provides a precanned task that automatically refreshes inventory once a day.	Yes. You can disable this feature.	Devices that are monitored by OpenManage Enterprise.
Warranty	OpenManage Enterprise provides a precanned task that automatically refreshes warranty once a day.	Yes. You can disable this feature.	Devices that are monitored by OpenManage Enterprise.
Health poll	Every one hour	Yes. You can change the frequency.	Not applicable
Firmware/Driver update	Need-basis		150/task
Configuration inventory	Need-basis		1500/baseline

Supported protocols and ports in OpenManage Enterprise

Supported protocols and ports on management stations

Table 8. OpenManage Enterprise Supported protocols and ports on management stations

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
22	SSH	TCP	256-bit	Management station	In	OpenManage Enterprise appliance	<ul style="list-style-type: none">Required for incoming only if FSD is used. OpenManage Enterprise administrator must enable only if interacting with the Dell EMC support staff.
25	SMTP	TCP	None	OpenManage Enterprise appliance	Out	Management station	<ul style="list-style-type: none">To receive email alerts from OpenManage Enterprise.

Table 8. OpenManage Enterprise Supported protocols and ports on management stations (continued)

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
53	DNS	UDP/TCP	None	OpenManage Enterprise appliance	Out	Management station	<ul style="list-style-type: none"> For DNS queries.
68 / 546 (IPv6)	DHCP	UDP/TCP	None	OpenManage Enterprise appliance	Out	Management station	<ul style="list-style-type: none"> Network configuration.
80*	HTTP	TCP	None	Management station	In	OpenManage Enterprise appliance	<ul style="list-style-type: none"> The Web GUI landing page. This will redirect a user to HTTPS (Port 443).
123	NTP	TCP	None	OpenManage Enterprise appliance	Out	NTP Server	<ul style="list-style-type: none"> Time synchronization (if enabled).
137, 138, 139, 445	CIFS ¹	UDP/TCP	None	iDRAC/ CMC	In	OpenManage Enterprise appliance	<ul style="list-style-type: none"> To upload or download deployment templates. To upload TSR and diagnostic logs. To download firmware/driver DUPs. For Emergency FSD process, if web UI is not available. Boot to network ISO. <p>For more information, refer Built-in Appliance Share in Manage Console preferences on page 173.</p>
				OpenManage Enterprise appliance	Out	CIFS share	<ul style="list-style-type: none"> To import firmware/driver catalogs from CIFS share.
111, 2049 (default)	NFS	UDP/TCP	None	OpenManage Enterprise appliance	Out	External NFS share	<ul style="list-style-type: none"> To download catalog and DUPs from the NFS share for firmware updates. For manual console upgrade from network share.
162*	SNMP	UDP	None	Management station	In/Out	OpenManage Enterprise appliance	<ul style="list-style-type: none"> Event reception through SNMP. The direction is 'outgoing' only if

Table 8. OpenManage Enterprise Supported protocols and ports on management stations (continued)

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
							using the Trap forward policy.
443 (default)	HTTPS	TCP	128-bit SSL	Management station	In/Out	OpenManage Enterprise appliance	<ul style="list-style-type: none"> • Web GUI. • To upload or download Deployment templates. • To upload TSR and diagnostic logs. • To download firmware/driver DUPs. • FSD process. • Boot to Network ISO. • To download updates and warranty information from Dell.com. 256-bit encryption is allowed when communicating with the OpenManage Enterprise by using HTTPS for the web GUI. • Server-initiated discovery. <p>For more information, refer Built-in Appliance Share in Manage Console preferences on page 173.</p>
514	Syslog	TCP	None	OpenManage Enterprise appliance	Out	Syslog server	<ul style="list-style-type: none"> • To send alert and audit log information to Syslog server.
3269	LDAPS	TCP	None	OpenManage Enterprise appliance	Out	Management station	<ul style="list-style-type: none"> • AD/ LDAP login for Global Catalog.
636	LDAPS	TCP	None	OpenManage Enterprise appliance	Out	Management station	<ul style="list-style-type: none"> • AD/ LDAP login for Domain Controller.

1. CIFS protocol is not needed if the built-in appliance share is configured for HTTPS.

*Port can be configured up to 499 excluding the port numbers that are already allocated.

Supported protocols and ports on managed nodes

Table 9. OpenManage Enterprise supported protocols and ports on the managed nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
22	SSH	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed node	<ul style="list-style-type: none">For the Linux OS, Windows, and Hyper-V discovery.
161	SNMP	UDP	None	OpenManage Enterprise appliance	Out	Managed node	<ul style="list-style-type: none">For SNMP queries.
162*	SNMP	UDP	None	OpenManage Enterprise appliance	In/ Out	Managed node	<ul style="list-style-type: none">Send and receive SNMP traps.
443	Proprietary/ WS-Man/ Redfish	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed node	<ul style="list-style-type: none">Discovery and inventory of iDRAC7 and later versions.For the CMC management.
623	IPMI/ RMCP	UDP	None	OpenManage Enterprise appliance	Out	Managed node	<ul style="list-style-type: none">IPMI access through LAN.
69	TFTP	UDP	None	CMC	In	Management station	<ul style="list-style-type: none">For updating CMC firmware.

* Port can be configured up to 499 excluding the port numbers that are already allocated.

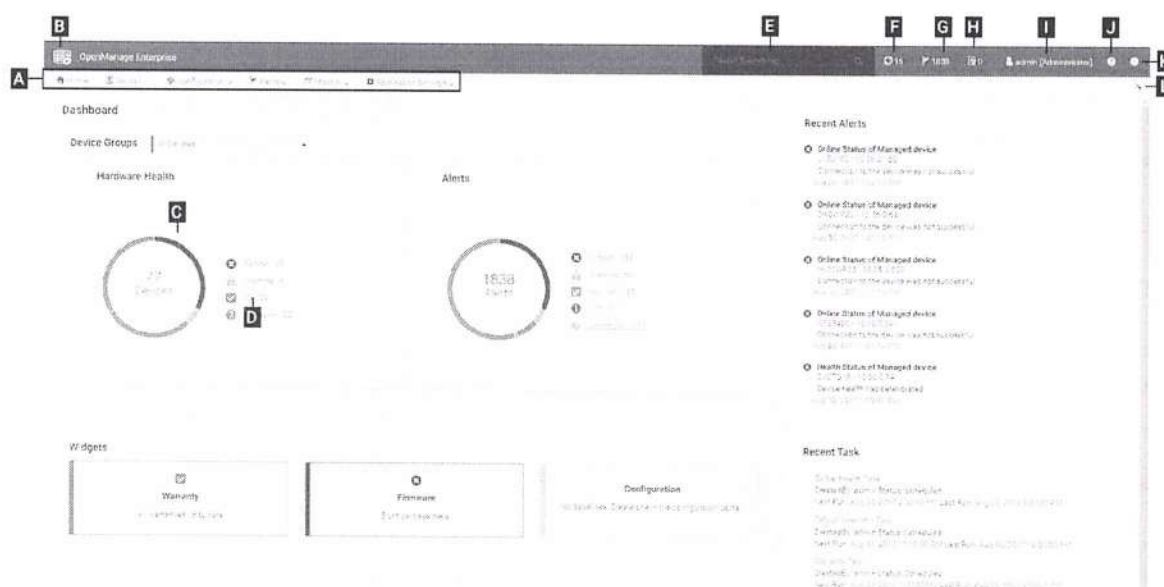
Use case links for the supported protocols and ports in OpenManage Enterprise

Table 10. Use case links for the supported protocols and ports in OpenManage Enterprise

Use case	URL
Upgrade OpenManage Enterprise appliance	https://downloads.dell.com/openmanage_enterprise/
Access device warranty	https://apigtwb2c.us.dell.com/PROD/sbil/capi/v5/asset-entitlements
Update catalogs	https://downloads.dell.com/catalog/
Push new alert notifications using the OpenManage Mobile application	https://openmanagecloud.dell.com

OpenManage Enterprise Graphical User Interface overview

On the OpenManage Enterprise Graphical User Interface (GUI), you can use menu items, links, buttons, panes, dialog boxes, lists, tabs, filter boxes, and pages to navigate between pages and complete device management tasks. Features such as devices list, Donut charts, audit logs, OpenManage Enterprise settings, system alerts, and firmware/driver update are displayed at more than one place. It is recommended that you familiarize yourself with the GUI elements for easily and effectively using OpenManage Enterprise to manage your data center devices.



- A—The **OpenManage Enterprise** menu, on all the pages of OpenManage Enterprise, provides links to features that enable administrators view the dashboard (**Home**), manage devices (**Devices**), manage firmware/driver baselines, templates, and configuration compliance baselines (**Configuration**), create and store alerts (**Alerts**), and then run jobs, discover, collect inventory data, and generate reports (**Monitor**). You can also customize different properties of your OpenManage Enterprise (**Application Settings**). Click the pin symbol in the upper-right corner to pin the menu items so they appear on all the OpenManage Enterprise pages. To unpin, click the pin symbol again.
- B—The Dashboard symbol. Click to open the dashboard page from any page of OpenManage Enterprise. Alternately, click **Home**. See [Dashboard](#).
- C—The Donut chart gives a snapshot of health status of all the devices monitored by OpenManage Enterprise. Enables you to quickly act upon the devices that are in critical state. Each color in the chart represents a group of devices having a particular health state. Click respective color bands to view respective devices in the devices list. Click the device name or IP address to view the device properties page. See [View and configure individual devices](#) on page 72.
- D—The symbols used to indicate the device health state. See [Device health statuses](#) on page 42.
- E—In the **Search Everything** box, enter about anything that is monitored and displayed by OpenManage Enterprise to view the results such as device IP, job name, group name, firmware/driver baseline, and warranty data on all the devices in your scope as defined by the Scope Based Access Control (SBAC). You cannot sort or export data that is retrieved by using the Search Everything feature. On individual pages or dialog boxes, enter or select from the **Advance Filters** section to refine your search results.
 - The following operators are not supported: +, -, and ".
- F—Number of OpenManage Enterprise jobs currently in the queue. Jobs that are related to discovery, inventory, warranty, firmware and/or drivers update, and so on. Click to view the status of jobs run under Health, Inventory, and the Report category on the Job Details page. To view all the events, click **All Jobs**. See [Using jobs for device control](#) on page 136. Click to refresh.

- **G**—The number of events generated in the alerts log. Also, based on your settings to whether or not view the unacknowledged alerts, the number of alerts in this section varies. By default, only the unacknowledged alerts are displayed. To hide or unhide the acknowledged alerts, see [Customize the alert display](#) on page 176. Deleting the alerts reduces the count. For information about symbols that are used to indicate severity statuses, see [Device health statuses](#) on page 42. Click a severity symbol to view all events in that severity category on the Alerts page. To view all the events, click **All events**. See [Managing device alerts](#).
- **H**—Total number of device warranties in Critical (expired) and in Warning (expiring soon) statuses. See [Managing device warranty](#).
- **I**—Username of the user who is currently logged in. Pause the pointer over the username to view the roles that are assigned to the user. For more information about the role-based users, see [Role and scope-based access control in OpenManage Enterprise](#) on page 18. Click to log out, and then log in as a different user.
- **J**—Currently, the context-sensitive help file is displayed only for the page you are on, and not the Home portal pages. Click to view task-based instructions to effectively use links, buttons, dialog boxes, wizards, and pages in OpenManage Enterprise.
- **K**—Click to view the current version of OpenManage Enterprise installed on the system. Click **Licenses** to read through the message. Click appropriate links to view and download OpenManage Enterprise-related open-source files, or other open-source licenses.
- **L**—Click the symbol to pin or unpin the menu items. When unpinned, to pin the menu items, expand the **OpenManage Enterprise** menu and click the pin symbol.

Data about items that are listed in a table can be comprehensively viewed, exported in total, or based on selected items. See [Export all or selected data](#) on page 71. When displayed in blue text, in-depth information about items in a table can be viewed and updated, which either opens in the same window or on a separate page. Tabulated data can be filtered by using the **Advanced Filters** feature. The filters vary based on the content you view. Enter or select data from the fields. Incomplete text or numbers will not display the expected output. Data matching the filter criteria is displayed in the list. To remove filters, click **Clear All Filters**.

To sort data in a table, click the column title. You cannot sort or export data that is retrieved by using the Search Everything feature.

Symbols are used to identify major main items, dashboard, status of device health, alert category, firmware and driver compliance status, connection state, power status, and others. Click the forward and backward buttons of the browser to navigate between pages on OpenManage Enterprise. For information about supported browsers, see the *Dell EMC OpenManage Enterprise Support Matrix* available on the support site.

Where appropriate, the page is split into left, working, and right panes to simplify the task of device management. Where necessary, online instructions and tool-tips are displayed when the pointer is paused over a GUI element.

Preview about a device, job, inventory, firmware/driver baseline, management application, virtual console, and so on, are displayed in the right pane. Select an item in the working pane and click **View Details** in the right pane to view in-depth information about that item.

When logged in, all pages are automatically refreshed. After deploying the appliance, during subsequent login, if an updated version of OpenManage Enterprise is available, you are alerted to update the version immediately by clicking **Update**. Users with all the OpenManage Enterprise privileges (Administrator, Device Manager, and Viewer) can view the message, but only an Administrator can update the version. An Administrator can choose to get reminded later or dismiss the message. For more information about updating the OpenManage Enterprise version, see [Check and update the version of the OpenManage Enterprise and the available plugins](#) on page 178.

For all the job-based actions by OpenManage Enterprise, when a job is created or started to run, the lower-right corner displays an appropriate message. Details about the job can be viewed on the **Job Details** page. See [View job lists](#) on page 136.

OpenManage Enterprise Home portal

By clicking **OpenManage Enterprise > Home**, the Home page of OpenManage Enterprise is displayed. On the Home page:

- View the Dashboard to get a live snapshot about the health statuses of devices, and then take actions, where necessary. See [Dashboard](#).
- View alerts under the critical and warning categories and resolve those. See [Managing device alerts](#).
- The Widgets section lists the rollup warranty, firmware/driver compliance, and configuration compliance statuses of all devices. For more information about the features under Widgets, see [Monitor devices by using the OpenManage Enterprise dashboard on page 40](#). The right pane lists the recent alerts and tasks generated by OpenManage Enterprise. To view more information about an alert or task, click the alert or task title. See [Monitor and Manage device alerts on page 124](#) and [Using jobs for device control on page 136](#).
- If an updated version of OpenManage Enterprise is available, you are immediately alerted when an update is available. To update, click **Update**. For more information about updating the OpenManage Enterprise version, see [Check and update the version of the OpenManage Enterprise and the available plugins on page 178](#).
- The **Recent Alerts** section lists the most recent alerts generated by devices that are monitored by OpenManage Enterprise. Click the alert title to view in-depth information about the alert. See [Managing device alerts](#).
- The **Recent Tasks** section lists the most recent tasks (jobs) created and run. Click the task title to view in-depth information about the job. See [View job lists on page 136](#).

i NOTE: If logged in as a device manager, the Home Portal displays information related to the device/device group the DM owns. Also, the Device Groups dropdown lists only the device groups that the device manager has operational access to. See [Role and scope-based access control in OpenManage Enterprise on page 18](#).

Topics:

- [Monitor devices by using the OpenManage Enterprise dashboard](#)
- [Donut chart](#)
- [Device health statuses](#)

Monitor devices by using the OpenManage Enterprise dashboard

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

Apart from the first-time login, Dashboard is the first page you see after every subsequent login to OpenManage Enterprise.

To open the Dashboard page from any page of OpenManage Enterprise, click the dashboard symbol in the upper-left corner. Alternately, click **Home**.

Using the real-time monitoring data, the dashboard displays the device health, firmware/driver compliance, warranty, alerts, and other aspects of devices and device groups in your data center environment.

Any available console updates are also displayed on the Dashboard. You can upgrade the OpenManage Enterprise version immediately, or set OpenManage Enterprise to remind you later.

By default, when you start the application the first time, the Dashboard page appears empty. Add devices to OpenManage Enterprise so that they can be monitored and displayed on the dashboard. To add devices, see [Discovering devices for monitoring or management on page 43](#) and [Organize devices into groups on page 58](#).

- [Manage the device firmware and drivers on page 80](#)
- [Managing device alerts](#)
- [Discovering devices](#)
- [Creating reports](#)
- [Managing OpenManage Enterprise appliance settings on page 156](#)

NOTE: If you select any device group in the **Device Groups** drop down, then all the data displayed on the Dashboard will be for only the selected device group.

By default, the **Hardware Health** section displays a Donut chart that indicates the current health of all the devices monitored by OpenManage Enterprise. Click sections of the Donut chart to view information about devices with respective health statuses.

A Donut in the **Alerts** section lists the alerts received by devices in the selected device groups. See *Monitor and Manage device alerts* on page 124. The total number of alerts in the Donut chart varies based on the setting to whether or not view the unacknowledged alerts. By default, only the unacknowledged alerts are displayed. See *Customize the alert display* on page 176. To view alerts under each category, click the respective color bands. In the **Alerts** dialog box, the Critical section lists the alerts in critical status. To view all the generated alerts, click **All**. The **SOURCE NAME** column indicates the device that generated the alert. Click the name to view and configure device properties. See *View and configure individual devices* on page 72.

For more information about a Donut chart, see *Donut chart* on page 41 and *Device health statuses* on page 42. To view the summary of devices in a different device group monitored by OpenManage Enterprise, select from the **Device Groups** drop-down menu. To view the list of devices that belong to a health state, you can either click the color band associated with a health category, or click the respective health status symbol next to a Donut chart.

NOTE: In the Devices list, click the device name or IP address to view device configuration data, and then edit. See *View and configure individual devices* on page 72.

The Widgets section provides a summary of some of the key features of OpenManage Enterprise. To view summary under each category, click the Widget title.

- **Warranty:** Displays the number of devices whose warranty is about to expire. This is based on the **Warranty Settings**. If the user opts for expire warranty notification, then the number of devices whose warranty is expired is shown. Otherwise, the number of expiring soon or the active warranty count is shown. Click to view more information in the **Warranty** dialog box. For information about managing device warranty, see *Manage the device warranty* on page 145. Pause the pointer over the **Warranty** section to read definitions about the symbols used in the section.
- **Firmware/Drivers:** Displays the status of firmware/driver compliance of the device baselines created on OpenManage Enterprise. If available, the Critical and Warning firmware/driver baselines are listed in this section.
 - For more information about Rollup Health status, see the *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* technical white paper on the Dell TechCenter.
 - Click to view more information in the **Firmware/Driver Compliance** page.
 - For information about updating a firmware, creating firmware catalog, creating firmware baseline, and generating baseline compliance report, see *Manage the device firmware and drivers* on page 80.
- **Configuration:** Displays the rolledup status of configuration compliance baselines created on OpenManage Enterprise. If available, the Critical and Warning configuration baselines are listed. See *Manage compliance templates* on page 117.
- **Resource Utilization:** Displays the CPU and the memory utilization by the appliance. The following color-coded checks are used to indicate the various stages of utilization:
 - Green — A less than 80% utilization of the resource
 - Yellow — A greater than 80% but less than 95% utilization of the resource
 - Red — A greater than 95% utilization of the resource

NOTE: The overall resource utilization, shown as a color-coded vertical bar on the left of the widget, is the worst-case rollup of any of the resource.

Donut chart

You can view a Donut chart in different sections of your OpenManage Enterprise. The output displayed by the Donut chart is based on the items you select in a table. A Donut chart indicates multiple statuses in OpenManage Enterprise:




- The health status of devices: Displayed on the Dashboard page. Colors in the Donut chart split the ring proportionally to indicate the health of devices monitored by OpenManage Enterprise. Every device status is indicated by a color symbol. See *Device health statuses* on page 42. If the Donut chart indicates the health status of 279 devices in the group, in which 131=critical, 50=warning, and 95=ok, the circle is formed by using color bands proportionately representing these numbers.

NOTE: The Donut chart of a single device is formed by a thick circle by using only one color that indicates the device status. For example, for a device in Warning state, a yellow color circle is displayed.

- The alert statuses of devices: Indicates the total alerts generated for the devices monitored by OpenManage Enterprise. See *Monitor and Manage device alerts* on page 124.

NOTE: The total number of alerts in the Donut chart varies based on the setting to whether or not view the unacknowledged alerts. By default, only the unacknowledged alerts are displayed. See [Customize the alert display](#) on page 176.





- The firmware version compliance of a device against the version on the catalog: See [Manage the device firmware and drivers](#) on page 80.
- The configuration compliance baseline of devices and device groups: See [Managing the device configuration compliance](#) on page 116.

NOTE: The compliance level of the selected device is indicated by a Donut chart. When more than one device is associated with a baseline, the status of a device with the least compliance level to the baseline is indicated as the compliance level of that baseline. For example, if many devices are associated to a firmware baseline, and the compliance level of few devices is Healthy  or Downgrade , but if the compliance of one device in the group is Upgrade , the compliance level of the firmware baseline is indicated as Upgrade. The rollup status is equal to the status of the device that has high severity. For more information about Rollup Health status, see the *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* technical white paper on the Dell TechCenter.

NOTE: The Donut chart of a single device is formed by a thick circle by using only one color that indicates the device firmware compliance level. For example, for a device in Critical state, a red color circle is displayed indicating that the device firmware must be updated.

Device health statuses

Table 11. Device health statuses in OpenManage Enterprise

Health status	Definition
Critical 	Indicates an occurrence of a failure of an important aspect of the device or environment.
Warning 	The device is about to fail. Indicates that some aspects of the device or environment are not normal. Requires immediate attention.
Ok 	The device is fully functional.
Unknown 	The device status is unknown.

NOTE: The data displayed on the dashboard depends on the privileges you have for using OpenManage Enterprise. For more information about users, see [Managing users](#).

Discovering devices for monitoring or management

By clicking **OpenManage Enterprise > Monitor > Discovery**, you can discover devices in your data center environment to manage them, improve their usability, and improve resource availability for your business-critical operations. The **Discovery** page displays the number of devices discovered in task and information about the status of discovery job for that device. The job statuses are Queued, Completed, and Stopped. The right pane displays information about the task such as the total possible devices, device discovered with Device Types and their respective count, next run time if scheduled, and last discovered time. **View Details** in the right pane displays individual discovery job details.

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.
- In order to support discovery with domain credentials, OpenManage Enterprise (version 3.2 and later) uses the OpenSSH protocol instead of the WSMAN protocol used in the previous versions. Hence, all the Windows and Hyper-V devices discovered prior to updating the appliance have to be deleted and re-discovered using their OpenSSH credentials. Refer the Microsoft documentation to enable OpenSSH on Windows and Hyper-V.
- On the **Discovery and Inventory Schedules** pages, the status of a scheduled job is indicated as **Queued** in the **STATUS** column. However, the same status is indicated as **Scheduled** on the **Jobs** page.
- By default, the last discovered IP of a device is used by OpenManage Enterprise for performing all operations. To make any IP change effective, you must rediscover the device.
- For third party devices, you might see duplicate entries if they are discovered using multiple protocols. This duplication can be corrected by deleting the entries and rediscovering the device(s) using only the IPMI protocol.

By using the Discovery feature, you can:

- View, add, and remove devices from the global exclusion list. See *Global exclusion of ranges* on page 51.
- Create, run, edit, delete, and stop the device discovery jobs.

Related tasks

Delete a device discovery job on page 56

View device discovery job details on page 49

Stop a device discovery job on page 50

Run a device discovery job on page 50

Specify discovery mode for creating a server discovery job on page 52

Create customized device discovery job protocol for servers – Additional settings for discovery protocols on page 52

Specify discovery mode for creating a Dell storage discovery job on page 55

Create customized device discovery job protocol for SNMP devices on page 56

Specify discovery mode for creating a MULTIPLE protocol discovery job on page 56

Edit a device discovery job on page 50

Topics:

- Discover servers automatically by using the server-initiated discovery feature
- Create a device discovery job
- Protocol support matrix for discovering devices
- View device discovery job details
- Edit a device discovery job
- Run a device discovery job
- Stop a device discovery job
- Specify multiple devices by importing data from the .csv file

- Global exclusion of ranges
- Specify discovery mode for creating a server discovery job
- Create customized device discovery job protocol for servers – Additional settings for discovery protocols
- Specify discovery mode for creating a chassis discovery job
- Create customized device discovery job protocol for Chassis – Additional settings for discovery protocols
- Specify discovery mode for creating a Dell storage discovery job
- Specify discovery mode for creating a network switch discovery job
- Create customized device discovery job protocol HTTPS storage devices – Additional settings for discovery protocols
- Create customized device discovery job protocol for SNMP devices
- Specify discovery mode for creating a MULTIPLE protocol discovery job
- Delete a device discovery job

Discover servers automatically by using the server-initiated discovery feature


OpenManage Enterprise allows automatic discovery of servers that have iDRAC firmware version 4.00.00.00 or later. The appliance can be configured to allow these servers to automatically locate the console by querying the DNS and initiate their discovery.

Prerequisites

For a server-initiated discovery, the following prerequisites must be met:

- This feature is applicable only for servers with iDRAC firmware version 4.00.00.00 or later.
- The servers must be on the same domain or subdomain as OpenManage Enterprise.
- OpenManage Enterprise must be registered with the DNS to add the configuration information to the DNS by using TUI. It is preferred that the DNS allows automatic updates from OpenManage Enterprise.
- Old records of the appliance console on the DNS, if any, should be cleaned up to avoid multiple announcements from the servers.

About this task

 **NOTE:** Scope-Based Access Control (SBAC) does not affect the device listings on the **Monitor > Server Initiated Discovery** page and the device managers would see devices which are beyond their scope on this page.

The following steps are followed for an automatic discovery of servers in OpenManage Enterprise :

Steps

1. Add the configuration information of OpenManage Enterprise on the DNS using one of following methods:
 - TUI—By using the TUI interface, enable the **Configure Server Initiated Discovery** option. For more information, see *Configure OpenManage Enterprise by using Text User Interface* on page 29.
 - Manually—Add the following four records to your DNS server on the network for which the interface is configured on the appliance. Ensure that you replace all instances of <domain> or <subdomain.domain> with the appropriate DNS domain and the system hostname.
 - <OME hostname>.<domain> 3600 A <OME IP address>
 - _dcimprovsrv._tcp.<domain> 3600 PTR ptr.dcimprovsrv._tcp.<domain>
 - ptr.dcimprovsrv._tcp.<domain> 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence
 - ptr.dcimprovsrv._tcp.<domain> 3600 SRV 0 0 443 <hostname>.<domain>

To create the records with nsupdate in Linux, use the following commands:

- To create hostname record

```
>update add omehost.example.com 3600 A XX.XX.XX.XX
```

- To add records for server-initiated discovery

```
>update add _dcimprovsrv._tcp.example.com 3600 PTR ptr.dcimprovsrv._tcp.example.com.
```

```
>update add ptr.dcimprovsrv._tcp.example.com 3600 TXT URI=/api/
DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence

>update add ptr.dcimprovsrv._tcp.example.com 3600 SRV 0 0 443
omehost.example.com.
```

To create the records with `dnscmd` on a Windows DNS server, use the following commands:

- o To create hostname record

```
>dnscmd <DnsServer> /RecordAdd example.com omehost A XX.XX.XX.XX
```

- o To add records for server-initiated discovery

```
>dnscmd <DnsServer> /RecordAdd example.com _dcimprovsrv._tcp PTR
ptr.dcimprovsrv._tcp.example.com
```

```
>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp TXT URI=/api/
DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence
```

```
>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp SRV 0 0 443
omehost.example.com
```

2. By default, the Discovery-Approval policy, in the appliance, is set to Automatic and the servers that establish contact with the console are automatically discovered. To change the settings, see *Manage Console preferences* on page 173.
3. Once the appliance is configured as mentioned in the previous steps, the servers can initiate contact with OpenManage Enterprise by querying the DNS. The appliance verifies the servers after ensuring that the client certificate of the servers is signed by the Dell CA.

NOTE: If there are any changes in the server IP address or SSL certificate, the server reinitiates contact with OpenManage Enterprise.

4. The **Monitor > Server Initiated Discovery** page lists the servers that establish contact with the console. Also, the servers whose credentials have been added in the console, but which are yet to initiate contact are also listed. The following statuses of the servers based on the previously mentioned conditions are displayed:
 - **Announced**—Server initiates contact with the console, however, the credentials of the server are not added to the console.
 - **Credentials Added**—The credentials of the server are added in the console, however, the server has not initiated contact with the console.
 - **Ready to Discover**—The credentials of the server are added and the server has initiated contact.

NOTE: The appliance triggers a Discovery job every 10 minutes to discover all the servers in the 'Ready to Discover' status. However, if the Discovery-Approval policy in the appliance is set as 'Manual,' then the user should manually trigger the Discovery job for each server. For more information, see *Manage Console preferences* on page 173
 - **Job submitted for Discovery**—This status indicates that the discovery job is initiated either automatically or manually for the server.
 - **Discovered**—The server is discovered and is listed on the All Devices page.

The following tasks can be performed on the **Monitor > Server Initiated Discovery** page:


Steps

1. **Import**—To import the server credentials:
 - a. Click **Import**.
 - b. In the Import From File wizard, click **Upload Service Tags File** to navigate and select the .csv file.
To view a sample CSV file of the server credentials, click **Download sample CSV file**.
 - c. Click **Finish**
2. **Discover**—To manually discover the servers in 'Ready to Discover' status:
 - a. Select the servers listed on the Server-Initiated Discovery page which are in 'Ready to Discover' Status.
 - b. Click **Discover**.

A Discover job is triggered to discover the servers and post discovery these servers are listed on the All Devices page.
3. **Delete**—To delete the servers listed on the Server-Initiated Discovery page:

- a. Select the servers on the Server-Initiated Discovery page which are already discovered and listed on the All Devices page.
- b. Click **Delete**.


The servers are deleted from the Server-Initiated Discovery page.

 **NOTE:** Entries corresponding to discovered servers are automatically be purged after 30 days.

4. **Export**—To export the server credentials in HTML, CSV, or PDF formats:
 - a. Select one or more servers on the Sever-Initiated Discovery page.
 - b. Click **Export**.
 - c. In the Export All wizard, select any of the following file formats: HTML, CSV, and PDF.
 - d. Click **Finish**. A job is created, and the data is exported to the selected location.

Create a device discovery job


About this task


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


To discover a device:


Steps

1. Click **Monitor > Discovery > Create**.
2. In the **Create Discovery Job** dialog box, a default job name is populated. To change it, enter the discovery job name.
By default, the dialog box enables you to define properties of similar devices at a time.
 - To include more devices or ranges to the current discovery job, click **Add**. Another set of the following fields is displayed where you can specify the device properties: Type, IP/Hostname/Range, and Settings.

 **WARNING: A maximum of 8,000 devices can be managed by OpenManage Enterprise. Hence, do not specify large networks that have devices more than the maximum number of devices supported by OpenManage Enterprise. It may cause the system to abruptly stop responding.**

 **NOTE:** When discovering a large number of devices, avoid creating multiple discovery jobs using individual IP address and instead use IP range of the devices.

 - To discover devices by importing ranges from the .csv file. See *Specify multiple devices by importing data from the .csv file* on page 50.
 - To exclude certain devices, remove devices from being excluded, or to view the list of devices excluded from being discovered, see *Globally excluding device(s) from discovery results*.
3. From the **Device Type** drop-down menu, to discover:
 - A server, select **SERVER**. See *Specifying discovery mode for creating a server discovery job*.
 - A chassis, select **CHASSIS**. See *Specifying discovery mode for creating a chassis discovery job*.
 - A Dell EMC storage device, or network switch, select **DELL STORAGE**, or **NETWORKING SWITCH**. See *Specifying discovery mode for creating a storage, Dell storage, and network switch discovery job*.
 - To discover devices by using multiple protocols, select **MULTIPLE**. See *Specify discovery mode for creating a MULTIPLE protocol discovery job* on page 56.
4. In the **IP/Hostname/Range** box, enter the IP address, host name, or the range of IP address to be discovered or included. For more information about the data you can enter in this field, click the  symbol.

 **NOTE:**

 - The range size is limited to 16,385 (0x4001).
 - IPv6 and IPv6 CIDR formats too are supported.
5. In the **Settings** section, enter the username and password of the protocol that is used for discovering the ranges.
6. Click **Additional Settings**, to select a different protocol, and change the settings.
7. In the **Scheduling Discovery Job** section, run the job immediately or schedule for a later point of time. See *Schedule job field definitions* on page 192.
8. Select **Enable trap reception from discovered iDRAC servers and MX7000 chassis** to enable the OpenManage Enterprise receive the incoming traps from the discovered servers and MX7000 chassis.

NOTE: Enabling this setting will enable alerts on the iDRAC (if disabled), and set an alert destination for the OpenManage Enterprise server's IP address. If there are specific alerts that must be enabled, you must configure these on the iDRAC by enabling the appropriate alert filters and SNMP traps. For more information, see the iDRAC User's Guide.

9. Select **Set Community String for trap destination from Application Settings**. This option is available only for the discovered iDRAC servers and MX7000 chassis.
10. Select the **Email when complete** check box, and then enter the email address that must receive notification about the discovery job status. If the email is not configured, the **Go to SMTP Settings** link is displayed. Click the link, and configure the SMTP settings. See *Configure SMTP, SNMP, and Syslog alerts* on page 129. If you select this but do not configure SMTP, the **Finish** button is not displayed to continue the task.
11. Select the **Email when complete** check box, and then enter the email address that must receive notification about the discovery job status. If the email is not configured, the **Go to SMTP Settings** link is displayed. Click the link, and configure the SMTP settings. If you select this but do not configure SMTP, the **Finish** button is not displayed to continue the task.
12. Click **Finish**. The Finish button is not displayed if the fields are incorrectly or incompletely filled. A discovery job is created and run. The status is displayed on the **Job Details** page.

Results

During device discovery, the user account that is specified for the discovery range is verified against all available privileges that are enabled on a remote device. If the user authentication passes, the device is automatically onboarded or the device can be onboarded later with different user credentials. See *Onboarding devices* on page 47.

NOTE: During CMC discovery, the servers, and IOM and storage modules (configured with IP and SNMP set to "public" as community string), residing on CMC are also discovered and are onboarded. If you enable trap reception during CMC discovery, the OpenManage Enterprise is set as the trap destination on all the servers and not on the chassis.

NOTE: During CMC discovery, FN I/O Aggregators in Programmable MUX (PMUX) mode are not discovered.

Onboarding devices

About this task

Onboarding enables servers to be managed, rather than just be monitored.

- If administrator-level credentials are provided during discovery, the servers are onboarded (the device status is displayed as "managed" in the All Devices view).
- If lower privileged credentials are provided during discovery, the servers are not onboarded (the status is displayed as "monitored" in the All Devices view).
- If the console is also set as a trap receiver on the servers then their Onboarding status is indicated as "managed with alerts".
- **Error:** Indicates an issue in onboarding the device.
- **Proxied:** Available only for MX7000 chassis. Indicates that the device is discovered through an MX7000 chassis and not directly. For the supported and unsupported actions on the proxied sleds, see *Supported and unsupported actions on 'Proxied' sleds* on page 192.

If you want to onboard devices with a different user account apart from the account specified for discovery, or re-attempt onboarding because of a failure in onboarding during discovery, do the following:

- NOTE:**
- All devices that have been onboarded through this wizard remain onboarded through this user account and is not substituted by the discovery user account during future discoveries against these devices.
 - For the already discovered devices, if the SNMP trap destination is 'manually' set in iDRAC as OpenManage Enterprise, the alerts are received and processed by the appliance. However, the device's Managed State displayed on the All Devices page remains the same as its initial discovered state of 'Monitored,' 'Managed' or 'Managed with Alerts.'
 - The All Devices page displays the **Managed State** of all the onboarded chassis as "Managed" irrespective of which chassis user-role credentials were used at the time of onboarding. If the chassis was onboarded with credentials of a "read-only" user, then there may be a failure during update activities performed on chassis. Hence, It is recommended to onboard chassis with credentials of a chassis Administrator to perform all activities.

- 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.

Steps

1. From the **OpenManage Enterprise** menu, under **Devices**, click **All Devices**.

A Donut chart indicates status of all devices in the working pane. See the *Donut chart*. The table lists the properties of devices selected along with their following onboarding status:

- **Error:** Device cannot be onboarded. Try by logging in by using the recommended privileges. See *Role and scope-based access control in OpenManage Enterprise* on page 18.
- **Managed:** Device successfully onboarded, and can be managed by the OpenManage Enterprise console.
- **Monitored:** Device does not have management option (such as the one discovered by using SNMP).
- **Managed with alerts:** Device is successfully onboarded, and the OpenManage Enterprise console has successfully registered its IP address with the device as a trap destination during discovery.

2. In the working pane, select a check box corresponding to the device(s), click **More Actions > Onboarding**.

Ensure that you select only the device types from the All Devices page that are supported for onboarding. You can search for suitable devices in the table by clicking **Advanced Filters**, and then select or enter onboarding status data in the filter box.

- i** NOTE: All devices that are discovered are not supported for onboarding and only iDRAC and CMC are supported. Ensure that you select onboarding option for the supported device type.

3. In the **Onboarding** dialog box, enter the WS-Man credentials—username and password.

4. In the **Connection Settings** section:

a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.

b. In the **Timeout** box, enter the time after which a job must stop running.

- i** NOTE: If the timeout value entered is greater than the current session expiry time, you are automatically logged out of OpenManage Enterprise. However, if the value is within the current session expiration timeout window, the session is continued and not logged out.

c. In the **Port** box, enter the port number that the job must use to discover.

d. Optional field. Select **Enable Common Name (CN) check**.

e. Optional field. Select **Enable Certificate Authority (CA) check** and browse to the certificate file.

5. Click **Finish**.

- i** NOTE: The **Enable trap reception from discovered** check box is effective only for servers discovered by using their iDRAC interface. Selection is ineffective for other servers—such as those devices discovered by using OS discovery.

Protocol support matrix for discovering devices

The following table provides information about the supported protocols for discovering devices.

- i** NOTE: The functionality of the supported protocols to discover, monitor, and manage the PowerEdge YX1X servers with iDRAC6 is limited. See *Generic naming convention for Dell EMC PowerEdge servers* on page 197 for more information.

Table 12. Protocol support matrix for discovery

Device/ Operating System	Protocols						
	Web Services- Managemen t (WS-Man)	Redfish	Simple Network Management Protocol (SNMP)	Secure Shell (SSH)	Intelligent Platform Management Interface (IPMI)	ESXi (VMWare)	HTTPS
iDRAC6 and later	Supported	Supported Only for iDRAC9 Version 4.40.10.00 and later	Not supported	Not supported	Not supported	Not supported	Not supported

Table 12. Protocol support matrix for discovery (continued)

Device/ Operating System	Protocols						
	Web Services- Managemen t (WS-Man)	Redfish	Simple Network Management Protocol (SNMP)	Secure Shell (SSH)	Intelligent Platform Management Interface (IPMI)	ESXi (VMWare)	HTTPS
		Not supported					
PowerEdge C*	Supported	Not Supported	Not supported	Not supported	Not supported	Not supported	Not supported
PowerEdge chassis (CMC)	Supported	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
PowerEdge MX7000 chassis	Not supported	Supported	Not supported	Not supported	Not supported	Not supported	Not supported
Storage devices	Not supported	Not supported	Supported	Not supported	Not supported	Not supported	Not supported
Ethernet switches	Not supported	Not supported	Supported	Not supported	Not supported	Not supported	Not supported
ESXi	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Not supported
Linux	Not supported	Not supported	Not supported	Supported	Not supported	Not supported	Not supported
Windows	Not Supported	Not supported	Not supported	Supported	Not supported	Not supported	Not supported
Hyper-V	Not Supported	Not supported	Not supported	Supported	Not supported	Not supported	Not supported
Non-Dell servers	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Not supported
PowerVault ME	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported

View device discovery job details

About this task

Steps

1. Click **Monitor > Discovery**.
2. Select the row corresponding to the discovery job name, and then click **View Details** in the right pane.
The **Job Details** page displays the respective discovery job information.
3. For more information about managing jobs, see *Using jobs for device control* on page 136.

Related information

Discovering devices for monitoring or management on page 43

Edit a device discovery job

You can edit only one device discovery job at a time.

Steps


1. Select the check box corresponding to the discovery job you want to edit, and then click **Edit**.
2. In the **Create Discovery Job** dialog box, edit the properties.
For information about the tasks to be performed in this dialog box, see [Creating device discovery job](#).

Related information

[Discovering devices for monitoring or management on page 43](#)

Run a device discovery job

About this task

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

To run a device discovery job:

Steps

1. In the list of existing device discovery jobs, select the check box corresponding to the job you want to run now.
2. Click **Run**.
The job starts immediately and a message is displayed in the lower-right corner.

Related information

[Discovering devices for monitoring or management on page 43](#)


Stop a device discovery job

About this task

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

Steps

1. In the list of existing discovery jobs, select the check box corresponding to the job you want to stop.

 **NOTE:** Multiple jobs cannot be stopped at a time.

2. Click **Stop**.
The job is stopped and a message is displayed in the lower-right corner.



Related information

[Discovering devices for monitoring or management on page 43](#)

Specify multiple devices by importing data from the .csv file

About this task



Steps

1. In the **Create Discovery Job** dialog box, by default, a discovery job name is populated in **Discovery Job Name**. To change it, type a discovery job name.
2. Click **Import**.
 **NOTE:** Download the sample .CSV file, if necessary.
3. In the **Import** dialog box, click **Import**, browse through to the .CSV file which contains a list of valid ranges, and then click **OK**.
 **NOTE:** An error message is displayed if the .CSV file contains invalid ranges, and duplicate ranges are excluded during the import operation.



Global exclusion of ranges

Using the Global Exclusion of Ranges wizard, you can enter the address(es) or range of the devices that must be excluded from OpenManage Enterprise monitoring and management activities. The following steps describe how you can exclude the range of devices:

About this task

-  **NOTE:** To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See *Role and scope-based access control in OpenManage Enterprise* on page 18.
-  **NOTE:** Currently, you cannot exclude a device by using its hostname, but exclude only by using its IP address or FQDN.

Steps

1. To activate the Global Exclusion of Ranges wizard, you can do one of the following:
 - From the All Devices page (**OpenManage Enterprise > Devices**), **Discovery** drop-down menu, click **Edit Exclude Ranges**.
 - From the **Monitor > Discovery**, click the **Global Exclusion List** on the top right corner.
2. In the **Global Exclusion of Ranges** dialog box:
 - a. In the **Description of Exclude Range** box, enter the information about the range that is being excluded.
 - b. In the **Enter Ranges to Exclude** box, enter address(es) or range of devices to be excluded. The box can take up to 1000 address entries at a time, but separated by a line break. Meaning, every exclusion range must be entered in different lines inside the box.
The range that can be excluded is same as the supported ranges that are applicable while discovering a device. See *Create a device discovery job* on page 46. **NOTE:**
 - The range size is limited to 16,385 (0x4001).
 - The IPv6 and IPv6 CIDR formats too are supported.
3. Click **Add**.
4. When prompted, click **YES**.
The IP address or the range is globally excluded, and then displayed in the list of excluded ranges. Such devices are globally excluded which implies that they do not take part in any activity performed by OpenManage Enterprise.
 **NOTE:** The device that is globally excluded is clearly identified as 'Globally excluded' on the **Job Details** page.
To remove a device from the global exclusion list:
 - a. Select the check box and click **Remove from Exclusion**.
 - b. When prompted, click **YES**. The device is removed from the global exclusion list. However, a device removed from the global exclusion list is not automatically monitored by OpenManage Enterprise. You must discover the device so that OpenManage Enterprise starts monitoring.

Results

-  **NOTE:**

- Adding devices that are already known to the console (meaning, already discovered by the console) to the Global Exclusion List will remove the device(s) from OpenManage Enterprise.
- The newly-included devices to the Global Exclusion List continues to be seen in the All Devices grid till the next Discovery cycle. To avoid performing tasks on such devices, it is highly recommended that the user manually excludes them from the All Devices Page by selecting the check box corresponding to the device(s) and then clicking **Exclude**.
- Devices listed in the Global Exclusion List are excluded from all tasks in the console. If the IP of a device is in the Global Exclusion List and a discovery task is created where the range for discovery includes that IP, that device is not discovered. However, there will be no error indication on the console when the discovery task is being created. If you expect that a device must be discovered and it is not, you must check the Global Exclusion List to see if the device has been included in the Global Exclusion List.

Specify discovery mode for creating a server discovery job

About this task

Steps

1. From the **Device Type** drop-down menu, select **SERVER**.
2. When prompted, select:
 - **Dell iDRAC**: To discover by using iDRAC.
 - **Host OS**: To discover by using an VMware ESXi, Microsoft Windows Hyper-V, or Linux operating system.
 - **Non-Dell Servers (via OOB)**: To discover third party servers by using IPMI.
3. Click **OK**.
Based on your selection, the fields change under **Settings**.
4. Enter the IP address, host name, or IP range associated with the protocol in **IP/Hostname/Range**.
5. Under **Settings**, enter the username and password of the server to be discovered.
6. To customize discovery protocols by clicking **Additional Settings**, see [Creating customized device discovery job template for servers](#).
7. Schedule the discovery job. See [Schedule job field definitions](#) on page 192.
8. Click **Finish**.
A discovery job is created and displayed in the list of discovery jobs.


Related information

[Discovering devices for monitoring or management](#) on page 43

Create customized device discovery job protocol for servers –Additional settings for discovery protocols

About this task

In the **Additional Settings** dialog box, enter details for the appropriate protocol with which you want to discover the server(s):

 **NOTE:** The appropriate protocols are automatically preselected based on your initial inputs.

Steps


1. To **Discover using WS-Man/Redfish (iDRAC, Server, and/or Chassis)**
 - a. In the **Credentials** section, enter **User Name** and **Password**.
 - b. In the **Connection Settings** section:



- In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
- In the **Timeout** box, enter the time after which a job must stop running.
- Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 34
- Select the **Enable Common Name (CN)** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
- Select the **Enable Certificate Authority (CA)** check box, if needed.

2. To Discover using IPMI (non-Dell via OOB)

- In the Credentials section, enter **User Name** and **Password**.
- In the **Connection Settings** section:
 - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
 - In the **Timeout** box, enter the time after which a job must stop running.
 - In the **KeyKey** box, enter an appropriate value.

3. To Discover using SSH (Linux, Windows, Hyper-V)

 **NOTE:** Only OpenSSH on Windows and Hyper-V is supported. Cygwin SSH is not supported.

- In the Credentials section, enter **User Name** and **Password**.
- In the **Connection Settings** section:
 - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
 - In the **Timeout** box, enter the time after which a job must stop running.
 - Enter in the **Port** box to edit the port number. By default, 22 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 34
 - Select the **Verify the known Host key** check box to validate host against known host keys.
 -  **NOTE:** Known host keys are added via the `/DeviceService/HostKeys` REST API service. Please refer to the *OpenManage Enterprise RESTful API Guide* for more information on how to manage host keys.
 - Select the **Use SUDO Option** check box if sudo accounts are preferred.
 -  **NOTE:** For sudo accounts to work, the server(s) `/etc/sudoers` file must be configured to use NOPASSWD.

4. To Discover using ESXi (VMware)

- In the Credentials section, enter **User Name** and **Password**.
- In the **Connection Settings** section:
 - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
 - In the **Timeout** box, enter the time after which a job must stop running.
 - Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 34
 - Select the **Enable Common Name (CN)** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
 - Select the **Enable Certificate Authority (CA)** check box, if needed.

Related information



Discovering devices for monitoring or management on page 43

Specify discovery mode for creating a chassis discovery job

Steps

- From the **Device Type** drop-down menu, select **CHASSIS**.
Based on your selection, the fields change under **Settings**.
- Enter the IP address, host name, or IP range in **IP/Hostname/Range**.
- Under **Settings**, enter the username and password of the server to be detected.
- Type the community type.
- To create customized discovery template by clicking **Additional Settings**, see Create customized device discovery job protocol for Chassis – Additional settings for discovery protocols on page 54.

Results





-  **NOTE:** Currently, for any M1000e chassis that is discovered, the date in the **TIMESTAMP** column under **Hardware Logs** is displayed as **JAN 12, 2013** in the CMC 5.1x and earlier versions. However, for all versions of CMC VRTX and FX2 chassis, correct date is displayed.
-  **NOTE:** When a server in a chassis is separately discovered, slot information about the server is not displayed in the **Chassis Information** section. However, when discovered through a chassis, the slot information is displayed. For example, an MX740c server in an MX7000 chassis.

Create customized device discovery job protocol for Chassis – Additional settings for discovery protocols

About this task

In the **Additional Settings** dialog box:

Steps

1. Select the **Discover using WS-Man/Redfish (iDRAC, Server, and/or Chassis)** .
 -  **NOTE:** For chassis, the **Discover using WS-Man/Redfish** check box is selected by default. Implies that the chassis can be discovered by using either of these two protocols. The M1000e, CMC VRTX, and FX2 chassis support the WS-Man commands. The MX7000 chassis supports Redfish protocol.
2. Enter username and password of the chassis to be detected.
3. In the **Connection Settings** section:
 - a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
 - b. In the **Timeout** box, enter the time after which a job must stop running.
 - c. Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see *Supported protocols and ports in OpenManage Enterprise* on page 34.
 - d. Select the **Enable Common Name (CN) check** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
 - e. Select the **Enable Certificate Authority (CA) check** check box.
4. To discover IO modules, select the **Discover IO Modules with chassis** check box.
 -  **NOTE:** Applicable only for the CMC VRTX, M1000e, and FX2 chassis (models FN2210S, FN410T and FN410S). For the MX7000 chassis, the IO modules are automatically detected.
 -  **NOTE:** Only the IO Modules with Standalone, PMUX (Programmable MUX), VLT (Virtual Link Trunking) Modes are discoverable. Full switch and Stacked Modes will not be discovered.
 - a. Select **Use chassis credentials** if the M I/O Aggregator user credentials are the same as that of the chassis.
 - b. Select **Use different credentials** if the M I/O Aggregator user credentials are different from the chassis credentials and do the following:
 - Enter the **User Name** and **Password**.
 - Change the default values for **Retries**, **Timeout**, and **Port** if required.
 - Select **Verify known Host key**, to validate host against known host keys.
 -  **NOTE:** Known host keys are added via `/DeviceService/HostKeys` REST API service. Please refer to the *OpenManage Enterprise RESTful API Guide* for more information on how to manage host keys.
 - Select **Use SUDO Option** if needed.
5. Click **Finish**.
6. Complete the tasks in *Create a device discovery job* on page 46.

Specify discovery mode for creating a Dell storage discovery job

Steps

1. From the **Device Type** drop-down menu, select **DELL STORAGE**.
2. When prompted, select:
 - **PowerVault ME**: To discover the storage devices using the HTTPS protocol like the PowerVault ME.
 - **Others**: To discover storage devices which use SNMP protocol.Based on your selection, the fields change under **Settings**.
3. Enter the IP address, host name, or IP range in **IP/Hostname/Range**.
4. Under **Settings**, depending on your initial selection — enter the **User Name** and **Password** for Storage HTTPS or enter the **SNMP version** and the **community type** of the device to be detected.
5. Click **Additional Settings** to customize the respective discover protocol. See [Creating customized device discovery job template for SNMP devices](#) or see [Create customized device discovery job protocol HTTPS storage devices –Additional settings for discovery protocols](#) on page 55.
6. Complete the tasks in [Create a device discovery job](#) on page 46.

Related information

Discovering devices for monitoring or management on page 43

Specify discovery mode for creating a network switch discovery job

Steps

1. From the **Device Type** drop-down menu, select **NETWORK SWITCH**.
2. Enter the IP address, host name, or IP range in **IP/Hostname/Range**.
3. Under **Settings** enter the **SNMP version** and the **community type** of the device to be detected.
4. Click **Additional Settings** to customize the respective discover protocol. See [Creating customized device discovery job template for SNMP devices](#)
5. Complete the tasks in [Create a device discovery job](#) on page 46.

Create customized device discovery job protocol HTTPS storage devices –Additional settings for discovery protocols

About this task

In the **Additional Settings** dialog box:

Steps

1. Enter username and password of the PowerVault ME to be detected.
2. In the **Connection Settings** section:
 - a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
 - b. In the **Timeout** box, enter the time after which a job must stop running.
 - c. Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see [Supported protocols and ports in OpenManage Enterprise](#) on page 34.

- d. Select the **Enable Common Name (CN) check** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
- e. Select the **Enable Certificate Authority (CA) check** check box.
3. Click **Finish**.
4. Complete the tasks in [Create a device discovery job](#) on page 46.

Create customized device discovery job protocol for SNMP devices

About this task

By default, the **Discover using SNMP** check box is selected to enable you detect the storage, networking, or other SNMP devices.

NOTE: Only the IO Modules with Standalone, PMUX (Programmable MUX), VLT (Virtual Link Trunking) Modes are discoverable. Full switch and Stacked Modes will not be discovered.

Steps

1. Under **Credentials**, select the SNMP version, and then enter the community type.
2. In the **Connection Settings** section:
 - a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
 - b. In the **Timeout** box, enter the time after which a job must stop running.
 - c. In the **Port** box, enter the port number that the job must use to discover.

NOTE: Currently, the settings in the **Retries box** and the **Timeout box** do not have any functional impact on the discovery jobs for SNMP devices. Hence, these settings can be ignored.
3. Click **Finish**.
4. Complete the tasks in [Create a device discovery job](#) on page 46.

Related information

[Discovering devices for monitoring or management on page 43](#)

Specify discovery mode for creating a MULTIPLE protocol discovery job

Steps

1. From the **Type** drop-down menu, select **MULTIPLE** to discover devices using multiple protocols.
2. Enter the IP address, host name, or IP range in **IP/Hostname/Range**.
3. To create customized discovery template by clicking **Additional Settings**, see [Create customized device discovery job protocol for servers – Additional settings for discovery protocols on page 52](#).

Related information

[Discovering devices for monitoring or management on page 43](#)

Delete a device discovery job

About this task

NOTE: A device can be deleted even when tasks are running on it. Task initiated on a device fails if the device is deleted before the completion.

To delete a device discovery job:

Steps

1. Select the check box corresponding to the discovery job you want to delete, and then click **Delete**.
2. When prompted indicating if the job must be deleted, click **YES**.
The discovery jobs are deleted and a message is displayed in the lower-right corner of the screen.

Results

- ① **NOTE:** If you delete a discovery job, the devices associated with the job are not deleted. If you want the devices discovered by a discovery task to be removed from the console then delete them from the **All Devices** page.
- ① **NOTE:** A device discovery job cannot be deleted from the **Jobs** page.

Related information

Discovering devices for monitoring or management on page 43

Manage devices and device groups

By clicking **OpenManage Enterprise > Devices** you can view and manage the device groups and devices discovered in OpenManage Enterprise. If you are logged in as a device manager, only the device groups and its associated trees that are in your scope would be available for viewing and management.

The left pane displays the device groups as follows:

- All Devices — The top-level root group containing all groups.
- System groups — Default groups created by OpenManage Enterprise when shipped.
- Custom groups — Groups created by users such as administrators and device managers. you can create 'query' groups or 'static' groups under custom groups.
- Plugin groups — Groups created by plugins.

You can create child groups under these parent groups. For more information see [Device Groups](#).

On top of the working pane, donut charts display the health state and alerts of all devices by default. However, when a group is selected on the left pane these donut charts would display the health state and alerts of the group that is selected. Additionally, if a plugin is installed, a third donut chart might display the data of the installed plugin. For more information about Donut chart, see [Donut chart](#).

The table after the Donut chart lists the devices and displays their health state, power state, name, IP address and identifier. By default all the devices are listed, however when a group is selected in the left pane only the devices of that group are displayed. For more information about the device list, see [Device list](#).

The **Advanced Filters** can be used to further narrow down the devices displayed in the Device List based on their Health State, Power State, Connection status, Name, IP Address, Identifier, Device type, Managed state, etc.

When you select a device in the list, the right pane displays the preview about the selected devices. When multiple devices are selected, the preview about the last selected device is displayed. Under **Quick Actions**, the management links that are correlated to the respective device are listed. To clear selections, click **Clear Selection**.

NOTE:

- After you upgrade OpenManage Enterprise to the latest version, the devices list will be updated after the discovery jobs are rerun.
- You can select a maximum of 25 devices per page and navigate the pages to select more devices and perform tasks.
- Some of the device-related tasks that you can perform on the All Devices page—such as firmware update, inventory refreshing, status refreshing, server control actions—can also be performed on individual devices from the respective **Device Details** page.

Topics:

- [Organize devices into groups](#)
- [Devices list](#)
- [All Devices page — device list actions](#)
- [View and configure individual devices](#)

Organize devices into groups

In a data center, for effective and quick device management, you can:

- Group the devices. For example, you can group devices based on functions, OSs, user profiles, location, jobs run, and then run queries to manage devices.
- Filter the device-related data while managing devices, updating firmware, discovering devices, and managing alert policies and reports.
- You can manage the properties of a device in a group. See [View and configure individual devices](#) on page 72.

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

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

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

NOTE: The health status of a device or group is indicated by appropriate symbols. The health status of a group is the health of a device in a group that has the most critical health status. For example, among many devices in a group, if the health of a server is Warning then the group health is also 'Warning'. The rollup status is equal to the status of the device that has high severity. For more information about Rollup Health status, see the *MANAGING THE ROLLUP HEALTH STATUS BY USING iDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* technical white paper on the Dell TechCenter.

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

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

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

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

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

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

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

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

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

NOTE: Static and Query groups:

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

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

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

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

To delete the child group of a Static or Query group:

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

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

Related tasks

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

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

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

Create a custom group (Static or Query)

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

Prerequisites

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

Steps

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

Results

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

Create a Static device group

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

About this task

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

Steps

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

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

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

Results

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

Create a Query device group

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

Prerequisites

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

About this task

Steps

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

Select a query criteria

About this task

Define filters while creating query criteria for:

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

Define the query criteria by using two options:

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

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

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

Steps

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

Related information

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

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

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

Edit a static group

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

Prerequisites

- NOTE:**
- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See [Role and scope-based access control in OpenManage Enterprise on page 18](#).
 - Removal of groups from hierarchical static groups, does not affect any tasks that are scheduled on them. Any scheduled tasks, such as Blink device, Power Control, and Remote Command Change Virtual console will continue to run on the groups even when the groups are removed from the hierarchy.

Steps

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

Results

The changes made to the static group are implemented.

Edit a query group

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

Prerequisites

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

Steps

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

Results

The changes made to the query group are implemented.

Rename a static or query group

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

Steps

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


Delete a static or query device group

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

Prerequisites

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

About this task

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

Steps

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


Results

The group is deleted from the CUSTOM GROUPS.

Clone a static or query group

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

Prerequisites

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

Steps

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

Add devices to a new group


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

Prerequisites

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

Steps


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

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

Add devices to existing group

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

Prerequisites

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


Steps

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

All Devices page is displayed.

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




The devices are added to the selected existing group.

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

Refresh health on group

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

Prerequisites

-  **NOTE:**
- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See [Role and scope-based access control in OpenManage Enterprise](#) on page 18.
 - For the in-band devices discovered using the ESXi and Linux operating systems, the Health State () is displayed as Unknown ()

Steps


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

Results

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

Devices list

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

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

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

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

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

NOTE: In the Devices list, click the device name or IP address to view device configuration data, and then edit. See [View and configure individual devices on page 72](#).

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

All Devices page — device list actions

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

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

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

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

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

Delete devices from OpenManage Enterprise

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

About this task

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See [Role and scope-based access control in OpenManage Enterprise on page 18](#).
- A device on which a profile is assigned cannot be deleted unless the profile is unassigned from it. For more information, see [Unassign profiles on page 113](#).
- A device can be deleted even when tasks are running on it. Any tasks initiated on a device fails if the device is deleted before the completion of the tasks.

To delete the discovered devices:

Steps

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

Results

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

Related information

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

Exclude devices from OpenManage Enterprise

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

Prerequisites

NOTE:

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

About this task

Steps

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

Results

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

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

Run inventory on devices

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

Prerequisites

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

Steps

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

Results

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

Update the device firmware and drivers by using baselines

About this task


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

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See *Role and scope-based access control in OpenManage Enterprise* on page 18.
- Driver updates are applicable only for devices associated with 64-bit Windows versions.
- Driver updates on the devices cannot be rolled back.
- If the firmware update is done using the '**Stage for next server reboot**' option, then the inventory and baseline check must be executed manually after the package is installed in the remote device.
- If the device is not associated with any baseline, the **Baseline** drop-down menu is not populated. To associate a device to a baseline, see *Creating the firmware baseline*.
- If you select multiple devices, only the devices that are associated with the selected baseline are listed in the table.

Steps

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

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

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

- a. In the **Select Update Source** section select one of the following:
 - From the **Baseline** drop-down menu, select the baseline. A list of devices that are associated with the selected baseline is displayed. The compliance level of each device is displayed in the 'compliance' column. Based on the compliance level, you can update the firmware and/or driver version. For information about the field description on this page, see [Viewing device firmware compliance report](#).
 - i. Select the check boxes corresponding to the devices that must be updated.
 - ii. Click **Next**.
 - You can update the firmware and/or drivers by using Individual Update package also. Click **Individual Package**, and then complete the on-screen instructions. Click **Next**.
- b. In the **Schedule** section:
 - Under **Schedule Update**, click **Additional Information** to view the important information and select one of the following:
 - a. **Update Now:** To apply the firmware/driver updates immediately.
 - b. **Schedule Later:** To specify a date and a time when the firmware and/or driver version must be updated. This mode is recommended if you do not want to disturb your current tasks.
 - Under **Server Options** select one of the following reboot options :
 - a. To reboot the server immediately after the firmware/driver update, choose **Reboot server immediately** and from the dropdown menu select one of the following options:
 - i. **Graceful Reboot without Forced Shutdown**
 - ii. **Graceful Reboot with Forced Shutdown**
 - iii. **PowerCycle** for a hard reset of the device.
 - b. Select **Stage for next server reboot** to trigger the firmware/driver update when the next server reboot happens. If this option is selected, then the inventory and baseline check must be executed manually after the package is installed in the remote device.

3. Click **Finish**.

Results

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

Refresh the device health of a device group

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

Steps

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

Results

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

Related information



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

Refresh health on devices

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

Prerequisites

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See [Role and scope based access control in OpenManage Enterprise](#) on page 18.
- For the in-band devices discovered using the ESXi and Linux operating systems, the Health State () is displayed as Unknown ()

Steps

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

Results

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

Roll back an individual device's firmware version

About this task


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


NOTE:

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

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

Steps

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


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

Export the single device inventory

About this task

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

Steps

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

Performing more actions on chassis and servers

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

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

Hardware information displayed for MX7000 chassis

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

Export all or selected data

About this task

You can export data:

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

NOTE:

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

Steps

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

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

View and configure individual devices

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

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

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

- View information about the health and power status, device IP, and Service Tag.
 - View general information about the device and perform device control and troubleshooting tasks.
 - View device information such as RAID, PSU, OS, NIC, memory, processor, and storage enclosure. OpenManage Enterprise provides a built-in report to get an overview about the NIC, BIOS, Physical Disk and Virtual Disk used on the devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise > Monitor > Reports**.
 - Update or roll back firmware versions of components in a device that are associated with a firmware baseline. See [Manage the device firmware and drivers on page 80](#).
- NOTE:** Updating a device using the Individual Package workflow only supports executable (EXE) based Dell Update Packages. When updating an FX2 CMC, the executable DUP must be installed via one of the sleds in the chassis.
- Acknowledge, export, delete, or ignore the alerts pertaining to a device. See [Managing device alerts](#).
 - View and export hardware log data of a device. See [Managing individual device hardware logs on page 75](#).
 - View and manage the configuration inventory of the device for the purposes of configuration compliance. A compliance comparison is initiated when the configuration inventory is run against the devices.
 - View the compliance level of a device against the configuration compliance baseline it is associated with. See [Managing the device configuration compliance on page 116](#).

Device Overview

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