

Dell OpenManage Enterprise 4.5

User's Guide

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Revision history

The following table shows the revision history of this document:

Table 1. Revision history in OpenManage Enterprise 4.5

Revision	Date	Description
A00	July 2025	Initial release.

Preface

As part of an effort to improve product lines, new versions of software are released periodically. Therefore, some versions of the software that are available may not support functions that are described in this document. The product release notes provide the most up-to-date information about product features.

Contact your technical support professional if a product does not function properly or does not function as described in this document.

 **NOTE:** This document was accurate at publication time. Go to [Dell Online Support](#) to ensure that you are using the latest version of this document.

Purpose

This guide provides an overview of the security configuration controls and settings available in OpenManage Enterprise. It aims to facilitate secure deployment, usage, and maintenance of OpenManage Enterprise.

This document includes conceptual information about managing OpenManage Enterprise.

Audience

This document is intended for use by administrators, device managers, and viewers who use OpenManage Enterprise for systems management and monitoring.

Related documentation

The following publications provide additional information:

- OpenManage Enterprise Release Notes.
- OpenManage Enterprise Security Configuration Guide.
- OpenManage Enterprise User's Guide.
- [OpenManage Enterprise RESTful API](#).
- [OpenManage Enterprise 4.x.x Support Matrix](#).
- OpenManage Enterprise Modular Edition Release Notes.

In addition to the core documents, white papers, plug-in documentation, and demos on YouTube are available.

Typographical conventions

This document uses the following style conventions:

Table 2. Typographical conventions

Typographical conventions	Description
Bold	Names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths.
<i>Italic</i>	Full titles of publications referenced in the text.
Monospace	• System code • System output, such as an error message or script • Path names, filenames, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Variables.
Monospace bold	User input.

Table 2. Typographical conventions (continued)

Typographical conventions	Description
[]	Square brackets enclose optional values.
	Vertical bars indicate different selections - the bar means "or".
{ }	Braces enclose content that the user must specify, such as x or y or z.
...	Ellipses indicate nonessential information that is omitted from the example.

Product documentation

NOTE: For video demos and tutorials, search for the [Dell OpenManage Enterprise playlist](#) on **YouTube**, or see the following videos for demos of the **OpenManage Enterprise Graphical User Interface (GUI)** in action:

- [OpenManage Enterprise overview](#) (09:47 min)
- [Creating a firmware baseline in OpenManage Enterprise](#) (01:21 min)
- [OpenManage Enterprise systems management console](#) (03:01 min)
- For **OpenManage Enterprise**, go to [Enterprise Systems Management](#). To display the documentation of:
 - OpenManage Enterprise: Click **Dell OpenManage Enterprise > Dell OpenManage Enterprise > Documentation**.
 - OpenManage Mobile: Click **OpenManage Mobile > Select the required version > Documentation**.
- For **OpenManage Enterprise plugins**, go to [Enterprise Systems Management](#). To display the documentation of:
 - OpenManage Enterprise Services plugin: Click **OpenManage Enterprise Connected Services > OpenManage Enterprise Services > Documentation**.
 - OpenManage Enterprise Update Manager plugin: Click **OpenManage Enterprise Update Manager > OpenManage Enterprise Update Manager > Documentation**.
 - APEX AIOps Infrastructure Observability plugin: Click **OpenManage Enterprise Connected Services > APEX AIOps Infrastructure Observability > Documentation**.
 - VMM and Configuration Manager (Integration for Microsoft SCVMM and MCM): Click **OpenManage Enterprise Integration with Microsoft SCVMM and MECM > OpenManage Enterprise VMM and Configuration Manager > Documentation**.
 - OpenManage Enterprise Operations Manager (Integration for Microsoft System Center): Click **OpenManage Enterprise Integration with Microsoft SCOM > OpenManage Enterprise Operations Manager > Documentation**.
 - OpenManage Enterprise Integration for VMware vCenter (OMEVV): Under **Software**, click **Virtualization Solutions**, and then click **OpenManage Enterprise Integration for VMware vCenter > Documentation**.
- For **OpenManage Enterprise APIs**, go to [Dell Technologies developers portal](#). To display the API documentation of:
 - OpenManage Enterprise: Click **Servers > OpenManage Enterprise**
 - OpenManage Enterprise Modular Edition: Click **Servers > OpenManage Enterprise Modular**
 - OpenManage Enterprise Services plugin: Click **Servers > OpenManage Enterprise Services**
 - OpenManage Enterprise Update Manager plugin: Click **Servers > OpenManage Enterprise Update Manager**
 - OpenManage Enterprise Integration for VMware vCenter (OMEVV): Click **Servers > OpenManage Enterprise Integration for VMWare vCenter Plug-in**
 - VMM and Configuration Manager (Integration for Microsoft SCVMM and MCM): Click **Servers > OpenManage Enterprise SCVMM and MECM**
 - OpenManage Enterprise Operations Manager (Integration for Microsoft System Center): Click **Servers > OpenManage Enterprise Operations Manager**

Product information

For documentation, release notes, software updates, or information about products, go to **Online Support** at [Dell support](#).

Where to get help

Go to **Online Support** at [Dell support](#) and click **Contact Support**. To open a service request, you must have a valid support agreement. Contact your sales representative for details about obtaining a valid support agreement or with questions about your account.

 **NOTE:** For quick access to the content of the *OpenManage Enterprise User's Guide*, open the *OpenManage Enterprise Online Help* by clicking the **?** icon in the upper-right corner of a screen in the product UI.

Revision history.....	3
Preface.....	4
Chapter 1: Overview.....	16
New features.....	17
Licensing.....	18
Security.....	20
Scalability and performance.....	20
OpenManage Enterprise plug-ins.....	21
Chapter 2: Deployment.....	23
Host system requirements.....	24
Deployment prerequisites.....	24
OpenManage Enterprise hardware requirements.....	25
Network and access requirements.....	26
Management ports and protocols.....	27
Device ports and protocols.....	28
Firewall exceptions.....	29
Deployment best practices.....	30
Deploy in VMware vSphere.....	31
Deploy in Microsoft Hyper-V.....	32
Deploy in KVM	33
Deploy in KVM using virt-install.....	34
Deploy programmatically.....	35
Configure the system using the TUI.....	37
Chapter 3: Getting started.....	41
Log in to an appliance.....	41
Initial onboarding	42
The Welcome to OpenManage Enterprise dialog.....	42
The OpenManage Enterprise GUI.....	43
The OpenManage Enterprise menu bar.....	45
The OpenManage Enterprise dashboard.....	46
Doughnut charts.....	47
Device health statuses.....	48
The OpenManage Enterprise home screen.....	48
Chapter 4: System configuration.....	50
Configure network settings.....	50
Manage roles and privileges.....	51
User roles.....	52
Role and scope-based access.....	52
Add custom roles.....	59
Edit custom roles.....	60
Delete custom roles.....	60

Manage users and scopes.....	60
Add or edit local users.....	61
Edit OpenManage Enterprise user properties.....	62
Enable OpenManage Enterprise users.....	62
Disable OpenManage Enterprise users.....	63
Delete OpenManage Enterprise users.....	63
Import Active Directory and LDAP groups.....	63
Transfer of ownership of user entities.....	64
Ending user sessions.....	65
Directory services integration.....	65
Add or edit the Active Directory connection.....	66
Add or edit LDAP connection.....	67
Delete Directory services.....	68
Login using OIDC providers.....	68
Add an OIDC provider.....	70
Configure OIDC login using PingFederate.....	71
Configure OIDC login using Keycloak.....	72
Test OIDC registration.....	72
Edit an OIDC providers details.....	73
Enable OIDC providers.....	73
Delete OIDC providers.....	73
Disable OIDC providers.....	73
Security certificates.....	74
Generate and download a certificate signing request.....	74
Assign a web server certificate to an appliance.....	74
Manage console settings.....	75
Internal iDRAC credential management.....	79
Enable internal OME password rotation feature.....	80
Enable CyberArk integration for password management.....	80
Set the login security properties.....	81
Customize the alert display.....	83
Configure SMTP, SNMP, and Syslog.....	83
Manage incoming alerts.....	84
Important points to consider for SNMP listener profile configuration.....	86
Manage warranty settings.....	86
Configure remote commands and scripts.....	86
OpenManage Mobile settings.....	87
Enable or disable alert notifications for OpenManage Mobile.....	88
Enable or disable OpenManage Mobile subscribers.....	88
Delete an OpenManage Mobile subscriber.....	89
View the alert notification service status.....	89
Notification service status.....	89
View information about OpenManage Mobile subscribers.....	90
OpenManage Mobile subscriber information.....	90
Troubleshooting OpenManage Mobile.....	91
Chapter 5: Discovering devices.....	92
Server-initiated discovery	93
Creating and managing device discovery jobs.....	95
Create a device discovery job.....	95

View device discovery job details.....	105
Edit a device discovery job.....	106
Run a device discovery job.....	106
Stop a device discovery job.....	106
Delete a device discovery job.....	107
Onboarding devices.....	107
Protocol support matrix for device discovery and alert reception.....	109
Chapter 6: Managing devices and device groups.....	111
Create and manage custom groups.....	113
Create a custom static or query group.....	113
Create a static device group.....	114
Create a query device group.....	114
Edit a static group.....	115
Edit a query group.....	116
Rename a static or query group.....	116
Delete a static or query device group.....	116
Clone a static or query group.....	117
Add devices to a new group.....	117
Add devices to existing group.....	118
Refresh health on group.....	118
View devices associated with system and workload profiles.....	119
Manage physical groups.....	119
Rack management.....	120
Add or edit device details for power-monitored devices.....	120
Create physical groups in OpenManage Enterprise.....	121
Automatically create physical hierarchy.....	123
View physical groups and the hierarchies.....	124
View devices added in rack.....	124
View rack group information.....	125
Manage rack power operations.....	126
Edit physical groups.....	126
Manage physical groups.....	126
Delete physical group.....	127
Rearrange rack slot of devices.....	127
Move device to different rack.....	128
Remove device from rack.....	129
Power Distribution Unit.....	129
Associate PDU and UPS to rack	130
View PDU and UPS associated to rack.....	131
Remove PDU and UPS devices.....	133
All Devices screen device list.....	134
All Devices screen actions.....	134
Delete devices from OpenManage Enterprise.....	136
Exclude devices from OpenManage Enterprise.....	137
Run inventory on devices.....	137
Update the device firmware and drivers by using baselines.....	138
Refresh the device health of a device group.....	139
Refresh health on devices.....	140
Roll back an individual device's firmware version.....	140

Export the single device inventory.....	141
Performing more actions on chassis and servers.....	141
Hardware information displayed for MX7000 chassis	142
Export data.....	142
View and configure individual devices.....	142
View device inventory.....	143
Run and download diagnostic reports.....	147
Extract and download a Services report.....	148
Managing individual device hardware logs.....	148
Run remote commands on managed devices.....	149
Launch the iDRAC device management application.....	150
Launch the virtual console.....	150
Attaching iDRAC virtual media.....	151
Refresh device inventory of a single device.....	151
View installed and available licenses on a device.....	152
Chapter 7: Managing device inventory.....	153
Create an inventory job.....	154
Run an inventory job now.....	154
Stop an inventory job.....	155
Delete an inventory job.....	155
Edit an inventory schedule job.....	156
Chapter 8: Managing device firmware and drivers.....	157
Manage firmware and driver catalogs.....	159
Add a catalog by using Dell.com.....	159
Add a catalog to the local network.....	160
SSL Certificate Information.....	161
Update a catalog.....	161
Edit a catalog.....	161
Delete a catalog.....	162
Create a baseline.....	162
Edit a baseline.....	163
Delete a baseline.....	163
Check the compliance of firmware and drivers.....	163
View the baseline compliance report.....	164
Update the device firmware and drivers.....	165
Chapter 9: Managing device deployment templates.....	168
Create a deployment template from a reference device.....	169
Create a deployment template by importing a template file.....	170
View a deployment template information.....	171
Edit a server deployment template.....	171
Edit a chassis deployment template.....	173
Edit IOA deployment template.....	173
Edit network properties of a deployment template.....	173
Deploy device deployment templates.....	174
Deploy IOA deployment templates.....	177
Clone deployment templates.....	178

Export a deployment template.....	178
Delete deployment templates.....	178
Auto deploy device configuration before discovery.....	179
Create auto deployment targets	180
Delete auto deployment targets	181
Export auto deployed target details.....	182
Overview of stateless deployment.....	182
Managing identity pools for stateless deployment.....	182
Creating identity pools.....	183
Define networks.....	188
Network types.....	188
Edit or delete a configured network.....	189
Export VLAN definitions.....	189
Import network definitions.....	189
Chapter 10: Managing device warranty.....	191
View and renew device warranty.....	191
Internal warranty alerts.....	192
Chapter 11: Managing alerts.....	193
View alert logs.....	193
Manage alert logs.....	194
Alert policies.....	196
Configure and manage alert policies.....	196
Automatic alerts on the MX7000 chassis.....	201
Alert definitions.....	201
Chapter 12: Managing MIB files.....	203
Import MIB files.....	203
Edit MIB traps.....	204
Remove MIB files.....	205
Resolve MIB types.....	205
Download an OpenManage Enterprise MIB.....	205
Chapter 13: Configuring profiles.....	206
Create profiles.....	207
View a profiles details.....	208
View a profiles network.....	208
Edit a profile.....	209
Assign a profile.....	210
Unassign profiles.....	211
Redeploy profiles.....	212
Migrate a profile.....	212
Delete profiles.....	213
Chapter 14: Configuration compliance.....	214
Manage compliance templates.....	215
Create a compliance template from deployment template.....	216
Create a compliance template from reference device.....	217

Create a compliance template by importing from a file.....	217
Clone a compliance template.....	218
Edit a compliance template.....	218
Create a configuration compliance baseline.....	218
Edit a configuration compliance baseline.....	220
Delete configuration compliance baselines.....	220
Refresh compliance of the configuration compliance baselines	220
Remediate noncompliant devices	221
Export a compliance baseline report.....	222
Remove a configuration compliance baseline.....	222
Chapter 15: Managing licenses.....	224
Obtain licenses by connecting to Dell Digital Locker account.....	225
Import licenses.....	226
Bind licenses.....	226
Deploy licenses	227
Export licenses.....	228
Disconnect from Dell online.....	228
Delete licenses from OpenManage Enterprise.....	229
Chapter 16: Using jobs for device control.....	230
Create and manage jobs.....	230
View job lists.....	230
Jobs status and Jobs type description.....	231
Default jobs and job schedules.....	233
View job details.....	235
Create a job to blink device LEDs.....	236
Create a job for controlling device power.....	236
Create a remote command job for managing devices.....	237
Create a job to change the virtual console plugin type.....	238
Select target devices and device groups.....	238
Manage jobs.....	239
Chapter 17: Monitoring audit logs.....	240
Filtering audit logs.....	240
Exporting audit logs.....	241
Forward audit logs to remote Syslog servers.....	241
Chapter 18: Monitoring reports.....	243
Run reports.....	244
Run and email reports.....	245
Edit reports.....	245
Schedule and delivery options for reports.....	246
Copy reports.....	246
Delete reports.....	247
Create a report.....	247
Select the query criteria.....	248
Export selected reports.....	249
View and remove report schedule details.....	249

Chapter 19: Manage the Power Management features	251
Monitor and manage devices for power.....	251
Overview.....	252
View top ten power offenders.....	252
View top ten temperature offenders.....	253
View top ten underutilized racks for power and space.....	253
View power and space headroom.....	254
View power history of virtual machines and virtual machine groups.....	254
View idle servers.....	254
View devices and groups added for power management and monitoring.....	255
Add devices for power management and monitoring.....	256
Add static groups for power management and monitoring.....	258
Create physical groups through CSV file.....	260
Virtual machines.....	260
View virtual machines and virtual machine groups.....	261
Create virtual machine groups.....	262
Edit virtual machine groups.....	262
Delete virtual machine groups.....	262
View details of Unmonitored Devices.....	263
Add unmonitored device details.....	263
Edit Unmonitored Devices details.....	264
Delete Unmonitored Devices.....	264
Policies.....	265
Static policy.....	265
Temperature-triggered policy.....	265
Create static or temperature-triggered policy.....	265
View policy.....	269
Edit policy.....	269
Disable policy.....	270
Enable policy.....	270
Delete policy.....	271
Manage data center during power reduction.....	271
Enable Emergency Power Reduction.....	271
View active Emergency Power Reduction.....	273
Disable Emergency Power Reduction.....	273
View racks of physical groups.....	274
Compare server usage metrics.....	274
Analyze multivariate metrics using parallel coordinates.....	275
Set preferences.....	275
View metrics, and monitor devices and groups history.....	279
Monitor Graphics Processing Unit (GPU).....	283
Monitor Power Supply Unit (PSU).....	284
Monitor Central Processing Unit (CPU).....	284
Thresholds.....	284
Create alert thresholds.....	284
View alert thresholds.....	286
Edit alert thresholds.....	287
Delete alert thresholds.....	288

Chapter 20: Back up or restore.....	290
Appliance states.....	290
Backup an appliance.....	291
Restore an appliance.....	292
Chapter 21: Updating the console and plugins.....	294
Update prerequisites.....	295
Online update.....	296
Define online update settings.....	296
Update the appliance from dell.com.....	296
Configuring a local network share for offline update.....	297
Create the directory structure and download the update bundles.....	297
Configure an NFS network share on a Windows server.....	298
Configure an NFS network share on a Linux server.....	299
Configure an HTTP network share on a Windows server.....	299
Enable read and write access to your network share.....	301
Offline update.....	301
Download update files to local network share.....	302
Initiate update from a network share.....	303
System-generated postupgrade task	304
Chapter 22: Managing plugins.....	305
Install plugins.....	306
Enable plugins.....	306
Update plugins.....	307
Disable plug-ins.....	308
Uninstall plugins.....	308
Appendix A: Troubleshooting.....	310
Devices.....	310
Supported and unsupported actions on proxied sleds.....	310
Devices with unknown compliance status.....	311
Decommissioned or duplicate device entries in the discovery job.....	311
PowerEdge server displays multiple iDRAC management IPs in OpenManage Enterprise.....	311
Devices not getting removed from nested static groups after deleting from the parent group.....	312
Discovery.....	312
Device rediscovery running for a long time after deleting iDRAC service account.....	312
Troubleshooting power shelf onboarding failures.....	312
SONiC switch discovery or inventory fails.....	312
Onboarding job fails with error CUSR6004	313
Alerts.....	313
Alert categories after EEMI relocation.....	313
Token substitution in alert policy actions.....	314
Configurations.....	315
Firmware and DSU requirements for HTTPS.....	315
Firmware schedule reference.....	316
Firmware baseline field definitions.....	316
Schedule job field definitions.....	316

Monitor.....	317
Misleading global health task status.....	317
Troubleshooting connectivity.....	317
Plugins.....	320
Plugin does not meet minimum requirements.....	320
Application Settings.....	320
Unable to create new users or edit existing users.....	320
Catalog Management field definitions.....	320
iDRAC virtual console fails to launch in OpenManage Enterprise.....	320
Upgrade.....	321
User roles lost during upgrade.....	321
Troubleshooting the Power Management features.....	321
The Power Management feature Frequently asked questions.....	323
Appendix B: Appendix.....	328

Overview

OpenManage Enterprise is a one-to-many systems management and monitoring web application that is delivered as a virtual appliance. It provides a comprehensive view of the Dell servers, chassis, storage, other third-party devices and components, and network switches, on the enterprise network. It is designed for the next generation IT professionals with a focus on simplicity, automation, and unification of data center management.

With OpenManage Enterprise, users can:

- Discover devices in a data center environment.
- View hardware inventory and monitor the health of devices.
- View and manage alerts that are received by the appliance and configure alert policies.
- Monitor firmware/driver versions.
- Manage firmware/driver updates on devices with firmware baselines.
- Manage remote tasks (such as power control) on devices.
- Manage configuration settings across devices using deployment templates.
- Configure and manage virtual identities for multiple devices efficiently using identity pools.
- Detect and remedy configuration deviations across devices using configuration baselines.
- Retrieve and monitor warranty information for devices.
- Group devices into static or dynamic groups.
- Create and manage OpenManage Enterprise users.
- Back up and restore appliances.
- Manage and monitor power using the Power Management feature on licensed devices, static groups, physical groups, system profile, workload profile, virtual machines, and virtual machine groups.
- View data about power consumption, carbon emissions, system anomalies, and resource utilization on servers.
- Monitor device metrics using parallel coordinate visualization.

NOTE:

- OpenManage Enterprise does not support managing a single device through multiple OpenManage Enterprise instances. Doing this can lead to failures (that is, Profile deployment failure, I/O identity conflicts, so forth).
- OpenManage Enterprise's system management and monitoring is best suited for enterprise LANs and is not recommended for usage over WANs.
- For information about supported browsers, see the *OpenManage Enterprise Support Matrix* on the support site.

OpenManage Enterprise contains security features like:

- Role-based access that limits access to console settings and device actions.
- Scope-based access control allowing administrators to restrict the device groups that device managers can access and manage.
- A hardened appliance with Security-Enhanced Linux (SELinux) and an internal firewall.
- Encryption of sensitive data in an internal database.
- Use of encrypted communication outside the appliance (HTTPS).
- Creation of firmware and configuration-related policies.
- Provision for configuring and updating the bare-metal servers.

OpenManage Enterprise has a task-based UI, where the navigation is designed by considering the sequence of tasks that are predominately used by an administrator, device manager, and a custom role user. When you add a device to an environment, OpenManage Enterprise automatically detects the device properties, places it under the relevant device groups, and enables you to manage the device.

OpenManage Enterprise users perform tasks in the following sequence.

1. [Deployment](#)
2. [Configure the system using the TUI](#)
3. [Discovering devices](#)
4. [Managing devices and device groups](#)
5. [The OpenManage Enterprise dashboard](#)

6. [Create and manage custom groups](#)
7. [Managing device firmware and drivers](#)
8. [View and configure individual devices](#)
9. [Managing alerts](#)
10. [View and renew device warranty](#)
11. [Managing device deployment templates](#)
12. [Configuration compliance](#)
13. [Manage compliance templates](#)
14. [Monitoring audit logs](#)
15. [System configuration](#)
16. [Run an inventory job now](#)
17. [Managing device warranty](#)
18. [Monitoring reports](#)
19. [Managing MIB files](#)
20. [Role and scope-based access](#)
21. [Directory services integration](#)

Topics:

- [New features](#)
- [Licensing](#)
- [Security](#)
- [Scalability and performance](#)
- [OpenManage Enterprise plug-ins](#)

New features

The following features and enhancements were added in this release:

Table 3. New features in OpenManage Enterprise 4.5

Functional area	Feature name	Feature description
Security enhancements	Support for SHA-384 and SHA-512 hash algorithms	You can now select SHA-384 and SHA-512 cryptographic hash algorithms when generating Certificate Signing Requests (CSRs), enhancing data protection. Signed certificates can be uploaded into OpenManage Enterprise.
Security enhancements	AES-256 Encryption for Credentials	Credentials are now encrypted using the AES-256 symmetric encryption algorithm.
Integration	Integration of Power Manager plugin into OpenManage Enterprise	All Power Manager features are now built into the OpenManage Enterprise interface. A separate plugin is no longer required.
Deployment and system requirements	Increased RAM requirement due to the integration of Power Manager plugin into OpenManage Enterprise	Due to the integration of Power Manager, OpenManage Enterprise now requires: • 40 GB RAM for large deployments (up to 8,000 devices) • 19 GB RAM for smaller deployments (up to 1,000 devices) Additional RAM is recommended for plugin installations. Refer to the <i>OpenManage Enterprise and plugins hardware requirements</i> section in the user guide for details.
Scalability and performance	Improved scalability for discovery and inventory	Discovery, inventory, and health collection tasks now run asynchronously, improving performance and scalability in large environments.
Live message notification	In-console system messages	Dell can now send critical, warning, and informational messages directly to users. These

Table 3. New features in OpenManage Enterprise 4.5 (continued)

Functional area	Feature name	Feature description
		appear as banners in the console, similar to upgrade notifications, and provide timely updates, known issue workarounds, and other important information.
Support	Azure Stack HCI 23H2 on PowerEdge R760	Enables discovery, inventory, monitoring, and alerting for PowerEdge R760 servers running Azure Stack HCI 23H2.
Support	Azure Stack HCI 24H2	Enables discovery, inventory, and alerting for platforms running Azure Stack HCI 24H2.
Support	Dell ToR switches with SONiC operating system	Supports discovery, inventory, and status monitoring for Dell Top-of-Rack switches running the SONiC operating system.
Support	Rack management for power shelves (Delta 21-inch and Lite-On 21-inch)	Enables discovery, inventory, monitoring, rack management, and SNMP alerting for power shelves.
Support	New hardware and operating system support	Adds support for new hardware models and operating system versions. For details, see the latest support matrix.
Power management	Staggered power operation for rack group	Added support for performing a staggered power on or power off operation for rack groups.
Power management	Power management setting for data gathering	Added a setting to enable data gathering on monitored devices.
Power management	Automatic grouping based on physical hierarchy	Added support for automatically adding the devices to groups based on the physical hierarchy.
Power management	Support for GPU and CPU data for rack groups	Added support for rack-level GPU and CPU reporting.
Power management	GPU metrics	Added support for new GPU metrics.
Power management	Carbon emission metrics	Added support for carbon emission metrics.

Licensing

Describes the features that require OpenManage Enterprise Advanced and Advanced+ license .

Installing and using OpenManage Enterprise does not require the *OpenManage Enterprise Advanced* or *OpenManage Enterprise Advanced+* license. However, an *OpenManage Enterprise Advanced* or *Advanced+* license provides support for additional advanced automation and configuration features. The *OpenManage Enterprise Advanced* or *Advanced+* are perpetual licenses that are valid for the life of a server and can be bound to the Service Tag of only one server at a time. For information about viewing a list of managed devices and their licenses, see [Run reports](#).

Enabling the server configuration management feature in OpenManage Enterprise does not require any separate license. If the *OpenManage Enterprise Advanced* or *Advanced+* license is installed on a target server, you can use the server configuration management feature on that server.

License-based features

Here are the licensing requirements to use the following features in OpenManage Enterprise:

Table 4. License requirements for PowerEdge servers

Feature	PowerEdge 16G servers and below	PowerEdge 17G servers and above
Deploy automatically with service tag or node IDs (Auto deploy)	Advanced license	Advanced license along with either an iDRAC Enterprise or Datacenter license
MX platform profile management	Advanced license	Advanced license
Power Management	Advanced license	Advanced license
Monitor and enforce configuration compliance	Advanced license	Advanced license along with either an iDRAC Enterprise or Datacenter license
Virtual address management and stateless provisioning (Identity Pools)	Advanced license	Advanced license along with either an iDRAC Enterprise or Datacenter license
VLAN management	Advanced license	Advanced license
Boot to ISO	Advanced license	Advanced license along with either an iDRAC Enterprise or Datacenter license
Server configuration deployment	Advanced license	Advanced license along with either an iDRAC Enterprise or Datacenter license
Server configuration compliance baseline creation and remediation	Advanced license	Advanced license along with either an iDRAC Enterprise or Datacenter license
iDRAC password management	Advanced license	Advanced license

OpenManage Enterprise Advanced+ license Features: The *OpenManage Enterprise Advanced+* license contains all the features of *OpenManage Advanced license*.

Table 5. Advanced+ License Features

Feature	License requirement
Support for all partner plugins (VMware vCenter plugin, Microsoft System Center plugins)	OpenManage Enterprise Advanced+ license.  NOTE: Plugin workflows that use OpenManage Enterprise features, such as Boot to ISO and Server configuration deployment, require an Advanced license along with either an iDRAC Enterprise or Datacenter license for successful execution.
Support for partner integration (ServiceNow integration, CyberArk integration)	OpenManage Enterprise Advanced+ license

 NOTE:

- To access features of OpenManage Enterprise such as the Virtual Console Support function, which depends on the target iDRAC device, you would need an iDRAC enterprise license. For more details, see the iDRAC documentation available on the support site.
- License-based features for PowerEdge 17G servers, using iDRAC 10, are supported with firmware version 1.20.25.00 or later.
- CyberArk integration for password management and ServiceNow integration are not supported for 17G, iDRAC 10 based, PowerEdge servers.

Supported servers

You can deploy the *OpenManage Enterprise Advanced* or *Advanced+* license on the following PowerEdge servers:

- 14G and above servers that have the iDRAC9 3.10.10.10 or later firmware versions.

Purchasing a license

You can purchase the *OpenManage Enterprise Advanced* or *Advanced+* license when you purchase a server or by contacting your sales representative. You can download the purchased license from the **Software License Management** screen at Dell.com/support/retail/lkm.

Verify license information

OpenManage Enterprise provides an integrated report to view the list of devices monitored by OpenManage Enterprise, and their licenses. Click **Monitor > Reports > License Report**. Click **Run**. See [Run reports](#). You can verify if the *OpenManage Enterprise Advanced* or *Advanced+* license is installed on a server by:

- On all screens of OpenManage Enterprise, in the upper-right corner, click the **i** symbol, and then click **Licenses**.
- In the **Licenses** dialog box, read through the message and click appropriate links to view and download OpenManage Enterprise related open-source files, or other open-source licenses.

Security

OpenManage Enterprise enables you to securely manage devices using Role-based and Scope-based access control (RBAC and SBAC) using a hardened appliance with end-to-end encryption.

Some of the security features of OpenManage Enterprise are:

- By using Role-based access control, one can assign various management permissions to end-users based on their role within your organization. Built-in roles include: Super Administrator, Administrator, Device Manager, and Viewer. Additionally, custom roles can be created to further customize user privileges.
- Scope-based access control allows an administrator to determine the device groups that the device managers or custom role users are expected to manage.
- The appliance is hardened with Security-Enhanced Linux (SELinux) and an internal firewall.
- Sensitive data is encrypted in an internal database.
- All communication outside the appliance (HTTPS) is encrypted.
- Only browsers with 256-bit encryption are supported. For more information, see [Host system requirements](#).

NOTE:

- Any change to the user role takes effect immediately and the impacted user is logged out of their active session.
- AD and LDAP directory users can be imported and assigned to one of the OpenManage Enterprise roles (Administrator, Device Manager, Viewer, or custom created user role).
- Running device management actions requires an account with appropriate privileges on the device.

Scalability and performance

The following table lists the performance parameters of the supported features in OpenManage Enterprise. Dell Technologies recommends running tasks at the frequency and scale that is mentioned below.

Table 6. Scalability and performance

Tasks	Recommended frequency of running the tasks	Predefined task?	Maximum devices that are recommended per task.	Job Name	Frequency	Scope
Discovery	Run the task everyday if the environment has frequent network changes.	No (user-defined)	10,000/task	User-defined	Choose a schedule between Run Now, Run Later, or Run on a Schedule.	User-defined.
Inventory	Everyday	Yes	OpenManage Enterprise monitored devices.	Default Inventory Task	Everyday	OpenManage Enterprise managed devices.

Table 6. Scalability and performance (continued)

Tasks	Recommended frequency of running the tasks	Predefined task?	Maximum devices that are recommended per task.	Job Name	Frequency	Scope
Warranty	Everyday	Yes	OpenManage Enterprise monitored devices.	Warranty Task	Everyday	OpenManage Enterprise managed devices.
Health poll	Hourly	Yes	Not applicable	Global Health Task	Hourly. Users can modify how often this job runs.	OpenManage Enterprise managed devices.
Firmware or Driver update	Need-basis	No	150/task	Device Update: <Baseline Name>	User-defined	User-defined.
Configuration inventory	Need-basis	Yes	8,000/baseline	Configuration Inventory	Everyday	All devices that are assigned to a configuration baseline.
Bind and Deploy Licenses	Need-basis	No	1000	Bind Entitlements and Deploy License Task	User-defined	Based on the selected license name and subsequent applicable nodes that are managed on the appliance.
Metric task	System defined	Yes	8000	Metric task	- For devices less than 1000, 5, 15, and 30 minutes. - For devices more than 1000, 15 and 30 minutes.	Devices added for metric monitoring
Physical Group creation using device location task	Need-basis	No	3000	Creation of Physical hierarchy based on the Device location field	User-defined or automatically initiated after discovery and inventory job	Devices reporting valid location information that are not added to physical hierarchy groups.
Physical Group CSV Import Task	Need-basis	No	3000	Physical Group CSV Import Task	User-defined	Devices that are listed in the CSV file with valid location information and are not added to physical hierarchy groups.

 **NOTE:** Running the physical group creation using the device location information and CSV import tasks with more devices than recommended prolongs the execution time.

OpenManage Enterprise plug-ins

The table lists the available plugins to install in OpenManage Enterprise plug-ins for enhanced capabilities.

The following plug-ins are available:

Table 7. OpenManage Enterprise plug-ins

Plugin name	Description
Services	Enables proactive and predictive monitoring and management support for your devices with ProSupport and ProSupport Plus.
Update Manager	Enables managing custom Repositories and Catalogs of firmware and Windows Driver updates available for Dell PowerEdge servers.
APEX AIOps Infrastructure Observability (formerly called as CloudIQ plugin)	Enables monitoring data and reporting for efficiently managing your Dell devices.
Operations Manager	Enables monitoring of the Dell hardware using the System Center Operations Manager(SCOM) capabilities.
Virtual Machine Manager and Configuration Manager	Enables operating system deployment, firmware update, and Dell servers and modular system maintenance.
OpenManage Enterprise Integration for VMware vCenter	Enables managing physical and virtual servers within vCenter, with features like monitoring, provisioning, and managing your PowerEdge devices.

See [Managing plugins](#) for more information.

Deployment

OpenManage Enterprise is delivered as a ready-to-deploy virtual appliance that runs on a supported hypervisor platform. After deploying the appliance, initial setup is completed through the built-in Text User Interface (TUI) to configure network settings. Once this is done, you can access and manage the application through the intuitive web-based client interface.

To view and update the current OpenManage Enterprise version, see [Updating the console and plugins](#).

Step 1: Understand what you need

Before you begin, ensure your environment meets the following requirements:

- [Host system requirements](#)
- [Maximum recommended hardware configuration](#).
 - You can also determine the hardware requirements based on your deployment size (Small or large deployment). For more details, see [Manage memory and CPU requirements based on deployment size](#)
- [Deployment prerequisites](#)
- [Deployment best practices](#)

Step 2: Network and access requirements

- [Network requirements](#)
- [Port and protocol requirements](#)
- [Firewall and external access](#)

Step 3: Choose your deployment method

Select the platform you want to deploy on:

- [Deploy in VMware vSphere](#)
- [Deploy in Microsoft Hyper-V](#)
- [Deploy in KVM](#)
- [Deploy on KVM using virt-install \(CLI\)](#)
- [Deploy Programmatically](#)

Step 4: Configure the OpenManage Enterprise

Configure the appliance using the TUI

Topics:

- [Host system requirements](#)
- [Deployment prerequisites](#)
- [Deployment best practices](#)
- [Deploy in VMware vSphere](#)
- [Deploy in Microsoft Hyper-V](#)
- [Deploy in KVM](#)
- [Deploy programmatically](#)
- [Configure the system using the TUI](#)

Host system requirements

Ensure that you have the minimum system requirements for deploying OpenManage Enterprise.

NOTE: For the latest list of system requirements, see the most current version of the *OpenManage Enterprise Support Matrix* on the support site.

Table 8. Minimum host system requirements

System components	Minimum requirements
Hypervisors	- VMware vSphere supported on ESXi 8.0, ESXi 8.0 U1, ESXi 8.0 U2, ESXi 8.0 U3, and ESXi 9.0. NOTE: - Secure boot requires a firmware boot option as Extensible Firmware Interface, and is only supported on ESXi 8.0, ESXi 8.0 U1, ESXi 8.0 U2, ESXi 8.0 U3, and ESXi 9.0. - Ensure that any ESXi to be deployed is disconnected from vCenter. - Microsoft Hyper-V Generation 2 virtual machines that are supported on Windows Server 2019 or later. - KVM is supported on Red Hat Enterprise Linux 8.0 or later. - QEMU deployments supported on type q35 and above.
Networks	Available virtual NIC with access to the management networks of all devices managed from OpenManage Enterprise.
Browsers	- Internet Explorer (64-bit) 11 or later - Mozilla Firefox 52 or later - Google Chrome 58 or later - Microsoft Edge version 41.16299 or later
User interfaces	HTML 5, JS-based

Related information

[Deployment](#)

Deployment prerequisites

Requirements for OpenManage Enterprise deployment.

Before you deploy OpenManage Enterprise, ensure:

- You have the necessary rights to deploy a virtual machine within the hypervisor.
- You have access to the Virtual Machine console. This is required to complete the initial setup using the Text User Interface (TUI).
- Your hypervisor system meets the [Host system requirements](#).
- Your appliances must meet the [OpenManage Enterprise hardware requirements](#).
- Your platforms, operating systems, and browsers must meet the minimum requirements that are defined in the most current version of the *OpenManage Enterprise Support Matrix* on the support site.
- Ensure that all necessary subnets are routable to the interface given to the OpenManage Enterprise appliance.
- Ensure that the firmware boot option is set to EFI.

Related information

[Deployment](#)

OpenManage Enterprise hardware requirements

The section provides recommended hardware requirements for OpenManage Enterprise running with and without plug-ins in small and large deployments. For more specific information about plug-in hardware requirements, see the User's Guide of the respective OpenManage Enterprise plug-in.

Maximum recommended hardware configuration

OpenManage Enterprise appliance is shipped with the maximum recommended hardware requirements to provide you with a hassle-free deployment and installation of the appliance and plug-ins respectively. However, if your environment does not require the maximum hardware configuration, see *Manage memory and CPU requirements based on deployment size* below to determine the appropriate hardware resources required for your specific requirements. The following table lists recommended hardware requirements for installing OpenManage Enterprise and all its plugins.

Table 9. Appliance default hardware configuration

Hardware	Configuration
RAM	64 GB
Processor cores	8
Hard drive space	830 GB ^a

- a. • OpenManage Enterprise appliance is configured with two VDs, each with an initial storage space of 415 GB. The primary VD is leveraged for the core application and database while the secondary VD is required for additional features and supporting plugins. However, even without the secondary VDs selected during deployment, the appliance can still boot up for TUI configuration using only the primary VHD.
- Ensure that your hypervisor storage has enough free space to support the recommended virtual disk size of the appliance, and enough overhead to support snapshots and future expansion of the virtual disk.
 - Ensure that the primary disk and the secondary disk are identical in size always.

Manage memory and CPU requirements based on deployment size

If your environment does not require the maximum hardware configuration, review the following table to determine the appropriate hardware resources required for your specific requirements.

Table 10. Large deployment where the maximum number of devices managed by OpenManage Enterprise is up to 8,000

OpenManage Enterprise appliance and plugins	Minimum RAM	Minimum cores
OpenManage Enterprise	40 GB	8
Additional requirements for each plug-in		
APEX AIOps Infrastructure Observability (formerly called as CloudIQ) (Default plug-in)	+4 GB	
Services (Default plug-in)	+8 GB	
Update Manager	+1 GB	
OpenManage Enterprise Integration for VMware vCenter (OMEVV)	+5 GB	
Operations Manager (Integration for Microsoft SCOM)	+3 GB	
VMM and Configuration Manager (Integration for Microsoft SCVMM and MCM)	+1 GB	

Table 10. Large deployment where the maximum number of devices managed by OpenManage Enterprise is up to 8,000 (continued)

OpenManage Enterprise appliance and plugins	Minimum RAM	Minimum cores
Total recommended hardware configuration with all plug-ins installed	64 GB	8 CPU cores

Table 11. Small deployment where the maximum number of devices managed by OpenManage Enterprise is up to 1,000

OpenManage Enterprise appliance and plugins	Minimum RAM	Minimum cores
OpenManage Enterprise	19 GB	4
Additional requirements for each plug-in		
AIOps Infrastructure Observability (Default plug-in)	+2 GB	
Services (Default plug-in)	+8 GB	
Update Manager	+1 GB	
OpenManage Enterprise Integration for VMware vCenter (OMEVV)	+5 GB	
Operations Manager (Integration for Microsoft SCOM)	+3 GB	
VMM and Configuration Manager (Integration for Microsoft SCVMM and MCM)	+1 GB	
Total recommended hardware configuration with all plug-ins installed	40 GB	4 CPU cores

Related information

[Deployment](#)

Network and access requirements

Effective deployment of OpenManage Enterprise also relies on specific network and access configurations.

- **Virtual NIC Access:** OpenManage Enterprise requires an available virtual Network Interface Card (NIC) with access to the management networks of all devices intended for management.
- **Routable Subnets:** All necessary subnets must be routable to the interface assigned to the OpenManage Enterprise appliance.
- **DNS Configuration:** For server-initiated discovery and overall functionality, it is preferred that your DNS environment allows automatic updates from OpenManage Enterprise. Servers should be on the same domain or subdomain as the OpenManage Enterprise appliance. OpenManage Enterprise can be registered with DNS using its Text User Interface (TUI). Old DNS records for the appliance should be cleared to prevent multiple announcements from servers.
- **LAN:** OpenManage Enterprise's system management and monitoring are best suited for enterprise LANs and are not recommended for usage over WANs.

Related information

[Deployment](#)

Management ports and protocols

Provides information about supported ports and protocols running on managed nodes and management stations.

Table 12. Ports and protocols on management stations

Port	Protocol	Type	Encryption	Source	Direction	Destination	Usage
N/A	ICMP	N/A	None	OpenManage Enterprise appliance	Out	Managed device	Used to verify that the provided IP or FQDN for discovery is reachable from the appliance.
22	SSH	TCP	256-bit	Management station	In	OpenManage Enterprise appliance	Incoming network access is only required if FSD is used. The OpenManage Enterprise administrator must enable only when interacting with the Dell support staff.
25	SMTP	TCP	None	OpenManage Enterprise appliance	Out	Management station	Email alerts
53	DNS	UDP or TCP	None	OpenManage Enterprise appliance	Out	Management station	DNS queries
68 / 546 (IPv6)	DHCP	UDP or TCP	None	OpenManage Enterprise appliance	Out	Management station	Network configuration
80*	HTTP	TCP	None	Management station	In	OpenManage Enterprise appliance	The Web UI landing screen. All Web UI content is rerouted to port 443 (HTTPS).
123	NTP	TCP	None	OpenManage Enterprise appliance	Out	NTP Server	Time synchronization (if enabled)
137, 138, 139, 445	CIFS ^a	UDP or TCP	None	iDRAC/ CMC	In	OpenManage Enterprise appliance	- This port is used to upload or download deployment templates. - This port is used to upload TSR and diagnostic logs. - This port is used to download firmware or driver DUPs. - Emergency FSD process, if web UI is not available. For more information, see Appliance Share in Manage console settings .
				OpenManage Enterprise appliance	Out	CIFS share	Import firmware or driver catalogs from CIFS share.
111, 2049 (default)	NFS	UDP or TCP	None	OpenManage Enterprise appliance	Out	External NFS share	- Download catalog and DUPs from the NFS share for firmware updates. - Manual console upgrades
162 ^b	SNMP	UDP	None	Management station	In or Out	OpenManage Enterprise appliance	Event reception through SNMP. Enable outgoing traffic on this port only if using the Trap forward policy.

Table 12. Ports and protocols on management stations (continued)

Port	Protocol	Type	Encryption	Source	Direction	Destination	Usage
443 (default)	HTTPS	TCP	128-bit SSL	Management station	In or Out	OpenManage Enterprise appliance	- Web UI - This port is used to upload or download deployment templates. - This port is used to upload TSR and diagnostic logs. - This port is used to download firmware or driver DUPs. - FSD process - This port is used 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 UI. - Server-initiated discovery - This port is used to download firmware or driver DUPs. For more information, see Appliance Share in Manage console settings.
514	Syslog	UDP	None	OpenManage Enterprise appliance	Out	Syslog server	This port is used to send alert and audit log information to the Syslog server.
3269	LDAPS	TCP	None	OpenManage Enterprise appliance	Out	Management station	AD or LDAP login for Global Catalog
636	LDAPS	TCP	None	OpenManage Enterprise appliance	Out	Management station	AD or LDAP login for domain controller

a. If the appliance share is configured for HTTPS, the CIFS protocol is not required.

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

Related information

[Deployment](#)

Device ports and protocols

Provides information about supported ports and protocols running on managed devices.

Table 13. Supported ports and protocols on managed devices

Port	Protocol	Type	Encryption	Source	Direction	Destination	Usage
N/A	ICMP	N/A	None	OpenManage Enterprise Appliance	Out	Managed device	Used to establish a connection to a device during discovery. It validates the IP address or FQDN provided.
22	SSH	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed device	Discover servers running the Linux operating system, Windows, and Hyper-V.

Table 13. Supported ports and protocols on managed devices (continued)

Port	Protocol	Type	Encryption	Source	Direction	Destination	Usage
161	SNMP	UDP	None	OpenManage Enterprise appliance	Out	Managed device	SNMP queries
162 ^a	SNMP	UDP	None	OpenManage Enterprise appliance	In or Out	Managed device	Send and receive SNMP traps.
443	Proprietary, WS-Man, or Redfish	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed device	- Discover and maintain an inventory of iDRAC9 and later versions. - Manage CMC. - To download firmware or driver DUPs. - To upload or download deployment templates. - For ESXi host management.
443	HTTPS	TCP	256-bit	Managed device	In	OpenManage Enterprise appliance	Send and receive Redfish events.
623	IPMI/RMCP	UDP	None	OpenManage Enterprise appliance	Out	Managed device	Allow IPMI access through LAN.
69	TFTP	UDP	None	CMC	In	Management station	Update the CMC firmware.
137, 138, 139, 445	CIFS	UDP or TCP	None	iDRAC or CMC	In or Out	External CIFS share	Boot to ISO
111, 2049 (default)	NFS	UDP or TCP	None	iDRAC or CMC	In or Out	External NFS share	Boot to ISO

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

Related information

[Deployment](#)

Firewall exceptions

Some OpenManage Enterprise features require access to external resource URLs.

Table 14. External resources

Feature	External resource URL ^a
Upgrade appliance, install, or upgrade plugins.	https://downloads.dell.com/openmanage_enterprise https://dl.dell.com/openmanage_enterprise
Access device warranty	https://apigtwb2c.us.dell.com/PROD/sbil/eapi/v5/asset-entitlements?
Update catalogs	https://downloads.dell.com/catalog https://dl.dell.com/catalog
Push alert notifications to OpenManage Mobile.	https://openmanagecloud.dell.com
Connect to the Dell Digital Licensing portal.	https://www.dell.com/di/v3/fp/device/authorization https://www.dell.com/di/v3/fp/device/token

Table 14. External resources (continued)

Feature	External resource URL ^a
	• https://www.dell.com/di/v3/fp/oidc/revoke • https://www.dell.com/di/v3/fp/oidc/token
Get entitlements from Dell Digital Locker.	https://apigtwb2c.us.dell.com/NetworkApi/api/v2/NetworkApi/GetEntitlements
Bind entitlement to the device.	https://apigtwb2c.us.dell.com/NWAPI/api/NetworkV3/BINDENTITLEMENT/v3
Get a license from Dell Digital Locker.	https://apigtwb2c.us.dell.com/NWAPI/api/NetworkV3/GETLICENSE/v3

a. Browser access to these URLs is not supported. Only OpenManage Enterprise appliances can access these URLs.

Allow Akamai Technologies IP

Dell websites are replicated by Akamai Technologies for load balancing and faster downloads. If connectivity issues occur, ensure to allow Akamai domains and IP addresses in your proxy/firewall.

 **NOTE:** Akamai IPs and servers can vary by region, so check firewall logs and routing to identify the correct IPs/servers to allow.

Related information

[Deployment](#)

Deployment best practices

Consider the following best practices when deploying OpenManage Enterprise.

Table 15. Deployment best practices

Do	Don't
• Allocate memory and virtual CPUs to increase performance. OpenManage Enterprise is configured to use additional resources to increase performance. • Locate OpenManage Enterprise on a hypervisor with local or fast storage. Faster storage supports receiving and processing a larger number of incoming events. • Ensure that ports are opened between OpenManage Enterprise and the devices you want to manage. • Encrypt the drives where the virtual disks are stored to make unauthorized access difficult. Customers must also ensure that the files can be decrypted later else the device would not be bootable. • Verify integrity of the downloaded files before deployment. For more information, see <i>OpenManage Enterprise Security Configuration Guide</i>.	• Leave unnecessary VM snapshots that result in performance degradation. • Decrease memory to less than 16 GBs or the number of CPUs to less than four.

Related information

[Deployment](#)

Deploy in VMware vSphere

Deploy OpenManage Enterprise in VMware vSphere by downloading the virtual machine template from the Dell support site.

Prerequisites

- Use a VMware vSphere version that is supported by ESXi 8.0, ESXi 8.0 U1, ESXi 8.0 U2, ESXi 8.0 U3, and ESXi 9.0.
- When deploying OpenManage Enterprise on Open Virtualization Format (OVF) specification-based hypervisors, it is recommended to use thick provisioning.
- Deploy VMDKs using the supplied OVF template, which is configured with the minimum hardware requirements for running the OpenManage Enterprise appliance.
- If the ESXi host is managed by a VMware vCenter server, you must perform the deployment through VMware vCenter. Deployment through VMware vSphere will only succeed if the ESXi host is disconnected from vCenter.

About this task

After performing an in-band discovery of an ESXi server, the Management IP on the device details page displays the ESXi IP. Clicking the IP directs you to the VMware vCenter linked to the ESXi. This happens because VMware assigns the vCenter IP as the management IP when a host is attached to a vCenter. If the host is not attached to any vCenter, the management IP is the host IP itself. To redirect the management IP to the ESXi server, remove the host from the vCenter after discovery and rediscover the host to refresh the management IP.

Steps

1. Download the `openmanage_enterprise_ovf_format.zip` file from the Dell support site and extract the file to a location accessible by VMware vSphere Client. It is recommended to use a local drive or CD/DVD, because installing from a network location can take up to 30 minutes.
2. On the **Virtual Machines** screen, click **Create/Register VM**. The **New virtual machine** wizard opens.
3. On the **Select creation type** screen, click **Deploy a virtual machine from an OVF file**. Click **Next**.
4. On the **Select OVF and VMDK files** screen, set the name of the virtual machine. Drag the downloaded files onto the screen or click the screen to upload all three extracted files. Click **Next**.
5. On the **Select storage** screen, verify that the datastore being used has enough free space to satisfy the [OpenManage Enterprise hardware requirements](#). Click **Next**.
6. On the **Deployment options** screen, set **Disk provisioning** to **Thick** to preallocate physical storage space to VMs at the time a drive is created. Click **Next**.
7. On the **Ready to complete** screen, review your settings selection. Click **Finish**.
A completion status window is displayed where you can track job progress. Once the job is completed, the VM is booted.

Results

OpenManage Enterprise is deployed.

Next steps

1. Connect to the virtual machine console.
2. Complete the appliance setup [using the Text User Interface \(TUI\)](#).

If a secondary adapter is added before powering on the appliance for the first time, the adapter is configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **Disabled** and requires configuration by the user.

Related information

[Deployment](#)

Deploy in Microsoft Hyper-V

Deploy OpenManage Enterprise on Hyper-V 2019 and later by downloading compressed virtual machine templates from the support site.

About this task

If a secondary adapter is added before powering on the appliance for the first time, the adapter is configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.

Steps

1. Download the `openmanage_enterprise_vhdx_format.zip` file from the Dell support site. Extract the file and then move or copy the enclosed files into an appropriate location on your system where you want to store the appliance. Two `VHDX` files of different sizes should be enclosed in the ZIP file.
2. Start the **Hyper-V Manager** in the Windows server. The Windows Hyper-V should be displayed under the Hyper-V Manager. If not, right-click **Hyper-V Manager**, and then select **Connect to Server**.
3. Click **Actions > Import Virtual Machine** to start the **Import Virtual Machine** wizard.
4. Click **Next** on the initial **Before You Begin** screen.
5. Click **Browse** to select the location of the appliance files and click **Next**.
6. Select the virtual machine to import and click **Next**.
7. Select your preferred import type and click **Next**.
8. When prompted, on the **Connect Network** screen, select the virtual switch to connect to and click **Next**.
9. Review the import summary and when ready, click **Finish**.
10. Rename the virtual appliance once the import is completed.
11. Before powering on the virtual machine, open the **Settings** screen to ensure the assigned CPUs, hard drives, boot options, and memory are correctly configured:
 - a. Click **Processor** to assign the number of virtual processors in compliance with [OpenManage Enterprise hardware requirements](#).
 - b. Click **Memory** to assign the amount of virtual memory in compliance with [OpenManage Enterprise hardware requirements](#).
 - c. Click **Security**.
 - i. Optionally, select **Enable Secure Boot** if it is not already enabled.
 - ii. Set **Template** to **Microsoft UEFI Certificate Authority**.
 - iii. Click **Apply**.

Results

OpenManage Enterprise is deployed.

Next steps

1. Power on the virtual machine.
2. Connect to the virtual machine console.
3. [Configure the system using the TUI](#) complete the appliance setup.

Related information

[Deployment](#)

Deploy in KVM

Deploy OpenManage Enterprise in a kernel-based virtual machine (KVM) by downloading the KVM file from the support site.

Steps

1. Install the required virtualization packages while installing the operating system.
 2. Download the `openmanage_enterprise_kvm_format.zip` file from the Dell support site. Extract the file to an appropriate location on your system where you want to store the OpenManage Enterprise virtual drives. Two QCOW files of varying sizes should be enclosed in the ZIP file.
 3. Start the virtual manager and select **File > Properties**.
 4. On the **Network Interfaces** screen, click **Add**.
 5. Select **Bridge** as the interface type and click **Forward**.
 6. Set the start mode to **onboot** and select the **Activate now** check box.
 7. Select the interface to bridge from the list and ensure the properties match with the host device, and then click **Finish**.
- NOTE:** If a secondary adapter is added before powering on the appliance for the first time, IPv4 and IPv6 are disabled on it. Upon login to the TUI, and after accepting the EULA and changing the admin password, configure the secondary adapter and enable it.

A virtual interface is now created. Configure the firewall settings using the terminal.

8. On the **Virtual Machine Manager**, click **File > New**.
9. Select the **Import existing disk image** option. Click **Forward**.
10. Enter the following details:
 - **Name:** Name of the new virtual machine instance. This name must be unique among all VMs known to the hypervisor on the connection, including inactive guests.
 - **Disk image:** The local file path where the larger QCOW2 image was downloaded and extracted earlier.

NOTE: Set the **Bus** type to SATA.

- **Operating system** is the intended operating system for the virtual machine. For OpenManage Enterprise 4.1 and later, the operating system is *SUSE Linux Enterprise 15 SP4 (15.4)*.
- **Memory** is the user configurable memory for the virtual machine. The amount of memory that is assigned is based on [OpenManage Enterprise hardware requirements](#).

Click **Import and run**.

11. Open the virtual console of the newly created virtual machine and click **Force shutdown**.
12. Click **Add disk** to assign the required space for the virtual machine.
 - a. Set **Source** to **Custom path**.
 - b. Set **Custom path** to the file path where the smaller `qcow2` file was downloaded and extracted earlier.
 - c. Set **Device** to *Disk image file*.
 - d. Set **Bus** to SATA.
 - e. Click **Add**.
13. Set **Firmware** to *UEFI*. Click **Save**.
14. Edit **vCPU Allocation**. For information about the number of vCPUs required, see [OpenManage Enterprise hardware requirements](#). Click **Apply**.
15. Click **Run**.

The virtual machine begins booting.

Results

OpenManage Enterprise appliance is now deployed on KVM.

Next steps

[Configure the system using the TUI](#)

Related information

Deployment

Deploy in KVM using virt-install

Deploy OpenManage Enterprise in a kernel-based virtual machine (KVM) over command-line interface.

Steps

1. Install the required virtualization packages while installing the operating system.
2. Download the `openmanage_enterprise_kvm_format.zip` file from the Dell support site. Extract the file to an appropriate location on your system where you want to store the OpenManage Enterprise virtual drives.
Two QCOW files of varying sizes should be enclosed in the ZIP file.
3. Start a terminal and use the `cd` command to choose the path for the VM.
4. Run `virt-install` with the below parameters based on [OpenManage Enterprise hardware requirements](#).

Table 16. Parameters and Descriptions

Parameter	Details
<i>name</i>	Name of the new virtual machine instance. This name must be unique among all VMs known to the hypervisor on the connection, including inactive guests.
<i>memory</i>	Memory to allocate for guest instance in megabytes.
<i>vcpus</i>	The number of virtual processors that are assigned to the VM
<i>disk</i>	The hard drive images that are assigned to the VM. This parameter is listed twice in the command for the primary and secondary QCOW files. NOTE: Ensure that the disk bus is set to SATA by including <code>bus=sata</code> after the image file names as shown in the example below.
<i>os-variant</i>	For OpenManage Enterprise 4.1 and later, the operating system is <i>SUSE Linux Enterprise 15 SP4 (15.4)</i> . NOTE: Use the below command to find a list of accepted <code>os-variant</code> values for your version of <code>virt-install</code> : <pre>virt-install --os-variant list</pre>
<i>network</i>	Connect the VM to the host network.
<i>graphics</i>	When set to true, a graphical console is allocated to the VM.
<i>listen</i>	When set to 0.0.0.0, a VNC display is used.
<i>noautoconsole</i>	If this modifier is provided, the VM does not automatically try to connect to the guest console.
<i>boot</i>	[Optional] The postinstall VM boot configuration is modified here. NOTE: If required, ensure that this parameter is provided with a comma-separated list of boot options including UEFI and secure loading. They cannot be changed post deployment.

A sample command for a large deployment with secure boot:

```
virt-install --name 4.1_154ca --memory 65536 --vcpus 8 --disk  
openmanage_enterprise.qcow2,bus=sata --disk openmanage_enterprise.qcow2-1,bus=sata --  
import --os-variant opensuse15.4 --network default --graphics vnc,listen=0.0.0.0 --  
noautoconsole --boot firmware=efi,loader_secure=yes
```

The virtual machine begins booting.

Results

OpenManage Enterprise appliance is now deployed on KVM.

Next steps

[Configure the system using the TUI](#)

Related information

[Deployment](#)

Deploy programmatically

OpenManage Enterprise can be deployed programmatically (using a script) on VMware ESXi version 7.0 or later. Download Open Virtualization Format (OVF) files from the Dell support site.

Prerequisites

- Programmatic or scripted deployment is only supported using the primary interface.
- If a secondary adapter is added before powering on the appliance for the first time, the adapter is configured with IPv4 and IPv6 disabled. Log in to the TUI, accept the EULA and change the admin password, the user must configure the **Disabled** adapter.
- Ensure that the server has enough resources to support the deployment of the appliance. For more information, click here: [OpenManage Enterprise hardware requirements](#)
- Use the latest versions of OVF Tool and Python 3.0 or later.

Steps

1. Download the `openmanage_enterprise_ovf_format.zip` file from the Dell Support site.
2. Extract the contents of the file to a known location. The extracted files include:
 - `openmanage_enterprise.x86_64-0.0.1-disk-0.vmdk`
 - `openmanage_enterprise.x86_64-0.0.1-disk-1.vmdk`
 - `openmanage_enterprise.x86_64-0.0.1.mf`
 - `openmanage_enterprise.x86_64-0.0.1.ovf`
 - `ovf_properties.config`
 - `update_ovf_property.py`
3. Place the files in the same folder where the OVF tool is installed (The default location is `C:\Program Files\VMware\VMware OVF Tool`).
4. Open the `ovf_properties.config` and set the following parameters:

Table 17. Parameters in `ovf_properties.config`

Parameter	Accepted Values	Description
<code>bEULATxt</code>	true or false	By setting this value to true, you agree to the terms and conditions in the End-User License Agreement (EULA). The EULA is available at the bottom of the <code>ovf_properties.config</code> file.
<code>adminPassword</code>	• The password should contain a minimum of eight characters. • The password should contain at least one numerical character. • The password should contain at least one special character.	Type a new administrator password for the OpenManage Enterprise.
<code>bEnabledDHCP</code>	true or false	Set to true if you want the appliance to enable IPv4 DHCP and to ignore the static IPv4.

Table 17. Parameters in `ovf_properties.config` (continued)

Parameter	Accepted Values	Description
<code>bEnableIpv6AutoConfig</code>	true or false	Set to true if you want the appliance to enable IPv6 auto configuration and to ignore the static IPv6.
<code>staticIP</code>	static IP in CIDR format	IP addresses can be IPv4 or IPv6. (You cannot set both the IPv4 and IPv6 types at a time.) NOTE: Static IP addresses with CIDR/32 or /0 are not allowed.
<code>gateway</code>	IPv4 or IPv6	You cannot set static Gateway as IPv4 and IPv6 types at a time.

5. Run the `update_ovf_property.py` script.

This script modifies the `openmanage_enterprise.x86_64-0.0.1.ovf` file for deployment in accordance with the values set in the `ovf_properties.config` file. When the script finishes execution, a sample `ovftool` command is displayed. It contains tags such as `<DATASTORE>`, `<user>`, `<password>`, `<IP address>`, and so on, that you must replace as per your deployment environment. These settings define the resources that are used on the target ESXi system and also the credentials and IP address of the target system.

NOTE: Remember to replace the entire tag including the `<` and `>` symbols.

6. Open a command prompt terminal where the above files are located and run `ovftool.exe` while passing the following parameters:

- `--datastore=<>` indicates the VMware datastore that assigns storage to the appliance.
- `-dm=<thin/thick>` indicates whether storage is allocated to the appliance using thin or thick provisioning.
- `--name=<>` is the user-defined name of the appliance.
- `--noSSLVerify` skips SSL verification for vSphere connections.
- `--acceptAllEulas` accepts all end-user license agreements without being prompted.
- `--X:logToConsole=true` enables console logging during the deployment.
- `--X:logLevel="info"` indicates the level of console logging. Possible levels of logging are none, quiet, panic, error, warning, info, verbose, or trivia.
- `--X:injectOvfEnv` injects the passed parameters into the appliance when it is powering on.
- `--powerOn openmanage_enterprise.x86_64-0.0.1.ovf` powers on the appliance post successful deployment.
- `vi://%{TEST_USERNAME}:%{TEST_PASSWORD}@%{TEST_URL}/%{TEST_RESOURCE}`: The target locator indicates a local file path for the VMX, OVF or vApprun workspace. Alternatively, it could indicate a vSphere locator identifying a cluster, host, or a vSphere location.

NOTE:

- The `ovftool` command must be run with the `--X:injectOvfEnv` and `--powerOn` flags because they are required for programmatic deployment.
- Remember to replace the entire tag including the `<` and `>` symbols.

For example, `ovftool.exe --datastore=datastore2 -dm=thin --name=SampleAppliance --noSSLVerify --acceptAllEulas --X:logToConsole=true --X:logLevel="info" --X:injectOvfEnv --powerOn openmanage_enterprise.x86_64-0.0.1.ovf"vi://root:user@xx.xx.xx.xx"`.

After the `ovftool` command is run, the manifest validates and the deployment begins.

Results

OpenManage Enterprise is deployed.

Next steps

[Configure the system using the TUI](#)

Related information

[Deployment](#)

Configure the system using the TUI

Use the Text User Interface (TUI) for password changes, status viewing, network configuration, parameter setting, debug request enablement, primary network selection, and automatic server discovery.

When you boot the system for the first time from the TUI, you are prompted to accept the End User License Agreement (EULA). Next, change the administrator password and configure network parameters for the appliance and load the web console in a supported browser to get started. Only users with OpenManage Administrator privileges can configure OpenManage Enterprise.

Navigate the TUI using:

- The arrow keys or **Tab** to set focus to different menu options.
- **Shift + Tab** to go back to previous menus.
- **Enter** to select an option.
- **Space bar** to enable or disable a checkbox's status.

NOTE:

- To configure IPv6, ensure that it is already configured on a vCenter Server.
- By default, the appliance uses the last discovered IP of a device for performing all operations. To make any IP change effective, you must rediscover the device.

You can configure OpenManage Enterprise by using the TUI. The **TUI** screen has the following options:

Table 18. Text User Interface options

Options	Descriptions
Change the Admin Password	Select the Change the Admin Password screen to enter a new password and confirm the password. For the first time, you must change the password by using the TUI screen.
Display Current Appliance Status	Select Display Current Appliance Status to view the URL and the status of the appliance. You can also view statuses of the Task Execution, Event Processing, Monitor, Tomcat, Database, Backup and Restore, and Volume Binding services.  NOTE: The Backup and Restore status is listed with its status.
Display Current Network Configuration	Select Display Current Network Configuration to view the IP configuration details. The Choose Network Adapter menu lists all the available NICs. Click a NIC to display its current settings.
Set Appliance Hostname	Select Set Appliance Hostname to configure the appliance hostname on the DNS. This field supports the following valid characters for host names: • Alphanumeric (a-z, A-Z, 0-9) • Periods (.) • Dashes (-)  NOTE: Using periods designate domain name information. If the appliances DNS information is statically configured instead of obtaining details from DHCP, set the hostname using the fully qualified domain name (FQDN) to populate domain search information.
Set Networking Parameters	Select Set Networking Parameters to reconfigure the NICs. Choose Network Adapter menu lists all the available NICs. Select a NIC to reconfigure the following parameters: • Enable IPv4: Allow the appliance to communicate over IPv4. • Enable DHCP: Allow the appliance to connect to the network using DHCP. • Use DHCP to Obtain DNS Server Address: Allow the appliance to identify the DNS server over DHCP. • Static Preferred DNS server: Set the IP address of the primary DNS server. • Static Alternate DNS server: Set the IP address of the secondary DNS server. • Enable IPv6: Allow the appliance to communicate over IPv6. • Enable Autoconfiguration: Allow the appliance to automatically configure IPv6 interfaces.

Table 18. Text User Interface options (continued)

Options	Descriptions
	• Use DHCPv6 to Obtain DNS Server Addresses: Allow the appliance to identify the DNS server over DHCP 6. • Static Preferred DNS server: Set the IP address of the primary DNS server. • Static Alternate DNS server: Set the IP address of the secondary DNS server. • Register OME with DNS: Allow the appliance to create an FQDN entry on the DNS server. • If you plan to enable RSA on the appliance, ensure that the appliance is registered with the same DNS server as the RSA authentication manager host. • Use DHCP for DNS Domain Name: Allow the appliance to receive the domain name from the DNS. • DNS name: Set the FQDN of the appliance as registered on the DNS. • Domain Name: Set the domain name of the appliance. By default, only IPv4 is enabled on the primary network interface with a private static IP in the appliance. However, if a new network interface is added, both IPv4 and IPv6 are enabled for multihoming. If the appliance cannot obtain an IPv6 address, verify if the environment is configured with router advertisements and the managed bit (M) is enabled. Network Manager from current Linux distributions causes a link failure when this bit is on, but DHCP 6 is not available. Ensure that DHCP 6 is enabled on the network or disable the managed flag for router advertisements. NOTE: • A total of five NICs are supported on OpenManage Enterprise devices. • DNS configuration is only available on the primary network interface. If DNS resolution is wanted on this interface, all host names must be resolvable by the DNS server that is configured on the primary interface. • For more information about multihoming, see the <i>Multihoming on OpenManage Enterprise technical white paper</i> on the OpenManage Enterprise support site.
Select Primary Network Interface	Select Primary Network Interface allows you to designate a primary network. Primary interface selection gives priority to the selected interface in terms of routing and is used as the default route. This interface has the routing priority if there is any ambiguity. The primary interface is also expected to be the 'public facing' interface which allows for corporate network or Internet connectivity. Different firewall rules are applied to the primary interface, which allow for tighter access control such as access restriction by IP range. For information about firewall exceptions, see <i>Firewall exceptions</i> section in the user's guide. NOTE: If multihoming is enabled, the appliance can be accessed from up to five networks. In this case, the appliance uses the primary interface for all external communication and when proxy settings are used. For more information about multihoming, see the <i>Multihoming on OpenManage Enterprise technical white paper</i> on the OpenManage Enterprise support site.
Configure Static Routes	Select Configure Static Routes if the networks require a static route to be configured to reach a specific subnet over the IPv4 and IPv6 networks. NOTE: A maximum of 20 static routes per interface is supported.
Configure Server Initiated Discovery	Select Configure Server Initiated Discovery to allow the appliance to automatically register the required records with the configured DNS server. NOTE: • Ensure that the appliance is registered with DNS, and can dynamically update records. • The target systems must be configured to request registration details from DNS. • To change the DNS Domain Name, ensure that Dynamic DNS registration is enabled on the DNS server. Also, for the appliance to be registered on

Table 18. Text User Interface options (continued)

Options	Descriptions
	the DNS server, select the Nonsecure and secure option under Dynamic updates.
Configure Appliance Disk Size	Select Configure Appliance Disk Size to scan for the available disk space and allocate additional disk space if required. Only the primary disk size can be increased; any changes to the secondary disk size are not considered. NOTE: - It is highly recommended to take a VM snapshot of the console as a backup before applying any disk configuration changes. - Post addition of the disk space, deletion, or reduction of the expanded disk space is not supported. To reverse the increase in size of an existing disk, you must revert to a prior VM snapshot. - If the initial scan detects no unallocated space, then allocate additional disk space or disks to the console on your hypervisor and rescan.
Enable Field Service Debug (FSD) Mode	Select Enable Field Service Debug (FSD) Mode if directed to by a Dell support representative. For more information, see Field service debug. NOTE: A warning banner is displayed on the Web UI while Field Service Debug mode is active.
Restart Services	Select Restart Services with the following options to restart the services and networking: Restart All Services Restart Networking
Setup Debug Logging	Select Setup Debug Logging using the following options : Enable All Debug Logs - To collect the Debug logs of the all the application monitoring tasks, events, the task execution history, and installed plug-ins. NOTE: While the debug log collection is active, a warning banner is on display. Disable All Debug Logs - To disable all the Debug logs. NOTE: The warning banner indicating the debug log collection is removed. Configure Debug Logging - To selectively enable debug logging for an appliance and plug-in services. - Use the Options menu to select all services, clear all selections, or restore state before you make changes. NOTE: Changing the log configuration of the Volume Binding Service restarts the service, aborts any in-progress license binding tasks, and drops the connection to Dell Digital Locker. Enable SCP Retention—to collect the template .xml files. NOTE: SCP file retention is not applicable for MX7000 chassis templates. Disable SCP Retention—to disable the SCP retention. You can create a console log archive from the Monitor > Troubleshoot screen by clicking Log > Generate Log. To download the archived console log, click Download Log.
Enable CIFS share for FSD (emergency use only)	Select Enable CIFS share for FSD (emergency use only) if directed to by a Dell support representative. For more information, see Field service debug.

Table 18. Text User Interface options (continued)

Options	Descriptions
	 NOTE: A warning banner is displayed on the Web UI while Field Service Debug mode is active.
Change keyboard layout	Select Change keyboard layout to change the keyboard layout if needed.
Reboot the Appliance	Select Reboot the Appliance to restart the appliance.  NOTE: - After running a command to restart the services, the TUI may display the following message: <code>NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439]</code>. - The soft lockup issue likely occurs as a result of the hypervisor being overloaded. In such situations, it is recommended to have at least 16 GB of RAM and a CPU of 8000 MHz reserved to the OpenManage Enterprise appliance. It is also recommended that the OpenManage Enterprise appliance be restarted when this message is displayed.

Related information

[Log in to an appliance](#)

[Deployment](#)

Getting started

Provides information about logging in to, configuring, and supported ports for OpenManage Enterprise.

Topics:

- [Log in to an appliance](#)
- [Initial onboarding](#)
- [The Welcome to OpenManage Enterprise dialog](#)
- [The OpenManage Enterprise GUI](#)
- [The OpenManage Enterprise menu bar](#)
- [The OpenManage Enterprise dashboard](#)
- [The OpenManage Enterprise home screen](#)

Log in to an appliance

Log in to an appliance running OpenManage Enterprise.

Prerequisites

When you boot the system for the first time, use the TUI to:

- Accept the EULA.
- Set the administrator password.

See [Configure the system using the TUI](#).

 **CAUTION:** If you forget the administrator password, it cannot be recovered from the OpenManage Enterprise appliance.

Steps

1. Open a supported browser window.
2. In the **Address** field, enter the OpenManage Enterprise appliance IP address.
On the **Login** screen, the OpenManage Enterprise logo and a security notice are displayed. Administrators can customize the security notice over REST API. For more information, see the *OpenManage Enterprise API guide* at [Dell Developer Portal](#).
3. Type the login credentials, and then click **Login**.

 **NOTE:** The default username is admin.

Next steps

If you are logging in to OpenManage Enterprise for the first time, the **Welcome** screen is displayed. Click **Initial Settings**, and complete the basic configuration setup. See [The Welcome to OpenManage Enterprise dialog](#). To discover the devices, click **Discover Devices**.

 **NOTE:** By default, after three failed login attempts, your OpenManage Enterprise account gets locked and you cannot log in until the account lockout duration is over. The account lockout duration is 900 s by default. To change this duration, see [Set the login security properties](#).

Initial onboarding

If you are logging into the OpenManage Enterprise version 4.1 or later for the first time, the **Initial onboarding** dialog box is displayed.

Steps

1. Log in to the appliance using the login credentials.
The **Initial onboarding** dialog box opens.
2. By default, the internal iDRAC credential management feature is installed (enabled). This feature allows the appliance to create a local service account on supported iDRACs after the initial discovery. Further configuration can allow periodic password changes to the service account. For more information regarding this feature, see [Configure iDRAC Password Management](#).
To disable this feature, clear the **Enable Internal iDRAC credential management** checkbox.
 **CAUTION:** If the Password Strength Policy is configured on target iDRACs, do not enable the internal iDRAC credential management feature. The password policy sets certain complexity requirements for passwords. If the password generated by the OpenManage Enterprise service account does not meet these requirements, iDRAC will disable the service account. Therefore, you cannot manage the corresponding iDRACs from OpenManage Enterprise. For more information about Password Strength Policy, see the *iDRAC user's guide*.
-  **NOTE:** Once the internal iDRAC credential management feature is installed, it cannot be uninstalled during the lifetime of the OpenManage Enterprise instance without redeploying the appliance. Similarly, if the feature is not enabled at onboarding, it cannot be enabled later.
3. Click **Next**.
4. To proceed with default plug-in (AIOps Infrastructure Observability and Service plug-ins) installation, select the **End User License Agreement** individually and click **Accept**. If you choose to **Decline** either or both of these agreements, the default plug-ins are not installed. You can install these plug-ins later after the onboarding is complete. See [Install plugins](#).
5. Click **Finish**.
 - If default plug-ins are accepted, the appliance proceeds with the default plug-in installation.
 - The **Login** screen opens. See [Log into an appliance running OpenManage Enterprise](#) for first-time login.

Results

The initial onboarding is complete.

Next steps

[Update the installed plugins](#) to ensure compatibility with the latest version OpenManage Enterprise.

The Welcome to OpenManage Enterprise dialog

If you are logging in to OpenManage Enterprise for the first time, the **Welcome to OpenManage Enterprise** dialog is displayed. Use this dialog to set your time (either manually or using NTP time synchronization) and proxy configurations.

Prerequisites

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

Steps

1. To configure the time manually, in the **Time Configuration** section:
 - Use the **Time zone** drop-down menu to select an appropriate time zone.
 - In the **Date** box, enter or select a date.
 - In the **Time** box, fill the time.
 - Click **Apply** to save the settings.

[Manually restart the appliance](#) to apply the time configuration changes.

2. 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 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 **NTP Server 1**, **NTP Server 2** (optional), and **NTP Server 3** (optional) for time synchronization.
3. If you want to set a proxy server for external communication, In the **Proxy Configuration** section:
- 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 username and password.
 - Select the **Ignore Certificate Validation** check box if the configured proxy intercepts SSL traffic. Using this option ignores the built-in certificate checks used for the warranty and catalog updates.
 - Enter IPv4, IPv6 addresses, or domain names of devices exempt from the proxy server in the **Proxy Exclusion list** field.

4. Click **Apply** to save the settings.

Related concepts

[The OpenManage Enterprise GUI](#)

[The OpenManage Enterprise menu bar](#)

[The OpenManage Enterprise dashboard](#)

[The OpenManage Enterprise home screen](#)

The OpenManage Enterprise GUI

The OpenManage Enterprise Graphical User Interface (UI) contains the tools that you must navigate between and complete device management tasks. It is recommended that you familiarize yourself with the UI elements to use OpenManage Enterprise to manage your data center devices easily and effectively.

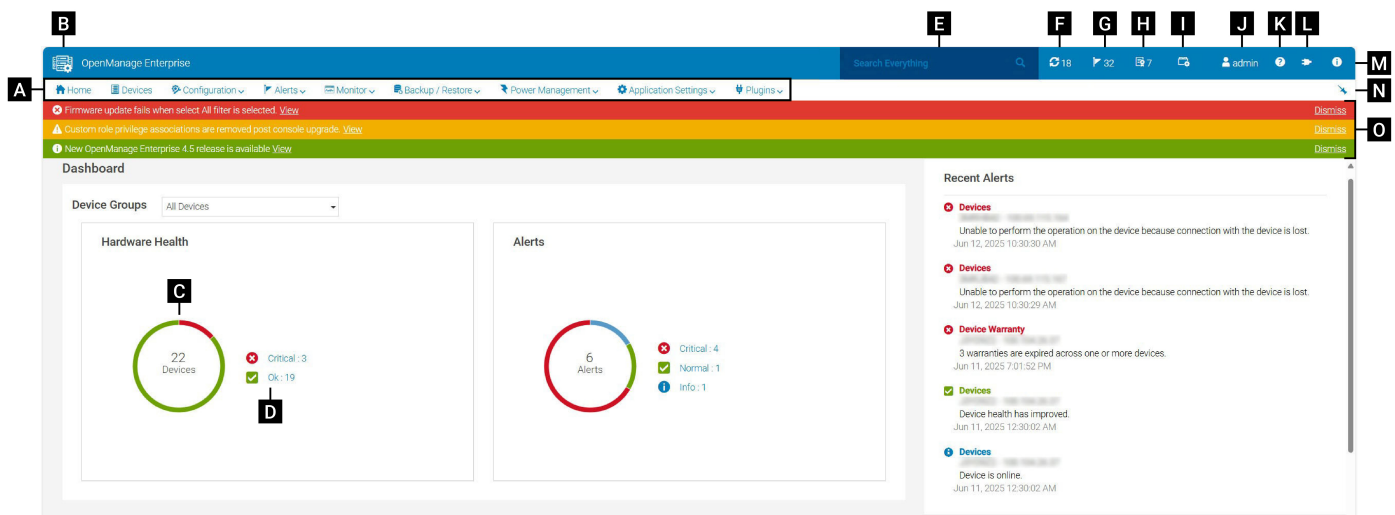


Figure 1. OpenManage Enterprise Graphical User Interface

- **A** : The OpenManage Enterprise **Menu bar** that is on all the screens of OpenManage Enterprise, provides links to features that enable administrators to:
 - View the dashboard (**Home**).
 - Manage devices (**Devices**).
 - Manage firmware or driver baselines (**Configuration**).
 - Manage templates (**Configuration**).
 - Manage configuration compliance baselines (**Configuration**).

- Create and store alerts (**Alerts**).
- Run jobs.
- Discover devices.
- Collect inventory data.
- Generate reports (**Monitor**).
- Customize different properties of your appliance (**Application Settings**).

Click the pin symbol in the upper-right corner to unpin the **Menu bar**, as described in [The OpenManage Enterprise menu bar](#).

- **B** is the Dashboard symbol. Click to open the **Dashboard** screen from any screen of OpenManage Enterprise. Alternately, click **Home**. See [The OpenManage Enterprise dashboard](#).
- **C** is the Donut chart which gives a snapshot of the health status of all the devices that OpenManage Enterprise monitors. You can quickly act upon the devices that are in a 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 screen. See [View and configure individual devices](#).
- **D**: The symbols used to indicate the device health state. See [Device health statuses](#).
- **E**: Enter any monitored or displayed item in the **Search Everything** box to view results, including device IP, job name, group name, firmware or driver baseline, and warranty data for all devices within your Scope-Based Access Control (SBAC) defined scope. You cannot sort or export data that is retrieved by using the Search Everything feature. On individual screens or dialog boxes, enter or select from the **Advance Filters** section to refine your search results.
 - The following operators are not supported: **+**, **-**, and **"**.
 - Searches are restricted to the following categories: Alert Policies, Alerts, Audit Logs, Devices, Links, Tasks, and Users.
- **F**: The number of OpenManage Enterprise jobs in the queue. Jobs that are related to discovery, inventory, warranty, firmware 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** screen. To view all the events, click **All Jobs**. See [Using jobs for device control](#). Click to refresh.
- **G**: The number of events that are generated in the alerts log. Also, based on whether unacknowledged alerts are displayed, the number of alerts that are displayed varies. By default, only the unacknowledged alerts are displayed. To hide or unhide the acknowledged alerts, see [Customize the alert display](#). Deleting the alerts reduces the count. For information about symbols that are used to indicate severity statuses, see [Device health statuses](#). Click a severity symbol to view all events in that severity category on the **Alerts** screen. To view all the events, click **All events**. See [Managing device alerts](#).
- **H**: The total number of device warranties in Critical (expired) and in Warning (expiring soon) statuses. See [Managing device warranty](#).
- **I**: The **software status button** shows a red dot when a plug-in is not installed, or when the plug-in catalog includes a compatible installation version. It also indicates the same when the plug-in is installed, and the catalog has a compatible upgrade version.
- **J**: Username of the user who is 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](#). Click to log out, and then log in as a different user.
- **K**: The context-sensitive help file is displayed only for the screen that you are on, and not the **Homepage** screen. Click to view task-based instructions to use links, buttons, dialog boxes, wizards, and screens in OpenManage Enterprise.
- **L**: The **Plugins Documentation** icon is displayed when plug-ins are installed. Click a plug-in name to open the plug-in documentation.
- **M**: 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.
- **N**: Click the pin to show or hide the **Menu bar**, as described in [The OpenManage Enterprise menu bar](#).
- **O**: **Live messages** are displayed on color-coded banners—red for critical, yellow for warnings, and green for informational messages. These banners provide notifications on critical updates, workarounds for known issues, enhancements, and other important system-related information relevant to the version of OpenManage Enterprise in use. An audit log is maintained for messages that are dismissed. Note that appliances without access to downloads.dell.com do not receive live-message notifications.

Data about items that are listed in a table can be comprehensively viewed, exported in total, or based on selected items. See [Export data](#). In blue text, detailed information about table items can be viewed and updated, either opening in the same window or on a separate screen. Tabulated data can be filtered by using the **Advanced Filters** feature. The filters vary based on the content that you view. Enter or select data from the fields. Incomplete text or numbers do 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 screens on OpenManage Enterprise. For information about supported browsers, see the *OpenManage Enterprise Support Matrix* available on the support site.

Where appropriate, the screen 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 UI element.

Preview about a device, job, inventory, firmware or 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 screens are automatically refreshed. Upon subsequent login after deploying the appliance, if a newer version of OpenManage Enterprise is available, you receive an alert prompting immediate update by clicking **Update**. Users with all the OpenManage Enterprise roles (Administrator, Device Manager, Custom role, 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 [Updating the console and plugins](#).

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** screen. See [View job lists](#).

NOTE: The maximum number of browser connections is limited to three connections per domain. Launching the console multiple times within the same browser result in an error. Close all unused sessions and refresh the page.

Related tasks

[The Welcome to OpenManage Enterprise dialog](#)

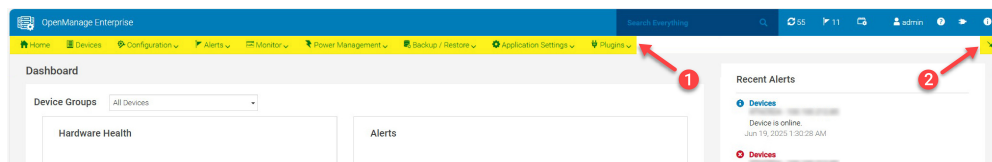
The OpenManage Enterprise menu bar

Hide the OpenManage Enterprise **Menu bar** to add viewing area to your screen. Display the menu bar from the **Mega menu**.

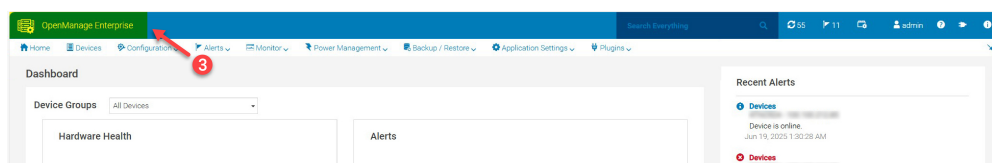
NOTE: The state of the **Menu bar** (pinned or unpinned) is saved for each user role. This means that if the **Administrator** unpins the **Menu bar**, it will remain unpinned with every subsequent **Administrator** log-in, until the **Administrator** pins it again.

(1) By default, the **Menu bar** is displayed at the top of every OpenManage Enterprise GUI screen.

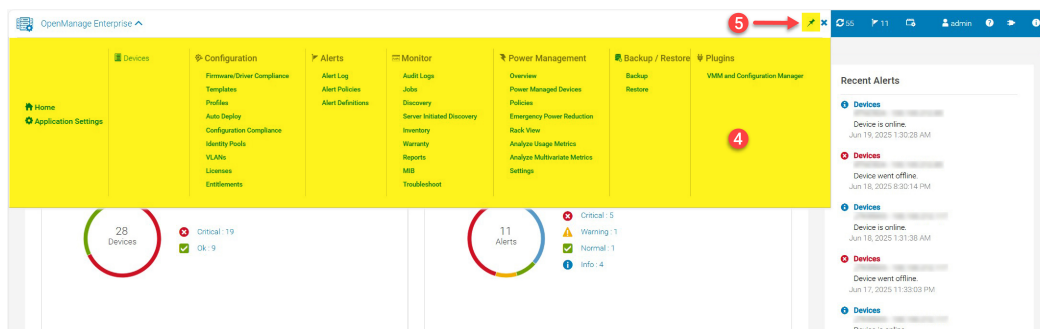
(2) Click the **pin** to the far right of the **Menu bar** to hide it.



(3) The **OpenManage Enterprise** logo becomes a drop-down menu . Click the **OpenManage Enterprise** menu to display the **Mega menu**.



(4) All of the OpenManage Enterprise **Menu items** are accessible through the **Mega menu**.



(5) Click the **pin** in the **Mega menu** to pin the **Menu bar**, displaying it on every screen again.

Related tasks

[The Welcome to OpenManage Enterprise dialog](#)

The OpenManage Enterprise dashboard

Apart from your first-time login, the **Dashboard** is the first screen that you see after every login to OpenManage Enterprise. To open the Dashboard from any screen of OpenManage Enterprise, click the dashboard symbol in the upper-left corner or click **Home**. The dashboard displays the device health, firmware or driver compliance, and other aspects of devices and device groups in your data center environment using real-time monitoring data.

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** screen appears empty. Add devices to OpenManage Enterprise so that they can be monitored and displayed on the dashboard. To add devices, see [Discovering devices](#) and [Create and manage custom groups](#).

- [Managing device firmware and drivers](#)
- [Managing alerts](#)
- [Discovering devices](#)
- [Create a report](#)
- [System configuration](#)

 **NOTE:** If a device group is selected from the **Device Groups** drop-down, then all the data that is displayed on the Dashboard only pertains to the selected device group.

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

Device alerts that are displayed in by the donut in the **Alerts** section are based on the device groups that are selected. See [Managing alerts](#). The total number of alerts in the Donut chart varies based on the setting to view the unacknowledged alerts. By default, only the unacknowledged alerts are displayed. See [Customize the alert display](#). 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](#).

For more information about a Donut chart, see [Doughnut charts](#) and [Device health statuses](#). 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 [All Devices screen device list](#) by health state:

- Click the color band that is associated with a health category.
- 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](#).

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

- **Warranty** displays the number of devices whose warranty is about to expire. The number 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 [Managing device warranty](#). Pause the pointer over the **Warranty** section to read definitions about the symbols used in the section.
- **Firmware/Drivers** displays the status of firmware or driver compliance of the device baselines that are created on OpenManage Enterprise. If available, the Critical and Warning firmware or driver baselines are listed here.
 - For more information about Rollup Health status, see the *Managing The Rollup Health Status By Using iDRAC On The Dell 14th Generation And Later PowerEdge Servers technical white paper* on the Dell TechCenter.
 - Click to view more information in the **Firmware/Driver Compliance** screen.
 - For information about updating a firmware, creating a firmware catalog, creating a firmware baseline, and generating a baseline compliance report, see [Managing device firmware and drivers](#).
- **Configuration** displays the rollup status of configuration compliance baselines that are created on OpenManage Enterprise. If available, the Critical and Warning configuration baselines are listed. See [Manage compliance templates](#).
- **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 color-coded vertical bar on the left of the widget represents the worst-case rollup of resource utilization.

Power Management data

- To view the power or thermal history of a group, click the **Power History** or **Thermal History** tab.
 - To add groups to the **Power History** or **Thermal History** graphs, click the edit icon. You can add a maximum of three groups to the dashboard.
 - Search for a group in **Power History** or **Thermal History** graphs search box.
- To view the top five energy consumers, click the **Top Energy Consumers** tab.
- To view the ratio of devices discovered in OpenManage Enterprise to devices added in Power Management, click the **Devices Statistics** tab.

Related tasks

[The Welcome to OpenManage Enterprise dialog](#)

Doughnut charts

The output displayed by the doughnut charts changes based on the items you select in a table. It can indicate device properties such as health or alerts in different colors.

A doughnut chart can indicate one or more statuses:

- **The health status of devices** is displayed on the **Dashboard** screen. Colors are used to indicate device statuses, that are described in [Device health statuses](#).

NOTE: The doughnut 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 circle is displayed.

- **The alert statuses of devices** displays the total alerts generated for the currently monitored devices, and can be customized as described in [Managing alerts](#).

NOTE: By default, only the unacknowledged alerts are displayed. The total number of alerts in the doughnut chart varies based on whether acknowledged alerts are displayed, as described in [Customize the alert display](#).

- **The firmware version compliance of a device against the version on the catalog** as described in [Managing device firmware and drivers](#).
 - The doughnut 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.
 - The compliance level of the selected device is indicated by a doughnut chart. Compliance levels can be:

Table 19. Device firmware compliance

Icon	Health status
	Healthy
	Downgrade
	Urgent or Recommended (Upgrade)
	Optional (Upgrade)

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*. However, 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 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 14th Generation And Later Powerededge Servers technical white paper*.

- **The configuration compliance baseline of devices and device groups** as described in [Configuration compliance](#).
- The compliance level of the selected device is indicated by a doughnut chart. Compliance levels can be:

Table 20. Device configuration compliance

Icon	Health status
	Compliant
	Not compliant

Device health statuses

Describes the statuses of monitored devices.

Table 21. Device health statuses

Icon	Health status	Definition
	Critical	An important aspect of the device or environment has failed.
	Warning	The device is about to fail. Some aspects of the device or environment are not normal. The device requires immediate attention.
	OK	The device is fully functional.
	Unknown	The device status is unknown.

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

 **NOTE:** The data that is displayed on the dashboard depends on the privileges you have for using OpenManage Enterprise. For more information about users, see Managing users section in the *OpenManage Enterprise User's Guide*.

The OpenManage Enterprise home screen

Click **Home** to display the home screen of OpenManage Enterprise.

On the home screen:

- View the **Dashboard** to get a live snapshot about the health statuses of devices, and then take actions, where necessary. See [The OpenManage Enterprise dashboard](#).
- View alerts under the critical and warning categories and resolve those. See [Managing alerts](#).
- The **Widgets** section lists the rollout warranty, firmware/driver compliance, and configuration compliance statuses of all devices. For more information about the features under Widgets, see [The OpenManage Enterprise dashboard](#). 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 [Managing alerts](#) and [Using jobs for device control](#).
- 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 [Updating the console and plugins](#).
- Live messages appear as colored banners at the top of the OpenManage Enterprise console interface, making important information visible and accessible to users. Messages are color-coded to indicate their severity level: **CRITICAL** (Red), **WARNING** (Yellow), or **INFORMATIONAL** (Green). A live message can be dismissed, but this action is specific to each user. When one user dismisses a message, it remains visible to others until they choose to dismiss it themselves. For more information about live messages, see [The OpenManage Enterprise GUI](#).
- The **Recent Alerts** section lists the most recent alerts generated by monitored devices that are monitored by OpenManage Enterprise. Click the alert title to view in-depth information about the alert. See [Managing 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](#).
-  **NOTE:** If logged in as a device manager or a custom role user, the **Home** screen displays information related to the device/device group the user owns. Also, the **Device Groups** dropdown lists only the device groups that the user has operational access to. See [Role and scope-based access](#).

Related tasks

[The Welcome to OpenManage Enterprise dialog](#)

System configuration

Configure your system using the **Application Settings** screen. From this screen, you can view and modify network settings, manage users, define console preferences, configure security and alert settings, as well as manage console updates and plugin installation.

Related tasks

[Delete Directory services](#)

Topics:

- [Configure network settings](#)
- [Manage roles and privileges](#)
- [Manage users and scopes](#)
- [Ending user sessions](#)
- [Directory services integration](#)
- [Login using OIDC providers](#)
- [Security certificates](#)
- [Manage console settings](#)
- [Set the login security properties](#)
- [Customize the alert display](#)
- [Configure SMTP, SNMP, and Syslog](#)
- [Manage incoming alerts](#)
- [Manage warranty settings](#)
- [Configure remote commands and scripts](#)
- [OpenManage Mobile settings](#)

Configure network settings

Set session inactivity timeouts, time configuration, and network proxy information.

Prerequisites

You must be a super administrator, administrator, or custom role user with appliance management privileg. For more information about roles and privileges, see [User roles](#).

Steps

1. To view the current network settings of the active network connections on the appliance such as DNS domain name, FQDN, IPv4, and IPv6 settings, expand **Current Settings**.
2. To configure the session timeouts and the maximum number of sessions for the OpenManage Enterprise API and web interface users, expand **Session Inactivity Timeout Configuration** and do the following:
 - a. Select the **Enable** checkbox to activate the Universal Timeout and enter the **Inactivity timeout** value. Set the Inactivity timeout value between 1 minute to 1440 minutes (24 hours). By default, the Universal timeout is disabled. Enabling the Universal timeout disables the API and Web Interface fields.
 - b. Change the API **Inactivity timeout (1-1440)** and the **Maximum number of sessions (1-100)** values. These attributes are by default set as 30 minutes and 100 respectively.
 - c. Change the Web Interface **Inactivity timeout (1-1440)** and the **Maximum number of sessions (1-100)** values. These attributes are by default set as 30 minutes and 6 respectively.
 - d. Click **Apply** to save the settings or click **Discard** to retain the default values.

 **NOTE:** Custom role user must have security management privilege for configuring Session Inactivity Timeout Configuration.

The current system time and the source—local time zone or NTP server IP are displayed.

3. Configure the system time zone, date, time, and NTP server updates by expanding **Time Configuration**.
 - a. Select the time zone from the drop-down list.
 - b. Enter the date or click the **Calendar** icon to select the date.
 - c. Enter the time in hh:mm:ss format.
 - d. To synchronize with an NTP server, select the **Use NTP** checkbox, and enter the server address of the primary NTP server.

You can configure up to three NTP servers in OpenManage Enterprise.

 **NOTE:** The **Date** and **Time** options are not available when you select **Use NTP**.

- e. Click **Apply**.
 - f. To reset the settings to default attributes, click **Discard**.

[Manually restart the appliance](#) to apply the time configuration changes.

4. Configure the OpenManage Enterprise proxy settings by expanding **Proxy Configuration**.
 - a. Select the **Enable HTTP Proxy Settings** checkbox to configure the HTTP proxy, and then enter HTTP proxy address and HTTP port number.
 - b. Select the **Enable Proxy Authentication** checkbox to enable proxy credentials, and then enter the username and password.
 - c. Select the **Ignore Certificate Validation** checkbox if the configured proxy intercepts SSL traffic. Using this option ignores the built-in certificate checks used for the warranty and catalog updates.
 - d. In the **Proxy Exclusion List** box, enter the following:
 - IPv4 or IPv6 addresses, or domain names of HTTP/HTTPS destinations that OpenManage Enterprise should bypass the proxy and access directly.
 - e. Click **Apply**.
 - f. To reset the settings to default attributes, click **Discard**.

 **NOTE:** Device discovery and communication with managed devices do not use the proxy configuration.

Results

To understand all the tasks that you can perform by using the Application Settings feature, see [System configuration](#).

Manage roles and privileges

Add, modify, and delete custom created user role.

The roles feature allows administrators to add, modify, and assign roles with specific privileges, tailored to organizational requirements. This provides better control over user access, ensuring that each user can only perform tasks relevant to their role, preventing unnecessary or potentially risky access to other functions.

By clicking **Application Settings > Users > Roles**, users with SECURITY_SETUP privilege can manage roles including adding, modifying, and deleting custom roles. You must be a super administrator or administrator to manage roles and users. For more information about roles and privileges, see [User roles](#).

Click the **Roles** tab to view predefined roles such as Super Administrator, Administrator, Device Manager, and Viewer, along with any custom roles, if created. Each role displays the following attributes:

- Name: The name of the role.
- Description of the role.
- Type: Indicate if the role is default or custom.
- Privilege: Lists the privileges associated with the role.

When you select a role, the associated privileges and the list of assigned users appear on the right side of the page.

User roles

All local and directory-based (Active Directory or LDAP) users should be assigned a role to determine the privileges they have in OpenManage Enterprise. Active Directory and LDAP directory groups can be imported and assigned to one or more OpenManage Enterprise roles.

Table 22. User roles

Role	Privileges
Super Administrator	The ability to perform all actions on the console by UI or REST API, including backup and restore. • Users cannot manage or edit this role as it is internal and predefined. • This role is only assigned to the preconfigured local admin user.
Administrator	The ability to perform all actions on the console by UI or REST API except backup and restore. This role can: • Read, view, create, edit, delete, export, and remove information that is related to devices and groups that are available on OpenManage Enterprise. • Create local users, import directory based groups, and assign roles. • Enable and disable users. • Add and modify the roles of existing users. • Delete the users. • Change the user password. • Update device health.
Device Manager	The ability to view and manage user-created entities (jobs, firmware, or configuration templates and baselines, alert policies, profiles, and so on). Also, the ability to run tasks, policies, and other actions on the devices (scope) assigned by the administrator.
Viewer	Read-only access to the console and all groups and cannot run tasks or create and manage policies. • View information that is displayed on OpenManage Enterprise and run reports.
Custom role	An administrator can create custom roles to assign specific privileges to users, enabling more granular control over what features they can access within OpenManage Enterprise.

- Any change to the user role takes effect immediately and all impacted users are logged out of their active sessions.
- An audit log is recorded when:
 - A group is assigned, or access permission is changed.
 - The user role is modified.

Role and scope-based access

Role-Based Access Control (RBAC) defines the user privileges into three categories: Administrator, Device Manager, and Viewer. Scope-Based Access Control (SBAC) enables administrators to limit the device groups that a device manager can access. The following topics further explain the RBAC and SBAC features.

Role-based access control (RBAC) privileges

Users are assigned roles that determine their level of access to the appliance settings and device management features. This feature is termed as Role-Based Access Control (RBAC). The console enforces the privilege that is required for a certain action before allowing the action. For more information about managing users in OpenManage Enterprise, see [Manage OpenManage Enterprise users](#).

The privileges for the custom roles created by an administrator are assigned at the time the role is created.

The table below lists the privileges of each role.

Table 23. Privileges of OpenManage Enterprise roles

Privilege	Description	User roles				
		Super Administrator	Administrator	Device Manager	Viewer	Custom Role User
Appliance Management						
Backup and restore	Back up and restore appliance.	Yes	No	No	No	No
Alert management	Acknowledge, unacknowledge, and delete alerts in the system.  NOTE: Ignoring alerts require Monitoring setup management privilege.	Yes	Yes	No	No	Yes
Appliance management/Setup	Global appliance settings involving the setting up of the appliance and enabling FSD.	Yes	Yes	No	No	Yes
Security setup	Appliance security settings	Yes	Yes	No	No	No
Infrastructure Management						
Firmware update	Update device firmware and apply updated baselines.	Yes	Yes	Yes	No	Yes
Device configuration	Perform actions on devices, including deleting, troubleshooting devices, updating settings, launching virtual console, resetting devices, and controlling power.  NOTE: This privilege requires the Job management privilege.	Yes	Yes	Yes	No	Yes
Operations Management						
Monitoring setup management	Manage alert policies, manage incoming alerts, ignore alerts, and OpenManage Mobile push notifications.	Yes	Yes	Yes	No	Yes
Template management	Create and manage templates and configuration baseline policies.	Yes	Yes	Yes	No	Yes

Table 23. Privileges of OpenManage Enterprise roles (continued)

Privilege	Description	User roles				
		Super Administrator	Administrator	Device Manager	Viewer	Custom Role User
Report management	Create, read, update, and delete reports.	Yes	Yes	Yes	No	Yes
Trap management	Import, parse, and delete MIBs.	Yes	Yes	No	No	Yes
Auto-deploy management	Manage auto-deploy configuration operations.	Yes	Yes	No	No	Yes
License management	Manage licenses, including importing, exporting, binding to device service tags, and deleting from OpenManage Enterprise.	Yes	Yes	Yes	No	Yes
License deployment	Bind and deploy licenses acquired from Dell Digital Locker to devices.	Yes	Yes	Yes	No	Yes
Job management	Execute and manage jobs.  NOTE: This privilege requires the Device configuration privilege.	Yes	Yes	Yes	No	Yes
Baseline management	Create and manage firmware baseline policies.	Yes	Yes	Yes	No	Yes
Inventory management	Create, read, update, delete, and run inventory tasks.	Yes	Yes	Yes	No	Yes
Discovery management	Create, read, update, delete, and run discovery tasks.	Yes	Yes	No	No	Yes
Group management	Create, read, update, and delete static and dynamic groups, including plugin groups.	Yes	Yes	No	No	Yes
Network management	Manage VLANs and import VLANs from the target chassis device to synchronize networks between OpenManage Enterprise and the chassis.	Yes	Yes	No	No	Yes
Report run	Run reports	Yes	Yes	Yes	Yes	Yes

Table 23. Privileges of OpenManage Enterprise roles (continued)

Privilege	Description	User roles				
		Super Administrator	Administrator	Device Manager	Viewer	Custom Role User
View	View all data, report execution or management, and so on.	Yes	Yes	Yes	Yes	Yes

Table 24. Role-based user privileges for the Power Management feature

Privilege	Super Administrator	Administrator	Device Manager (scope for assigned groups)	Viewer	Custom role
Add or remove supported devices and static groups for power management	Yes	Yes	Yes	No	Yes
Add or remove unmonitored devices	Yes	Yes	No	No	Yes
Add or remove Power Distribution Units (PDUs)	Yes	Yes	No	No	Yes
Monitor PDUs	Yes	Yes	Yes	Yes	Yes
Create, edit, or delete Physical Groups.	Yes	Yes	No	No	Yes
Import physical groups through CSV file.	Yes	Yes	No	No	Yes
Manage the devices in the rack.	Yes	Yes	No	No	Yes
Monitor metrics	Yes	Yes	Yes	Yes	Yes
Manage power policies for devices and groups.	Yes	Yes	Yes	No	Yes
Manage temperature-triggered policies for group.	Yes	Yes	Yes	No	Yes
Manage alert thresholds for devices and groups.	Yes	Yes	Yes	No	Yes
View alert thresholds	Yes	Yes	Yes	Yes	Yes
Manage Emergency Power Reduction (EPR) for devices and groups.	Yes	Yes	Yes	No	Yes

Table 24. Role-based user privileges for the Power Management feature (continued)

Privilege	Super Administrator	Administrator	Device Manager (scope for assigned groups)	Viewer	Custom role
Modify Power Management Settings	Yes	Yes	No	No	Yes
View Settings	Yes	Yes	Yes	Yes	Yes
Run and view reports for devices and groups.	Yes	Yes	Yes	Yes	Yes
Manage custom reports for devices and groups.	Yes	Yes	Yes	No	Yes
Dashboard	Yes	Yes	Yes	Yes	Yes
Create, edit, or delete VM groups.	Yes	Yes	No	No	Yes
Analyze usage metrics.	Yes	Yes	Yes	Yes	Yes
Automatically create a physical hierarchy.	Yes	Yes	No	No	Yes
View maximum and minimum power consumption of VMs on the Overview screen.	Yes	Yes	Yes	Yes	Yes
Disable LCS Event-triggered EPR	Yes	Yes	No	No	Yes
Enable and disable Liquid cooling system alert policy	Yes	Yes	No	No	Yes
View maximum and minimum power consumption of VM groups on the Overview screen	Yes	Yes	Yes	Yes	Yes
Update device location in device console	Yes	Yes	No	No	Yes
View idle servers.	Yes	Yes	Yes	Yes	Yes
Add or remove Uninterruptible Power Supply (UPS).	Yes	Yes	No	No	Yes
Monitor UPS	Yes	Yes	Yes	Yes	Yes
Monitor GPU	Yes	Yes	Yes	Yes	Yes
Monitor PSU	Yes	Yes	Yes	Yes	Yes
Analyze multivariate metrics.	Yes	Yes	Yes	Yes	Yes

Table 24. Role-based user privileges for the Power Management feature (continued)

Privilege	Super Administrator	Administrator	Device Manager (scope for assigned groups)	Viewer	Custom role
View devices associated with system and workload profiles	Yes	Yes	Yes	Yes	Yes

Details of user privileges

Details of user privileges in OpenManage Enterprise.

Appliance Management

Users with the **Appliance Management** privilege can manage the following tabs in the GUI, except where noted:

Table 25. Appliance management user privileges

Tab	Functionalities
Application Settings	• Network (Except Session Inactivity Timeout configuration) • Console Preferences • Certificates • Alerts • Warranty • Console and Plugins • Script Execution

The following settings require additional privileges beyond **Appliance Management**:

Table 26. Additional privileges required for Appliance management

Setting	Required Privilege
Application Settings > Network > Session Inactivity Timeout Configuration	Security Management
Application Settings > Users	Security Management
Application Settings > Security	Security Management
Application Settings > Console Preferences > iDRAC Password Management	Security Management
Application Settings > Backup/Restore Settings	Backup Management
Application Settings > Device Health	Only administrator can manage device health
Application Settings > Incoming Alerts	Monitoring Setup Management
Application Settings > Mobile	Monitoring Setup Management

Scope-based access control (SBAC)

Scope-Based Access Control (SBAC) is an extension of Role-Based Access Control (RBAC). With RBAC, administrators assign roles while creating users. These roles define the user's access level to appliance settings and device management features. SBAC further refines this by allowing administrators to restrict a Device Manager or Custom Role user to a specific subset of device groups, known as a scope.

Assigning scope

When creating or updating a device manager or custom role user, administrators can assign a scope to limit the operational access of the user to specific system groups, custom groups, and plug-in groups. However, Administrator and Viewer roles have unrestricted scope, meaning they have operational access to all devices and group entities as specified by their RBAC privileges.

An administrator can assign the scope while creating a Device Manager or a user with a custom role. Additionally, the scope can be modified at a later time by editing the user. Scopes can be implemented as follows:

1. Go to **Application Settings > Users**.
2. Add or Edit User or Import Directory Group.
3. Assign Device Manager or custom role to user or Directory Group.
4. Assign the user scope to all devices or a specific device group to restrict operational access.

For more information about managing users, see [Manage users and scopes](#).

Restricted view

With SBAC, administrators can implement a Restricted View feature. With Restricted View, Device Managers or Custom Role users can only see:

- Groups (therefore, the devices in those groups) in their scope.
- Entities that they own (such as jobs, firmware templates, configuration templates, and baselines, alert policies, profiles, and so on).
- Community entities such as Identity Pools and VLANs which are not restricted to specific users and can be used by everyone accessing the console.
- Built-in entities of any kind.

If a Device Manager or Custom Role user's scope is unrestricted, they can view all devices and groups. However, they can only see entities owned by them, such as jobs, alert policies, and baselines along with the community and built-in entities of any kind.

When a Device Manager or Custom Role user with an assigned scope logs in, they can see and manage only the devices within their scope. They can also see and manage entities associated with scoped devices, but only if they own the entity (i.e., they created it or were assigned ownership). For more information about the entities a Device Manager or Custom Role user can create, see Role-Based Access Control (RBAC) privileges in *OpenManage Enterprise User's Guide*.

Examples

By clicking **Configuration > Templates**, Device Manager or Custom Role users can view the default and custom templates they own. They can also perform other tasks on owned templates as permitted by their RBAC privileges.

By clicking **Configuration > Identity Pools**, Device Manager or Custom Role users can see all the identities created by an administrator or by themselves. The user can also perform actions on those identities as specified by RBAC privilege. However, the user can only see the usage of those identities that are associated with the devices under the user's scope.

Similarly, by clicking **Configuration > VLANs Pools**, Device Manager users can see all the VLANs created by the admin and export them. The Device Manager cannot perform any other operations. If they have a template, they can edit the template to use the VLAN networks, but it cannot edit the VLAN network.

In OpenManage Enterprise, the scope can be assigned while creating a local user or importing an AD or LDAP user. Scope assignment for OIDC users can only be done on Open ID Connect (OIDC) providers.

SBAC for local users

- While creating or editing a local user with Device Manager or custom role, an admin can select one or more device groups that defines the scope for the user. For example, if you (as an administrator) create a Device Manager user named *dm1* and assign to group *g1* present under custom groups, then *dm1* can only access devices within *g1*. The user *dm1* cannot access any other groups or entities that are related to any other devices.
- Furthermore, with SBAC, *dm1* can only view entities they own. If *dm1* and *dm2* are both assigned to group *g1*, *dm1* cannot see entities created by *dm2*, and vice versa. For example, you (as an administrator) create another Device Manager user with a name *dm2* and assign the same group *g1* present under custom groups. If *dm2* creates configuration template, configuration baselines, or profiles for the devices in *g1*, then *dm1* cannot access to those entities and vice-versa.
- A Device Manager with scope to All Devices has operational access as specified by RBAC privileges to all devices and group entities that are owned by the Device Manager.

SBAC for AD and LDAP users

While importing or editing AD and LDAP groups, administrators can assign scopes to user groups with the Device Manager or Custom role. If a user is a member of multiple AD groups, each with a Device Manager role, and each AD group has distinct scope assignments, then the scope of the user is the union of the scopes of those AD groups.

For example:

- User *dm1* is a member of two AD groups (*RR5-Floor1-LabAdmins* and *RR5-Floor3-LabAdmins*). Both AD groups have been assigned the Device Manager role, with scope assignments for the AD groups as follows: *RR5-Floor1-LabAdmins* gets *ptlab-servers* and *RR5-Floor3-LabAdmins* gets *smdlab-servers*. Now the scope of the Device Manager *dm1* is the union of *ptlab-servers* and *smdlab-servers*.
- User *dm1* is a member of two AD groups (*adg1* and *adg2*). Both AD groups have been assigned the Device Manager role, with scope assignments for the AD groups as follows: *adg1* is given access to *g1* and *adg2* is given access to *g2*. If *g1* is the superset of *g2*, then the scope of *dm1* is the larger scope (*g1*, all its child groups, and all leaf devices).

When a user is a member of multiple AD groups that have different roles, the higher-functionality role takes precedence (in the order Administrator, Custom Role, Device Manager, and Viewer).

A Device Manager with unrestricted scope has operational access as specified by RBAC privileges to all device and group entities.

SBAC for OIDC users

Scope assignment for OIDC users does not happen within the OpenManage Enterprise console. You can assign scopes for OIDC users at an OIDC provider during user configuration. When the user logs in with OIDC provider credentials, the role and scope assignment is available to OpenManage Enterprise. For more information about configuring user roles and scopes, see [Configure OIDC login using PingFederate](#).

 **NOTE:** If PingFederate is being used as the OIDC provider, then only administrator roles can be used. For more information, see [Configure OIDC login using PingFederate](#) and the Release Notes at [Dell Support](#).

Add custom roles

Add roles with specific privileges.

Prerequisites

Ensure you have the security setup privileges. For more information about privileges, see [Role and scope-based access](#).

Steps

1. In OpenManage Enterprise, click **Application Settings > Users > Roles**.
2. In the **Roles** tab, click **Add** to create a role.
3. Enter the following details:
 - Role Name: A user-defined custom role name, up to 32 characters long, supporting all alphanumeric and special characters.
 - Role Description: Role description up to 63 characters long, supporting all alphanumeric and special characters.
 - Privileges: A list of privileges. For more information about privileges, see [Role and scope-based access](#).
4. Click **Finish**. The system validates to check if the specified role exists.
Once the validation is successful, a new role is created and displayed on the Role page.

Results

- Newly created custom roles are automatically assigned with Report Run and View privileges by default.
- Newly created custom roles are available for selection when creating or modifying local and AD/LDAP users in OpenManage Enterprise.

Next steps

Newly created custom roles are available for selection when creating or modifying local and AD/LDAP users in OpenManage Enterprise. For creating users and assigning roles, see [Manage users](#).

Edit custom roles

Prerequisites

Ensure you have the security setup privileges. For more information about privileges, see [Role and scope-based access](#).

Steps

1. Click **Application Settings** > **Users** > **Roles**, and select the checkbox corresponding to the role.
2. Click **Edit**. The **Edit** option is only available for custom roles.
3. Follow the steps as mentioned in [Add custom roles](#).

Results

Once the validation is successful, the custom role is updated and displayed on the Roles page.

 **NOTE:** Any changes made to deleted privileges will be transferred to the logged-in user.

Delete custom roles

Prerequisites

Ensure you have the security setup privileges. For more information about privileges, see [Role and scope-based access](#).

Steps

1. Click **Application Settings** > **Users** > **Roles** and select the checkbox corresponding to the role.
2. Click **Delete**. The **Delete** option is only available for custom roles.
3. If no users are associated with the role, a confirmation window appears. Click **Yes** to delete the role. If any users are associated with the role, the system notifies the logged-in user and prevents its deletion.
To delete such roles, modify the user to select a different role and then delete the role. For modifying the user, see [Manage users](#).

Manage users and scopes

View, add, enable, edit, disable, or delete the OpenManage Enterprise local users.

By clicking **Application Settings** > **Users**, you can:

- View, add, enable, edit, disable, or delete the OpenManage Enterprise local users, as described in [Add or edit local users](#).
- Assign OpenManage Enterprise roles to directory services-based users by importing directory groups. AD and LDAP directory users can be assigned Admin, Device Manager, Viewer, or Custom roles in OpenManage Enterprise. For more information, see [Import Active Directory and LDAP groups](#).
- View details about the logged-in users.
- Terminate a user session.
- Manage Directory Services, as described in [Add or edit the Active Directory connection](#).
- View, add, enable, edit, disable, or delete OpenID connect providers. For more information, see [Login using OIDC providers](#).

NOTE:

- Ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in [User roles](#).
- A maximum of 1000 user accounts can exist in an appliance.
- Any change to a user role does not affect the active session of the impacted users and takes effect from subsequent login.
- If a **Device Manager** (DM) is demoted to a **Viewer**, that DM loses access to all entities that the DM owned originally. Possible entities include jobs, firmware, or configuration templates and baselines, alert policies, and profiles. Only administrators can manage these entities. Management rights are not restored to user accounts that have been promoted from 'Viewer' to 'Device Manager'.

By default, the list of users is displayed under **Users**. The right pane displays the properties of a username that you select in the working pane.

- **Username:** Along with the users you created, OpenManage Enterprise displays the built-in local admin account that cannot be deleted. However, you can edit the login credentials by selecting the default username and clicking **Edit** as described in [Enable OpenManage Enterprise users](#).
- The recommended characters for usernames are:
 - 0–9
 - A – Z
 - a – z
 - - ! # \$ % & () * / ; ? @ [\] ^ _ ` { | } ~ + < = >
 - The recommended characters for passwords are:
 - 0–9
 - A–Z
 - a–z
 - ' - ! " # \$ % & () * , . / : ; ? @ [\] ^ _ ` { | } ~ + < = >
- **User Type** indicates if the user logged in locally or remotely.
- **Enabled** indicates with a tick mark when the user is enabled to perform OpenManage Enterprise management tasks as described in [Enable OpenManage Enterprise users](#) and [Disable OpenManage Enterprise users](#).
- **Role** indicates the user role in using OpenManage Enterprise. For a list of user roles and their scope, see [User roles](#).

Related tasks

[Delete Directory services](#)

[Delete OpenManage Enterprise users](#)

[Ending user sessions](#)

Add or edit local users

Create and edit properties of local users based on the role that is assigned to a user.

Prerequisites

- Log in to OpenManage Enterprise as an **Administrator**, as described in [User roles](#).
- Before enabling **RSA SecurID** on a user account, the appliance must have [RSA securID configured](#).
- Before enabling **RSA SecurID** on a OpenManage Enterprise user, create a corresponding account on the RSA server.

About this task

This procedure is specific to adding and editing local users. While editing local users, you can edit all the user properties. To integrate Directory Services in OpenManage Enterprise and to import the Directory users, see [Directory services integration](#) and [Import Active Directory and LDAP groups](#).

NOTE:

- You cannot enable, disable, or delete the *admin*, *system*, or *root* users. You can only change their passwords by clicking **Edit** in the right pane.

Steps

1. Select **Application Settings > Users > Users > Add**.
2. In the **Add New User** dialog box:
 - a. From the **User Role** drop-down menu under **User Details**, select a pre-defined role such as Administrator, Device Manager, or Viewer, or select a custom role, if available.
For more information, see [Role and scope-based access](#).
By default, the user is enabled, indicating that the user privileges setup are enabled for a user.
 - b. For the Device Manager role, the scope defaults to **All Devices** (unrestricted scope). However, the administrator can restrict the scope by choosing the **Select Groups** option and selecting the device groups.
 - c. Under **User Credentials**, enter **Username**, **Password**, and reenter the password in the **Confirm Password** fields.
 - The username must contain only alphanumeric characters (underscores are allowed).

- The password must be at least 8 characters long and include at least one uppercase letter, one lowercase letter, one digit, and one special character.
 - The password must not exceed 32 characters.
- d. Under **RSA SecurID**, select **Enable** or **Disable** to indicate whether the user account requires RSA authentication in addition to the password while logging into the appliance.

**NOTE:**

- Only **Super Administrator** accounts can enable or disable multifactor authentication on themselves.
- Each time an **RSA SecurID** enabled user logs in, the appliance contacts the RSA Authentication server. If a proxy is configured, ensure that the appliance can still communicate with the RSA Authentication server to avoid service disruption.
- User IDs on RSA are not case-sensitive. However, user IDs with the same name but different casings are considered to be different accounts on the appliance. For example, while 'test' and 'TEST' are considered the same account on RSA, they are treated as two different accounts on OpenManage Enterprise.
- Accounts with **RSA SecurID** enabled cannot initiate any REST API calls to the appliance or any plugins outside the appliance. Authenticated REST API calls from third-party tools are also restricted. If external REST API calls to the appliance or plugins are required, allocate a user with **RSA SecurID** disabled.

3. Click **Finish**.

Results

A message is displayed that the user is successfully saved. A job is started to create a user. After running the job, the new user is created and displayed in the list of users.

Edit OpenManage Enterprise user properties

Edit the properties of a user based on the user role that they are assigned.

Prerequisites

Ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in [User roles](#).

Steps

1. Click **Application Settings** > **Users**, and select the checkbox corresponding to the user.
2. [Add or edit local users](#).

Results

The updated user properties are saved.

User role changes and entity retention: When a user's role is changed, the retention of entities they have created depends on the privileges of the new role. If the new role includes the same privileges as the old role (for example, Job Management), the user retains access to the relevant entities. The entities that are not covered by the new role's privileges are reassigned to the administrator, while entities within the scope of the new role's privileges remain with the user.

Example: suppose *User1* has the role *custom1* with both Job Management and Template Management privileges, and this role is changed to *custom2*, which includes Job Management but does not include Template Management privileges. In this case, *User1* retains access to job-related entities but lose access to template baseline entities. The template baseline entities are reassigned to the administrator, ensuring that *User1* retains only those entities that fall within the privileges of their new role.

Enable OpenManage Enterprise users

Select a user to enable specific roles to the user.



NOTE: Before you begin, ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in [User roles](#).

Select the check box corresponding to the username and click **Enable**. The user is enabled and a tick mark is displayed in the corresponding cell of the **Enabled** column. If the user is already enabled while creating the username, the **Enable** button appears grayed-out.

Related tasks

[Delete Directory services](#)
[Delete OpenManage Enterprise users](#)
[Ending user sessions](#)

Disable OpenManage Enterprise users

Disable a user from one or more tasks.

 **NOTE:** Before you begin, ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in [User roles](#).

Select the check box corresponding to the username and click **Disable**. The user is disabled, and a tick mark disappears in the corresponding cell of the **Enabled** column. If the user is disabled while creating the username, the **Disable** button appears grayed-out.

Related tasks

[Delete Directory services](#)
[Delete OpenManage Enterprise users](#)
[Ending user sessions](#)

Delete OpenManage Enterprise users

Remove one or more users from performing tasks.

Prerequisites

Ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in [User roles](#).

Steps

1. Select the check box corresponding to the username and click **Delete**.
2. When prompted, click **YES**.

Related references

[Disable OpenManage Enterprise users](#)
[Enable OpenManage Enterprise users](#)
[Manage users and scopes](#)

Import Active Directory and LDAP groups

This topic describes how to import users in active directory or LDAP for authentication into the appliance.

Prerequisites

- Ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in [User roles](#).
- Users other than **Administrator** cannot enable or disable the Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) users.
- Ensure Active Directory groups have a Universal group scope.
- AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Administrator, DeviceManager, or Viewer). The Single-Sign-On (SSO) feature stops at login to the console. Actions run on the devices require a privileged account on the device.

- If **RSA SecurID** authentication is required on users from the Active Directory or LDAP groups, ensure the active directory or LDAP groups are integrated with the RSA server.

Steps

1. Click **Import Directory Group**.
2. In the **Import Active Directory** dialog box:
 - a. From the **Directory Source** drop-down menu, select an Active Directory or LDAP source that must be imported for adding groups.
For more information on support services, see [Add or edit the Active Directory connection](#).
 - b. In the dialog box, type the username and password of the domain where the directory is saved. Use tool tips to enter the correct syntax.
 - c. Click **Finish**.
3. In the **Available Groups** section:
 - a. In the **Find a Group** box, enter the initial few letters of the group name available in the tested directory. All the groups names that begin with the entered text are listed under GROUP NAME.
 - b. Select the check boxes corresponding to the groups be imported, and then click the **>>** or **<<** buttons to add or remove the groups.
4. In the **Groups to be Imported** section:
 - a. Select the check boxes of the groups, and then select a role from the Assign Group Role drop-down menu. For more information about the role-based access, see [Role and scope-based access](#).
 - b. Click **Assign Role**.

NOTE: For a logged-in Active Directory user belonging to an imported child Active Directory group, multiple roles such as Device Manager and Viewer are displayed upon a mouse-over on the username on the appliance masthead. This happens if the parent directory group and child directory group are imported with different privileges. For such Active Directory users, the role with the maximum privilege will be applied.

The users in the group under the selected directory service are assigned the selected user roles.

 - c. For the Device Manager role, the scope is defaulted to **All Devices**, however, the administrator can restrict the scope by choosing the **Assign Scope** option followed by selecting the device group(s).
5. Repeat steps 3 and 4, if necessary.
6. Click **Import**.
The directory groups are imported and displayed in the Users list. However, all users in those groups will log in to OpenManage Enterprise by using their domain username and credentials.

Example

It is possible for a domain user, for example john_smith, to be a member of multiple directory groups, and also for those groups to be assigned different roles. In this case, multiple roles such as Device Manager and Viewer are displayed upon a mouseover on the username on the appliance masthead right-hand corner. Such users will receive the highest level role for all the directory groups they are assigned to.

- Example 1: The user is a member of three groups with admin, DM, and viewer roles. In this case, user becomes an administrator.
- Example 2: The user is a member of three DM groups and a viewer group. In this case, the user will become a DM with access to the union of device groups across the three DM roles.

Transfer of ownership of user entities

This topic describes how an administrator can transfer entities such as jobs, firmware/configuration templates and baselines, alert policies, and profiles that are created by a user with a device manager or custom role to another device manager or custom role. Administrators can initiate a 'transfer of ownership' when a user with a device manager role or custom role leaves the organization.

Prerequisites

- Ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in [User roles](#).
- Reassign the device groups that are owned by the former device manager to the device manager who will take over.

About this task

- **Transfer of ownership** transfers only the entities and not the device groups (scope) owned by a user with device manager or custom role to another.
- The appliance only transfers ownership to other active directory or local device manager accounts.

Steps

1. Initiate the **Transfer Ownership** wizard by clicking **Application Settings > Users > Transfer Ownership**.
2. From the **Source User** drop-down list, select the device manager or custom role account from where the ownership of entities must be transferred.

 **NOTE:** The **Source User** drop-down lists only local users. It does not include Active Directory, OIDC, or deleted users.

3. In the **Target User** drop-down list, select the user who can receive the transferred entities. The appliance displays only valid target users based on the entities associated with the source users and the privileges of the target users. For example, if *User1* has Job Management and Template Management privileges, then the valid target users for *User1* would be Device Manager or Custom Role users with at least Job Management and Template Management privilege.
4. Click **Finish** and then click **Yes** at the prompt message.

Results

All the owned entities such as jobs, firmware/configuration templates, alert policies, and profiles are transferred from the source user to the target user.

The **Updated By** field appears in the right pane of the **Jobs** screen when a job is selected. It shows the user who last modified the job. If ownership has been transferred, this field may still display the original user unless the new owner edits the job. This behavior is by design to preserve audit history.

Next steps

The new user with a device manager or custom role should review and reschedule any tasks that were previously scheduled by the former user. This includes tasks that are related to firmware updates or template deployments.

Ending user sessions

End one or more user sessions.

Prerequisites

Ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in [User roles](#).

Steps

1. Select the check box corresponding to the username, and click **Terminate**.
2. When prompted to confirm, click **Yes**.

Results

The selected user session is ended and the user is logged out.

Related references

[Disable OpenManage Enterprise users](#)

[Enable OpenManage Enterprise users](#)

[Manage users and scopes](#)

Directory services integration

Directory Services enable you to import directory groups from Active Directory, or LDAP for use on the console.

Before you begin directory service integration:

- The BindDN user and the user that is used for 'Test connection' should be the same.
- If the User Login attribute is provided, only the corresponding username value that is assigned to the attribute is allowed for appliance login.
- The user that is used for Test connection should be part of any nondefault group in LDAP.
- Attribute of Group Membership should have either the 'userDN' or the short name (used for logging in) of the user.
- When a MemberUid is used as 'Attribute of Group Membership,' the username that is used in appliance login is considered case sensitive in some LDAP configurations.
- When the search filter is used in LDAP configuration, user logins are not allowed for those users who are not part of the search criteria mentioned.
- Group search works only if the groups have users that are assigned under the provided Attribute of Group Membership.
- DNS should be set to return IPv6 as preferred address when queried with FQDN.
- DC certificate must have IPv6 in the SAN field.

 **NOTE:** If the appliance is hosted on an IPv6 network, SSL authentication against the domain controller using FQDN fails if the DNS prefers IPv4. To avoid this failure, do one of the following:

To use directory services:

1. Add a directory connection as described in [Add or edit the Active Directory connection](#).
2. Import directory groups and map all users in the group to a role as described in [Import Active Directory and LDAP groups](#).
3. Device managers should edit the directory groups to add the groups they can manage as described in [Add or edit local users](#).

Add or edit the Active Directory connection

Use directory services to add Active Directory (AD) users to the appliance user groups and assign privileges as required.

Prerequisites

If **RSA SecurID** authentication is required on Active Directory users, ensure that the active directory groups are integrated with the RSA server.

Steps

1. Click **Application Settings > Users > Directory Services**, and then click **Add**.
2. In the **Connect to Directory Service** dialog box, by default, **AD** is selected to indicate that the directory type is Active Directory (AD):
To create an LDAP user group by using Directory Services, see [Add or edit LDAP connection](#).
 - a. In the **Directory Name** box, enter the name for the AD directory.
 - b. Select the domain controller Lookup method:
 - **DNS:** In the **Method** box, enter the domain name to query DNS for the domain controller.
 - **Manual:** In the **Method** box, enter the FQDN or the IP address of the domain controller. For multiple servers, you can use a comma-separated list with a maximum of three servers.
 - c. In the **Group Domain** box, enter the group domain as suggested in the tooltip syntax.
3. In the **Advanced Options** section:
 - a. In the **Server Port** field, Global Catalog Address port number 3269 is populated by default. For the domain controller access, enter 636 as the port number.
Only LDAPS ports are supported.
 - b. Enter the **Network Timeout** and **Search Timeout** duration in seconds. The maximum timeout duration that is supported is 300 s.
To avoid timeouts when using Manual Lookup on multiple domain controllers, ensure that the cumulative **Search Timeout** value does not exceed the **Network Timeout** value.
For example, for a list of three domain controllers, and a **Network Timeout** value of 300 s, the **Search Timeout** must not exceed 100 s.
 - c. To upload an SSL certificate, select **Certificate Validation** and click **Select a file**. The certificate should be a root CA Certificate encoded in Base 64 format.
The **Test connection** tab is displayed.
4. Click **Test connection**.
5. In the dialog box, enter the **username** and **password** of the domain to be connected to.

The username must be entered in one of the following formats:

- User Principal Name (UPN) format: **username@domain** (example: **admin@fwad.local**)
- NetBIOS format: **domain\username** (example: **fwad\admin**)
- Slash-separated format: **domain/username** (example: **fwad.local/admin**)

These formats use the following special characters: @ (in UPN format), \ (in NetBIOS format), and / (in Slash-separated format)

 **NOTE:** If your NetBIOS name and UPN are different, use your UPN to log in.

6. Click **Test connection**.

In the **Directory Service Information** dialog box, a message is displayed to indicate a successful connection.

7. Click **Ok**.

8. Click **Finish**.

Results

A job is created and run to add the requested directory in the Directory Services list.

Editing Active Directory (AD) groups to be used with Directory Services

1. In the **DIRECTORY NAME** column, select the directory. The Directory Service properties are displayed in the right pane.
2. Click **Edit**.
3. In the **Connect to Directory Service** dialog box, edit the data, and click **Finish**. The data is updated and saved.

Add or edit LDAP connection

Add or edit properties of Lightweight Directory Access Protocol (LDAP) groups that must be used with directory services. Use either DNS or manual methods to select domain controllers.

Prerequisites

If **RSA SecurID** authentication is required on LDAP users, ensure that the LDAP groups are integrated with the RSA server.

Steps

1. Click **Application Settings > Users > Directory Services**, and then click **Add**.
2. In the **Connect to Directory Service** dialog box, select the **Type of Directory** as **LDAP**.

 **NOTE:** To create an AD user group by using Directory Services, see [Add or edit the Active Directory connection](#).

- a. In the **Directory Name** box, enter a name for the LDAP directory.
- b. Select the **Domain Controller Lookup** method:
 - **DNS:** In the **Method** box, enter the domain name to query DNS for the domain controller.
 - **Manual:** In the **Method** box, enter the FQDN or the IP address of the domain controller. For multiple servers, you can use a comma-separated list with a maximum of three servers.
- c. Enter the LDAP Bind Distinguished Name (DN) and password.

 **NOTE:** Anonymous bind is not supported for AD LDS.

3. In the **Advanced Options** section:

- a. By default, in the **Server Port** field, the LDAP port number 636 is populated. To change, enter a port number.

 **NOTE:** Only LDAPS ports are supported.

- b. To match the LDAP configuration on the server, enter the group base DN to search for.
- c. In the **Attribute of User Login** field, enter the user attributes that are already configured in the LDAP system. It is recommended that this value is unique within the selected Base DN. Else, provide a **Search Filter** to ensure that it is unique.

 **NOTE:**

- The user attributes should be configured in the LDAP system that is used to query before integrating on the directory services.

- You must enter the user attributes as **cn** or **sAMAccountName** for AD LDS configuration and **UID** for LDAP configuration.
- If more than one user DN is found for the search combination of attribute and search filter, the login operation fails.

- In the **Attribute of Group Membership** box, enter the attribute that stores the groups and member information in the directory.
- Enter the **Network Timeout** and **Search Timeout** duration in seconds. The maximum timeout duration that is supported is 300 s.

NOTE: To avoid timeouts when using Manual Lookup on multiple domain controllers, ensure that the cumulative Search Timeout value does not exceed the Network Timeout value. For example, for a list of three domain controllers, and a Network Timeout value of 300 s, the Search Timeout must not exceed 100 s.

- To upload an SSL certificate, select **Certificate Validation** and click **Select a file**. The certificate should be a root CA Certificate encoded in Base 64 format.

The **Test connection** button is enabled.

- Click **Test connection**, and then enter the bind user credentials of the domain to be connected to.

NOTE: While testing the connection, ensure that the **Test username** is the value of the **Attribute of User Login** entered previously.

- Click **Test connection**.
In the **Directory Service Information** dialog box, a message is displayed to indicate a successful connection.
- Click **OK**.
- Click **Finish**.

Results

A job is created and run to add the requested directory in the Directory Services list.

Editing LDAP groups to be used with Directory Services

- In the **DIRECTORY NAME** column, select the directory. The Directory Service properties are displayed in the right pane.
- Click **Edit**.
- In the **Connect to Directory Service** dialog box, edit the data, and click **Finish**. The data is updated and saved.

Delete Directory services

To remove imported users from LDAP, directory services can be deleted.

Steps

- Select the check box corresponding to the Directory Services to be deleted.
- Click **Delete**

Related references

[System configuration](#)

[Disable OpenManage Enterprise users](#)

[Enable OpenManage Enterprise users](#)

[Manage users and scopes](#)

Login using OIDC providers

You can log in using OpenID Connect (OIDC) providers. OpenID Connect providers are the identity and user management software that allow users to securely access applications. OpenManage Enterprise supports PingFederate and Keycloak.

CAUTION:

- **User roles and scopes are reset to 'default' on client re-registration with an OIDC provider PingFederate (PingIdentity).** This issue might lead to resetting of the privileges and scope of non-admin roles (DM and Viewer) to that of the Administrator.
- **OIDC provider is triggered during an appliance upgrade, change in network configuration, or change in SSL certificate.**
- **To avoid security concerns post any of the above-mentioned re-registration events, the administrator must reconfigure all the OpenManage Enterprise Client IDs on the PingFederate site. Also, it is highly recommended that Client IDs are created only for Administrator users with Pingfederate till this issue is resolved.**

Overview

When an OIDC provider is configured and enabled, users can log in to OpenManage Enterprise using their federated credentials. Upon first login to OpenManage Enterprise, the appliance creates a corresponding user object. This object is used to associate any entities the user creates, such as baselines, reports, or alert policies.

The OIDC user objects appear under **Application Settings > Users** in OpenManage Enterprise.

Prerequisites

Before enabling an OpenID Connect provider login:

1. To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See [Role and scope-based access](#).
 2. **Add an OIDC provider in the OpenManage Enterprise:** In OpenManage Enterprise Application Settings, add an OpenID Connect provider. When you add the OpenID Connect provider, a **Client ID** is generated for the OpenID Connect provider. For more information, see: [Add an OIDC provider](#).
-  **NOTE:** Only a maximum of four OpenID Connect provider IDs can be added in the appliance.
3. **Configure the OpenID Connect provider using the Client ID:** In the OpenID Connect provider, locate the Client ID, and define a login role (Administrator, Device Manager, Viewer, or Custom Role if any) by adding and mapping the scope that is called **dx cua** (Dell extended claim for user authentication). For more information, see:
 - [Configure OIDC login using PingFederate](#)
 - [Configure OIDC login using Keycloak](#)

View OIDC provider in OpenManage Enterprise

When you add an OpenID Connect provider, it is listed on the **Application Settings > Users > OpenID Connect Providers** screen. The following OIDC provider details are displayed:

- **Name** lists the name of the OpenID Connect provider when it was added in the appliance.
- **Enabled** indicates whether the OpenID Connect provider is enabled in the appliance.
- **Discovery URI** lists the Uniform Resource Identifier (URI) of the OpenID Connect provider.
- **Registration Status** can be one of the following:
 - **Successful** indicates a successful registration with the OpenID Connect provider.
 - **Failed** indicates an unsuccessful registration with the OpenID Connect provider. The 'Failed' OpenID Connect provider registration is allowed even when they are enabled.
 - **In Progress** is displayed when the appliance tries to register with the OpenID Connect provider.

On the right pane, Client ID, Registration Status, Discovery URI are displayed for the selected OpenID Connect provider. Click **See details** to view the certificate details of the OpenID Connect provider.

On the **Application Settings > Users > OpenID Connect Providers** screen, the following tasks are available:

- [Add an OIDC provider](#)
- [Edit an OIDC providers details](#)
- [Test OIDC registration](#)
- [Enable OIDC providers](#)

- [Disable OIDC providers](#)
- [Delete OIDC providers](#)

OIDC user management limitations

When an OIDC user logs in to OpenManage Enterprise for the first time, the appliance creates a corresponding user object. These OIDC user objects appear under **Application Settings > Users** in OpenManage Enterprise, but they cannot be deleted, disabled, or transferred by administrators. This is because the user identity is managed externally by the OIDC provider, and OpenManage Enterprise maintains only a cached reference for internal mapping.

To revoke access for an OIDC user, remove or disable the user in the identity provider.

Related tasks

[Configure OIDC login using Keycloak](#)

[Configure OIDC login using PingFederate](#)

Add an OIDC provider

Adding, enabling, and registering an OpenID Connect (OIDC) provider (Keycloak or PingFederate) allows for an authorized client login to OpenManage Enterprise. This process generates a Client ID.

About this task

To add an OpenID Connect provider to OpenManage Enterprise, go to the **Application Settings > Users > OIDC** screen and do the following:

 **NOTE:** Only a maximum of four OpenID Connect provider clients can be added.

Steps

1. Click **Add** to activate the **Add New OpenID Connect Provider** screen.
2. Fill the following information in the respective fields:
 - a. **Name:** Name for the OIDC client.
 - b. **Discovery URI:** OpenManage Enterprise uses this path to access the provider. For example: `https://keycloak.exampledomain.com:8443/realm/<realmname>`.
 - c. **Authentication type:** Choose from one of the following methods that the access token must use to access the appliance:
 - i. **Initial Access Token:** Provide the Initial access token. The OIDC provider supplies this value.

 **NOTE:** If the DNS name of the key cloak generates the Initial Access Token, the registration must use the DNS name. Similarly, if the IP address of the key cloak generates the Initial Access Token, then the registration must use the IP Address.

- ii. **Username** and **Password:** Provide the username and password to the OIDC provider.
 - d. (Optional) **Certificate Validation** check box: Check the box, upload the OIDC providers certificate by clicking **Browse** or dragging and dropping it into the designated box.
 - e. (Optional) Click **Test URI and SSL Connection** to test the connection with the OpenID Connect provider.
-  **NOTE:** Test connection does not depend on the username and password or the initial access token details. It only checks for the validity of the Discovery URI provided.
- f. (Optional) **Enabled** check box - You can select the check box to allow the authorized client access tokens to log in to the appliance.
3. Click **Finish**.

Results

The newly added OpenID Connect provider is listed on the **Application Settings > Users > OpenID Connect Providers** screen, and the Client ID is displayed on the right pane.

Next steps:

[Configure OIDC login using PingFederate](#)

[Configure OIDC login using Keycloak](#)

Configure OIDC login using PingFederate

To enable OpenManage Enterprise OpenID Connect (OIDC) login using PingFederate, add and map a scope **dx cua** (Dell extended claim for user authentication) to the Client ID and define the user privileges.

About this task

 **CAUTION:** When the appliance console is re-registered with the OIDC provider PingFederate (PingIdentity), user roles and scopes are reset to default. This re-registration can occur during an appliance upgrade, a network configuration change, or an SSL certificate update. As a result, non-administrator roles such as Device Manager or Viewer may be reassigned as Administrator.

To avoid security risks after re-registration, administrators must reconfigure all OpenManage Enterprise Client IDs on the PingFederate site. Until this issue is resolved, it is strongly recommended to create Client IDs only for Administrator users.

The default signing algorithm should be RS256 (RSA Signature with SHA-256).

Steps

1. Add an 'exclusive' or 'default' scope called **dx cua** under Scope Management in OAuth Settings.
2. Map the scope that is created in **OpenID Connect Policy Management > Policy** using the following steps.
 - a. Enable **Include User info in Token**.
 - b. In the Attribute Scope, add the scope and attribute value as **dx cua**.
 - c. In Contract fulfillment, add **dx cua** and select the type as 'Text'. Then, define the user roles for OpenManage Enterprise OpenID Connect provider login using one of the following attributes. The role must be a system-defined role.
 - i. Administrator: **dx cua** : [{"Role": "AD"}]
 - ii. Device Manager: **dx cua** : [{"Role": "DM"}]

 **NOTE:** To restrict access of the device manager to select device groups, say G1 and G2, in OpenManage Enterprise use **dx cua** : [{"Role": "DM", "Entity": "G1, G2"}].

 - iii. Viewer: **dx cua** : [{"Role": "VE"}]
 - iv. Custom Role: **dx cua** : [{"Role": "Custom role name"}]

 **NOTE:** Custom role name should be replaced with the actual name as it appears in the OpenManage Enterprise **Roles** tab.
- d. If an 'exclusive' scope is configured after the client registration in OpenManage Enterprise, edit the configured client in PingFederate and enable the created 'dx cua' exclusive scope.
3. **Dynamic client registration** should be enabled in PingFederate for OpenManage Enterprise client registration. If the 'Require Initial access token' option is disabled on the OpenID Connect provider client settings, the registration works with Username and password. If the option is enabled, then the registration works only with the Initial Access token.

Related concepts

[Login using OIDC providers](#)

Configure OIDC login using Keycloak

To enable OpenManage Enterprise OpenID Connect (OIDC) login using Keycloak, add and map **dx cua** to the Client ID. Define the user privileges as follows:

Prerequisites

The Discovery URI specified in the **OpenID Connect Provider** configuration wizard should have a valid endpoint of the provider listed. For example: `https://keycloak.exampledomain.com:8443/realms/<realmname>`.

Steps

1. In the **Attributes** section of Keycloak Users, define the 'Key and Value' for OpenManage Enterprise login roles using one of the following attributes.

- Administrator: dx cua : [{"Role": "AD"}]
- Device Manager: dx cua : [{"Role": "DM"}]

NOTE: To restrict access of the device manager to select device groups, say G1 and G2, on the appliance use
dx cua : [{"Role": "DM", "Entity": "G1, G2"}].

- Viewer: dx cua : [{"Role": "VE"}]
- Custom Role: dx cua : [{"Role": "Custom role name"}]

NOTE: Custom role name should be replaced with the actual name as it appears in the OpenManage Enterprise **Roles** tab.

2. Once the client is registered in Keycloak, in the Mappers section, add a "User Attribute" mapper type with the below values:

- Name: dx cua
- Mapper Type: User Attribute
- User Attribute: dx cua
- Token Claim Name: dx cua
- Claim JSON Type: String
- Add to ID Token: Enable
- Add to access Token: Enable
- Add to user info: Enable

Related concepts

[Login using OIDC providers](#)

Test OIDC registration

Based on the validity of discovery URI, test the registration status of the appliance with a OpenID Connect (OIDC) provider.

Steps

1. Click **Application Settings > Users > OpenID Connect Providers**.
2. Select an OpenID Connect provider.
3. On the right pane, click **Test Registration Status**.

NOTE: The appliance does not depend on the username and password or the initial access token details. It only checks for the validity of the Discovery URI.

Results

The latest registration status ('Successful' or 'Failed') with the OIDC provider is updated.

Edit an OIDC providers details

Based on the Registration Status of the OpenID Connect (OIDC) provider client, edit the client information.

Steps

1. Navigate to **Application Settings > Users > OpenID Connect Providers**
2. Select an OpenID Connect provider.
3. Click **Edit** on the right pane.
4. Depending on the Registration Status of the OpenID Connect provider client, you can do the following:
 - a. If the Registration Status is 'Successful,' only the Certification Validation, Test Connection, and Enabled check box can be edited.
 - b. If the Registration Status is 'failed,' then you can edit the Username, Password, Certification Validation, Test Connection, and Enabled check box.
5. Click **Finish** to implement, or click **Cancel** to discard the changes.

Enable OIDC providers

The login of an OpenID Connect (OIDC) provider may not be enabled when added to the appliance. These logins must be 'enabled' before use.

Steps

1. Click **Application Settings > Users > OpenID Connect providers**.
2. Select the OpenID Connect providers.
3. Click **Enable**.

Results

Enabling the OpenID Connect providers in OpenManage Enterprise allows the authorized client access tokens to log in to the appliance.

Delete OIDC providers

Delete one or more OpenID Connect (OIDC) providers.

Steps

1. Click **Application Settings > Users > OpenID Connect Providers**.
2. Select the OIDC providers.
3. Click **Delete**.

Disable OIDC providers

Disable one or more OpenID Connect (OIDC) providers.

Steps

1. Click to **Application Settings > Users > OpenID Connect providers**.
2. Select the OpenID Connect provider.
3. Click **Disable**.

Results

The appliance rejects client access tokens from the 'disabled' OIDC providers.

Security certificates

Secure your appliance to device connection by using SSL security certificates.

Click **Application Settings > Security > Certificates** to display information about the currently available SSL certificate of a device.

 **NOTE:** Ensure you have the necessary user privileges as described in [Role and scope-based access](#).

To generate a **Certificate Signing Request (CSR)**, see [Generate and download a certificate signing request](#).

Related concepts

[Set the login security properties](#)

Generate and download a certificate signing request

Generate and download a certificate signing request (CSR).

About this task

Generate the CSR only from within the OpenManage Enterprise appliance.

Steps

1. Click **Application Settings > Security > Certificates** to display information about the currently available SSL certificate of a device.
2. Click **Generate Certificate Signing Request**.
3. In the **Generate Certificate Signing Request** dialog box, enter information in the fields.
 - To ensure optimal security, select the appropriate hash algorithm from the **Hash Algorithm** drop-down list based on your specific requirements. The available options are SHA-256, SHA-384, and SHA-512.
4. Click **Generate**.
A CSR is created and displayed in the **Certificate Signing Request** dialog box.
5. In the **Certificate Signing Request** dialog box, copy the CSR data and submit it to the Certificate Authority (CA) while applying for an SSL certificate.
 - To download the CSR, click **Download Certificate Signing Request**.
 - Click **Finish**.

Assign a web server certificate to an appliance

Assign a dedicated web server certificate to an appliance using the Microsoft Certificate Services.

Prerequisites

- The certificate chain can be in crt, .cer, .ca-bundle, .p7b, .der, and .pem format.
- Generate and download the Certificate Signing Request (CSR) as described in [Generate and download a certificate signing request](#).
- Certificates must be signed with the SHA-256, SHA-384, or SHA-512 algorithm because OpenManage Enterprise does not support certificates signed with the SHA-1 algorithm.

Steps

1. Open a web session to the certification server (for example; <https://x.x.x.x/certsrv>) and click **Request a certificate**.
2. On the **Request a Certificate** screen, click the **submit an advanced certificate request**.
3. On the **Advanced Certificate Request** screen, click the **Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS#7 file**.
4. On the **Submit a Certificate Request or Renewal Request** screen:

- a. In the **base-64-encoded certificate request (CMC or PKCS#10 file or PKCS#7)** field, copy and paste the entire content of downloaded CSR.
 - b. For **Certificate Template**, select **Web Server**.
 - c. Click **Submit** to issue a certificate.
5. On the **Certificate Issued** screen, select **Base 64 encoded**, and click either **Download certificate** or **Download certificate chain**.
 6. Upload the certificate to OpenManage Enterprise by clicking **Application Settings > Security > Certificates**, and then, clicking **Upload**.

A **New Certificate** dialog box opens.

In the **New Certificate** dialog box:

- a. Select **Certificate** or **Chain Certificate**. The formats can be in .crt, .cer, .ca-bundle, .p7b, .der, and .pem format.
- b. Click **Select File** to upload the certificate.

 **NOTE:** Ensure the certificate chain does not contain more than 10 certificates.

Results

Your dedicated web server certificate has been assigned to the appliance.

Manage console settings

Set and manage console preferences such as backup and restore settings, report settings, device discovery and health monitoring frequency, and device naming. Click **Application Settings > Console Preferences** to set the default console settings.

 **NOTE:** To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See [Role and scope-based access](#).

The following options are available:

Configure Backup and Restore settings

Expand **Backup/Restore** settings to set **Backup/Restoration Timeout** (Max: 120 minutes) and **Max Number of Backups** (Range: 2-20). When the user crosses the **Max Number of Backups**, the system automatically replaces the earlier backup with the latest one.

1. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.

Customize report rows limit

To set the maximum number of rows that you can view on OpenManage Enterprise reports:

1. Expand **Report Settings**.
2. Enter a number in the **Reports row limit** box. The default limit is 1,000 rows, however, the maximum rows that are permitted are 2,000,000,000.
3. Click **Apply**.

Automate device health monitoring frequency

To set the time after which the health of the devices are automatically monitored and updated on the OpenManage Enterprise Dashboard:

1. Expand **Device Health**.
2. Enter the frequency at which the device health is recorded and the data that is stored.
3. Select:
 - **Last Known:** Display the latest recorded device health when the power connection was lost.

- **Unknown:** Display the latest recorded device health when the device status moved to 'unknown'. A device becomes unknown to OpenManage Enterprise when the connection with iDRAC is lost and OpenManage Enterprise does not monitor the device anymore.
4. Click **Apply** to save the changes to the settings or click **Discard** to reset the settings to default attributes.

Set device names for clear identification

Expand the **Discovery Setting** to set the device naming used by the OpenManage enterprise to identify the discovered iDRACs and other devices using the **General Device Naming** and the **Server Device Naming** settings.

 **NOTE:** Device naming choices in General Device Naming and Server Device Naming are independent and do not affect each other.

1. **ICMP Ping** affects the discovered devices while using the **Multiple** option as the Device Type while creating a Discovery job:
 - **Enable** check box is selected by default. Clear to allow the appliance to pursue discovery without an initial ICMP ping.
 - In the **Retries** box, specify the number of ICMP ping attempts (retries) the appliance makes on the target devices. By default, the value is set to 3.
 - In the **Timeout** box, specify the duration that the appliance must wait for a response before the next attempt. By default, the timeout is set to 30 seconds.
2. **General Device Naming** applies to all the discovered devices other than the iDRACs. Select from one of the following naming modes:
 - **DNS** to use the DNS name.
 - **Instrumentation (NetBIOS)** to use the NetBIOS name.

 **NOTE:**

- The default setting for General Device Naming is **DNS**.
- If a discovered device lacks a DNS or NetBIOS name, the appliance uses its IP address for identification.
- When the **Instrumentation(NetBios)** option is selected in **General Device Naming**, for chassis devices the **Chassis name** is displayed as the device name entry on the **All Devices** screen.

3. **Server Device Naming** applies to iDRACs only. Select from one of the following naming modes for the discovered iDRACs:
 - **iDRAC Hostname** to use the iDRAC hostname.
 - **System Hostname** to use the system hostname.

 **NOTE:**

- The default naming preference for iDRAC devices is the **System Hostname**.
- If an iDRAC lacks a hostname or system hostname, the appliance identifies it by its IP address.

4. To specify the invalid device hostnames and the common MAC addresses expand the **Advance Settings**
 - a. Enter one or more invalid hostnames that are separated by a comma in **Invalid Device Hostname**. By default, a list of invalid device hostname is populated.
 - b. Enter the common MAC addresses separated by a comma in **Common MAC Addresses**. By default, a list of common MAC addresses is populated.
5. Click **Apply** to save the changes to the settings or click **Discard** to reset the settings to the default attributes.

Choose between automatic or manual server-initiated discovery

In **Server Initiated Discovery**, select one of the following discovery-approval policies:

- **Automatic:** Allows the console to automatically discover servers with iDRAC firmware version 4.00.00.00 that are on the same network.
- **Manual:** To allow the user to manually discover the servers.
- Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.

MX7000 Onboarding Preferences

In **MX7000 Onboarding Preferences**: Specify one of the following alert-forwarding behaviors on MX7000 chassis when they are on-boarded:

- Receive All Alerts
- Receive 'Chassis' category alerts only.

Manage appliance access control

Appliance Access control lets users choose whether managed devices access the internal share of the appliance using its IP address or FQDN:

- **IP** [default]: Requires all communication to happen using IP address.
- **FQDN** : Enables iDRACs to communicate with appliances in environments where access is controlled by DNS or routing policies, such as when the appliance is part of a software-defined network.

NOTE:

- The FQDN option cannot be selected unless a DNS hostname and domain name are specified for the appliance; they must be set [via the TUI tool](#).
- Windows driver updates are not supported on devices managed via FQDN.

Built-in Appliance Share

In **Built-in Appliance Share**, select an external network share the appliance uses for firmware updates, template deployment, and downloading diagnostics or support reports:

NOTE:

- The share type or the credentials of an active network share cannot be changed if the appliance tasks are using that network share.
 - Managing device configuration and deployment of templates are not supported on M1000e chassis.
- **CIFS v2**(Default): To enable SMBv2.

 **NOTE:** On OpenManage Enterprise 4.1 and later versions, SMBv1 is not a supported protocol for accessing the built-in appliance share.

Table 27. Minimum firmware version required for SMBv2 support

Device Type	Minimum FW version
PowerEdge VRTX chassis	3.21
PowerEdge M1000e chassis	6.10
PowerEdge FX2 and FX2s sleds	2.21
iDRAC9 and 10	All versions

- **HTTPS:** To disable the default CIFS and to enable HTTPS.
 - Device operations using HTTPS may fail on PowerEdge servers with older iDRAC firmware versions that do not support HTTPS. See [Firmware and DSU requirements for HTTPS](#).
 - When the internal share uses HTTPS then template creation, template deployment, Boot to Network ISO, and firmware updating are not supported on FX2, VRTX chassis, and M1000e chassis.
 - The credentials to the HTTPS share are automatically rotated every 6 hours.

 **NOTE:** When the built-in appliance share in OpenManage Enterprise is configured to use HTTPS with a custom-signed certificate, you must install the root CA certificate on the remote host operating system.

Configure the sender's email address for outgoing messages

Expand the **Email Sender Settings** to set the address of the user who is sending an email message:

1. Enter an email address in the **Sender Email ID** box.
2. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.

Configure trap forwarding format

Expand **Trap Forwarding Format** to set the trap forwarding format—

1. Select one of the following options.
 - **Original Format (Valid for SNMP traps only)**: To retain the trap data as-is.
 - **Normalized (Valid for all events)**: To normalize the trap data. When the Trap-forwarding format is set to 'Normalized,' the receiving agent such as the Syslog receives a tag containing the device IP from which the alert was forwarded.

NOTE: To forward audit logs, internal alerts, and incoming Redfish events to an SNMP destination, select **Normalized (Valid for all events)**. Redfish events are converted and forwarded as SNMP trap. By default **Original Format (Valid for SNMP traps only)** is selected that does not forward audit logs, internal alerts, and Redfish events via SNMP trap forwarding.

2. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.

iDRAC vConsole Settings

Expand **iDRAC vConsole Settings** to set **Maximum Allowed Session Cache**. This setting determines the maximum number of sessions that can be cached. The default value is 10.

1. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.

Alert Correlation Settings

In **Alert Correlation Settings**: This feature considers correlating alerts from a managed or monitored device. When enabled, an internal correlation task correlates any outstanding Critical or Warning alerts to the corresponding Informational alert. While there is no visible difference on the UI, the API (`/api/AlertService/Actions/AlertService.GetCorrelatedAlerts`) can be used to get the last correlated alerts.

NOTE: Enable Alert Correlation is disabled by default.

1. **Interval (minutes)** can be set at 3 minutes minimum or 60 minutes maximum. The default value is 3 minutes.
2. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.

NOTE: Alert Correlation is not supported for CDU and power shelves.

Power Management metric collection settings

In **Metrics Collection Settings**: To set the frequency of the Power Management data maintenance and purging do the following:

1. In the **Data purge interval** box, enter the frequency to delete the Power Management data. You can enter values within 30 to 365 days.
2. Click **Apply** to save changes or click **Discard** to reset the settings to the default attributes.

Configure iDRAC password management

iDRAC Password Management feature enables the management of credentials for supported iDRACs either internally by OME (if the feature is installed during initial-onboarding) or externally via CyberArk integration to perform various device

management operations. Expand **iDRAC Password Management** to configure the preferred management solution. When password management is enabled, it applies to all eligible iDRACs, resulting in password rotation for each of them.

NOTE:

- To avoid performance issues in a scaled environment, it is recommended to schedule iDRAC password rotation tasks with the longest interval possible.
- When changing password management and/or rotation settings on the appliance or CyberArk, all saved discovery jobs are triggered to ensure the eligible devices have the appropriate credentials.

Related tasks

[Internal iDRAC credential management](#)

[Enable internal OME password rotation feature](#)

[CyberArk integration for password management](#)

Internal iDRAC credential management

Enabling the internal iDRAC credential management feature during the initial onboarding process allows OpenManage Enterprise to create a local service account on supported iDRACs after the first successful discovery of the target devices. The local account username is of the following format: OME_[application-GUID]. You can retrieve the application GUID for the appliance by using a GET request to the `/api/ApplicationService/Info` REST API.

Prerequisites

- OpenManage Enterprise Advanced or Advanced+ license is required to use the internal iDRAC credential management feature.

NOTE: Internal iDRAC credential management is also supported on iDRACs that contain OpenManage Essential Server Configuration Management license.

- The internal iDRAC credential management feature requires creating a service account on each eligible iDRAC device. iDRAC supports up to 16 local user accounts, and when exceeded, the service account cannot be created. In such cases, communication between the appliance and iDRAC will rely on discovery credentials.
- Ensure Password Strength Policy is not configured on supported iDRACs. If the Password Strength Policy is configured on iDRACs, it sets certain complexity requirements for passwords. If the password generated by the OpenManage Enterprise service account fails to meet these requirements, iDRAC will disable the service account. Refer to the *iDRAC user's guide* for more information about Password Strength Policy.

Steps

To enable the internal iDRAC credential management, select **Enable Internal iDRAC credential management** during the initial onboarding screen.

OpenManage Enterprise creates a local service account on supported iDRACs after the first successful discovery of the target devices.

Results

Currently, OpenManage Enterprise does not provide an option to opt out of the iDRAC credential management feature. Consequently, if a service account is disabled because of the password strength policy, customers will be unable to manage the corresponding iDRACs from OME. Furthermore, no user roles are assigned to this service account.

Next steps

(Optional) [Enable internal OME password rotation feature](#)

Related references

[Configure iDRAC password management](#)

Enable internal OME password rotation feature

Prerequisites

- [Enable internal iDRAC credential management](#) option must be enabled during the initial onboarding.
- OpenManage Enterprise Advanced or Advanced+ license is required to use the internal OME password rotation feature.

Steps

To enable the internal iDRAC credential management:

1. Select **Internal OME Password Rotation**. This option is only available if the **Enable Internal iDRAC credential management** was selected during the initial onboarding.
2. Select the **Enable** check box for the **Password Rotation** setting to enable password rotation.
3. Set the password rotation schedule:
 - a. Set the time period to monthly, weekly, or daily.
 - b. Set the start time.
 - c. Set the months during which password rotation will be active.
4. Click **Apply** to save the changes or click **Discard** to reset the settings to the previous values.
5. After enabling the internal OME password rotation, to disable it, clear the **Enable** check box and click **Apply**.

Results

To disable Internal OME Password Rotation, clear the **Enable** check box and click **Apply**.

 **NOTE:** A system previously managed by the internal password management feature has an OpenManage Enterprise created local service account. This account remains on the target system until removed by a system administrator.

Related references

[Configure iDRAC password management](#)

Enable CyberArk integration for password management

OpenManage Enterprise offers integration with CyberArk, a third-party identity management system, to manage privileged credentials in secure vaults for enhanced security and access control. This guide outlines the steps to integrate a CyberArk Privileged Access Manager (PAM) (deployed on-site using self-hosted architecture) with OpenManage Enterprise. See the CyberArk Documentation for more details.

Prerequisites

- CyberArk integration is only available on devices with the OpenManage Enterprise Advanced+ license.

 **NOTE:** CyberArk integration for password management is not supported for 17G, iDRAC 10 based, PowerEdge servers.

- Ensure that the target devices are onboarded within a single CyberArk safe. OpenManage Enterprise supports one safe.
- Only local iDRAC passwords can be rotated using CyberArk. Accounts that are managed using directory services like active directory and LDAP cannot be used with CyberArk integration.
- Ensure that the appliance is accessible to the Central Credential Provider Host.

Steps

To enable CyberArk password rotation:

1. Select **Enable CyberArk Integration** to enable CyberArk integration. Once Cyberark is enabled, the appliance retrieve the credentials for iDRACs, which are already configured in the CyberArk.
2. Click **Export** to generate a downloadable list of iDRACs eligible for this feature.
3. Click **Upload** to upload the certificate that is used for authenticating the **Central Credential Provider Host** to the appliance. Only Certificate-Based Authentication is supported.
4. Enter the **Central Credential Provider Host** IPv4 address or FQDN and **Port #**.
5. Enter the **Application ID** assigned to the appliance from CyberArk to provide a single sign-on to mobile applications.
6. Enter the **Safe** name to allow the appliance to locate the required iDRAC credentials.

7. Select an **IP address**, **FQDN**, or **Service Tag** to decide how credentials are retrieved. Confirm that the account name configured for iDRACs on Password Vault Web Access (PVWA) matches the **IP address**, **FQDN**, or **Service Tag**. This value is based on the chosen value for the **Retrieve Credentials By** field.
8. Click **Test Connection** to verify that the appliance can access and authenticate the central credential provider host. Testing the connection fails when CyberArk is configured without any accounts that are added in the Password Vault Web Access (PVWA).
9. Click **Apply** to save the changes or click **Discard** to reset the settings to the previous values.

Results

To disable CyberArk integration, clear the **Enable CyberArk Integration** check box and click **Apply**. All saved discovery jobs are triggered to ensure that the eligible devices have the appropriate credentials.

NOTE: Important things to consider when enabling CyberArk Integration:

- Ensure proper configuration of CyberArk to prevent disruptions in accessing iDRAC devices through OpenManage Enterprise. Dell Technologies is not responsible for CyberArk software. As a customer of CyberArk, you are responsible for your business, technical, and support relationship with CyberArk. Ensure that you work directly with CyberArk for installing, testing functionality and scalability and the overall management of their software.
- When using CyberArk to manage device credentials, OpenManage Enterprise periodically retrieves passwords from the vault before performing specific tasks. If the retrieval process fails due to vault inaccessibility, incorrect credentials, or ongoing rotation, device tasks also fail, causing the device to enter an unknown state.
- Whenever OpenManage Enterprise cannot connect to a device, an internal event CDEV6131 is generated. If you observe such events for CyberArk managed devices, inform your CyberArk administrator to determine whether the correct credentials are being retrieved.
- When a device managed by CyberArk is discovered with new credentials, the credential type changes to 'discovery.' However, any tasks that are initiated from the appliance on the device use CyberArk credentials.
- Disable CyberArk password management for a specific iDRAC by removing the device account from CyberArk and rediscovering it in OpenManage Enterprise for updated credentials in all management operations.

Related references

[Configure iDRAC password management](#)

Set the login security properties

Set the properties to securely log in to the appliance.

Prerequisites

- You must be a super administrator or administrator to set the login security properties. For more information about roles and privileges, see [User roles](#).
- AD and LDAP directory users can be imported and assigned to one of the OpenManage Enterprise roles (Administrator, DeviceManager, Viewer, or Custom Role user if any).

About this task

By clicking **Application Settings > Security**, you can secure your OpenManage Enterprise by specifying the **Restrict Allowed IP Range**, **Login Lockout Policy**, configuring **TLS Protocol** or **RSA SecurID**.

Steps

1. Expand **Restrict Allowed IP Range**:

 **NOTE:** When "Restrict Allowed IP Range" is configured in the appliance, any inbound connection to the appliance, such as alert reception, firmware update, and network identities are blocked for the devices which are outside the given range. However, any connection that goes out of the appliance works on all devices.

- a. To specify the IP address range that must be allowed to access OpenManage Enterprise, select the **Enable IP Range** check box.
- b. In the **IP Range Address (CIDR)** box, you can enter multiple comma-separated IP address ranges.

- c. Click **Apply**. To reset to default properties, click **Discard**.

NOTE: **Apply** button will not be enabled if multiple IP ranges are entered in the **IP Range Address (CIDR)** box.

2. Expand **Login Lockout Policy** :

- Select the **By User Name** check box to prevent a specific username from logging in to OpenManage Enterprise.
- Select the **By IP address** check box to prevent a specific IP address from logging in to OpenManage Enterprise.
- In the **Lockout Fail Count** box, enter the number of unsuccessful attempts after which OpenManage Enterprise must prevent the user from further logging in. By default, 3 attempts.
- In the **Lockout Fail Window** box, enter the duration for which OpenManage Enterprise must display information about a failed attempt.
- In the **Lockout Penalty Time** box, enter the duration for which the user is prevented from making any login attempt after multiple unsuccessful attempts.
- Click **Apply**. To reset the settings to default attributes, click **Discard**.

3. Expand **TLS Protocol Configuration**:

- Set the **TLS Protocol** to **TLS 1.2 and Higher**, **TLS 1.2**, or **TLS 1.3**.
- Enter a **Custom TLS 1.2 Cipher String** to customize the types of encryption supported by the appliance while using TLS 1.2.
- Enter a **Custom TLS 1.3 Cipher String** to customize the types of encryption supported by the appliance while using TLS 1.3.

4. Expand **RSA SecurID Configuration** to allow administrators to select which appliance users, including other administrators, need multifactor authentication to log in to the appliance:

- To enable **RSA SecurID**, check the **Enabled** checkbox.
- Log in to the RSA Authentication Server and download the RSA Server CA Certificate required. Ensure that the certificate meets the following requirements:
 - Certificate chain is not supported for RSA SecurID configuration.
 - Supported certificate formats:
 - X.509 PEM certificate with extensions: *.pem*, *.cer*, *.crt*
 - X.509 PKCS7 certificate with extensions: *.p7b*, *.p7c*
 - Supported encoding:
 - ASCII Base64 encoding
 - Supported certificates: Root CA or Intermediate certificate
 - Mandatory certificate attributes:
 - Key Usage: Must include "Certificate Signing"
 - Basic Constraints: Subject Type must be set to CA
- Click **Upload** to upload the downloaded certificate and **View** to see the details of the certificate.
- Enter the **RSA SecurID Authentication Server** URL and **Port #** for HTTPS access.
- Enter the **RSA SecurID Client ID**. The ClientID is the hostname/ IP address of the system on which the RSA Authentication Agent application (RSA SecurID SoftwareToken) is installed. Configure the Client ID on the external RSA server's Security Console by clicking **Access > Authentication Agents > Add New** to create a ClientID.
- Enter the **RSA SecurID Access Key**. Retrieve the access key on the RSA authentication server by going to **Setup > System Settings > RSA SecurID > Authentication API** section.

NOTE: Old access keys do not get invalidated when new keys are generated. The life of an access key is determined by the time frame (Default: 60 days) set on the RSA authentication server. If there is a suspected security breach, regenerate the access key twice on the RSA authentication server before entering the key on the appliance.

- Enter the **Connection Timeout**. This is the time period for which the RSA authentication server waits for a response from identity routers.
- Enter the **Read Timeout**. This is the time in seconds a collector waits to read data after the previous read before the read attempt is aborted.
- Use the **Test Connection** button to verify whether the appliance can reach the RSA authentication server via the port provided. If a proxy is configured, ensure that the appliance can still communicate with the RSA Authentication server to avoid service disruption.

To verify whether the certificate provided is valid, send an **HTTP GET** request to `api/ApplicationService/MfaCertificate`.
- Click **Apply** to initiate registration to the RSA authentication server. To discard the changes made, click **Cancel**.

NOTE: After 3 invalid passcode entries, the RSA account goes into 'next token mode'. You are prompted to provide the next 2 passcodes provided by your RSA token generator. If a 4th invalid passcode is entered, your account may

be locked. Although the appliance permits login attempts, RSA authentication for the user fails. Before retrying logins on the appliance, ensure that the RSA server account status is verified.

Related tasks

[Security certificates](#)

Customize the alert display

Specify to indicate if the console must display only acknowledged, unacknowledged, or all alerts.

Steps

1. Click **Application Settings** > **Alerts** and expand the **Alert Display Settings**.
 2. Select one of the following:
 - a. **All** — to enable the display of both acknowledged and unacknowledged alerts.
 - b. **Unacknowledged** — to enable the display of only the unacknowledged alerts.
-  **NOTE:** By default, the **Alert Display Settings** is set as **Unacknowledged**.
- c. **Acknowledged** — to enable the display of only the acknowledged alerts.
3. Click **Apply**.

Changes to the Alert Display Settings would be impact the following OpenManage Enterprise screens:

- The upper-right corner of all the OpenManage Enterprise screens. See [The OpenManage Enterprise GUI](#).
- The **Dashboard** screen. See [The OpenManage Enterprise dashboard](#).
- The **Devices** screen. See [Doughnut charts](#).
- The **Alert Log** table under the **Alerts** screen. See [View alert logs](#).

Configure SMTP, SNMP, and Syslog

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

To 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](#). To configure and authenticate the SMTP server that manages the email communication between the users and OpenManage Enterprise:

1. Expand **Email Configuration**.
2. Enter the SMTP server network address that sends email messages.
3. To authenticate the SMTP server, select the **Enable Authentication** check box and enter the username and password.
4. By default, the SMTP port number to be accessed is 25. Edit if necessary.
5. The **Connection Encryption** can be updated using the drop-down to **STARTTLS** or **SSL/TLS**.
6. You can change the **Email Content-Type** from **HTML**(default) to **Plain Text**.
7. To test if the SMTP server is working properly, click the **Send Test Email** check box and enter an **Email Recipient**.
8. Enter the **SMTP timeout**. The default value for the SMTP timeout is 2 minutes, and the allowed values range from 2 minutes to a maximum of 30 minutes. The SMTP timeout in the appliance indicates the maximum duration the appliance waits for a response from the SMTP server during email communication. If the server does not respond within this time, the appliance considers the operation as timed out. Increasing the timeout may be necessary for users with slower network connections or servers that take longer to process emails.
9. Click **Apply**.
10. To reset the settings to default attributes, click **Discard**.

 **NOTE:** Users with DM privileges are unable to use any SMTP (email) based features until an Admin sets up SMTP.

To configure the SNMP alert forwarding configuration:

1. Expand **SNMP Alert Forwarding Configuration**.

- Click the left-most check box on any of the four rows on which you want to add/edit the SNMP Alert Forwarding Configuration details.
- Select the **Enabled** check box to enable the respective SNMP traps to send alerts if there are predefined events.
- In the **Destination Address** box, enter the IP address of the destination device that must receive the alert.

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

- From the **SNMP Version** menu, select the SNMP version type as SNMPv1, SNMPv2, or SNMPv3 and fill the following fields:
 - In the **Community String** box, enter the SNMP community string of the device that must receive the alert.
 - Edit the **Port Number** if needed. Default port number for SNMP traps=162. See Management ports and protocols in the user's guide.
 - If **SNMPv3** is selected, provide the following additional details:
 - Username:** Provide a username.
 - Authentication Type:** Select *SHA*, *MD_5*, or *None*.
 - Authentication Passphrase:** Enter a minimum of eight characters.
 - Privacy Type:** Select *DES*, *AES_128*, or *None*.
 - Privacy Passphrase:** Enter a minimum of eight characters.
- To test an SNMP message, click the **Send** button of the corresponding trap.
- Click **Apply**. To reset the settings to default attributes, click **Discard**.

 **NOTE:** To forward internal alerts, select the option **Normalized (Valid for all events)** under **Application Settings > Console Preferences > Trap Forwarding Format**. See [Manage console settings](#).

To update the Syslog forwarding configuration:

- Expand **Syslog Forwarding Configuration**.
- Select the check box to enable the Syslog feature on the respective server in the **Server** column.
- In the **Destination Address / Host Name** field, enter the IP address of the device that receives the Syslog messages.
- Default port number by using UDP=514. Edit if necessary by entering or selecting from the box. See Management ports and protocols in the user's guide.
- Click **Apply**.
- To reset the settings to default attributes, click **Discard**.

Manage incoming alerts

Configure SNMP listener profiles to receive device alerts in OpenManage Enterprise and prevent trap loss.

Prerequisites

- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See [Role and scope-based access](#).
- For SNMP v3 configuration, ensure that the device you want to receive alerts from is configured and enabled with the SNMPv3 settings. Have the following SNMPv3 credentials ready: username, authentication type, authentication passphrase, privacy type, and privacy passphrase.

About this task

OpenManage Enterprise supports receiving SNMP traps using SNMP v1, SNMP v2, or SNMP v3 configurations for discovered devices.

To manage incoming alerts in OpenManage Enterprise, go to **Application Settings > Incoming Alerts**. Here, you can set the TrapForward properties that are related to incoming alerts. The default community string is *public* and the default port is 162. Also, you can enhance the security of trap notifications by enabling SNMPv3.

Steps

- In the **Community** box, enter the community string to receive the SNMP traps. The default string is *public*.
For iDRAC servers and MX7000 chassis, you can set the community string during device discovery by selecting the **Set Community String for trap destination from Application Settings**. option. This ensures the community string is configured consistently between OpenManage Enterprise and the devices.

2. By default, the SNMP port number for the incoming traps is 162. Edit this field to change the port number if required.
3. To configure SNMP v1 or v2 settings, click **Apply** to save the changes. Ensure the same configuration exists in the device so that OpenManage Enterprise can receive the SNMP traps.
4. Add or modify SNMP v3 configuration:
 - a. To create a new SNMPv3 configuration, select the **SNMPV3 Enable** check box.
 - b. To add another configuration, click **Add**. You can add up to four unique SNMPv3 configurations.
 - c. Under **SNMP Credentials**, enter the following details:

Fields	Description
User Name	Enter the login ID of the SNMPv3-enabled iDRAC user responsible for managing the settings. The username must be unique for each SNMPv3 listener profile.
Authentication Type	Select the authentication type to authenticate SNMPv3 messages. • SHA • MD5 • SHA-224 • SHA-256 • SHA-384 • SHA-512 NOTE: iDRAC 10 supported authentication types are: SHA-384 and SHA-512. iDRAC 9 supported authentication types are: SHA and MD5.
Authentication Passphrase	Enter the passphrase related to your chosen authentication type.
Privacy Type	Select from the following options: • DES • AES-128 • AES-192 • AES-256 NOTE: iDRAC 10 supported the privacy type is AES-256. iDRAC 9 supported the privacy types are AES-128, DES, and AES-256.
Privacy Passphrase	Enter the passphrase based on your privacy type.
Apply	Click Apply to save the changes. The SNMP credentials and settings are now saved.

- d. To modify an SNMPv3 listener profile, enter the **Authentication Passphrase** and **Privacy Passphrase**, then click **Apply** to save the changes.
 - e. To delete an SNMPv3 listener profile, select the profile and click **Delete**. Click **Apply** to save the changes or click **Discard** to reset to cancel.
5. To go back to the last saved attributes, click **Discard**.

Results

Updating the SNMP configuration does not create any jobs in OpenManage Enterprise. The success or failure of the SNMPTrapListener is recorded in the audit logs. It may take up to one minute to configure the SNMP listener profiles in the appliance. Once configured, `SNMP listener configuration updated successfully` entry appears on the Audit Logs page.

Related information

[Important points to consider for SNMP listener profile configuration](#)

Important points to consider for SNMP listener profile configuration

Unique usernames required for SNMPv3 configurations

If you are using a 16G server with SNMPv3 configured in OpenManage Enterprise, you cannot use the same username for SNMP configuration on 17G servers. This restriction occurs because different SNMP configurations and protocol types require unique usernames. Follow these steps to configure SNMPv3 on 17G servers:

1. Create a user in the iDRAC of the 17G PowerEdge server.
2. Enable and configure the SNMPv3 settings in the iDRAC.
3. Configure the new user in the OpenManage Enterprise SNMPv3 configurations. Ensure you use a unique username for each SNMPv3 listener profile.

Handling SNMP configurations during appliance upgrade

Existing SNMP listener configurations are retained during the upgrade and become effective after the post-upgrade tasks are completed. OpenManage Enterprise will start listening to and receiving alerts based on these settings once the post-upgrade tasks are finished. No additional action is required from the user.

Manage warranty settings

Warranty settings determine the display of warranty statistics by the OpenManage Enterprise web UI—**Home** screen widget, warranty scoreboard located in the banner, and the Warranty screen.

Steps

1. Click **Application Settings > Warranty**
2. Click **Warranty Settings** to activate the dialog box.
3. In the **Show warning if warranties are expiring in the next** box, enter the number of days. You can enter a value 0–1000(both included). The default value is set as 90 days. The warranties expiring based on this setting are represented as  in the report and the widget.
4. From the **Hide expired warranties** options, you can select one of the following:
 - a. **All:** To hide the display of all the 'initial' and 'extended' warranties that are expired.
 - b. **Initial Only:** To hide only the 'initial' warranties that are expired.
 - c. **None:** To display all the expired warranties.

 **NOTE:** **Hide expired warranties** setting does not filter expired warranties from reports or internal alerts that are generated by OpenManage Enterprise.
5. Click **Apply** or **Discard** to either save the warranty settings or to discard the changes and retain the old settings.

Configure remote commands and scripts

Configure remote commands and scripts on the appliance that can be executed by an alert policy Remote Script Execution action.

About this task

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

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

- Remote script execution is not supported on certain device types. Although alert jobs are created for these devices, they fail during execution with the following error: Unable to process action because the operation is not supported by the target device.

Steps

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

OpenManage Mobile settings

Configure OpenManage Mobile settings for using OpenManage Enterprise on either Android or iOS devices.

OpenManage Mobile (OMM) is a systems management application that allows you to securely perform a subset of data center monitoring and remediation tasks on one or more OpenManage Enterprise consoles and/or integrated Dell Remote Access Controllers (iDRACs) by using your Android or iOS device. Using OMM you can:

NOTE:

- Receive alert notifications from OpenManage Enterprise.
- View the group, device, alert, and log information.
- Turn on, turn off, or restart a server.

By default, the push notifications are enabled for all alerts and critical alerts. This chapter provides information about the OMM settings that you can configure by using OpenManage Enterprise. It also provides information required to troubleshoot OMM.

-  **NOTE:** For information about installing and using OMM, see the *OpenManage Mobile User's Guide* at [Dell.com/OpenManageManuals](https://dell.com/OpenManageManuals).

Related references

[Troubleshooting OpenManage Mobile](#)

Related tasks

[Enable or disable alert notifications for OpenManage Mobile](#)

[Enable or disable OpenManage Mobile subscribers](#)

[Delete an OpenManage Mobile subscriber](#)

[View the alert notification service status](#)

[Troubleshooting OpenManage Mobile](#)

Enable or disable alert notifications for OpenManage Mobile

Enable or disable OpenManage Mobile alert notifications from OpenManage Enterprise.

Prerequisites

- The administrator rights are required for enabling or disabling alert notifications for OpenManage Mobile.
- To enable or disable alert notifications for OpenManage Mobile 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](#).
- For OpenManage Enterprise to send alert notifications to OpenManage Mobile, ensure that the OpenManage Enterprise server has outbound (HTTPS) Internet access.

About this task

By default, OpenManage Enterprise is configured to send alert notifications to the OpenManage Mobile application. However, alert notifications are sent from OpenManage Enterprise only when a OpenManage Mobile user adds OpenManage Enterprise to the OpenManage Mobile application.

Steps

1. Click **Application Settings > Mobile**.
2. Select the **Enable push notifications** check box.
3. Click **Apply**.

Related concepts

[OpenManage Mobile settings](#)

Enable or disable OpenManage Mobile subscribers

Enable or disable OpenManage Enterprise to send notifications to OpenManage Mobile subscribers.

About this task

The check boxes in the **Enabled** column in the **Mobile Subscribers** list allow you to enable or disable transmission of alert notifications to the OpenManage Mobile subscribers.

NOTE:

- To enable or disable OpenManage Mobile subscribers 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](#).
- OpenManage Mobile subscribers may be automatically disabled by OpenManage Enterprise if their mobile service provider push notification service indicates that the device is permanently unreachable.
- Even if an OpenManage Mobile subscriber is enabled in the **Mobile Subscribers** list, they can disable receiving alert notifications in their OpenManage Mobile application settings.

Steps

1. Click **Application Settings > Mobile**.
2. To enable, select the corresponding check box and click **Enable**. To disable, select the check box and click **Disable**.

You can select more than one subscriber at a time.

Related concepts

[OpenManage Mobile settings](#)

Delete an OpenManage Mobile subscriber

As an OpenManage Enterprise administrator, delete OpenManage Mobile subscribers so they do not receive any notifications.

Prerequisites

To delete an OpenManage Mobile subscribers 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](#).

About this task

Deleting an OpenManage Mobile subscriber removes the user from the subscribers list, preventing the user from receiving alert notifications from OpenManage Enterprise. However, the OpenManage Mobile user can re-subscribe to alert notifications from the OpenManage Mobile application at a later time.

Steps

1. Click **Application Settings > Mobile**.
2. Select the check box corresponding to the subscriber name and click **Delete**.
3. When prompted, click **Yes**.

Related concepts

[OpenManage Mobile settings](#)

View the alert notification service status

Verify if OpenManage Mobile subscribers are receiving alerts from OpenManage Enterprise.

OpenManage Enterprise forwards alert notifications to OpenManage Mobile subscribers through their respective device platform alert notification service. If the OpenManage Mobile subscriber has failed to receive alert notifications, you can check the **Notification Service Status** to troubleshoot alert notification delivery.

To view the status of the alert notification service, click **Application Settings > Mobile**.

Related concepts

[OpenManage Mobile settings](#)

Notification service status

The alerts sent by OpenManage Enterprise to OpenManage Mobile have statuses such as normal, temporary issue in delivering message, or an issue in delivering that requires troubleshooting or help from tech support teams.

The following table provides information about the **Notification Service Status** displayed on the **Application Settings > Mobile** screen.

Table 28. Notification service status

Status Icon	Status Description
	The service is running and operating normally. NOTE: This service status only reflects successful communication with the platform notification service. If the device of the subscriber is not connected to the

Table 28. Notification service status (continued)

Status Icon	Status Description
	Internet or a cellular data service, notifications will not be delivered until the connection is restored.
	The service experienced an error delivering a message which may be of a temporary nature. If the issue persists, follow troubleshooting procedures or contact technical support.
	The service experienced an error delivering a message. Follow troubleshooting procedures or contact technical support as necessary.

View information about OpenManage Mobile subscribers

View information about subscribers who receive alerts from OpenManage Enterprise to OpenManage Mobile. Export data to a CSV file.

After an OpenManage Mobile user successfully adds OpenManage Enterprise, the user is added to the **Mobile Subscribers** table in OpenManage Enterprise. To view information about the mobile subscribers, click **Application Settings > Mobile**.

You can also export the information about mobile subscribers to a .CSV file by using the **Export** drop-down list.

OpenManage Mobile subscriber information

Specify properties of subscribers who receive alerts from OpenManage Enterprise to OpenManage Mobile.

The following table provides information about the **Mobile Subscribers** table displayed on the **Application Settings > Mobile** screen.

Table 29. OpenManage Mobile subscriber information

Field	Description
ENABLED	Select or clear the check box, and then click Enable or Disable respectively to enable or disable the alert notifications to an OpenManage Mobile subscriber.
STATUS	Displays the status of the subscriber, indicating whether or not OpenManage Enterprise is able to send alert notifications successfully to the Alert Forwarding Service.
STATUS MESSAGE	Status description of the status message.
USER NAME	Name of the OpenManage Mobile user.
DEVICE ID	Unique identifier of the mobile device.
DESCRIPTION	Description about the mobile device.
FILTER	Filters are policies that the subscriber has configured for alert notifications.
LAST ERROR	The date and time the last error occurred when sending an alert notification to the OpenManage Mobile user.
LAST PUSH	The date and time the last alert notification was sent successfully from OpenManage Enterprise to the Alert Forwarding Service.
LAST CONNECTION	The date and time the user last accessed OpenManage Enterprise through OpenManage Mobile.
REGISTRATION	The date and time the user added OpenManage Enterprise in OpenManage Mobile.

Troubleshooting OpenManage Mobile

Troubleshooting issues between OpenManage Enterprise and OpenManage Mobile in successfully exchanging messages.

If OpenManage Enterprise is unable to register with the Message Forwarding Service or successfully forward notifications, the following resolutions are available:

Table 30. Troubleshooting OpenManage Mobile

Problem	Reason	Resolution
OpenManage Enterprise is unable to connect to the Dell Message Forwarding Service. [Code 1001/1002]	Outbound Internet (HTTPS) connectivity is lost.	By using a web browser, check if outbound Internet connectivity is available. If connection is unavailable, complete the following network troubleshooting tasks: • Verify if the network cables are connected. • Verify the IP address and DNS server settings. • Verify if the firewall is configured to allow outbound traffic. • Verify if the ISP network is operating normally.
	Proxy settings are incorrect.	Set proxy host, port, username, and password as required.
	Message Forwarding Service is temporarily unavailable.	Wait for the service to become available.
The Message Forwarding Service is unable to connect to a device platform notification service. [Code 100-105, 200-202, 211-212]	The platform provider service is temporarily unavailable to the Message Forwarding Service.	Wait for the service to become available.
The device communication token is no longer registered with the platform provider service. [Code 203]	The OpenManage Mobile application has been updated, restored, uninstalled, or the device operating system has been upgraded or restored.	• Reinstall OpenManage Mobile on the device or follow the OpenManage Mobile troubleshooting procedures specified in the <i>OpenManage Mobile User's Guide</i> and reconnect the device to OpenManage Enterprise. • If the device is no longer connected to OpenManage Enterprise, remove the subscriber.
The OpenManage Enterprise registration is being rejected by the Message Forwarding Service. [Code 154]	An obsolete version of OpenManage Enterprise is being used.	Upgrade to a newer version of OpenManage Enterprise.

Related concepts

[OpenManage Mobile settings](#)

Related tasks

[OpenManage Mobile settings](#)

Discovering devices

To manage a device using OpenManage Enterprise, perform a device discovery.

To manage a device using OpenManage Enterprise, you must first perform a device discovery. The Device Discovery feature allows you to discover devices in your data center environment. The primary purposes of device discovery are to enable you to manage these devices, improve their usability, and enhance resource availability for your business-critical operations.

OpenManage Enterprise performs discovery tasks asynchronously, improving performance and scalability in large environments. For detailed information on scalability and performance improvements, refer to the *OpenManage Enterprise Scale and Performance Whitepaper*.

Using the device **Discovery** feature, you can also create, run, edit, delete, and stop device discovery jobs. It also provides the ability to view, add, and remove devices from a global exclusion list. See [Global exclusion of ranges](#).

There are two main methods for discovering devices in OpenManage Enterprise:

- Creating and managing device discovery jobs: This involves setting up specific jobs to scan network ranges, hostnames, or import lists of devices, scheduling these jobs, and specifying discovery protocols and credentials. See [Create a device discovery job](#).
- Server-initiated discovery: This method allows servers running supported iDRAC firmware versions to automatically locate and initiate contact with the OpenManage Enterprise console by querying the DNS. See [Server-initiated discovery](#).

Once devices are discovered, they can be managed by OpenManage Enterprise. During device discovery, if the user account specified for the discovery range authenticates successfully on the remote device, the device is automatically onboarded. Alternatively, devices can be onboarded later with different user credentials.

Onboarding devices is the process that enables servers to be managed, rather than merely monitored. If administrator-level credentials are provided during discovery, servers are onboarded, and their status appears as **Managed** in the **All Devices** view. If lower-privileged or custom-role credentials are used during discovery, servers are not onboarded, and their status is shown as **Monitored**. If the console is also configured as a trap receiver on the servers, the onboarding status may be indicated as **Managed with Alerts**. Onboarding jobs can be used to update the management credentials of devices if they differ from those used during discovery. Devices in the 'Discovered' status after a server-initiated discovery job are listed on the All Devices screen. Devices that were previously excluded and removed from the exclusion list must be rediscovered for OpenManage Enterprise to start monitoring them.

Prerequisites

User Privileges: To discover devices, you must have the necessary user privileges within OpenManage Enterprise. This requires being a Super Administrator, Administrator, or a Custom Role user with discovery management privileges and scope-based operational access to the devices. For discovering CDU devices, you must also be a CDU super administrator user.

Network Connectivity and Protocol Configuration:

- Target devices must be reachable from the OpenManage Enterprise appliance over the network using the required protocols.
- Appropriate discovery protocols (such as WS-Man, Redfish, SNMP, SSH, IPMI, or HTTPS) must be enabled and configured correctly on the target devices based on their type and the chosen discovery method.
- For in-band OS discovery on Windows devices, ensure the target server's firewall is configured to allow **Echo Request - ICMPv4-In** and **Echo Request - ICMPv6-In** under **Windows Firewall with Advanced Security > File and Printer Sharing**.
- By default, batch discovery is pursued only on devices that return a positive ICMP ping to reduce the overall duration for discovery. To forego the ICMP ping, disable the ICMP ping Enable checkbox under **Application Settings > Console Preferences > Discovery setting**.

Credentials: You must have valid credentials for the target devices that match the selected discovery protocol. These credentials can include usernames and passwords for WS-Man, Redfish, SSH, ESXi, HTTPS storage, IPMI, SNMP community strings for SNMP devices, or an SSH Enable Password for privileged access on networking devices. The level of credentials provided during discovery determines the initial onboarding status (administrator-level for 'Managed', lower privileged and custom role for 'Monitored').

Managed Device Limit: OpenManage Enterprise can manage a maximum of 8,000 devices. Avoid specifying large networks in discovery jobs that would result in discovering devices exceeding this maximum number, as it may cause the system to abruptly stop responding.

Certificate Validation Considerations: If performing discovery with CA validation, the appliance identifies the device by its DNS name instead of its IP address. Ensure DNS resolution is correctly configured for these devices.

Specific device considerations

- IPMI discovery functionality is limited for Non-Dell servers (such as HP iLO and Lenovo XClarity). Discovery for these devices is primarily supported through their respective Redfish profiles (HP Redfish and Lenovo Redfish).
- Discovery functionality is limited for PowerEdge 11G servers with iDRAC6. WS-Man is not supported in iDRAC 10.
- The Motivair CDU does not support automatic trap destination configuration using the Enable trap reception option during discovery. You must manually configure the CDU UI to set OpenManage Enterprise as the trap destination for SNMP events to be received.
- To support discovery with domain credentials, OpenManage Enterprise (version 3.2 and later) uses the OpenSSH protocol instead of the WSMAN protocol that is used in the previous versions. Hence, all the Windows and Hyper-V devices that are discovered before updating the appliance to 3.2 have to be deleted and rediscovered using their OpenSSH credentials. See the Microsoft documentation to enable OpenSSH on Windows and Hyper-V.
- 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.

Related tasks

[Delete a device discovery job](#)

[View device discovery job details](#)

[Stop a device discovery job](#)

[Run a device discovery job](#)

[Specify a discovery mode for server discovery](#)

[Create a custom discovery job for devices](#)

[Specify discovery mode for Dell storage discovery](#)

[Create a custom discovery job for SNMP devices](#)

[Specify the discovery mode for multiple discovery jobs](#)

[Edit a device discovery job](#)

Topics:

- [Server-initiated discovery](#)
- [Creating and managing device discovery jobs](#)
- [Onboarding devices](#)
- [Protocol support matrix for device discovery and alert reception](#)

Server-initiated discovery

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

- Servers should be running iDRAC firmware version 2.65.65.65 or later.
- Ensure that the iDRAC server is set up for auto-discovery as detailed in the *Integrated Dell Remote Access Controller 9 User's Guide*.
 - Ensure that the iDRAC server is able to obtain console addresses via **Unicast DNS**.
 - Update the **Periodic Refresh** option on iDRAC to customize how often an auto-discovery takes place.

 **NOTE:** Reducing the value of **Periodic Refresh** will increase the traffic on the network.

- The servers must be on the same domain or sub-domain as OpenManage Enterprise.
- Register OpenManage Enterprise 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.
- Enable **Server-initiated discovery** on the TUI.
- Clear old records of the appliance on the DNS to avoid multiple announcements from the servers.

About this task

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

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 the system using the TUI](#).
 - 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:

- To create hostname record

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

- 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 settings](#).
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** screen 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 settings](#)

- **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** screen.

NOTE: The status changes to Discovered when iDRAC re-announces the device and updates the announcement timestamp. The iDRAC Auto Discovery Periodic Refresh setting may delay this re-announcement.

The following tasks can be performed on the **Server Initiated Discovery** screen:

- **Import:** To import the server credentials:
 - a. Click on **Import**.
 - b. In the **Import From File** wizard, click on **Upload Service Tags File** to select a local .csv file.
 - c. To view a sample .csv file of the server credentials, click on **Download sample CSV file**.
 - d. Click on **Finish**.
- **Discover:** To manually discover the servers in 'Ready to Discover' status:
 - a. Select the servers listed on the **Server-Initiated Discovery** screen which are in 'Ready to Discover' Status.
 - b. Click on **Discover** to trigger a discover job and add servers to the **All Devices** screen.
- **Delete:** To delete the servers listed on the **Server-Initiated Discovery** screen
 - a. Select the servers on the **Server-Initiated Discovery** screen which are already discovered and listed on the **All Devices** screen.
 - b. Click on **Delete** to delete from the **Server-Initiated Discovery** screen.

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

- **Export:** To export the server credentials in HTML, CSV, or PDF formats
 - a. Select one or more servers on the **Sever-Initiated Discovery** screen.
 - b. Click on **Export**.
 - c. In the **Export All** wizard, select any of the following file formats: HTML, CSV, and PDF.
 - d. Click on **Finish** to initiate the export job.

Creating and managing device discovery jobs

This topic explains setting up scheduled or on-demand jobs within OpenManage Enterprise to scan specific network ranges, hostnames, or imported lists to find and identify devices in your environment.

Create a device discovery job

Create a job to discover either server, chassis, storage, network devices, power shelves, or coolant distribution units (CDU).

Prerequisites

- You must be a Super Administrator, Administrator, or Custom Role user with discovery management privileges and scope-based operational access to the devices.

- To discover Delta 21" power shelves, you must use an account with administrator privileges of power shelves.
- To discover CDU devices, you must use an account with CDU Super Administrator privileges.
- To reduce the run time of the discovery job, consider the following:
 - Select only the required protocols.
 - Create separate IP ranges for specific protocols.
 - Reduce timeout values and retry attempts where appropriate.

About this task

Creating a discovery job allows you to define the type of devices to discover, their IP addresses or ranges, connection settings, and scheduling options.

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.
3. To include more devices or ranges in this job, click **Add**. This displays additional fields for specifying device properties: Type, IP/Hostname/Range, and Settings.
 -  **CAUTION: OpenManage Enterprise manages a maximum of 8,000 devices. Do not specify large networks with more devices than the supported maximum, as this may cause the system to stop responding abruptly.**
 - When discovering many devices, use IP ranges instead of individual IP addresses.
 - You can also discover devices by importing ranges from a .csv file. See [Discover multiple devices by .csv import](#).
 - To exclude specific devices from discovery, see [Global exclusion of ranges](#). You can add or remove devices from the global exclusion list using the Global Exclusion of Ranges wizard. Devices currently on the global exclusion list will not be discovered, even if included in a discovery range.
4. From the **Device Type** drop-down menu, select the type of device to discover:
 - For servers, select **Server**. See [Specify a discovery mode for server discovery](#).
 - For chassis, select **Chassis**. See [Specify discovery mode for chassis discovery](#).
 - For Dell storage devices or network switches, select **Storage**. See [Specify discovery mode for Dell storage discovery](#).
 - For network switch devices, select **Network Switch**. See [Specify discovery mode for network switch discovery](#).
 - For power shelves, select **Power Shelves**.
 - For Power Distribution Unit (PDU) devices, select **PDU**.
 - When you discover the primary Dell PDU, the chained PDU is automatically discovered.
 - When you discover a primary Dell PDU that has a chained PDU connected, the appliance runs an automatic re-discovery job after the initial inventory completes. This re-discovery is triggered during both scheduled inventory and on-demand inventory tasks to discover any newly added chained PDUs.
 - For Uninterruptible Power Supply (UPS), select **UPS**.
 - For Coolant Distribution Unit (CDU) devices, select **CDU**. See [Specify discovery mode for CDU discovery](#).
 - To discover devices by using multiple protocols, select **MULTIPLE**. See [Specify the discovery mode for multiple discovery jobs](#).
5. In the **IP/Hostname/Range** box, enter the IP address, hostname, 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 **i** symbol.
 - The range size is limited to 16,385 (0x4001).
 - IPv6 and IPv6 CIDR formats are supported.

 **NOTE:** IPv6-based discovery is not supported for Delta 21-inch and Lite-On 21-inch power shelves. These devices must be discovered using IPv4 addresses.
6. In the **Settings** section, enter the username and password of the protocol that is used to discover the ranges.
7. Click **Additional Settings**, to select a different protocol, and change the settings.

 **NOTE:** Ensure that you select the SNMP protocol to discover PDU devices. To discover Dell PDUs, enable Redfish and provide the credentials.
8. In the **Scheduling Discovery Job** section, run the job immediately or schedule it for a later time. See [Schedule job field definitions](#).
9. Select **Enable alert reception from discovered devices**, to enable OpenManage Enterprise to receive SNMP and Redfish-based alerts from discovered devices.

- Alert reception is supported using the following protocols:
 - SNMP protocol for PowerEdge servers, MX7000 chassis, and MotivAir MCDU-4U-T-010.
 - Redfish protocol for power shelf.

NOTE:

- Enabling this setting enables alerts on the iDRAC (if disabled), and set an alert destination for the OpenManage Enterprise server 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.
- For CMC discovery, trap reception is set on the servers, not the chassis.
- The Motivair CDU does not support automatic trap destination configuration; you must manually configure its GUI.

10. Select **Set Community String for trap destination from Application Settings**. This option is available only for the discovered iDRAC servers and MX7000 chassis.
11. Select the **Email when complete** checkbox, 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](#). 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.

Results

A discovery job is created and run. The status is displayed on the **Job Details** screen. During discovery, the user account specified for the range is verified against the privileges on the remote device. If authentication passes, the device is automatically onboarded or can be onboarded later. See [Onboarding devices](#).

Devices like iDRAC-based PowerEdge servers and MX7000 chassis are automatically onboarded if administrator-level credentials are provided during discovery, resulting in a 'Managed' status. Devices discovered with lower-privileges or custom-role credentials would have a 'Monitored' status.

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](#).

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

Discover multiple devices by .csv import

Import data in a .csv file to specify the range of device IP addresses to discover.

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**.
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**.

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.

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](#)

About this task

 **NOTE:** Currently, devices cannot be excluded 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** screen (**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](#).

-  **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** screen.

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

- 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 screen 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 a discovery mode for server discovery

Specify if you want a server to be discovered by using an iDRAC IP address, OS type, or IPMI (for non-Dell servers using out-of-band method).

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)::**
 - Select **HP iLO** to discover and monitor HP iLO devices via Redfish.
 - Select **Lenovo XClarity** to discover and monitor Lenovo XClarity via Redfish.
 - Select **Other** to discover and manage non-Dell servers via 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 [Create a custom discovery job for devices](#).
7. Schedule the discovery job. See [Schedule job field definitions](#).
8. Click **Finish**.
A discovery job is created and displayed in the list of discovery jobs.

Related concepts

[Discovering devices](#)

Create a custom discovery job for devices

While creating a discovery job, use the **Additional Settings** dialog box to enter the details for the protocol with which you want to discover devices.

Steps

1. From the **Create Discovery Job** window, click **Additional Settings**.
Select the protocols that you want to use for discovery. Supported protocols are automatically pre-selected based on your initial inputs. Ensure that you select protocols that are supported; using unsupported protocols can cause the discovery job to fail.
2. To discover using WSMAN/Redfish protocol, select the following options based on your device type:
 - Discover using WS-Man/Redfish (iDRAC, Server, and/or Chassis)
 - Discover using Redfish (HP iLO)
 - Discover using Redfish (Lenovo XClarity)
 - Discover using Redfish (CDU)
 - Discover using Redfish (Power Shelf)
 - a. In the **Credentials** section, enter a **User Name** and **Password**.
 - b. In the **Connection Settings** section:
 - **Retries** field, enter the number of repeated attempts that must be made to discover a server. The default value is 3.
 - **Connection Timeout** field, enter the time after which a job must stop running. The default value is 60 seconds.
 - To check the WS-MAN response from a target before establishing a connection, set the **WS-MAN Service Check Timeout**. By default the value is set to 1 second with a hard coded number of retries. If a target iDRAC is slow to respond or there are network delays, increase the timeout value to avoid connection failures. The console generates CDEV6131 alerts if a device connection fails.
 - Change the **Port** number. By default, 443 is used to connect to the device. For supported port numbers, see [Management ports and protocols](#)
 - Select the **Enable Common Name (CN)** check box if the common name of the device is the same as the hostname used to access the OpenManage Enterprise.

 **NOTE:** CDU only supports **Enable Common Name (CN)** option.

- Select the **Enable Certificate Authority (CA)** check box, if needed.

 **NOTE:**

- If protocols are disabled or modified post-discovery, rediscover the device with valid credentials to ensure correct protocol usage. This applies to both enabling and disabling protocols post-discovery.
- For a successful in-band device discovery, ensure that the target server's firewall allows **Echo Request - ICMPv4-In** and **Echo Request - ICMPv6-In** under **Windows Firewall with Advanced Security > File and Printer Sharing**.
- When discovering a device using with CA validation, the appliance identifies the device by its DNS name instead of the IP address.

3. To discover using SNMP, see [Create a custom discovery job for SNMP devices](#).

4. To **Discover using IPMI (non-Dell via OOB)**:

a. In the **Credentials** section, enter a **User Name** and **Password**.

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

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

5. To **Discover using SSH (Linux, Windows, Hyper-V)**:

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

a. In the **Credentials** section, enter **User Name** and **Password**.

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

- In the **Retries** field, enter the number of repeated attempts that must be made to discover a server.
- In the **Timeout** field, enter the time after which a job must stop running.
- Change the **Port** number. By default, 22 is used to connect to the device. For supported port numbers, see [Management ports and protocols](#)
- Select the **Verify the known Host key** check box to validate the host against known host keys.

 **NOTE:** Known host keys are added using the `/DeviceService/HostKeys` REST API service. See the *OpenManage Enterprise RESTful API Guide* for more information about how to manage host keys.

- Select the **Use SUDO Option** check box if sudo accounts are preferred.

 **NOTE:** For sudo accounts to work, the servers `/etc/sudoers` file must be configured to use NOPASSWD.

6. To **Discover using ESXi (VMware)**:

a. In the **Credentials** section, enter a **User Name** and **Password**.

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

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

7. To discover storage devices using HTTPS, see [Create a custom discovery job for HTTPS storage devices](#).

8. To discover Dell SONiC switches using HTTPS protocol, enter the credentials in the **Network HTTPS** section.

Related concepts

[Discovering devices](#)

Specify discovery mode for chassis discovery

Create a chassis discovery job by using the chassis IP address, range, or by creating a customized discovery template.

About this task

Complete Chassis Discovery (CCD) is a feature in OpenManage Enterprise that enables you to discover all the components of a chassis in one operation. CCD discovers all the components of a chassis, including the chassis itself, blades, and I/O modules.

Steps

1. From the **Device Type** drop-down menu, select **CHASSIS**.
Based on your selection, the fields change under **Settings**.
2. Enter the IP address, hostname, or IP range in **IP/Hostname/Range**.
3. Under **Settings**, enter the username and password of the server to be detected.
4. Type the community type.
5. To create a customized discovery template by clicking **Additional Settings**, see [Create a custom discovery job for the chassis](#).

Results

- 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.
- 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 a custom discovery job for the chassis

Use the **Additional Settings** dialog box to enter the details for the protocol with which you want to discover the chassis.

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. This section 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 the 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. To check the WS-MAN response from a target before establishing a connection, set the **WS-MAN Service Check Timeout**. By default the value is set to 1 s with a hard coded number of attempts. Increase the timeout value beyond the default if a target iDRAC is slow to respond or experiences network delays to prevent connection failures. If the device fails to connect, the console generates CDEV6131 alerts.
 - d. 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 [Management ports and protocols](#).
 - e. If the common name of the device is the same as the hostname used to access the appliance, **Enable Common Name (CN) check**
 - f. Select the **Enable Certificate Authority (CA) check** check box.

 **NOTE:** When a certificate is used for device discovery with CA entries, the device is identified with the DNS name, not the IP address.

4. Select the **Enable SSH Credentials for FX2 IO Module actions** to enable template actions for FX2 I/O modules.
 - a. Select **Use chassis credentials** if the M I/O Aggregator user credentials are the same as 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:

 **NOTE:** If WS-MAN or Redfish discovery encounters different credentials or port numbers for a chassis and its sleds, the discovery group job fails, and the sleds are discovered with a **Proxied** state.

- To check the WS-MAN response from a target before establishing a connection, set the **WS-MAN Service Check Timeout**. By default the value is set to 1 s with a hard coded number of attempts. Increase the timeout value beyond the default if a target iDRAC is slow to respond or experiences network delays to prevent connection failures. If the device fails to connect, the console generates CDEV6131 alerts.
- Enter the **User Name** and **Password**.
- Change the default values for **Retries**, **Timeout**, and **Port** if required.
- Select **Verify known Host key**, to validate the host against known host keys.

 **NOTE:** Known host keys are added using /DeviceService/HostKeys REST API service. See the *OpenManage Enterprise RESTful API Guide* for more information about how to manage host keys.

- Select **Use SUDO Option** if needed.

5. Click **Finish**.
6. Complete the tasks in [Create a device discovery job](#).

Specify discovery mode for Dell storage discovery

Create a storage device discovery job by using HTTPS protocol for PowerVault devices and SNMP protocol for other storage devices.

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 [Create a custom discovery job for SNMP devices](#) or see [Create a custom discovery job for HTTPS storage devices](#).
6. Complete the tasks in [Create a device discovery job](#).

Next steps

To ensure alert reception in OpenManage Enterprise, configure the Openmanage Enterprise IP address in the storage device SNMP settings.

For PowerVault ME4 series storage devices, SNMP traps are sent only by the primary controller.

Related concepts

[Discovering devices](#)

Specify discovery mode for network switch discovery

Create a network switch device discovery job by using IP address, hostname, or IP address range.

About this task

When Dell Networking Switches (OS10) are updated to Dell SONiC Switches, they may not be recognized properly in OpenManage Enterprise, and their connection status may appear as disconnected. As a result, tasks such as refresh status and inventory may fail for this device. To resolve this, rediscovers the device using the HTTPS protocol. After rediscovery, the switch is correctly identified and categorized under the Dell SONiC Switches group, and tasks will resume functioning.

 **NOTE:** After installing the Services plug-in, the SSH protocol will be enabled for network discovery. The SSH protocol is used to collect support bundle logs from managed switches.

Steps

1. Click **Monitor > Discovery > Create**.
The **Create Discovery Job** dialog box is displayed.
2. From the **Device Type** drop-down menu, select **Network Switch**.
3. Choose the switch type: **Dell SONiC Switch** or **Dell OS9 and OS10 Switches**.
4. In the **IP/Hostname/Range** field, enter the IP address, hostname, or IP range of the switch.
5. If the OpenManage Enterprise Services plug-in is installed on OpenManage Enterprise, select the protocol that is used to discover the **Dell OS9 and OS10 Switches**.
 - **SNMP v1/v2:** OpenManage Enterprise supports SNMP v1/v2 protocols for discovering switches.
 - Provide SNMP community string.
 - **SSH:** To ensure the Services plug-in can interact with the network switch using the SSH protocol, fill out the following information:
 - SSH Username (Available under **Additional Settings**)
 - SSH Password (Available under **Additional Settings**)
 - SSH Enable Password (Available under **Additional Settings**)
6. HTTPS protocol is used to discover **Dell SONiC Switches**. Enter the **username** and **password** in the **Settings** section.
 - Click **Additional Settings** to configure retries, timeout, and port details for **Network HTTPS**, if needed.
 - The **Enable Common Name (CN) check** and **Enable Certificate Authority (CA) check** options are not supported for Dell SONiC Switches.
7. Click **Additional Settings** to customize the respective discover protocol according to [Create a custom discovery job for SNMP devices](#) or [Create a custom discovery job for SSH devices](#).
8. Complete the tasks in [Create a device discovery job](#).

Create a custom discovery job for HTTPS storage devices

Create customized discovery jobs for storage devices that use the HTTPS protocol in the **Additional Settings** dialog box. For example, PowerVault devices.

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 [Management ports and protocols](#).
 - d. Select the **Enable Common Name (CN) check** check box if the common name of the device is the same as the hostname used to access the OpenManage Enterprise.
 - e. Select the **Enable Certificate Authority (CA) check** check box.

 **NOTE:** When a certificate is used for device discovery with CA entries, the DNS name identifies the device, not the IP.
3. Click **Finish**.

Next steps

Complete the tasks in [Create a device discovery job](#).

Create a custom discovery job for SSH devices

By default, discover by SSH is selected when discovering Linux based servers.

If the OpenManage Enterprise Services plug-in is installed, network switches can also be discovered using SSH. This discovery method is preferred as it allows the plug-in to interact with the switch. To do so, select **Multiple** for the **Device Type**, and add both SNMP and SSH protocols.

1. Under **Credentials**, enter the **Username** and **Password** that is used to log in to the target device.

 **NOTE:** If the SSH option is not automatically selected, click **Additional Settings** and select the **Discover using SSH** option. The username and password can also be provided here.

2. Enter the **Enable Password** (if required) to allow access to the privileged level of a networking device. This password may also be known as a root or service password.
3. Enter the fields **Retry**, **Timeout**, and **Port** based on your network or firewall settings.
4. Click **Finish**.
5. Complete the tasks in [Create a device discovery job](#).

Create a custom discovery job for SNMP devices

Create discovery jobs for SNMP based devices such as storage and networking 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:** Full switch and Stacked Modes are not currently discoverable by SNMP.

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](#).

Related concepts

[Discovering devices](#)

Specify discovery mode for CDU discovery

Discover Coolant Distribution Units (CDU) using OpenManage Enterprise.

Prerequisites

For discovering CDU devices:

- You must be a Super Administrator, Administrator, or Custom Role user with discovery management privileges and scope-based operational access to the devices. For more information, see [Role and scope-based access](#).
- You must be a CDU super administrator user.

Steps

1. From the **Device Type** drop-down menu, select **CDU**.
Based on your selection, the fields change under **Settings**.
2. Enter the IP address, hostname, or IP range in **IP/Hostname/Range**.
3. Under **Settings**, enter the username and password of the CDU to be detected.
 **NOTE:** The Motivair CDU does not support automatic trap destination configuration using the **Enable trap reception from discovered iDRAC servers and MX7000 chassis** option. You must manually configure the CDU GUI to set OpenManage Enterprise as the trap destination; otherwise, SNMP events will not be received.
4. To create a customized discovery by configuring protocol and credentials, click **Additional Settings**. See [Create a custom discovery job for devices](#).

Specify the discovery mode for multiple discovery jobs

Create discovery jobs for devices that respond to the pings sent by using the ICMP protocol.

About this task

-  **NOTE:** By default, batch discovery is pursued only on devices that return a positive ICMP ping to reduce the overall duration for discovery. To forego the ICMP ping, disable the ICMP ping **Enable** checkbox under **Application Settings > Console Preferences > Discovery setting**. For more information, see [Manage console settings](#).

Steps

1. From the **Type** drop-down menu, select **MULTIPLE** to discover devices using multiple protocols.
2. Enter the IP address, hostname, or IP range in **IP/Hostname/Range**.
3. To create a customized discovery template by clicking **Additional Settings**, see [Create a custom discovery job for devices](#).

Results

You can view the execution status and execution details of the discovery job in the **Job Details** screen. For more information, see [View job details](#).

Related concepts

[Discovering devices](#)

View device discovery job details

View information about a device discovery job.

Steps

1. Click **Monitor > Discovery**.
2. On the main **Discovery** screen, you will see a list of your configured discovery jobs.
The right pane displays a summary of information for the selected job, including:
 - Total possible devices.
 - Whether devices were discovered with specific device types, and their counts.
 - The next scheduled run time for scheduled tasks.
 - The last time the job ran and found devices.
3. The **STATUS** column on this screen shows the current state of a discovery job.
Possible statuses displayed here are:
 - **Queued**. For scheduled jobs, this status appears as **Scheduled** on the **Jobs** screen.
 - Completed.
 - Stopped.
4. To access more detailed information about a particular discovery job, select the row corresponding to the job name, and then click **View Details** in the right pane.

The **Job Details** screen displays the respective discovery job information.

5. For more information about managing jobs, see [Using jobs for device control](#).

Related concepts

[Discovering devices](#)

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 concepts

[Discovering devices](#)

Run a device discovery job

Run a device discovery job that is already created.

Steps

1. In the list of existing device discovery jobs, select the check box corresponding to the job you want to run now.
You cannot re-run a job that is already running.
2. Click **Run**.
The job starts immediately and a message is displayed in the lower-right corner.

Related concepts

[Discovering devices](#)

Stop a device discovery job

Stop a discovery job only if it is already running.

About this task

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 concepts

[Discovering devices](#)

Delete a device discovery job

Delete a device discovery job. However, the devices associated with a job are not deleted.

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.

Steps

1. Click **Monitor > Discovery**.
2. Select the check box corresponding to the discovery job you want to delete, and then click **Delete**.
3. 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

- 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** screen.
- A device discovery job cannot be deleted from the **Jobs** screen.

Related concepts

[Discovering devices](#)

Onboarding devices

Upon device discovery, iDRAC based PowerEdge servers, MX7000 chassis, and Power Shelves devices are automatically onboarded. For PowerEdge servers and MX7000 chassis, onboarding jobs can be used to update management credentials of devices when the device credentials differ from what was used during discovery. If internal iDRAC credential management is enabled and the iDRAC is eligible, the onboarding operation also creates an appliance-managed service account on the target. For Power Shelves devices, onboarding is only used to subscribe for alert reception using redfish events and does not include credential management.

About this task

Onboarding enables devices to be managed, rather than monitored.

- Onboarding tasks only support iDRAC, Power Shelves, and MX7000 chassis-based devices that are not in a managed state of proxy.
- If a Delta 21" Power Shelf has more than 15 Redfish alert subscriptions, it will not be onboarded.
- If administrator-level credentials are provided during discovery, the devices are onboarded (the device status is displayed as **Managed** in the All Devices view).
- If lower-privileged credentials or custom roles are provided during discovery, the devices 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 devices, then their Onboarding status is indicated as **Managed with Alerts**.
- **Error** indicates an issue in onboarding the device.
- The **Proxied** status is available only for the MX7000 chassis. It 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](#).

If you want to change the credentials of a device or reattempt onboarding because of a failure in onboarding during discovery, use the following steps.

 **NOTE:**

- All devices that have been onboarded through this wizard remain onboarded through this user account. The discovery user account does not replace this user account during future discoveries of the device.

- For the already discovered devices, if the SNMP trap destination is manually set on iDRAC as OpenManage Enterprise, the appliance receives and processes alerts. However, the state of the device that is displayed on the **All Devices** screen remains the same as its initial discovered state.
- The **All Devices** screen lists all onboarded chassis as **Managed** despite the chassis user-role credentials that were used during onboarding. If the chassis was onboarded with credentials of a **Read-Only** user, then update activities on the chassis may fail. Hence, It is recommended to onboard chassis with the credentials of a chassis administrator to perform all activities.

Steps

1. Click **Devices** > **All Devices**.

A Donut chart indicates the status of all devices in the working pane. See the [Donut chart](#). The table lists the properties of devices that are selected along with their following onboarding status:

- **Error:** The device cannot be onboarded. Try by logging in by using the recommended privileges. See [Role and scope-based access](#).
- **Managed:** The device has been successfully onboarded. The OpenManage Enterprise console can manage it.
- **Monitored:** The device does not have management options. Devices that are discovered through SNMP may show this status.
- **Managed with alerts:** The device is successfully onboarded. 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 checkbox corresponding to the devices, click **Discovery** > **Onboarding**.

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

NOTE:

- If credentials with lower privileges or custom roles were used during discovery, the devices will not be onboarded.
- All devices that are discovered are not supported for onboarding - iDRAC and MX7000 are supported. Any device that is selected that does not support onboarding, the onboarding option is not available. If you choose devices using the **Across all pages** option, the onboarding action is accessible. However, if any devices that are selected on other pages lack onboarding support, the onboarding job is not generated. This limitation arises from the UI caching the device capabilities, limited to the current view (up to 25 devices at a time).

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

4. Configure **Connection Settings**:

- In the **Retries** box, enter the number of retry attempts for discovering a server.
- In the **Timeout** box, enter the time (in seconds) after which the discovery job should stop running.
 - If the timeout exceeds the current session expiration time, you are automatically logged out of OpenManage Enterprise.
 - If the timeout is within the session expiration window, the session continues without logging out.
- In the **Port** box, enter the port number that the job must use to discover the device.
- [Optional field] Select **Enable Common Name (CN) check** to validate the CN in the certificate.
- [Optional field] Select **Enable Certificate Authority (CA) check** and browse to the certificate file.
- [Optional field] Select **Enable alert reception from discovered devices** checkbox to enable OpenManage Enterprise to receive SNMP and Redfish-based alerts from discovered devices.
 - Alert reception is supported using the following protocols:
 - SNMP protocol for PowerEdge servers, MX7000 chassis, and MotivAir MCDU-4U-T-010.
 - Redfish protocol for Power Shelves.
- [Optional field] Select **Set Community String for trap destination from Application Settings** checkbox to apply the community string to discovered iDRAC servers and MX7000 chassis only.



NOTE: Power Shelves devices do not support the Enable CN and Enable CA options.

5. Click **Finish**.

Protocol support matrix for device discovery and alert reception

Discover devices that are based on the device or Operating System (OS) type by using different protocols such as WS-Man, Redfish SNMP, SSH, IPMI, HTTPS.

The following table lists the supported protocols for device discovery and for subscribing to alert reception when the **Enable alert reception from discovered devices** checkbox is selected during device discovery.

NOTE:

- The functionality of the supported protocols to discover, monitor, and manage the PowerEdge 11G servers with iDRAC6 is limited.
- IPMI discovery is not supported for Non-Dell servers (HP ILO and Lenovo XClarity servers) and hence all inventory data is not available. It is only supported through Redfish protocol, i.e., HP Redfish, and Lenovo Redfish profiles respectively.

For device types that do not support the **Enable alert reception from discovered devices** option, configure the device to send traps to the OpenManage Enterprise IP address.

Table 31. Protocol support matrix for device discovery and alert subscription

Device/ Operating System	Discovery protocols	Discovery/onboarding based alert reception protocols
PowerEdge servers with iDRAC6 and later versions	• Web Services-Management (WS-Man): Supported on iDRAC6 through iDRAC9. Not supported on iDRAC10. • Redfish: Supported on all versions of iDRAC10 and on iDRAC9 firmware version 4.40.10.00 and later.	SNMP
PowerEdge C- Series	Web Services-Management (WS-Man)	SNMP
PowerEdge chassis (CMC)	Web Services-Management (WS-Man)	SNMP
PowerEdge MX7000 chassis	Redfish	SNMP
Storage devices	Simple Network Management Protocol (SNMP)	N/A
Power Distribution Unit (PDU)	• Redfish supported on Dell PDUs. • SNMP supported on: ◦ APC by Schneider Electric rack PDU. ◦ Vertiv Geist rack PDUs	N/A
Uninterruptible Power Supply (UPS)	SNMP	N/A
Ethernet switches	SNMP	N/A
Dell SONiC Switches	HTTPS	N/A
Coolant Distribution Units (CDU)	Redfish	N/A
Power Shelf	Redfish	Redfish
ESXi	ESXi (VMware)	N/A
Linux	Secure Shell (SSH)	N/A
Windows	Secure Shell (SSH)	N/A
Hyper-V	Secure Shell (SSH)	N/A

Table 31. Protocol support matrix for device discovery and alert subscription (continued)

Device/ Operating System	Discovery protocols	Discovery/onboarding based alert reception protocols
Non-Dell servers	Intelligent Platform Management Interface (IPMI)	N/A
PowerVault ME	HTTPS	N/A
HP iLO Remote Server Management	• Redfish • During discovery, select the protocol 'HP Redfish'.	N/A
Lenovo XClarity Controller	• Redfish • During discovery, select the protocol 'Lenovo Redfish'.	N/A

Managing devices and device groups

Manage devices and device groups that the OpenManage Enterprise monitors. The OpenManage Enterprise dashboard enables you to view live information about the status and availability of devices.

OpenManage Enterprise allows you to organize discovered devices into groups. Grouping devices helps you manage them efficiently and quickly within your data center. By organizing devices, you can:

- **Manage devices efficiently:** Grouping devices by criteria such as function, operating system type, user profile, location, or job type allows for targeted management actions. You can manage the properties of devices within a group.
- **Filter data:** Grouping provides a basis for filtering device-related data across various tasks, including device management, firmware updates, discovery, alert policy management, and reporting.
- **Run queries:** Groups can be used to run queries for managing devices and for generating customized reports. Query groups are dynamically defined based on user-specified criteria.
- **Apply Role and Scope-Based Access Control (RBAC and SBAC):** Administrators can limit the operational access of Device Managers and custom role users to specific device groups (scope). Users can only perform tasks on devices within their assigned scope and with necessary RBAC privileges.

Prerequisites

For organizing devices into groups, you must be a Super Administrator, Administrator, or Custom Role user with group management privileges and scope-based operational access to the devices. For more information, see [Role and scope-based access](#).

Device group types

OpenManage Enterprise uses several types of device groups to help organize your discovered infrastructure. These group types are displayed in the left pane of the **All Devices** screen. The main types include:

- **All Devices:** This group is the top-level root group that contains all other groups within OpenManage Enterprise.
- **System Groups:** These groups are default groups that are created by OpenManage Enterprise. You cannot edit or delete a System Group. Access to view System Groups is based on user privileges. System Groups categorize devices based on physical device types or functions as follows:
 - **CDU Devices** includes Coolant Distribution Units. OpenManage Enterprise supports MotivAir MCDU-4U-T-010.
 - **HCI Appliances** includes Hyperconverged devices such as VxRAIL, Dell XC series, and AX devices. Note that depending on the configuration of the target system, discovered HCI devices may display their virtual management address. Also, a discovery job undertaken after Cluster IP or port changes might result in a new cluster group for these devices.
 - **Hypervisor Systems** includes Hyper-V servers, and VMware ESXi servers.
 - **Modular Systems** includes various chassis types such as PowerEdge Chassis, PowerEdge FX2, PowerEdge 1000e chassis, PowerEdge MX7000 chassis, and PowerEdge VRTX chassis. For MX7000 chassis specifically, they can be identified using syntax for Multi-Chassis Management (MCM) groups or Stand-alone Chassis groups, with details on which components (chassis, sleds, network IOMs) form these groups. An MX7000 lead chassis discovers member chassis using the lead's IP

An MX7000 chassis can be a lead, stand-alone, or member chassis. If the chassis is a lead and has a member chassis, the member is discovered using the IP address of the lead chassis. You can identify an MX7000 chassis using one of the following formats:

- **MCM Group:** Represents a Multi-Chassis Management (MCM) group that includes more than one chassis. Use the following format: `Group_<MCMGroupName>_<LeadChassisServiceTag>` where, `<MCMGroupName>` is the name of the MCM group. `<LeadChassisServiceTag>` is the service tag of the lead chassis. The chassis sleds, and network IOMs form this group.
- **Stand-alone Chassis:** Identified using the format: `<ChassisServiceTag>`. This group includes the chassis, sleds, and network IOMs.

- Network Devices: This group includes Dell Force10 networking switches, Fibre Channel switches, and Dell Sonic Switches.
 - When Dell Networking Switches (OS10) are updated to Dell Sonic Switches, they may not be recognized properly in OpenManage Enterprise, and their connection status may appear as disconnected. As a result, tasks such as refresh status and inventory may fail for this device. To resolve this, rediscover the device using the HTTPS protocol. After rediscovery, the switch is correctly identified and categorized under the Dell Sonic Switches group, and tasks will resume functioning.
- Power Shelves: Includes power shelves.
- Servers: This general category includes Dell iDRAC servers, Linux servers, Non-Dell servers, OEM servers, and Windows servers.
- Power Distribution Units (PDUs): View the details of a PDU.
- Uninterruptible Power Supply (UPS): View the details of a UPS.
- Storage Devices: This group includes Dell Compellent storage arrays, PowerVault MD storage arrays, and PowerVault ME storage arrays.
- Discovery Groups: These groups are tied to the range of a specific discovery task. They cannot be edited or deleted because the discovery job controls the group where the include or exclude condition is applied.
- **Custom Groups:** These groups are defined by administrators, device managers, or custom role users to meet specific organizational requirements. Custom groups can be either Static Groups or Query Groups. Users with the necessary privileges and scope can view, create, edit, delete, rename, and clone Custom Groups.
 - **Static Groups** are manually created by adding specific devices. Devices remain in a static group until they are manually added or deleted.
 - **Query Groups** membership is dynamically determined by matching devices against specific criteria you define. Devices are automatically included or excluded based on whether they meet the query criteria. Creating more Query groups in the device group hierarchy can impact the overall performance of OpenManage Enterprise. For optimized performance, OpenManage Enterprise captures the health-rollup status after every 10 s, having more Dynamic groups affects this performance.
 - **NOTE:**
 - Static and Query groups cannot have more than one parent group. Meaning, a group cannot be added as a subgroup 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 or driver compliance of the devices that are associated with these groups is not automatically refreshed. It is recommended that the user initiates a firmware or driver compliance for the newly added or deleted devices in such instances.
- **Plug-in Groups:** Created automatically when plugins are installed. Plug-ins, when installed, have their own system groups and some plug-ins allows users to create Custom groups under them.

Group hierarchy: Within OpenManage Enterprise, groups can be structured hierarchically, meaning a group can have a parent group and contain child groups. This hierarchy primarily applies to Custom Static groups. You can create child groups under existing parent groups. When creating a new Static group or adding selected devices to a new group, you have the option to select an existing group as the parent group for the new child group. This allows you to build a tree-like structure for organizing your devices and subgroups.

Group health

On top of the working pane, doughnut charts display the health state and alerts of all devices by default. When you select a specific device group from the left pane on the All Devices screen, the doughnut charts and the device list in the working pane update to display data pertaining only to that selected group. This includes showing the health state and alerts of the group. Also, if a plug-in is installed, a third doughnut chart might display the data of the installed plug-in. For more information, see [Donut chart](#).

All Devices screen interface and actions

- The table after the doughnut chart lists the devices and displays properties such as their health state, power state, name, IP address, and identifier. The Devices list displays a list of devices that the appliance monitors and manages, along with their health status and other data. For more information about the device list, see [Device list](#).
- On the All Devices screen, you can use Advanced Filters to narrow down displayed devices in the Device List based on criteria such as Name, IP Address, Identifier, and more. The filters vary depending on the content being viewed.

- When you select a device in the list, the right pane displays a preview about the selected device(s). When multiple devices are selected, the preview about the last selected device is displayed.
- Under **Quick Actions** in the right pane, management links correlated to the respective device are listed.
- To clear selections from the device list, you can click Clear Selection.
- After you upgrade OpenManage Enterprise to the latest version, the devices list will be updated after the discovery jobs are rerun.
- In the All Devices table, you can select a maximum of 25 devices per page. To perform tasks on more devices, navigate to the pages to select them.
- Tasks related to devices that are performed on the **All Devices** screen can also be performed individually from their respective Device Details screens. Clicking the device name or IP address in the list takes you to the **Device Details** screen.

Topics:

- [Create and manage custom groups](#)
- [Manage physical groups](#)
- [All Devices screen device list](#)
- [All Devices screen actions](#)
- [View and configure individual devices](#)

Create and manage custom groups

Group devices in your data center to manage them. Groups are based on functions, Operating system types, user profiles, locations, and job types.

Related tasks

- [Delete devices from OpenManage Enterprise](#)
- [Refresh device inventory of a single device](#)
- [Refresh the device health of a device group](#)

Create a custom static or query group

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

Prerequisites

Ensure you have the necessary privileges and access, as described in [Role and scope-based access](#).

Steps

1. To activate the **Create Custom Group** wizard:
 - Click **Devices** > **Custom Groups**, click the three dot vertical menu, and click **Create Custom Group**.
 - From the **All Devices** screen, **Group Actions** drop-down menu, click **Create Custom Group**.
2. On the **Create Custom Group** wizard, select from one of the following custom groups:
 - a. **Static Group**.
 - b. **Query Group**

 **NOTE:** The only special characters that are allowed in group names are hyphens, underscores, and spaces.
3. Click **Create**.
Depending on your selection (static or query), either the [Create a static device group](#) wizard or the [Create a query device group](#) wizard is activated.

Results

Once a group (static or query) is created, it is listed under the **Custom Groups**, **Static Groups**, or **Query Groups**.

Create a static device group

On the **All Devices** screen (**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

Ensure you have the necessary privileges and access, as described in [Role and scope-based access](#).

Steps

1. To activate the **Create Static Group** wizard:
 - 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** screen (**OpenManage Enterprise > Devices**). You create query groups using the **Create Query Group** wizard.

Prerequisites

Ensure you have the necessary privileges and access, as described in [Role and scope-based access](#).

Steps

1. To activate the **Create Query Group** wizard:
 - 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, as described in [Select a query criteria](#).
5. Click **Finish**.

Results

The query group is created and listed in the left pane query group section.

Select a query criteria

Define criteria so you can use them generating customized reports and creating query-based device groups. By default, OpenManage Enterprise provides a list of precanned query templates that you can use as-is or customize based on your requirements.

About this task

Define filters while creating query criteria for:

- Generating customized reports. See [Create a report](#).
- Creating Query-based device groups under the **CUSTOM GROUPS**. See [Create a query device group](#).

Define the query criteria by using two options:

- **Select existing query to copy:** By default, OpenManage Enterprise provides a list of system-defined query templates that you can copy and build your own query criteria. A maximum of six 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 a query is evaluated with multiple conditions, the order of evaluation is the same as SQL. To specify a particular order for the evaluation of the conditions, add or take off parenthesis when defining the query.
- When selected, the filters of an existing query criteria are copied only virtually to build a new query criteria. The default filters associated with an existing query criteria are not changed. The definition (filters) of a system-defined query criteria is used as a starting point for building a customized query criteria. For example:
 1. *Query1* is a system-defined query criterion that has the following predefined filter: `Task Enabled=Yes`.
 2. Copy the filter properties of *Query1*, create *Query2*, and then customize the query criterion by adding another filter: `Task Enabled=Yes AND (Task Type=Discovery)`.
 3. Verify that *Query1* still contains the filter criterion: `Task Enabled=Yes`.

Steps

1. In the **Query Criteria Selection** dialog box, select from the drop-down menu whether to create a query criterion for Query groups or generate a report.
2. Add or take off a filter by clicking the plus or dustbin symbol respectively.
3. Click **Finish**.

Results

A query criterion is generated and saved in the list of existing queries. An audit log entry is made and displayed in the Audit logs list. See [Monitoring audit logs](#).

Edit a static group

Modify existing static groups and add or remove devices within them using the **Edit Static Group** wizard on the **All Devices** screen (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](#).
- Scheduled tasks like Blink device, Power Control, and Remote Command Change Virtual console persist even when groups are removed from the hierarchy.

Steps

1. Right-click or use the three vertical dots menu next to the static group and select **Edit** to open 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 clear the devices to include or exclude them from the static group.
Parent groups list all devices that are in their child and nested groups. To remove devices from nested groups, first remove the devices from the child or nested groups, then remove them from the parent group if needed.
5. Click **Finish**.

Results

The changes made to the static group are implemented.

Edit a query group

On the **All Devices** screen, 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](#).

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

Rename a static or query group on the **All Devices** screen.

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** screen, 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](#).

About this task

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** screen. To remove devices from OpenManage Enterprise, see [Delete devices from OpenManage Enterprise](#).

Steps

1. Under **Custom Groups**, right-click the static or query group or click on the three dot 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 **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](#)

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** screen.

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](#).

Steps

1. Click **Devices**.
All Devices screen 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** screen.

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](#).

Steps

1. Click **Devices**.
All Devices screen 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](#). 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** screen by clicking **Devices**.
2. On the left pane, select the group on which you want to refresh the health.
After selection of the group, the device list contains the selected devices in the group.
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 shows the group that you had selected.
6. From the Scheduling drop-down, select one of the following options:
 - a. **Run Now:** Immediately run the **Refresh Health** on the selected group.
 - b. **Run Later:** Select **Run Later** and then select the Date and Time when the Refresh Health job on the group runs.
 - c. **Run on Schedule:** Select either Daily or Weekly and choose a specific time to schedule health refreshing for the group on a daily or weekly basis.

Results

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

View devices associated with system and workload profiles

System profile and workload profile are BIOS settings that are configured in servers for optimizing performance and power consumption. OpenManage Enterprise uses this information to automatically associate servers with the predefined integrated groups.

About this task

OpenManage Enterprise associates servers that are based on system and workload profiles that are configured on BIOS settings in iDRAC. Any configuration change to the system and workload profiles in the BIOS settings causes the device to move to the respective group after every inventory refresh.

Steps

1. In OpenManage Enterprise, click **Devices**.

2. Expand **System Profile Settings**.

The following workload profiles are displayed:

- **DataBase Optimized Performance Profile**—Optimize performance of database workloads.
- **Database Optimized Performance Per Watt Profile**—Optimize performance of database workloads when the system profile is selected as one of the **Performance per Watt** options.
- **HPC Profile**—Optimize performance of HPC workloads.
- **Low Latency Optimized Profile**—Optimize settings for latency-sensitive workloads.
- **NFVI FP Optimized Turbo Profile**—Optimize performance of Network Functions Virtualization Infrastructure with Float-Point (NFVI FP) workloads.
- **NFVI FP Energy-Balance Turbo Profile**—Provides a balance between maximizing performance and optimizing power consumption for achieving energy-efficient NFVI deployments.
- **SDS Optimized Performance Profile**—Optimize performance of Software Defined Storage workloads.
- **SDS Optimized Performance Per Watt Profile**—Optimize performance of Software Defined Storage workloads when the system profile is selected as one of the **Performance per Watt** options.
- **Telco Optimized Profile**—Optimize performance of Telco workloads.
- **Virtualization Optimized Performance Per Watt Profile**—Ensures that all the available virtualization options are enabled when the system profile is selected as one of the **Performance per Watt** options.
- **Virtualization Optimized Performance Profile**—Ensures that all the available virtualization options are enabled.
- **Workload Profile Not Configured**—The workload profile of servers is not configured.

For each workload profile, the following system profiles are displayed:

- **Custom**—Enables you to customize the system profile.
- **Performance**—Provides potentially increased performance by maximizing processor frequency and disabling certain power-saving features such as C-states.
- **Performance per Watt (DAPC)**—It is a default profile. It provides a combination of performance balance and reduction in power consumption.
- **Performance per Watt (OS)**—The operating system manipulates the processor frequencies for a higher power efficiency.
- **Workstation Performance**—Provides increased performance using C-States that are optimized for single-threaded workloads. Enables optimal performance allowing CPU to reach top turbo frequency.

Manage physical groups

OpenManage Enterprise enables you to replicate and update the physical organization and hierarchy of a data center. Using the following hierarchy—Data Center, Room, Aisle, and Rack create the physical groups and add the licensed devices at the rack level.

The physical groups that are created or deleted in OpenManage Enterprise are automatically added or removed from power management and monitoring.

Rack management

Manage the physical group hierarchy, and perform rack utilization for space and power using the rack management features.

Prerequisites

Ensure that the following prerequisites are met:

- The devices have **OpenManage Enterprise Advanced or Advanced+** and the required management console licenses.
- The devices are discovered in OpenManage Enterprise. For information about discovering devices, see OpenManage Enterprise User's Guide.
- The modular server is not in a **Proxied** state in OpenManage Enterprise.

About this task

To monitor and manage racks in your data center, perform the following steps:

Steps

1. Create the [physical groups](#) to replicate the group hierarchies in a data center.
2. Add the [unmonitored devices](#) for power management and monitoring.
3. Add the [individual devices and unmonitored devices](#) in physical groups.
4. View information like group metrics, policy, power and space headroom data, by expanding **Physical Hierachy** to a group level and clicking **Group Details**.
5. Associate Power Distribution Units (PDUs) and Uninterruptible Power Supply (UPS) to a rack. For more information, see [Associate PDU and UPS to rack](#) .
6. Monitor PDU and UPS information. For more information, see [View PDU and UPS associated to rack](#).

Add or edit device details for power-monitored devices

Add device details for devices monitored through the Power Management feature for accurate rack management.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view and edit the device details that are part of groups that are in the Device Manager DM1 user scope. However, as a Device Manager DM1 user, you cannot add any device to the group in your scope.

To add or edit the device details, perform the following steps:

Steps

1. Launch OpenManage Enterprise.
2. On the **Devices** page, select a device by selecting the check box.
3. Scroll down to the end of the page to update the power data in the bottom-right side of the page.
4. Click **Update Details**.
5. Provide the size of the device in the rack unit and the maximum power consumption of the device in Watts and click **Apply**.
The power value is automatically converted to BTU and displayed.

 **NOTE:** For UPS devices, only the device size can be updated.

The details for the device are updated.

Create physical groups in OpenManage Enterprise

OpenManage Enterprise enables you to replicate and update the physical organization and hierarchy of a data center. Using the following hierarchy—Data Center, Room, Aisle, and Rack create the physical groups and add the devices at the rack level.

About this task

After a server is discovered and inventory is successful, the server gets automatically placed in the respective physical group based on the location data available on the device.

Before you upgrade to OpenManage Enterprise version 4.5, if a device is already placed in a physical hierarchy, after the upgrade is completed, the location data on the device will not be used to place the device in a different location. A blue banner is displayed on the Rack Details page to update the device location to resolve inconsistency.

If no location data is available during discovery and inventory of servers, create physical groups manually or by importing a CSV file having the physical group details or replicate your data center hierarchy virtually in OpenManage Enterprise.

The physical groups that are created or deleted in OpenManage Enterprise are automatically added or removed from power management and monitoring.

NOTE: If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view only the devices and groups that are assigned to a Device Manager DM1 user.

Steps

1. Start OpenManage Enterprise.
2. On the **Devices** page, in the **Physical Hierarchy** section, click more options, and then click **Create New Physical Group**.
3. Provide a name and description for the group, select the **Group Hierarchy** and **Parent Group** with the defined power capacity.

NOTE:

The only special characters that are allowed in group names are hyphens, underscores, and spaces.

When selecting the **Group Hierarchy** and **Parent Group** fields, ensure that you use the following hierarchy.

Table 32. Supported parent and child group hierarchy information

Parent Group	Group Hierarchy
Data Center	Room, Aisle, Rack
Room	Aisle, Rack
Aisle	Rack
Rack	N/A

Table 33. Physical group attributes details

Field	Description	Mandatory	Value Range
Name	Provide a unique name for the physical group.	Yes	Combination of characters, special characters, and numbers. Limit: 1–255 characters
Description	Provide brief information about the physical group.	No	Combination of characters, special characters, and numbers. Limit: 0–255 characters
Group Hierarchy	Defines the category under Parent Group	Yes	• Data Center • Room • Aisle • Rack

Table 33. Physical group attributes details (continued)

Field	Description	Mandatory	Value Range
Parent Group	Defines the high-level hierarchy for the physical group.	Yes	- Physical Hierarchy - Previously created Physical Groups
Power Capacity (W)	Provide the maximum defined power consumption of the physical group.	Yes, for the Rack group. Optional for data center, room, and aisle groups.	Recommended limits: 1–629365631
Space Capacity (U-SIZE)	Provide the rack capacity for rack management purpose. <i>i</i> NOTE: This option is only applicable for Racks .	Yes	Recommended limits: 1U – 80U

i **NOTE:** The power capacity and space capacity of the device is updated only in OpenManage Enterprise and not in iDRAC or CMC consoles.

Add devices in physical groups

Add devices in physical groups for accurate rack management.

Prerequisites

Ensure that the following prerequisites are met:

- Add the size of the unmonitored device that you plan to add to a physical group.
- Before adding the UPS devices and non-Dell servers to rack slots, add the U-Size information. For more information about updating the U-Size, see [Add or edit device details for power-monitored devices](#).
- Emergency Power Reduction (EPR) is not enabled on the group.

i **NOTE:** If a device discovered through in-band method (operating system) or a compute without OpenManage Enterprise Advanced or Advanced license is added to a device group monitored by Power Management, and later out-of-band discovery is performed or required license is deployed, the device will automatically start monitoring metrics within 12 hours and contribute to group level metrics.

Steps

1. Start OpenManage Enterprise and perform one of the following steps:

- On the **Devices** page, expand the **Physical Hierarchy** group until a rack level and right-click and select the **Manage Rack** option.

The **Manage Rack** page is displayed.

Or

- Start OpenManage Enterprise, and then click **Power Management > Rack View**.

The **Rack View** page is displayed.

Optional: To filter and view the data, expand the **Advanced Filters** option. The following is a list of categories available:

- **Group Name**
- **Health State**
- **Power State**
- **Connection State**
- **Type**

Select the categories of your choice and view the filtered data.

- Click the rack name.

The **Manage Rack** page is displayed.

2. To add devices discovered in OpenManage Enterprise, click **Add To Rack Slot**.

NOTE: Rack management is supported from rack slot number one.

The **Add Device(s) To Rack Slots** wizard is displayed.

3. In the **Select Device(s)** section, select the devices and click **Next**.

Half-width compute sleds cannot be added directly to the Rack. The unmonitored chassis that encloses the sleds can be added to the Rack.

4. Optional: To filter and view the data, perform the following steps:

- a. Click **Advanced Filters**.
- b. Select your category of filters.

The following filters are displayed for devices:

- **Health State**
- **Power State**
- **Connection State**
- **Name**
- **Size of Device (U)**
- **Identifier**
- **Model**
- **Type**
- **Managed State**

5. In **Add device(s) to rack slots**, by default, the devices are automatically added in the available slots in the rack. To add a device at a specific slot, select the **Auto** drop-down menu and select the required slot.

6. Click **Finish**.

The devices that are added are graphically displayed on the **Manage Rack** page.

NOTE:

- The rack slot option is available for a chassis, Rack servers, non-Dell servers, storage, network switches, UPS, unmonitored devices, CDU, and power shelves.
- Only one CDU can be added to a rack.

To view details of modular servers inside a chassis and details of the connected Input Output Modules (IOM), locate the chassis in the **Manage Rack** page and hover the pointer at the IP address or device name.

Automatically create physical hierarchy

Automatically create a physical hierarchy for devices—server and chassis—based on the location that is configured on the device.

About this task

- Only administrators can automatically create a physical hierarchy.
- This feature is not supported on non-Dell servers.

Steps

1. Start OpenManage Enterprise and perform one of the following steps:

- Click **Power Management > Power Managed Devices > Physical groups > Automatically Create Physical Hierarchy**.
- Click **Power Management > Rack View > Automatically Create Physical Hierarchy**.
- On the **Devices** page, click more options in **Physical Hierarchy > Automatically Create Physical Hierarchy**.

NOTE: The only special characters that are allowed in group names are hyphens, underscores, and spaces. The groups are created based on the location that is configured on the device.

2. Select the devices that you want to add. If conflicts exist, see [Resolve conflicts to automatically create physical hierarchy](#).
3. To view the selected devices, click the **Selected Devices** tab.
4. Click **Create Hierarchy**.

If a hierarchy does not exist, it is automatically created. View the progress of the task in **Monitor > Jobs**.

Resolve conflicts to automatically create physical hierarchy

When you select devices to create a physical group, inconsistencies might exist because slot is occupied, rack size is insufficient, or EPR is enabled.

About this task

To resolve inconsistencies because a slot is occupied, rack size is inadequate, or EPR is enabled, do the following by selecting an option from the **CONFLICT** list:

Steps

1. If a slot is occupied, select **Modify Slot**, enter a slot number, and click **Apply**.
2. If a rack size is inadequate, select **Modify Rack Space Capacity**, enter a rack size, and click **Apply**.
3. If EPR is enabled, select **Disable EPR > Yes > Apply**.
Only EPRs that are manually applied can be disabled.
4. To change the hierarchy location, select **Modify Hierarchy Location** and provide an alternative location.
If devices associated with an unmonitored chassis report different location information, use the Modify Hierarchy Location option to provide the location information.
5. To view the conflicts for a device, hover over the information icon.

View physical groups and the hierarchies

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view only the devices and groups that are assigned to a Device Manager DM1 user.

 **NOTE:** To view a complete list of devices in a physical group (including the Unmonitored Devices), click the **Rack View** tab.

Steps

Start OpenManage Enterprise and perform one of the following steps:

- a. On the **Devices** page, expand the **Physical Hierarchy** group to view all the physical groups created.
OR
- a. Click **Power Management > Power Managed Devices**.
- b. Click **Physical Groups**.

All the physical groups that are created in OpenManage Enterprise are displayed with their name, location, total devices in the group, and information about when they were added to OpenManage Enterprise.

 **NOTE:** The location of the physical group is displayed based on the hierarchy that is selected for this particular group at the time of creation.

View devices added in rack

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, If you are logging in as a Device Manager DM1 user, you can view only the devices and groups that are assigned to a Device Manager DM1 user.

Steps

1. Start OpenManage Enterprise and perform one of the following steps:

- a. To view the devices, go to the **Devices** page.
- b. In the left pane, expand the **Physical Hierarchy** group until a rack level and right-click and select the **Manage Rack** option.

When you hover the mouse pointer over the rack group, data about most recent average power consumption, carbon emission value for the last one hour, and accelerator count is displayed.

Or

- a. Start OpenManage Enterprise, and then click **Power Management > Rack View**.

The **Rack View** page is displayed.

Optional: To filter and view the data, expand the **Advanced Filters** option. The following is a list of categories available:

- **Group Name**
- **Health State**
- **Power State**
- **Connection State**
- **Type**

Select the categories of your choice and view the filtered data.

- b. Click the rack name.

The **Manage Rack** page is displayed.

2. View the devices in the rack by navigating on the **Manage Rack** page.
All the devices added to the rack are displayed.
3. Optional: View the **Space Capacity** field at the upper right side of the page to know the amount of space consumed in the rack.

View rack group information

View information about the rack group.

Steps

1. Start OpenManage Enterprise and go to the **Devices** page.
2. In the left pane, expand the **PHYSICAL HIERARCHY** group until a rack level and select a rack group.
3. To view information about the group, click **Rack Details**.
4. On the **Overview** page, rack representation, location data, and telemetry data are displayed. To manage the devices in the rack, click **Manage Rack**.

A visual representation of the devices part of the rack consisting of device name, health status, model type, and chassis (the device is part of a chassis) are displayed.

The following telemetry data is displayed:

Table 34. View rack group information

Rack group data	Description
Capacity	Indicates the amount of capacity consumed.
Accelerators count	Indicates the total number of accelerators available in the servers of the rack group. The total count includes the processing accelerators, FPGA, and GPU.
Power and thermal	Indicates the minimum, maximum, and average values.
Power headroom	Indicates the amount of power headroom consumed.
Carbon emission	Indicates the carbon emission value for the last one hour.

Manage rack power operations

Perform a sequential and staggered power on or power off operation among the servers in a rack.

About this task

To configure the settings to set the delay for performing the power operation among the servers in a rack, see [Set preferences](#). This feature is supported only on Dell servers.

 **NOTE:** The Power On operation can be initiated even when EPR is enabled.

Steps

1. Start OpenManage Enterprise and click **Devices**.
2. In the left pane, expand the **PHYSICAL HIERARCHY** group until a rack level and right-click and select **Power Operations**.
3. To power on the server, select **Power On Servers**.
If you want to safely power on all the devices in the rack, then before you perform the operation, the following devices must be powered on in the recommended order: Power shelves, switches, and then CDUs.
4. To power off the server, select **Power Off Servers**.
If you want to safely power off all the devices in the rack, then after you perform the operation, the following devices must be powered off in the recommended order: CDUs, switches, and then power shelves.
5. To perform the operation later, select the schedule from the drop-down menu and enter the date and time, and then click **Apply**.

Edit physical groups

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can only view the groups and devices in the groups that are assigned to Device Manager DM1 user. You cannot perform any management tasks on the physical groups such as editing, moving devices to different racks and so on.

 **NOTE:** You cannot edit the **Group Hierarchy** after creating a physical group.

Steps

1. Start OpenManage Enterprise.
2. On the **Devices** page, in the left pane, expand **PHYSICAL HIERARCHY**.
3. To edit a physical group, do one of the following:
 - Expand the group, right-click the group, and then select **Edit Group**. The **Edit Physical Group** page is displayed.
 **NOTE:** The power capacity for a group is the sum of power consumption of the devices within the group, and a suggestion for the total group power capacity is displayed below the **Power Capacity** field.
 - To edit the power or space capacity of a physical group in the **PHYSICAL HIERARCHY** section, click the options, and then click **Attributes**. The **Group Attributes** page is displayed.
4. Make the changes and click **Finish** or **Save**.

Manage physical groups

Associate UPS devices to a data center, room, or aisle. When you add devices to a parent group in the hierarchy, the devices are also added in the child groups.

Steps

1. Start OpenManage Enterprise.

2. On the **Devices** page, in the left pane, expand **PHYSICAL HIERARCHY**.
3. In data center, room, or aisle groups, click the vertical ellipses and **Manage Group**.
4. To add UPS devices, click **Associate to Group**.
5. Select the devices and click **Next**.
6. Click **Finish**.
7. To remove the devices, select the devices and click **Remove Devices > Yes**.
The devices are also removed from the child groups.

Delete physical group

Delete physical groups that are no longer valid.

Prerequisites

Ensure that the Emergency Power Reduction (EPR) option is disabled on the physical group.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can only view the groups and devices in the groups that are assigned to Device Manager DM1 user. You cannot perform any management tasks on the physical groups such as editing, moving devices to different racks and so on.

To delete a physical group, perform the following steps:

 **NOTE:** After you apply a policy to a group, if you delete the group, the policy is also removed from power management and monitoring.

Steps

1. Start OpenManage Enterprise.
2. On the **Devices** page, in the left pane, expand **PHYSICAL HIERARCHY**.
3. Go to the group that you want to delete, right-click the group, and then click **Delete Group**.
4. In the confirmation screen, click **Yes**.

Results

The group is deleted.

Rearrange rack slot of devices

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can only view the groups and devices in the groups that are assigned to Device Manager DM1 user. You cannot perform any management tasks on the physical groups such as editing, moving devices to different racks and so on.

To rearrange the rack slot of the devices in a rack, perform the following steps:

Steps

1. Start OpenManage Enterprise and perform one of the following steps:
 - a. To view the devices, go to the **Devices** page.
 - b. In the left pane, expand the **Physical Hierarchy** group until a rack level and right-click and select the **Manage Rack** option.

When you hover the mouse pointer over the rack group, data about most recent average power consumption, carbon emission value for the last one hour, and accelerator count is displayed.

Or

- a. Start OpenManage Enterprise, and then click **Power Management > Rack View**.

The **Rack View** page is displayed.

Optional: To filter and view the data, expand the **Advanced Filters** option. The following is a list of categories available:

- **Group Name**
- **Health State**
- **Power State**
- **Connection State**
- **Type**

Select the categories of your choice and view the filtered data.

- b. Click the rack name.

The **Manage Rack** page is displayed.

2. Locate the device that you want to move using the vertical scroll bar of the rack and select the device.

3. Click **Rearrange Rack**.

The **Update Rack Slots** page is displayed.

4. To change the slot for a device, click the drop-down menu and select an empty slot.

5. Click **Finish**.

The device slot is updated.

Move device to different rack

Based on the changes in the data center, you can change the location of the device in a physical group.

Prerequisites

Ensure that the Emergency Power Reduction (EPR) is not enabled on the target rack.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing.

For example, if you are logging in as a Device Manager DM1 user, you can only view the groups and devices in the groups that are assigned to Device Manager DM1 user. You cannot perform any management tasks on the physical groups such as editing, moving devices to different racks and so on.

To move a device to another rack within the same physical group or to another physical group, perform the following steps:

Steps

1. Start OpenManage Enterprise and perform one of the following steps:

- a. To view the devices, go to the **Devices** page.
- b. In the left pane, expand the **Physical Hierarchy** group until a rack level and right-click and select the **Manage Rack** option.

When you hover the mouse pointer over the rack group, data about most recent average power consumption, carbon emission value for the last one hour, and accelerator count is displayed.

Or

- a. Start OpenManage Enterprise, and then click **Power Management > Rack View**.

The **Rack View** page is displayed.

Optional: To filter and view the data, expand the **Advanced Filters** option. The following is a list of categories available:

- **Group Name**
- **Health State**
- **Power State**

- **Connection State**
- **Type**

Select the categories of your choice and view the filtered data.

- Click the rack name.
The **Manage Rack** page is displayed.
- To move the device to another rack, click **Move Device to Another Rack**.
The **Select Group** page is displayed.
- Optional: To filter and view the data, click **Advanced Filters**.
Search the group using the **Group Name** field.
To clear the filters, click **Clear All Filters**.
- Select the rack and click **Move**.
The device is moved to the new rack.

Remove device from rack

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager user, you can delete the devices from the physical groups that are assigned to you from the **Individual Devices** tab. However, after removing the device from power management and monitoring, you cannot readd the device to the Power Management feature when logged in as a Device Manager user.

Steps

- Start OpenManage Enterprise and perform one of the following steps:
 - To view the devices, go to the **Devices** page.
 - In the left pane, expand the **Physical Hierarchy** group until a rack level and right-click and select the **Manage Rack** option.
When you hover the mouse pointer over the rack group, data about most recent average power consumption, carbon emission value for the last one hour, and accelerator count is displayed.

Or

- Start OpenManage Enterprise, and then click **Power Management > Rack View**.
The **Rack View** page is displayed.
Optional: To filter and view the data, expand the **Advanced Filters** option. The following is a list of categories available:
 - **Group Name**
 - **Health State**
 - **Power State**
 - **Connection State**
 - **Type**
 Select the categories of your choice and view the filtered data.
- Click the rack name.
The **Manage Rack** page is displayed.
- Select the devices and click **Remove Device(s) From Rack**.
- In the confirmation page, click **Yes**.
The devices are removed from the rack.

Power Distribution Unit

Power Distribution Unit (PDU) is a device with multiple outlets capable of supplying power to all the devices within a rack. PDUs can be classified into two categories:

- Non-Intelligent PDUs—Distribute power evenly to all the outlets.
- Intelligent PDUs—Provide advanced monitoring capabilities and remote control.

There are different types of PDU devices available in the market that you can choose from, however OpenManage Enterprise supports only metered PDUs.

Metered PDUs are intelligent rack PDUs that display power consumption over a secure network. They help Administrators in avoiding overloading the circuits and in calculating the Power Usage Effectiveness (PUE), provide accurate power usage, and available capacity at rack level. Also, they help in identifying the power consumption at server and various device levels to charge the customers of a data center as per their usage.

The Power Management feature supports the discovering and monitoring of Dell PDUs connected using the daisy chain method with only one chained PDU.

Uninterruptible Power Supply

Uninterruptible Power Supply (UPS) is a device that provides emergency power when the main power source stops working. UPS protects electrical equipment in data centers where an unexpected power disruption could cause data loss.

Associate PDU and UPS to rack

Associate the respective Power Distribution Unit (PDU) and Uninterruptible Power Supply (UPS) devices to a rack to monitor accurate power consumption.

Prerequisites

Ensure that the devices are discovered in OpenManage Enterprise.

About this task

You can associate only the primary Dell PDU to a rack. The chained PDU is automatically associated when the primary PDU is associated to the rack.

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager, you can view the added devices in the group that is defined in your scope. You cannot associate any PDUs to a group.

Steps

1. Start OpenManage Enterprise and perform one of the following steps:
 - Click **Power Management > Rack View**, and then right-click and select **Manage Rack** option. The **Manage Rack** page is displayed.

OR

- a. Click **Devices**.
The **Devices** tab is displayed.
 - b. Click **Physical Hierarchy**, expand until rack level and right-click the group, and select **Manage Rack** option.
The **Manage Rack** page is displayed.
2. To Associate the devices to a rack, perform one of the following steps:
 - Click the **Associated Devices** tab and then click **Associate to Rack**. =

 **NOTE:** Only the PDU and UPS devices are displayed.

- Or, click the **Add to Rack Slot** option.

 **NOTE:** All the devices added for power management and monitoring are displayed.

3. Optional: To filter and view the data:
 - a. Click **Advanced Filters**.

The following filters are displayed:

- **Health State**
- **Power State**
- **Connection State**
- **Name**
- **Identifier**
- **Model**
- **Type**
- **Managed State**

4. Optional: To clear the filters, click **Clear All Filters**.

5. In the **Select Device(s)** section, select the devices and click **Next**.

6. In the **Add device(s) to rack slots** section, click **Finish**.

The PDU and UPS devices are associated with the rack and are listed in the **Associated Devices** tab. UPS devices are not associated with the rack for the following cases:

- UPS devices can be associated with only one physical hierarchy.
- UPS devices cannot be moved to another hierarchy. If the UPS is associated to the rack but not associated to any group, then the device can be moved to a rack in another hierarchy.

View PDU and UPS associated to rack

View all the associated Power Distribution Units (PDUs) and Uninterruptible Power Supply (UPS) to a rack on a single page.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

If you are logging in as a Device Manager DM1 user, you can view all the devices that are part of the group that is assigned to a Device Manager DM1 user.

Steps

1. Start OpenManage Enterprise and perform one of the following steps:

- Click **Power Management** > **Rack View**, and then right-click and select **Manage Rack** option. The **Manage Rack** page is displayed.

OR

- a. Click **Devices**.
The **Devices** tab is displayed.
- b. Click **Physical Hierarchy**, expand until rack level and right-click the group, and select **Manage Rack** option.
The **Manage Rack** page is displayed.

2. Click the **Associated Devices** tab.

All the PDU and UPS devices that are associated with this rack are listed with all details.

View PDUs discovered in OpenManage Enterprise

View the details of a PDU after discovering it in OpenManage Enterprise.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

If you are logging in as a Device Manager DM1 user, you can view all the devices that are part of the group that is assigned to a Device Manager DM1 user.

Steps

1. Launch OpenManage Enterprise and click **Devices**.

2. Expand **SYSTEM GROUPS**, click **PDU Devices**, and click a PDU device.

The **Overview** tab is displayed.

All the information about the PDU is displayed.

3. To view the PDU role—primary and chained—information, select the check box of the PDU device. In the right pane, the PDU information is displayed.

4. To view the IP address details, click the **Hardware** tab.

The **Device Management Info** tab is displayed with IP and MAC address along with the device URL and name.

- To view the NIC card details, click the **NIC Information** section. The MAC, IPv4 address, and subnet mask information are displayed.



NOTE: Network Interface Controller (NIC) information is available only for PDUs by APC by Schneider Electric and Dell.

- To view the PDU Outlet information such as outlet number, name, and power rating, click **PDU Outlet Information**. The PDU outlet information is not available for Dell PDUs.

For more information about the actions you can perform on this page, see the **Managing Devices** section from OpenManage Enterprise User's Guide.

View UPS discovered in OpenManage Enterprise

View the details of a UPS after discovering it in OpenManage Enterprise.

Steps

1. Launch OpenManage Enterprise and click **Devices**.

2. Expand **ALL DEVICES** and **System Groups**.

3. Click **UPS Devices** and click a UPS device.

The health status of APC UPS is displayed as **Unknown**. APC UPS does not support the health status and hardware revision information.

The **Overview** tab containing information about the UPS is displayed.

4. To view the IP address details, click the **Hardware** tab.

The **Device Management Info** tab is displayed with IP and MAC address along with the device URL and name.

- To view the NIC card details, click **NIC Information**. The MAC, IPv4 address, and subnet mask information are displayed.
- To view battery information such as battery replacement required, total external battery packs, and recommended replacement date, click **Battery Information**.

5. To view the metric graphs, click **Metrics**.

6. In the **Recent Device Metrics** section, you can view the last collected UPS information—battery capacity, output state, battery time remaining.

The output state represents the current state of the UPS. For more information about the different output states, see [UPS output states](#).

7. In the **Device Metrics Trend** section, you can view the output energy, output power, and battery temperature at different time intervals.

Change the duration by selecting an option from the **Duration** drop-down list.

UPS output states

The UPS output states represent the current state of the UPS.

The different output states are as follows:

- **Unknown** (1)—The Management Card cannot determine the state of the UPS.
- **Online** (2)—The UPS is using acceptable input voltage to provide output voltage.
- **On Battery** (3)—The UPS is using battery power to provide output voltage.
- **On Smart Boost** (4)—The UPS is using the Automatic Voltage Regulation (AVR) boost feature with a low input voltage to provide sufficient output voltage without switching to battery operation.
- **Timed Sleeping** (5)—The UPS is waiting for a defined time before supplying output power to its supported equipment.

- **Software Bypass** (6)—The UPS is placed into bypass mode using SNMP or PowerChute plus or PowerNet Manager.
- **Off** (7)—The UPS is turned off.
- **Rebooting** (8)—The UPS is resetting its supported equipment by turning off its output power and then turning it back on.
- **Switched Bypass** (9)—The UPS is placed into bypass mode using the switch at the UPS.
- **Hardware Failure Bypass** (10)—The UPS places itself into a bypass mode in response to a hardware problem.
- **Sleeping Until Power Return** (11)—The UPS is waiting for the input power to return to an acceptable level before it provides output power to the supported equipment.
- **On Smart Trim** (12)—The UPS is using the AVR Trim feature with a high input voltage to provide output voltage without switching to battery operation.
- **Eco Mode** (13)—The UPS is operating in eco mode.
- **Hot Standby** (14)
- **On Battery Test** (15)—The UPS is running a self-test.
- **Emergency Static Bypass** (16)—The UPS is placed into static bypass mode.
- **Static Bypass Standby** (17)—The UPS is waiting to be placed into static bypass mode.
- **Power-Saving Mode** (18)
- **Spot Mode** (19)
- **eConversion** (20)—The UPS is operating in eConversion mode.
- **Charger Spot Mode** (21)—The UPS is running a charger power test.
- **Inverter Spot Mode** (22)—The UPS is running an inverter power test.
- **Active Load** (23)
- **Battery Discharge Spot Mode** (24)—The UPS is running a battery discharge power test.
- **Inverter Standby** (25)—The UPS is operating in standby mode.
- **Charger Only** (26)

Remove PDU and UPS devices

Remove faulty or old and decommissioned Power Distribution Unit (PDU) and Uninterruptible Power Supply (UPS) devices from a rack.

About this task

You can remove only the primary Dell PDU from a rack. The chained PDU is automatically removed when the primary PDU is removed from the rack.

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you cannot remove any PDU or UPS devices that are part of the group that is defined in the Device Manager DM1 user scope.

Steps

1. Start OpenManage Enterprise and perform one of the following steps:
 - Click **Power Management > Rack View**, and then right-click and select **Manage Rack** option. The **Manage Rack** page is displayed.

OR

 - a. Click **Devices**.
The **Devices** tab is displayed.
 - b. Click **Physical Hierarchy**, expand until rack level and right-click the group, and select **Manage Rack** option.
The **Manage Rack** page is displayed.
2. To remove a device, click the **Associated Devices** tab.
3. Select the device and click **Remove Device(s)**.
4. In the confirmation screen, click **Yes**.
The PDU or UPS device is removed successfully from the rack.

All Devices screen device list

The Devices list displays a list of devices that the appliance monitors and manages. Health status and other data about a device is listed to enable you to monitor and manage devices.

The list of devices displays the device properties such as IP address and service tag. In the **All Devices** table, 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** screen, see [All Devices screen actions](#).

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

- **Health State** indicates the working state of the device. Possible values include normal, warning, and critical. Filter devices by health status, select the corresponding color band on the donut. See [Device health statuses](#).
- **Power State** indicates if the device is turned on or off.
- **Connection State** indicates the connection status of the discovered devices to OpenManage Enterprise. Possible values include Connected, Disconnected, or Disconnected (Authentication failure).
- **Name** indicates the device name.
- **IP Address** indicates the IP address of the iDRAC installed on the device.

NOTE: Depending on the configuration of the target system, discovered HCI devices may display their virtual management address.

- **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, Power Shelf, and CDU.
- **Chassis Name** indicates the chassis name.
- **Slot Name** indicates the slot name for the chassis devices.
- **Managed State** column indicates if the device is monitored, managed, managed with alerts (if **Enable alert reception from discovered devices** checkbox is enabled during discovery), or is proxied. See [Discovering devices](#).
- **Credential Type** column indicates the type of password that is being used to manage the device. The password includes internal password rotation, CyberArk credentials, or the discovery credentials used during device discovery.
- **Device ID** column lists the unique identifiers that are assigned to each device, helps in identifying devices within the log for troubleshooting purposes.

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 and configure individual devices](#).
- 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 is dynamic. For more information about using the Donut chart, see [Donut chart](#).

All Devices screen actions

Click **Devices** to perform actions on one or more devices in the device list.

The available actions are context-sensitive, depending on:

- The selected group in the navigation tree.
- The devices selected in the grid.

Group-level actions such as **Run Inventory on Group** and **Refresh Health on Group** apply to the currently selected group. All device actions apply to the selected devices. However, few actions such as Discovery are always applicable without any selection. Also, the type of actions available per device depends on the type of device selected.

NOTE: You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Logging and system activity

Actions that require OpenManage Enterprise to communicate with an iDRAC generate entries in the iDRAC Lifecycle Log (LC Logs). Various operations, such as discovery and inventory, require authentication requests to the target to retrieve the necessary data. These log entries are temporary and occur during tasks like discovery or inventory. Also, when viewing a device's **View Details** screen, OpenManage Enterprise generates repeated, live requests to the iDRAC to maintain up-to-date data for display. Concurrent tasks such as multiple discoveries or compliance checks can further increase the authentication entries needed for a given device. If needed, use the Lifecycle Log display filters to restrict which log entries are displayed.

Group actions

From the **Group Actions** dropdown, you can:

- Create custom device groups. See [Create a custom static or query group](#).
- Create static groups. See [Create a static device group](#).
- Create query groups. See [Create a query device group](#).
- Edit static or query groups. See [Edit a static group](#) and [Edit a query group](#).
- Clone groups. See [Clone a static or query group](#).
- Rename group. See [Rename a static or query group](#).
- Delete groups. See [Delete a static or query device group](#).
- Add the devices to a new group. See [Add devices to a new group](#).
- Add the devices to an existing group. See [Add devices to existing group](#).

Discovery

From the **Discovery** dropdown, you can:

- Discover and onboard devices. See [Discovering devices](#) and [Onboarding devices](#).
- Exclude devices. See [Exclude devices from OpenManage Enterprise](#).
- Edit Exclude ranges. See [Global exclusion of ranges](#).

Inventory

From the **Inventory** dropdown, you can:

- Run inventory on a device group. See [Create an inventory job](#).
- Run inventory on devices. See [Run inventory on devices](#).

Refresh Health

From the **Refresh Health** dropdown, you can:

- Refresh health on group. See [Refresh health on group](#).
- Refresh health on devices. See [Refresh health on devices](#).

More Actions

From the **More Actions** dropdown, you can:

- Turn the LED on. See [Create a job to blink device LEDs](#).
- Turn the LED off. See [Create a job to blink device LEDs](#).
- Power on the devices. See [Create a job for controlling device power](#).
- Power off the devices. See [Create a job for controlling device power](#).
- Gracefully shutting down the devices. See [Create a job for controlling device power](#).
- Power Cycle a system (Cold Boot). See [Create a job for controlling device power](#).
- System reset (Warm Boot). See [Create a job for controlling device power](#).

- Perform an IPMI CLI remote command on a device. See [Run remote commands on managed devices](#).
- Perform a RACADM CLI remote command on a device. See [Run remote commands on managed devices](#).
- Update the firmware or driver version of a device by using either predefined baselines or individual update packages. See [Update the device firmware and drivers by using baselines](#). When selecting devices with the **Across all pages** option, the **Update** option is available in the drop-down menu only if the update is supported for all the devices by OpenManage Enterprise.
- Delete devices from OpenManage Enterprise. See [Delete devices from OpenManage Enterprise](#).
- Export data on all the devices. See [Export data](#)
- Export data on the selected devices. See [Export data](#)

Quick Actions

From the **Quick Actions** pane, on the right side of the Devices screen, provides fast access to commonly used console launch options. The available actions vary depending on the type of device selected:

- Compute Devices:
 - [Launch iDRAC Console](#)
 - [Launch Virtual Console](#)
- Chassis
 - Launch Console
 - Launch CMC Console
- Network IOM
 - Launch Console
- Network Switches
 - Launch SNMP Console

 **NOTE:** The **Launch Console** option is not supported for Dell SONiC switches. Although the option may appear in the Quick Actions pane when a SONiC switch is selected, it is nonfunctional for this device type.

Delete devices from OpenManage Enterprise

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

Prerequisites

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- A device on which a profile is assigned cannot be deleted unless the profile is unassigned from it. For more information, see [Unassign profiles](#).
- 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.

Steps

1. Go to the **All Devices** screen by clicking **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 device is fully removed from the console, including all associated onboarding metadata.
- Any user credential information that is used exclusively by the deleted device are also removed, unless shared with other devices.
- If the device was onboarded with Redfish-based alert subscriptions (for example, Power Shelf), OpenManage Enterprise performs automatic alert offboarding. This unsubscribes the console from the event destination list of the device, preventing stale or orphaned alert subscriptions.

- For devices using SNMP traps, if OpenManage Enterprise was manually configured as a trap destination, you must still remove the console IP from the device manually.
- Deleted devices may be rediscovered if they fall within a discovery range that is re-run. To permanently remove devices and prevent them from discovery, [Exclude devices from OpenManage Enterprise](#) instead.

 **NOTE:** After deleting multiple devices, the audit log confirmation for device deletion may take some time to appear. This delay can vary depending on the number of devices deleted.

Related concepts

[Create and manage custom groups](#)

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

You must be a Super Administrator, Administrator, or Custom Role user with discovery management privileges and scope-based operational access to the devices. For more information, see [Role and scope-based access](#).

Steps

1. Go to the **All Devices** screen by clicking **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

You must be a Super Administrator, Administrator, or Custom Role user with inventory management privileges and scope-based operational access to the devices. For more information, see [Role and scope-based access](#).

Steps

1. Go to the **All Devices** screen by clicking **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** screen (**Monitor > Inventory**).

Update the device firmware and drivers by using baselines

Update the firmware or driver version of a device by using either predefined baselines or individual update packages.

About this task

You can update the firmware and driver version of devices on the **All Devices** screen or from the **Compliance** screen (see [Update the device firmware and drivers](#)). Updating using the **All Devices** screen is recommended when updating firmware and driver of a single device.

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with firmware update privileges and scope-based operational access to the devices. For more information, see [Role and scope-based access](#).
- Driver updates are applicable only for devices that are associated with 64-bit Windows versions.
- Driver updates on the devices cannot be rolled back.
- For firmware updates using the **Stage for next server reboot** option, manual inventory and baseline checks are required after installing the package on 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** screen **Devices** table, select the devices and click **More Actions > Update**.

NOTE: When you select devices, ensure that they are associated with one or more firmware baselines. If not, the devices are not displayed in the compliance report, and 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. Bring the firmware and driver versions up to date in accordance with the compliance level. For information about the field description on this screen, 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 drivers by using Individual Update package also. Click **Individual Package**, and then complete the on-screen instructions. Click **Next**.
- b. Under **Schedule Update** section, select the update options:
 - Select **Update Now** to apply the firmware/driver updates immediately.
 - Select **Schedule Later** to specify a date and time when the firmware and/or driver version must be updated. This option is recommended if you do not want to disturb your current tasks.
- c. Under **Server Options**, select the reboot options to apply the firmware/driver update.
 - **Reboot server immediately** : Reboot the server(s) immediately after the firmware/driver update job is created on the target. Select the type of reboot from the drop-down list. Options include:
 - **Graceful Reboot without Forced Shutdown** : Attempts a graceful reboot of the operating system. If the operating system rejects the request, the graceful reboot operation fails; iDRAC performs no further action.
 - **Graceful Reboot with Forced Shutdown** : Attempts a graceful reboot of the operating system if the operating system accepts the request that a graceful reboot is performed. If the operating system rejects the request, the iDRAC forces a hard reset on the system.
 - **Power Cycle** : Performs a hard reset of the device.
 - Select **Stage for next server reboot**: Triggers the firmware/driver update when the next server reboot happens. This option is not available for **Schedule Later** update option. If this option is selected, then the inventory and baseline check must be performed manually after the package is installed in the remote device.

NOTE: If the firmware update/driver jobs are created with the **Stage for next server reboot** option, wait until the firmware update completes on the target device before collecting the latest inventory (That is, after the scheduled reboot). After the update is complete and the target device is in a steady state, manually run an [Inventory Job](#) to collect the latest device software details. Optionally, you can wait for the system-scheduled inventory job to run. Click **Check Compliance (Configuration > Firmware/Driver Compliance)** upon completion of the Inventory job. This action refreshes the Baseline Software Components with the most recent component version's provided by the target device.

Important points to consider when selecting components with reboot required as **If Needed** for update:

- When the selected components for the update include a combination of **If Needed** and **No**, or only **If Needed**, and the reboot type chosen is either **Reboot Now** or **Schedule Later**, the system will reboot only if necessary.
- Sometimes, **If Needed** components require a reboot to complete the update. It is recommended to select either **Update Now > Reboot server immediately** or **Schedule Later** for **If Needed** components. If you select **Update Now > Stage for next server reboot**, the devices might not install immediately and may require a reboot to complete the process. As a result, OpenManage Enterprise marks the firmware update job as **Completed**, and the job ID status shows as **USERINTERVENTION**.
- When updatable components display the **REBOOT REQUIRED** status as **If Needed**, and you select **Stage for next server reboot** for update, the components may undergo a soft reset. However, the server itself will not reboot unless you have chosen **Reboot server immediately**. For more details on if-needed devices, see [View the baseline compliance report](#).

3. Click **Finish**.

Results

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

- When compliant devices (that is, devices marked with a green check) are selected for a **Make Compliant job** that contains associated components those updates will be reapplied to the devices. If any of those components require a restart, the devices are restarted to complete the compliance operation.
- After submitting this job, the console first attempts to verify the service tag of the intended target to ensure the operation is performed on the correct system. If the verification fails, the job completes with errors, and the task execution history detail shows the following: Running Verifying if the device Service Tag is valid. The device Service Tag could not be verified. Task Failed. Completed With Errors. Please check the system to ensure the IP address has not changed since the last discovery was completed. Remediate by discovering the system with the updated IP address, and retrying the operation.
- After completing the job, devices that are selected during the update could be in the following states on the iDRAC.
 - **Completed**: The device was successfully updated.
 - **Failed**: The update operation could not be completed on the device.
 - **Scheduled**: The server must be rebooted for the new firmware to take effect.
 - **USERINTERVENTION**: Sometimes **If Needed** reboot type components require a reboot for the new firmware to take effect. This state indicates that a reboot action is pending on the server.

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** screen.

Prerequisites

You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

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](#).

Related concepts

[Create and manage custom groups](#)

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** screen.

Prerequisites

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- For the in-band devices discovered using the ESXi and Linux operating systems, the **Health State** () is displayed as Unknown ().

Steps

- Go to the **All Devices** screen by clicking **Devices**.
- Select the devices from the Devices list on which you want to refresh the health.
- 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** screen (**Monitor** > **Jobs**).

Roll back an individual device's firmware version

Roll back the firmware version of an individual device. In this mode, you can roll back the firmware version of only one device at a time.

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](#). 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.

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with firmware update privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- 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 OpenManage Enterprise 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.
- Firmware rollback is supported on PowerEdge 17G servers (iDRAC 10 based) with iDRAC firmware version 1.20.50.50 or later.
- To rollback iDRAC9 firmware to versions released before February 2021, you must first downgrade to iDRAC9 firmware version 4.40.10.00. This version supports the legacy hardware root of trust certificate and enables further downgrades to earlier versions.

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 baseline](#).

Steps

- In the left pane, select the group, and then click the device name in the list.
- On the device details screen, click **Firmware/Drivers**.
- 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](#).

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

Export the inventory of only one device to a CSV file.

Prerequisites

You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

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

Perform other actions on a server or chassis. For example, power on or off the device LED, power on or off a device, or gracefully shut down a device.

Before you begin: You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

By using the **More Actions** drop-down menu, you can perform the following actions on the **All Devices** screen. Select the devices and click the action that is required:

- **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 devices.
- **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** indicates that the device is discovered through an MX7000 lead chassis for Multi-Chassis Management (MCM). This action is only relevant to the MX7000 chassis.
- **IPMI CLI**: Click to run an IPMI command. See [Create a remote command job for managing devices](#).

- **RACADM CLI:** Click to run a RACADM command. See [Create a remote command job for managing devices](#).
- **Update Firmware:** See [Update the device firmware and drivers by using baselines](#).
- **Onboarding:** See [Onboarding devices](#).
- **Export All and Exported Selected:** See [Export data](#).

Hardware information displayed for MX7000 chassis

Displays information about the hardware components of an MX7000 chassis.

- **Chassis Power Supplies:** Details about the Power Supply Units (PSUs) that are used in the sleds and other components are provided.
- **Chassis Slots:** Details regarding the available slots in the chassis and information about any components that are installed in those slots are provided.
- **Chassis Controller:** Information about the Chassis Management Controller (CMC) and its version is provided.
- **Fans:** Details regarding the fans that are used in the chassis and their operational status are provided.
- **Temperature:** The temperature status and threshold values of the chassis are presented.
- **FRU:** Components or Field Replaceable Units (FRUs) that are installed in the chassis are listed.

Export data

Export data related to system alerts, reports, audit logs, group inventory, device lists, warranty information, OpenManage Enterprise Services, and other OpenManage Enterprise features into HTML, CSV, and PDF formats. For example, export devices in a device group to perform strategic and statistical analysis.

About this task

- A maximum of 1,000 devices can be exported.
- Avoid exporting 'wide' tables that have columns with long strings or too many columns to PDF or the right-most columns of the exported data may be truncated or cut off.
- To export a single device inventory in *.csv format, see [Export the single device inventory](#).
- To export specific reports or all reports, see [Export selected reports](#).

Steps

1. Click **Export All**, or select specific data and click **Export Selected**.
A job is created and the data is exported to the specified location.
2. Download the exported data from the specified location.

Results

The specified data is downloaded and available for strategic or statistical analysis.

View and configure individual devices

The Devices section in OpenManage Enterprise allows users to view detailed information about individual devices, perform configuration tasks, and manage firmware and alerts. Users can access device details, view hardware information, update firmware, and manage alerts, as well as view and export hardware logs and configuration inventory. The device details page also provides information on device warranty status, licenses, and monitoring metrics.

Access device details

To view and configure a device:

1. Go to **Devices**.
2. In the device list, click a device name or IP address to open the device details page.
3. Click **View Details** on the right pane to open the device overview screen.

Device actions you can perform

- View information about the device like health and power status, device IP, and service tag. See [View device inventory](#).
- Perform device control and troubleshooting tasks.
- View detailed hardware information such as RAID, PSU, operating system, NIC, memory, processor, and storage enclosure. See [View device inventory](#). OpenManage Enterprise provides a system-defined report to get an overview about the NIC, BIOS, Physical Disk, and Virtual Disk used on monitored devices. Click **Monitor > Reports**.
- Update or roll back firmware versions of components in a device that are associated with a firmware baseline. See [Managing device firmware and drivers](#).
 - For individual package updates, only EXE-based Dell Update Packages (DUPs) are supported.
 - For FX2 CMC devices, the EXE must be installed on 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 logs of a device. See [Managing individual device hardware logs](#).
- 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.
 - Configuration inventory and compliance features are disabled for Non-Dell servers.
- View installed and available licenses for PowerEdge 14G servers and newer, and MX7000 chassis. See [Managing licenses](#).
- View the device warranty status, warranty state, service level description, and days remaining until the warranty expires. See [Managing device warranty](#).
 - The **Warranty** screen is not available for sleds in a **Proxied** managed state.
- The **Monitoring Metrics** or **Services** tab is displayed on the device details screen when plug-ins are installed. For more information about plug-ins, see the respective plug-in documentation available on the Dell support site.

NOTE:

- Some device actions are not available for sleds in a **Proxied** managed state. See, [Supported and unsupported actions on proxied sleds](#).

View device inventory

The OpenManage Enterprise device details overview page provides a comprehensive view of a device's health, hardware, and operational status, including hardware details, operating system information, and subsystem health status. The page also allows users to launch iDRAC or Lifecycle Controller, manage power settings, run diagnostics, and export reports. Additionally, the page displays information on recent alerts, activity, and discovery jobs, as well as providing options for remote console, troubleshooting, and device management.

Device details overview

The **Overview** screen in OpenManage Enterprise provides a comprehensive view of your device's health, hardware, and operational status. From here, you can:

- View hardware details (e.g., processors, DIMMs, iDRAC, OS)
- Monitor alerts and recent activity
- Launch iDRAC or Lifecycle Controller
- Manage power settings
- Run diagnostics and export reports

The following table summarizes the sections and information available on the device details overview page. Displayed fields vary by device type: server, chassis, CDU, network device, and power shelf.

Table 35. Device overview of a server, chassis, CDU, network devices, and power shelf

UI element	Description
Information	• iDRAC servers/Chassis: DNS Name, Model, Identifier, Asset Tag, Express Service Code, Management IP, System Up Time, Power State: (On or Off), Connection State: (Connected or Disconnected, Total System Memory, Populated DIMM Slots, Total DIMM Slots, and Processor Summary.

Table 35. Device overview of a server, chassis, CDU, network devices, and power shelf (continued)

UI element	Description
	- When you update the slot name for an MX7000 chassis, the appliance indicates that the slot name is updated. However, the updated slot name does not reflect in the appliance. To ensure the updated slot name is displayed, refresh the inventory of the chassis. - CDU: DNS Name, Model, Identifier, Asset Tag, Management IP, Chassis Type, Equipment Type, Manufacturer, Firmware Version, Part Number, Production Date, Height (mm). - MotivAir MCDU-4U-T-010 does not display part number, asset tag, and production date. - Power shelves: DNS Name, Model, Identifier, Asset Tag, Management IP, Power State: (On or Off), Equipment Type, Manufacturer, Firmware Version, Height (mm). - Power shelf does not display part number. - Common attribute available for all network devices: Model, Identifier, Management IP, Power State, Hardware Version, and MAC Address. - For network switches: Asset Tag, Express Service Code, Firmware Version, Active Mode, and Fabric Type. - For SONiC switches: Description, Connection State, Host Name, Software Version, ONIE Version, Manufacturer, Part Number, Production Date, and System Up Time. - When Dell Networking Switches (OS10) are updated to Dell SONiC Switches, they may not be recognized properly in OpenManage Enterprise, and their Connection Status may appear as disconnected. As a result, tasks such as refresh status and inventory may fail for this device. To resolve this, rediscover the device using the HTTPS protocol. After rediscovery, the switch is correctly identified and categorized under the Dell SONiC Switches group, and tasks will resume functioning. - For Fiber channel switches: Asset Tag, Express Service Code, Firmware Version, Active Mode, and Fabric Type - Storage: Model, Identifier, Management IP, Power State (on or off), Connection state (connected or disconnected).
Chassis information	Includes FIPS status enabled or disabled, chassis name, model, identifier, asset tag, express service code, management IP, power state On or Off, and location information.
Location Information	- For servers and chassis: Data Center name, Room, Aisle, Rack, and Rack Slot. - For CDU/Power shelf: Displays physical placement details such as height, row, rack, rack offset unit, and rack offset.
Operating System Information	OS name, OS version, and, OS hostname.
Discovery Job Information	Shows the status of the completed discovery job used to discover the device.
Recent Alerts	Lists 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 .

Table 35. Device overview of a server, chassis, CDU, network devices, and power shelf (continued)

UI element	Description
Remote Console	Click Launch iDRAC to start a remote session with the iDRAC. Click Launch Virtual Console to start the virtual console. Click the Refresh Preview symbol to refresh the Overview screen. See Launch the virtual console .
Subsystems	- For servers/chassis, displays the health status of other components of the device such as PSU, fan, CPU, and battery. - For CDU, displays information about coolant pump, coolant leak detector, coolant filter, primary coolant connector, secondary coolant connector, and so on. - For power shelves, display health status for power supply units. NOTE: The time taken to collect subsystem data of sensor components that are discovered using IPMI depends on network connectivity, target server, and target firmware. If you experience timeouts while collecting the sensor data, reboot the target server.
Environment	- Displays server/chassis, power and temperature statistics. - Displays CDU environment data such as Dew Point, Room Temperature, Room Humidity, and so on.
Last Updated	Indicates the last time when the device inventory status was updated. Click the Refresh button to update the status. An Inventory job is started, and the status is updated on the screen.
Power Control	Turn on, turn off, power cycle, and gracefully shut down a device.
Troubleshoot	- Run and download the Diagnostics report. See Run and download diagnostic reports. - Reset iDRAC. - Extract and download the Services (SupportAssist) report. See Extract and download a Services report.
Blink LED	Turn On and Of device LED.
Refresh Status, Refresh Inventory	Refresh the device status and inventory. See Refresh device inventory of a single device .
Export Inventory	Export the device inventory that is collected. See Export data .
Remote Command Line	Run a remote RACADM or IPMI command on the device. See Run remote commands on managed devices .

Device hardware inventory

OpenManage Enterprise displays hardware inventory of the device immediately after device discovery. On the device details screen, under **Hardware**, the following information is displayed. Sections are dynamically hidden if the device cannot report the corresponding category of hardware inventory.

Table 36. Device hardware details

Hardware component	Description
Device Card Information	Provides information about cards that are used in the device.
Processor	Provides processor information such as sockets, family, speed, cores, and model.

Table 36. Device hardware details (continued)

Hardware component	Description
NIC Information	Provides information about NICs used in the device.
Operating System	Lists the operating system that is installed on the device. The Operating System page does not display the OS name and OS version for PowerEdge servers with Linux OS. This issue occurs when the iDRAC Service Module (iSM) is not installed on the Linux OS running on the server.
Power Supply Information	Provides information about the PSUs installed on the device.
Chassis Power Supplies	Provides information about the name, health status, presence whether enabled or disabled, power supply type AC or DC, capacity in watts, and input voltage in volts.
Chassis Controller	Information about the Chassis Management Controller (CMC) and its version is provided.
Chassis Slots	Details regarding the available slots in the chassis and information about any components that are installed in those slots are provided. Provides information about the slot number, slot type (such as sled slot, IO module slot), slot name, model installed on the slot, health, power status of the slot, and slot identifier.
Management Module	Indicates health, name, status, and the firmware version of the management module.
Fans	Details regarding the fans that are used in the chassis and their operational status are provided.
Array Disk	Provides information about the drives that are installed on the device. OpenManage Enterprise provides a system-defined report about the hard drives or virtual drives available on the OpenManage Enterprise monitored devices. Click Monitor > Reports > Physical Disk Report . Click Run . See Run reports .
Storage Controller	Provides a list of storage controllers that are installed on the device. Click the plus symbol to view individual controller data.
Memory Information	Provides data about DIMMs used in the device.
Storage Enclosure	Provides the status of storage enclosure with their EMM version.
Hard Drives	- Storage: Health State, Name, Size (GB), Media Type (Type of storage media), Encryption Capable, Serial Number, and Model Number. - For ME5 storage devices, the LUN ID attribute is not displayed in the inventory view.
Licenses	List the status of different licenses that are installed on the device. See View installed and available licenses on a device .
FRU	Lists Field Replaceable Units (FRUs). OpenManage Enterprise provides a system-defined report about the Field Replaceable Units (FRUs) installed on the OpenManage Enterprise monitored devices. Click Monitor > Reports > FRU Report . Click Run . See Run reports .
Device Management Info	Lists the IP address, MAC address, URL, and name of the device.
Installed Software	Lists firmware and software that are installed on different components in the device.

Table 36. Device hardware details (continued)

Hardware component	Description
RAID Controller Information	Lists PERC and RAID controllers that are used on the storage devices. The rollup status is equal to the status of the RAID that has high severity. For more information, see Managing the Rollup Health status by using iDRAC on the Dell 14th generation and later PowerEdge servers .
Virtual Flash	Lists virtual flash drives and its technical specification.
Guest Information	Displays the OpenManage Enterprise monitored devices that are guests. UUID is the Universally Unique Identifier of the device. The GUEST STATE column indicates the working status of the guest device.
Device Management Information	Lists the device name, IP address, MAC address, and management URL.
Coolant Information	Provides the coolant properties such as name, type, and additive mix percentage used in the CDU.
Coolant Pump Information	Details the properties of the coolant pumps that are used in the CDU.
Coolant Leak Detector Information	Indicates the properties of the coolant leak detectors used within the CDU.
Filter Information	Details the properties of the coolant filters used inside the CDU.  NOTE: MotivAir MCDU-4U-T-010 does not support coolant filters.
Primary Coolant Connector Information	Indicates the properties of the primary coolant connector for the CDU.
Secondary Coolant Connector Information	Indicates the properties of the secondary coolant connector.
Graphics Processor	Indicates the number of GPUs in a server.
PDU Outlet Information	Indicates the outlet number, name, and power rating data. The PDU outlet information is not available for Dell PDUs.
Battery Information	Indicates the battery replacement required, total external battery packs, and recommended replacement date.
Interface Information	Displays name, description, admin status, operational status, MAC address, MTU, speed, and auto negotiate for SONiC switches.
Port Neighbors Information	Displays network interface name, system name, port Id, system description, MAC address, and management address for SONiC switches.
VLAN Info	Displays network interface name, name, VLAN id, admin status, and auto state for SONiC switches.

Run and download diagnostic reports

Run diagnostics reports to resolve an issue or share with the technical support team. Running a report automatically restarts a server.

Prerequisites

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

- Ensure that you have the necessary privileges and access to the devices as described in [Role and scope-based access](#).
- Target iDRAC devices should be running firmware version 2.50.50.50 or higher.

Steps

1. On the device details screen, from the **Troubleshoot** drop-down menu, select **Run Diagnostics**.
2. In the **Remote Diagnostic Type** dialog box, from the **Remote Diagnostic Type** drop-down menu, select one of the following to generate a report.
 - **Express**: A smaller report that completes quickly.
 - **Extended**: An average report is that completes at a nominal pace.
 - **Long Run**: An in-depth report that completes slowly.

 **NOTE:** See [Diagnostics](#) in *Integrated Dell Remote Access Controller RACADM CLI Guide*.

3. To generate the Diagnostics report now, select **Run Now**.
4. Click **OK**. When prompted, click **YES**.

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

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

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

Extract and download a Services report

After running a services (SupportAssist) report, you can extract the report and download it for analytical purposes.

Prerequisites

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

1. On the device details screen, from the **Troubleshoot** drop-down menu, select **Extract SupportAssist Report**.
2. In the **Extract SupportAssist Report** dialog box:
 - a. Enter the file path where the SupportAssist report must be saved.
 - b. Select the check boxes corresponding to the log types whose SupportAssist report must be extracted.
3. Click **OK**.
A job is created and displayed on the **Jobs** screen. To view information about the job, click **View Details** in the right pane. See [View job lists](#). The job status is also displayed in the **Recent Activity** section. After the job is successfully run, the status of the job is indicated as **Diagnostic Completed**, and the **Download** link is displayed in the **Recent Activity** section.
4. To download the report, click the **Download** link, and then download the <Service Tag>.<Time>.TXT SupportAssist report file.
 - Else, click **Troubleshoot** > **Download SupportAssist Report**.
5. In the **Download SupportAssist Files** dialog box, click the .TXT file link, and then download the report. Each link represents the log type you selected.
6. Click **OK**.

Managing individual device hardware logs

View, export, and download hardware log data of a device.

 **NOTE:** Hardware logs are only available for iDRAC9 and newer supported servers, MX7000 chassis and sleds.

- On the device details screen, click **Hardware logs**. All the event and error messages that are generated for the device is listed. For field descriptions, see *View hardware logs*.
- For a chassis, the real-time data about the hardware logs are retrieved from the chassis.
- To add a comment, click **Add Comment**.

 **NOTE:** To add a comment, Custom Role user should have appliance management privilege. For more information about privileges, see [Role and scope-based access](#).

- In the dialog box, type the comment, and then click **Save**. A symbol in the **COMMENT** column indicates a saved comment.
- To export selected log data to a CSV file, select the corresponding check boxes, and then click **Export > Export Selected**.
- To export all the logs on a screen, click **Export > Export Current** screen.

View hardware logs

Table 37. View hardware logs

Advance filters	Description
Severity	Select the severity level of a log data. The available options are info, warning, and critical.
Start Time and End Time	To view hardware logs between a specific date period.
Message ID	Enter the full or partial message ID. If it matches your search criteria, only the logs with the corresponding message ID will be displayed.
Category	To view hardware logs that only apply to a certain category.  NOTE: Category filter is only applicable to MX7000 chassis.

Hardware logs for the following models do not include **Message ID** and **Category** information. Pagination is also not supported for these models:

- PowerEdge M1000e
- PowerEdge VRTX
- PowerEdge FX2s

Run remote commands on managed devices

Run remote commands to manage devices monitored by OpenManage Enterprise. RACADM and IPMI commands are supported.

Prerequisites

You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

About this task

RACADM and IPMI commands can be sent to a device's iDRAC from the device details screen to remotely manage the respective device.

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

Steps

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

 **NOTE:** The RACADM CLI tab is not displayed for the following servers because the corresponding task is not available in the device pack — MX740c, MX840c, and MX5016S.

3. In the **Send Remote Command** dialog box, type the command. Up to 100 commands can be entered with each command required to be on a new line. To display the results in the same dialog box, select the **Open results after sending** check box.

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

4. Click **Send**.
A job is created and displayed in the dialog box. The job is also listed on the Job Details. See [View job lists](#).
5. Click **Finish**.
The **Recent Alerts** section displays the job completion status.

Launch the iDRAC device management application

Launch the iDRAC device management application, and then log in.

Prerequisites

You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

1. Select the check box corresponding to the device.
The device working status, name, type, IP, and Service Tag are displayed.
2. In the right pane, click **Launch iDRAC Console**.
The iDRAC login screen is displayed. Log in by using the iDRAC credentials.

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

 **NOTE:** You can also start the management application by clicking the IP address in the **Device** list, as described in [All Devices screen device list](#).

Launch the virtual console

The virtual console is an HTML5-based interface that allows users to access iDRAC through OpenManage Enterprise without direct connectivity or authentication.

Prerequisites

Ensure the target iDRAC is:

- Discovered directly by OpenManage Enterprise via Redfish, rather than through the chassis discovery.
- Running firmware version is 6.10.30.0 or later.
- Configured on default port number 443.
- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

1. Select the checkbox corresponding to the device.
The device **Working Status**, **Name**, **Type**, **IP**, and **Service Tag** are displayed.
2. In the right pane, click **Launch Virtual Console**.

Results

The remote console screen on the server is displayed.

Attaching iDRAC virtual media

Update, install and remotely access the server using iDRAC virtual media.

Prerequisites

You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with device configuration and job management privileges and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

About this task

- Update all server firmware using the matching bootable image (ISO-file).
- Install an operating system on your server directly from the ISO.
- View video output from the server and use the local mouse and keyboard as if you were in the same room.

Steps

1. To access the virtual media dialog, see [Launch the virtual console](#).
2. In the upper right corner of the screen, click **Virtual Media > Connect Virtual Media**.
3. Map the remote ISO image file to the (CD/DVD or removable disk) device by clicking **Choose File** and selecting the ISO file. Mount the ISO file by clicking **Map Device**.



NOTE: **Map External Device** and **Reset USB using Java client** are currently not supported on OpenManage Enterprise. Clicking on **Launch** downloads a .jnlp file but it will not work.

Results

The ISO or external device file can now be used as a bootable device.

Refresh device inventory of a single device

View updated inventory data of devices or device groups.

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with inventory management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

About this task

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

Steps

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

Related concepts

[Create and manage custom groups](#)

View installed and available licenses on a device

View all licenses (installed or available for installation). You can also deploy and remove licenses as needed.

To view the list of licenses on a device:

1. Click **Devices** and select a device from the **All Devices** page.
2. Click **View Details** and then select the **Licensing** tab.

The **Licenses** section includes the following information:

Table 38. License attributes on a device

License attribute	Description
Deploy	To deploy licenses on a device, select licenses that are available and click Deploy . After the licenses are deployed on the target device, the device inventory is automatically refreshed to update the license capability for the device in the appliance.
Remove	To remove installed licenses from a device, select the installed licenses and click Remove . An uninstall license task is created on the Jobs page. After the license is successfully removed, the device inventory is refreshed automatically, and the related features stop working for the device in the appliance.
Check box	Select or de-select the license when executing bulk operations.
Status	• OK - License is installed and not expired. • Expired - License is installed and expired. • Available - License is bound but not installed.
Description	The description of a license.
Term	The license term. Possible values are: • Perpetual: The license has no expiration date. • Evaluation: The license will expire.
Entitlement ID	The unique identifier of a license.
Evaluation time remaining	Time remaining (days) for license evaluation. The value listed for perpetual licenses is NA.
Date of expiration	The date on which the license expires.
Date purchased	The date the license was purchased. The value listed for perpetual licenses is NA.
Date installed	The date the license was installed.
Assigned devices	Fully qualified device descriptor (FQDD) of devices or components that are assigned to the license

The **Features** section provides a lists of features that are enabled on the device based on the installed and active licenses. For information about the supported features related to OpenManage Enterprise licenses, see the [Licensing](#) section. To learn more about features supported by iDRAC licenses, see the latest *iDRAC user's guide*.

Managing device inventory

Create, edit, run, stop, or delete inventory schedules. A list of existing inventory schedule jobs is displayed.

NOTE:

- You must be a Super Administrator, Administrator, or Custom Role user with inventory management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- Users with DEVICE_MANAGEMENT privileges cannot use the **Run Inventory on Group** option available on **All Devices > Inventory**.

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

OpenManage Enterprise performs inventory collection tasks asynchronously, improving performance and scalability in large environments. For more information about asynchronous tasks, refer to the *OpenManage Enterprise Scale and Performance Whitepaper*.

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

- **NAME** lists the user-defined inventory schedule name.
- **SCHEDULE** indicates if the job is scheduled to run now or later.
- **LAST RUN** lists the timestamp at which the job was last run.
- **STATUS** indicates whether the job is running, complete, or failed.

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

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

Related tasks

[Run an inventory job now](#)
[Stop an inventory job](#)
[Delete an inventory job](#)
[Create an inventory job](#)

Topics:

- [Create an inventory job](#)
- [Run an inventory job now](#)
- [Stop an inventory job](#)
- [Delete an inventory job](#)
- [Edit an inventory schedule job](#)

Create an inventory job

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

Prerequisites

- You must be a Super Administrator, Administrator, or Custom Role user with inventory management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- Inventory collection on chassis storage sleds is not supported in OpenManage Enterprise if they are managed via chassis device management.

Steps

1. To initiate the **Inventory** wizard, do one of the following:
 - a. On the **All Devices** screen, select a group on the left pane and from **Inventory** drop-down menu click **Run Inventory on Group**.
 - b. On the **Inventory** screen (**Monitor > Inventory**), click **Create**.
 2. In the **Inventory** dialog box, a default inventory job name is populated in **Inventory Job Name**. To change, enter an inventory job name.
 3. From the **Select Groups** drop-down menu, select the device groups on which the inventory must be run.
If you have initiated the Inventory job from the **All Devices** screen after selecting a group, then Select Groups will be prepopulated with the selected group name. For information about device groups, see [Create and manage custom groups](#).
 4. In the **Scheduling** section, run the job immediately or schedule for a later time.
See [Schedule job field definitions](#).
 5. The following **Additional Options** can be selected while running the inventory job:
 - Select the **Collect configuration inventory** checkbox to generate an inventory of the configuration compliance baseline.
 - Select the **Collect driver inventory** checkbox to collect driver inventory information from the Windows server. Also, to install the Inventory Collector and Dell System Update on the Windows server if these components are not available on the server.

 **NOTE:**
 - 'Collect driver inventory' applies only to devices discovered as 64-bit Windows servers.
 - Inventory collection of Windows-based devices is supported only using OpenSSH. Other SSH implementations on Windows, like the CygWin SSH, are not supported.
 - **Additional Options** for Inventory job (Config inventory and Driver inventory) are not supported for CDU and power shelves.
- For information about configuration compliance baselines, see [Configuration compliance](#).
6. Click **Finish**.
 7. The job is created and listed in the queue.
An inventory job is created displayed in the list of inventory jobs. The **SCHEDULE** column specifies whether the job is Scheduled or Not Scheduled. See [Run an inventory job now](#).

Related concepts

[Managing device inventory](#)

Run an inventory job now

Run an existing inventory schedule job immediately.

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with inventory management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

About this task

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

Steps

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

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

Related concepts

[Managing device inventory](#)

Stop an inventory job

Stop an inventory schedule job that is currently running.

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with inventory management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

About this task

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

Steps

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

Related concepts

[Managing device inventory](#)

Delete an inventory job

Delete an inventory schedule job that is not running.

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with inventory management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

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

Related concepts

[Managing device inventory](#)

Edit an inventory schedule job

Edit an existing inventory schedule job.

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with inventory management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

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

Managing device firmware and drivers

Use the firmware and driver catalog available on Dell.com to create a firmware and driver baseline. Compare whether devices comply with the baseline and generate a compliance report, and then fix compliance issues. Use the **Configuration > Firmware/Driver Compliance** screen to manage the firmware of all the managed devices that are discovered out-of-band using iDRAC. You can also update drivers of the 64-bit Windows-based servers that are discovered and managed in-band using the SSH protocol.

Overview

Maintain optimal performance, security, and compatibility of your Dell infrastructure by managing firmware and drivers through OpenManage Enterprise. This feature enables you to:

- Create baselines using Dell-provided catalogs.
- Assess compliance across devices.
- Update firmware or drivers resolving discrepancies.

Prerequisites

Before proceeding, ensure:

- You have the necessary user privileges as described in [Role and scope-based access](#).
- Windows servers are discovered in-band using a supported protocol (SSH) to perform Windows driver updates. The catalog contains drivers only for 64-bit Windows devices. Ensure that your environment meets this requirement before proceeding with driver updates.
- Servers are discovered out-of-band using iDRAC to update both drivers and firmware.
- The onboarding status of the system is either *Managed* or *Managed with Alerts* to manage the firmware and driver of a device. See [Onboarding devices](#).
- Firmware and driver updates are performed during maintenance windows to prevent devices or the environment from going offline during business hours.

Compliance status definitions

Status	Description	Action required
OK 	Devices match the baseline version.	None.
Upgrade	Device has older firmware or drivers than the baseline. See Updating the device firmware version .	Initiate update.
Critical 	If the current firmware or driver version of the component is lower than the baseline version and if the importance that is assigned is either Recommended or Urgent.	Immediate action required.
Warning 	If the current firmware or driver version of the component is lower than the baseline version and the importance that is assigned is Optional.	Optional update.

Status	Description	Action required
Downgrade 	If the device firmware and driver is later than the baseline version.	Review baseline relevance.
Unknown	Compliance for these devices cannot be determined using Dell catalogs. These devices are network switches, modular IOAs, and Dell storage devices.	Update manually using device-specific DUPs. To perform individual firmware or driver updates, select a device on the All Devices screen, and click View Details > Firmware/Drivers and select the individual package option. For more information about the list of unsupported devices, see Devices with unknown compliance status .

Workflow summary

1. Create or import catalogs: Use a firmware and driver catalog from Dell.com either directly or after saving it on a network path. See [Add a catalog by using Dell.com](#) or [Creating a firmware catalog by using local network](#).
2. Define baselines: Create a firmware and driver baseline by using the available catalogs. These baselines serve as benchmarks to compare the firmware and driver version on the devices against the version in the catalog. See [Creating the firmware baseline](#).
3. Run compliance checks: Generate reports to check if the devices associated with the baseline comply with the baseline firmware and driver versions. See [Checking firmware compliance](#).
4. Remediate issues: Update device firmware and driver version by using the baseline. See [Update the device firmware and drivers by using baselines](#).

Handling unsupported devices

Devices like network switches, modular IOAs, and Dell storage devices show Unknown compliance status. To update them:

1. Go to **All Devices** screen, select the device, and click **View Details > Firmware/Drivers**.
2. Select the **Individual package** option under **Update**. For more information about the list of unsupported devices, see [Devices with unknown compliance status](#).

NOTE:

- Updating a device using the Individual Package workflow only supports executable (EXE) based Dell Update Packages. For FX2 CMCs, DUPs must be installed through chassis sled.
- OpenManage Enterprise does not support firmware updates on the CDU devices.

Monitoring compliance

The **Donut Chart** on the Firmware/Driver Compliance screen displays compliance status distribution. Select a baseline to view its compliance summary on the right pane. See [Donut chart](#).

 **NOTE:** When a baseline with many devices is checked for compliance, only one noncompliant device warning (CDE-V9000) is logged on the **Alerts** screen, regardless of the number of non-compliant devices.

Topics:

- [Manage firmware and driver catalogs](#)
- [Create a baseline](#)
- [Edit a baseline](#)
- [Delete a baseline](#)
- [Check the compliance of firmware and drivers](#)
- [View the baseline compliance report](#)
- [Update the device firmware and drivers](#)

Manage firmware and driver catalogs

Use firmware and driver catalogs (a collection of update packages) to create a baseline and check baseline compliance.

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

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

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

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

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

NOTE:

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

Add a catalog by using Dell.com

Based on your requirements, create a firmware catalog that can pick the latest components versions from Dell.com.

Prerequisites

- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See [Role and scope-based access](#).
- Ensure to enable CIFS (>v1) in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis. See [Manage console settings](#) for more information.
- OpenManage Enterprise supports UI internationalization, however, it is recommended that the functional content such as the file names and catalog content are entered only in English.

Steps

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

 **NOTE:** To get the latest firmware information in the baseline, click on **Check for Update** on the relevant catalog. Optionally, if your catalog is updated on schedule, the firmware information will be updated with the scheduled catalog update.
 - e. Click **Finish**.

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

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

Add a catalog to the local network

Create a firmware catalog on a local network. Currently, CIFS, NFS, HTTP, and HTTPS protocols are supported.

Prerequisites

- Ensure you have the necessary user privileges as described in [Role and scope-based access](#).
- For local network shares using Windows 2019 or later, the catalog must be generated using DRM version 3.3.2 and later.
- OpenManage Enterprise supports UI internationalization, however, it is recommended that the functional content such as the file names and catalog content are entered only in English.

About this task

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

Steps

1. On the **Catalog Management** screen, click **Add**.
 2. In the **Add Update Catalog** dialog box:
 - a. In the **Name** box, enter a catalog name.
 - b. For the Catalog Source, select the option **Network Path**. The **Share Type** drop-down menu is displayed.
 - c. Select one of the following:
 - NFS
 - i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
 - ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `nfsshare\catalog.xml`
 - CIFS
 - i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
 - ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `Firmware\m630sa\catalog.xml`
 - iii. In the **Domain** box, enter the domain name of the device.
 - iv. In the **User Name** box, enter the user name of the device where the catalog is stored.
 - v. In the **Password** box, enter the password of the device to access the share. Type the username and password of the shared folder where the catalog.xml file is stored.
 - HTTP
 - i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
 - ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `compute/catalog.xml`.
 - HTTPS
 - i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
 - ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `compute/catalog.xml`.
 - iii. In the **User Name** box, enter the user name of the device where the catalog is stored.
 - iv. In the **Password** box, enter the password of the device where the catalog is stored.
 - v. Select the **Certificate Check** check box. The authenticity of the device where the catalog file is stored is validated and a Security Certificate is generated and displayed in the [Certificate Information](#) dialog box.
 - d. After you have entered the **Share Address** and the **Catalog File Path**, the **Test now** link is displayed. To validate a connection to the catalog click **Test now**. If the connection to the catalog is established, a `Connection Successful` message is displayed. If connection to the share address or the catalog file path is not established, `Connection to path failed` error message is displayed. This is an optional step.
-  **NOTE:** You must have the Job management privilege to verify the test connection.
- e. In the **Update Catalog** box, select either **Manually** or **Automatically**.

If the **Update Catalog** is selected as **Automatically**, select either **Daily** or **Weekly** as the update frequency and enter time in the 12-hour format.

NOTE: To get the latest firmware information in the baseline, click **Check for Update** on the relevant catalog. Optionally, if your catalog is updated on schedule, the firmware information is updated with the scheduled catalog update.

3. Click **Finish**. The **Finish** button appears only after you have entered all the fields in the dialog box. A new firmware catalog is created and listed in the Catalog table on the **Catalog Management** screen.
4. To go back to the **Firmware/Driver Compliance** screen, click **Return to Firmware/Driver Compliance**.

SSL Certificate Information

If you add an update catalog from a secure web share and enable the certificate check option, the certificate information is displayed.

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

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

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

The following actions are available:

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

Update a catalog

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

Steps

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

Edit a catalog

Edit the catalog properties such as share location folder path and catalog file path.

About this task

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

Steps

1. On the **Catalog Management** screen, select a catalog.
The catalog details are displayed in the **<catalog name>** right pane.
2. Click **Edit** in the right pane.
3. In the **Edit Update Catalog** wizard, edit the properties.
The properties that you cannot edit are grayed-out. For field definitions, see [Add a catalog by using Dell.com](#) and [Add a catalog to the local network](#).

4. Enter the **Share Address** and the **Catalog File Path**, the **Test now** link is displayed. To validate a connection to the catalog click **Test now**. If the connection to the catalog is established, a **Connection Successful** message is displayed. If connection to the share address or the catalog file path is not established, **Connection to path failed** error message is displayed. This is an optional step.

 **NOTE:** You must have the Job management privilege to verify the test connection.

5. In the **Update Catalog** box, select either **Manually** or **Automatically**.
If the **Update Catalog** is selected as **Automatically**, select either **Daily** or **Weekly** as the update frequency and enter time in the 12-hour format.
6. Click **Finish**.
A job is created and run immediately. The job status is indicated in the **REPOSITORY LOCATION** column of the **Catalog Management** screen.

Delete a catalog

Delete catalogs that are not associated with a baseline.

Steps

1. On the **Catalog Management** screen, select the catalogs, and then click **Delete**.
The catalogs are deleted from the list.
2. To go back to the **Firmware/Driver Compliance** screen, click **Return to Firmware/Driver Compliance**.

 **NOTE:** Catalogs cannot be deleted if linked to a baseline.

Create a baseline

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

Prerequisites

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with baseline management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- Device manager user can only view and manage the firmware/driver baselines that the respective device manager created and owns. Also, while creating baselines, the target groups or devices (capable of firmware update) that are only in the device manager's scope are displayed.
- A non-compliant device with a firmware and/or driver version earlier than the catalog version is not automatically updated. You must update the firmware version. It is recommended to update device firmware during maintenance windows to prevent the devices or environment going offline during business hours.

Steps

1. Under **Firmware**, click **Create Baseline**.
2. In the **Create Update Baseline** dialog box:
 - a. In the **Baseline Information** section:
 - i. From the **Catalog** drop-down menu, select a catalog.
 - ii. To add a catalog to this list, click **Add**. See [Manage firmware and driver catalogs](#).
 - iii. In the **Baseline Name** box, enter a name for the baseline, and then enter the baseline description.
 - iv. (Optional) Select the **Select only components with no reboot required** check box to create a firmware/driver baseline that consists of only the components of the target devices that do not require a reboot of the target devices.
 - v. Click **Next**.
 - b. In the **Target** section:
 - To select the target devices:
 - i. Select **Select Devices**, and then click the **Select Devices** button.

- ii. In the **Select Devices** dialog box, all the devices that are monitored by OpenManage Enterprise, IOMs, and devices under static or query group are displayed in respective groups.
 - iii. In the left pane, click the category name. Devices in that category are displayed in the working pane.
 - iv. Select the check box corresponding to the device. The selected devices are listed under the **Selected Devices** tab.
 - To select the target device groups:
 - i. Select **Select Groups**, and then click the **Select Groups** button.
 - ii. In the **Select Groups** dialog box, all the devices that are monitored by OpenManage Enterprise, IOMs, and devices under static or query group are displayed in respective categories.
 - iii. In the left pane, click the category name. Devices in that category are displayed in the working pane.
 - iv. Select the check box corresponding to the groups. The selected groups are listed under the **Selected Groups** tab.
3. Click **Finish**.
A message is displayed that a job is created for creating the baseline.
- In the Baseline table, data about the device and baseline job are displayed. For field definitions, see [Firmware baseline field definitions](#).

Edit a baseline

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

Steps

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

Delete a baseline

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

Under **Firmware**, a list of available firmware baselines is displayed. Select the check box corresponding to the baseline and click **Delete**. The firmware baseline is deleted and removed from the baseline list.

Check the compliance of firmware and drivers

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

Prerequisites

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

Steps

1. Select the check box corresponding to the baseline(s), and click **Check Compliance**.

The baseline compliance job is run.

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

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

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

See [View the baseline compliance report](#).

NOTE: Rollback is not supported for drivers.

View the baseline compliance report

View if a firmware baseline complies with the catalog it is associated with, and then make it compliant if necessary.

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

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

- Select the check box corresponding to the baseline and click **View Report** in the right pane. On the **Compliance Report** screen, the list of devices that are associated with the baseline and their compliance level is displayed. By default, the devices in **Critical** and **Warning** statuses are displayed.

NOTE: If each device has its own status, the highest severity status is considered as the status of the group. For more information about Rollup Health status, see the *Managing The Rollup Health Status By Using iDRAC On The Dell 14th Generation And Later Poweredge Servers white paper* on the Dell TechCenter.

- **COMPLIANCE:** Indicates the compliance level of a device to the baseline. For more information about symbols used for device firmware/driver compliance levels, see [Managing device firmware and drivers](#).
- **TYPE:** Type of device for which the compliance report is generated.
- **DEVICE NAME/COMPONENTS:** By default, the Service Tag of the device is displayed.
 1. To view information about components in the device, click the > symbol. A list of components and their compliance with the catalog is displayed.

NOTE: For all the devices (except the MX7000 chassis) which are fully in compliance with the associate firmware baseline, the > symbol is not displayed.

2. Select one or more check boxes corresponding to the devices whose firmware compliance status is 'Critical' and requires an update.
 3. Click **Make Compliant**. See [Update the device firmware version by using the baseline compliance report](#).
- **SERVICE TAG:** Click to view complete information about the device on the device details screen. For more information about tasks you can complete on this screen, see [View and configure individual devices](#).
 - **REBOOT REQUIRED:** Indicates if the target server requires a reboot to apply the firmware update package.
 - **Yes**—Target server reboot is required to apply the device firmware.
 - Standard devices—Target server reboot is required to apply the firmware update via the LifeCycle Controller. This update can be considered as staged until a server reboot is initiated.
 - **If Needed**—Target server reboot might be required based on iDRAC's determination during firmware update execution.
 - Sideband Direct update supported devices- From release 6.10.00.00, iDRAC supports rebootless updates. This feature enables firmware updates on supported devices to be applied via iDRAC without rebooting the host server. However, there may be instances where a post-update reboot is still required.
 - **NOTE:** Important points to consider for rebootless updates:
 - After upgrading to OpenManage Enterprise version 4.3.x, the reboot required status for sideband direct update supported devices may still display as Yes. Rerun the compliance task to refresh the baseline and update the status to If Needed.

- Reboot behavior is determined after the firmware update is applied for components that support sideband direct. Therefore, the firmware compliance report displays **If Needed** under **REBOOT REQUIRED** for updates that support rebootless updates.

o **No**—The update will be applied to the device immediately, and no target server restart is required.

For more information about rebootless updates and information about how to identify if the DUP firmware supports sideband direct, see the latest iDRAC user's guide on the Dell support site at dell.com/idracmanuals.

- **Info**  : A symbol corresponding to every device component is linked to the support site screen from where the firmware/driver can be updated. Click to open the corresponding **Driver Details** screen on the support site.
- **CURRENT VERSION**: Indicates the current firmware version of the device.
- **BASELINE VERSION**: Indicates the corresponding firmware and driver version of the device available in the associated catalog.
- To export the compliance report to an Excel file, select the check boxes corresponding to the device, and then select from **Export**.
- To go back to the **Firmware** screen, click **Return to Firmware**.
- To sort data based on a column, click the column title.
- To search for a device in the table, click **Advanced Filters**, and select or enter data in the filter boxes. See Advanced Filters in [The OpenManage Enterprise GUI](#).

Update the device firmware and drivers

Maintaining up-to-date firmware and drivers is essential for the optimal performance and security of your IT infrastructure. This topic provides information about how to update firmware and driver for devices that are managed through OpenManage Enterprise.

Prerequisites

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with firmware update privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- You must create an inbound firewall rule to allow communication with port 22.
- Only one update task can be initiated on the target machine at a given time.
- Target devices with iDRAC should be running firmware versions 2.50.50.50 and above.

About this task

Initial preparations:

- The firmware and driver version of the associated baseline devices is not automatically updated, hence, the user must initiate the update.
- Run a firmware or driver compliance report to compare the current versions on your devices against those listed in the catalog. If the device's firmware or driver is outdated, the Compliance Report screen indicates the device firmware or driver

COMPLIANCE status as upgrade ( or .

- Update during scheduled maintenance windows to minimize disruptions to business operations.
- For device managers, firmware/driver update is only limited to devices within their scope.

NOTE:

- Inventory collection and firmware updates on chassis storage sleds managed via chassis device management are not supported in OpenManage Enterprise.
- The Reset iDRAC function is not supported for devices under an MCM chassis that are in a 'Proxied' onboarding state when only updating drivers. For more information about onboarding states, see [Onboarding devices](#).
- The firmware or driver compliance status of network switches, modular IOAs, and Dell storage devices is displayed as Unknown as these are not updatable using the Dell catalog. It is recommended to perform individual firmware or driver updates for these devices using their respective individual Update package. To perform individual firmware or driver updates, select a device on the **All Devices** screen, and click **View Details > Firmware/Drivers** and select the individual package option. For more information about the list of unsupported devices, refer [Devices with unknown compliance status](#).

Update considerations for MX7000 chassis and sleds:

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

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

Driver update specifics for Windows servers:

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

- Be aware that the rollback of the driver updates is not supported.
- To perform Windows driver update, ensure that the Windows servers are discovered in-band using the supported OpenSSH protocol. To update both drivers and firmware, you must additionally discover the servers' out-of-band using iDRAC.
- Driver updates on third party SSH hosted on Windows, such as the CygwinSSH, are not supported.
- To collect the inventory information, the Inventory Collector and Dell System Update must be available on the Windows server. If these components are not available on the server, then initiate an inventory job and select **Collect driver inventory**. The discovery job also collects driver inventory information, but only the inventory job installs the necessary components on the server. To collect the driver inventory information, create or edit an inventory job and select the **Collect driver inventory** check box. For more information, see [Create an inventory job](#) and [Edit an inventory schedule job](#).
- When OpenManage Enterprise has its built-in appliance share set to HTTPS and is using the default certificate, driver updates may fail.
- In OpenManage Enterprise, driver updates are not supported on Windows Server 2025 systems that have Windows Defender Application Control (WDAC) enabled.

Steps

1. On the **Configuration > Firmware/Driver Compliance** screen, select the check box corresponding to the baseline to which the device is attached, and then click **View Report** in the right pane.
On the **Compliance Report** screen, a list of devices associated with the baseline and their compliance level is displayed. For field descriptions, see [View the baseline compliance report](#).
2. Select the check box corresponding to the device(s) whose firmware or driver must be updated. You can select more than one device with similar properties.
 - Expand the device in the **DEVICE NAME/COMPONENTS** column to select components for update.
3. Click **Make Compliant**.
4. Under **Schedule Update Options**, select the update options:
 - Select **Update Now** to apply the firmware/driver updates immediately.
 - Select **Schedule Later** to specify a date and time when the firmware and/or driver version must be updated. This option is recommended if you do not want to disturb your current tasks.
5. Under **Server Options**, select the reboot options to apply the firmware/driver update.
 - **Reboot server immediately** : Reboot the server(s) immediately after the firmware/driver update job is created on the target. Select the type of reboot from the drop-down list. Options include:
 - **Graceful Reboot without Forced Shutdown** : Attempts a graceful reboot of the operating system. If the operating system rejects the request, the graceful reboot operation fails; iDRAC performs no further action.
 - **Graceful Reboot with Forced Shutdown** : Attempts a graceful reboot of the operating system if the operating system accepts the request that a graceful reboot is performed. If the operating system rejects the request, the iDRAC forces a hard reset on the system.
 - **Power Cycle** : Performs a hard reset of the device.
 - Select **Stage for next server reboot**: Triggers the firmware/driver update when the next server reboot happens. This option is not available for **Schedule Later** update option.

NOTE: If the firmware update/driver jobs are created with the **Stage for next server reboot** option, wait until the firmware update completes on the target device before collecting the latest inventory (That is, after the scheduled reboot). After the update is complete and the target device is in a steady state, manually run an [Inventory Job](#) to collect the latest device software details. Optionally, you can wait for the system-scheduled inventory job to run. Click **Check Compliance (Configuration > Firmware/Driver Compliance)** upon completion of the Inventory job. This action refreshes the Baseline Software Components with the most recent component version's provided by the target device.

- Select **Reset iDRAC** to initiate a reboot of the iDRAC before the update job is initiated. This function is not supported for updating the drivers.
 - Select **Clear job queue** to delete all jobs (scheduled, completed, and failed) on the target device, before the update job is initiated. This function is not supported for updating the drivers.
- NOTE:** When updating firmware for more than 20 devices, the appliance may display the **Server Options** for reboot even if the selected components do not require a reboot. This behavior may be influenced by applied filters, such as Component Contains, Current Version Contains, or Baseline Version Contains. In this case, select a reboot option and proceed with the update. The server will not reboot if the selected components do not require it.

Reboot behavior for components with reboot required as **If Needed** for update:

Table 39. Reboot behavior for if needed components

Update includes	Update option	Reboot behavior	Notes
Components with If Needed reboot requirement	Update Now > Reboot server immediately	System reboots only if required by the components	Recommended to ensure updates complete successfully.
Components with If Needed reboot requirement	Update Now > Stage for next server reboot	Components may undergo a soft reset (not a full reboot). Updates might not install immediately and may require a manual reboot to complete. The job is marked as Completed , with job ID status as USERINTERVENTION .	Not recommended.
Components with If Needed reboot requirement	Schedule Later	Update staged and applied on the next schedule reboot.	Recommended for planned maintenance scenarios.

6. Click **Finish** to proceed or click **Cancel** to discard the previous selections.

Results

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

- When compliant devices (that is, devices marked with a green check) are selected for a **Make Compliant job** that contains associated components those updates will be reapplied to the devices. If any of those components require a restart, the devices are restarted to complete the compliance operation.
- After submitting this job, the console first attempts to verify the service tag of the intended target to ensure the operation is performed on the correct system. If the verification fails, the job completes with errors, and the task execution history detail shows the following: Running Verifying if the device Service Tag is valid. The device Service Tag could not be verified. Task Failed. Completed With Errors. Please check the system to ensure the IP address has not changed since the last discovery was completed. Remediate by discovering the system with the updated IP address, and retrying the operation.
- After completing the job, devices that are selected during the update could be in the following states on the iDRAC.
 - **Completed:** The device was successfully updated.
 - **Failed:** The update operation could not be completed on the device.
 - **Scheduled:** The server must be rebooted for the new firmware to take effect.
 - **USERINTERVENTION:** Sometimes **If Needed** reboot type components require a reboot for the new firmware to take effect. This state indicates that a reboot action is pending on the server.
- When updating firmware that require a reboot, and the **Update Now > Reboot server immediately** option is selected, OpenManage Enterprise reboots the target server even if the job fails in iDRAC.

Managing device deployment templates

Create, deploy, and manage device deployment templates to configure configuration properties on servers and chassis.

The device deployment template in OpenManage Enterprise allows you to set the configuration properties of servers and chassis. These properties include BIOS, boot, network properties, and so on.

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

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

You can either use the predefined deployment templates or import the deployment templates from a reference device or an existing template file. Click **Configuration > Templates** to view the list of existing templates.

The following details of the existing templates are displayed.

Table 40. Template settings

Field	Description
Name	Template name
Description	Detailed template description
Status	Template state. Possible values are: • Running • Stopped • Complete
Device Type	The device type (server, chassis, or IOA) that is used for template creation.
Template	This field indicates whether the template is custom-created or sampled.
Custom Telemetry	Displays if the template contains a custom telemetry configuration. The custom telemetry statuses are: • No Telemetry: Template has no telemetry • Included for deployment: Template has telemetry, and it will be included for deployment • Excluded for deployment: Template has telemetry and is excluded during deployment. See Edit a server deployment template to exclude a telemetry.

NOTE:

- For successful template deployment, ensure that the source and target devices have the same hardware and configuration. Any mismatch in configuration may lead to deployment failures. If any hardware changes occur on the source device, delete the template and re-create it.

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

A device manager can view and perform tasks on default templates and custom templates they own.

Compatibility considerations

- If target iDRACs are running firmware version 4.40.10.00 and above, the appliance uses Redfish for template-related tasks. If Redfish fails, the task is retried using WSMAN. The appliance uses WSMAN to initiate template-related tasks on iDRACs running versions earlier than 4.40.10.00.
- iDRAC 10 templates cannot be used with iDRAC 9 or earlier versions, and vice versa. Ensure that you use the correct template for your devices to maintain compatibility.

Topics:

- Create a deployment template from a reference device
- Create a deployment template by importing a template file
- View a deployment template information
- Edit a server deployment template
- Edit a chassis deployment template
- Edit IOA deployment template
- Edit network properties of a deployment template
- Deploy device deployment templates
- Deploy IOA deployment templates
- Clone deployment templates
- Export a deployment template
- Delete deployment templates
- Auto deploy device configuration before discovery
- Overview of stateless deployment
- Define networks
- Edit or delete a configured network
- Export VLAN definitions
- Import network definitions

Create a deployment template from a reference device

Create a deployment template by capturing the configuration from a managed device.

Prerequisites

- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See [Role and scope-based access](#).
- With SMBv2-enabled CIFS share, deployment template creation is not supported on Fx2: 2.21 and VRTX 3.21 devices.
- Deployment template creation is not supported on M1000e chassis.
- To create a template with custom telemetry configuration, ensure that the server has a valid iDRAC DataCenter license and the iDRAC firmware is 4.40 and above.

About this task

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

Steps

1. Click **Configuration > Templates > Create Template**, and then select **From Reference Device**.
 2. In the **Create Template** dialog box:
 - a. In the **Template Information** section, enter a name for the deployment template and a description for the template.

 **NOTE:** The only special characters that are allowed in the **Template Name** are alphanumeric, dash, underscore, and space.
 - b. Select the Deployment template type:
 - **Clone Reference Server:** Enables you to clone the configuration of an existing server.

 **NOTE:** The **Custom Telemetry** option is available only when the **Template Type** is selected as **Clone Reference Server** and these configurations are captured only if the target server has a valid data center license.
 - **Clone Reference Chassis:** Enables you to clone the configuration of an existing chassis.
 - **Clone Reference IOA:** Enables you to clone the configuration of an existing M I/O aggregator.
-  **NOTE:**

 - The attributes in the IOA template are uneditable, only the **name** and **description** of an IOA template can be edited.

- c. Click **Next**.
 - d. In the **Reference Device** section, click **Select Device** to select the device whose configuration properties are used for creating the deployment template. For more information about selecting devices, see [Selecting target devices and device groups](#).

NOTE:

 - Only the IOA templates that were extracted at the time of chassis discovery are available for cloning . See [Create a custom discovery job for devices](#)
 - You can select only one device as a reference device.
 - e. In the **Configuration Elements** section, select the check boxes corresponding to the device elements that must be cloned. For creating a deployment template by using server as the device, select to clone the server properties such as iDRAC, BIOS, Lifecycle Controller, and Event Filters. By default, all elements are selected.
 - f. Optional: To enable custom telemetry configuration, under **Additional Elements**, select **Custom Telemetry**.

NOTE: Custom telemetry configuration is available only when the **Template Type** is selected as **Clone Reference Server**, and this configuration is enabled only if the target server has a valid data center license.
 - g. Click **Finish**.
After successful creation, the job is displayed in the list. A deployment template creation job starts, and its status is displayed in the **STATUS** column.
3. The job information is also displayed on the **Monitor > Jobs** screen. To view additional details of the job:
- Select the job.
 - Click **View Details** in the working pane.
 - On the **Job Details** screen, you will find the execution details of the job.
 - In the **Results** pane, click **View Details** to view detailed information of the job execution.

Results

When creating a template with a custom telemetry option selected on a server, the deployment template creation task marks the job as completed in the Job Details. However, a warning appears in the task execution details indicating: Custom telemetry was requested but not received from the target.. The warning occurs because of the following reasons:

- The server was discovered through Complete Chassis Discovery (CCD).
- The server does not have a valid data center license or valid a telemetry configuration.

Next steps

Templates that are created from a reference device may contain a discovery password. When deployed on target devices, this can cause communication failure. To resolve this issue:

- After deployment, rediscover the device with the new credentials.
- Export the SCP reference from the iDRAC without password hash values and import it to OpenManage Enterprise. Optionally, set the password value by editing the attributes and deploying it.

Create a deployment template by importing a template file

Create a deployment template from an existing template file.

Steps

1. Click **Configuration > Templates > Create Template**, and then select **Import from File**.
2. In the **Import Template** dialog box:
 - a. Enter a name for the new deployment template.

NOTE: The only special characters that are allowed in the **Template Name** are alphanumeric, dash, underscore and space.
 - b. Click **Select a File**, and then select a template file.
 - c. Select either **Server**, **Chassis**, or **IOA** to indicate the template type.

 **NOTE:** The custom telemetry configuration is available only when the **Template Type** is selected as **Server**.

3. Click **Finish**.

The properties of an existing template file is imported and a new deployment template is created.

Example

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

View a deployment template information

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

Steps

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

Edit a server deployment template

Edit the custom deployment templates using the **Guided** or **Advanced** view modes.

Prerequisites

To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See [Role-based access privileges](#).

About this task

System-defined deployment templates cannot be edited. Only the user-created deployment templates that are identified as 'Custom' can be edited. You can edit the attributes of a deployment template irrespective of whether you created it by using a reference template file or a reference device. If the template is exported, selecting, or discarding attributes does not change the template-stored attributes. All attributes remain part of the template however, discarded attributes are not applied during deployment.

Steps

1. On the **Configuration > Templates** screen, select the required custom template check box, and then click **Edit**.
2. In the **Edit Template** dialog box:

- a. In the **Template Information** section, edit the deployment **Template Name** and **Description**. The template type cannot be edited.

 **NOTE:** The only special characters that are allowed in the **Template Name** are alphanumeric, dash, underscore, and space.

- b. Click **Next**.
- c. In the **Edit Components** section, the deployment template attributes are displayed in:

- The **Guided view** displays only common attributes which are grouped based on function. Attributes from the following categories are shown:
 - i. In the **BIOS Settings** section, select :
 - **Manually:** If you want to customize the BIOS properties, select this option.
 - **System profile:** From the drop-down menu, select to specify the type of performance optimization to be achieved in the system profile.
 - **User-accessible USB ports:** From the drop-down menu, select to specify the ports that the user can access.
 - By default, the uses of logical processor and in-band manageability are enabled.
 - **Optimize based on workload:** From the **Select workload profile** drop-down menu, enable this option to specify the type of workload performance optimization that you want to achieve on the profile.
 - ii. Click **Boot** and define the boot mode:
 - If the boot mode is set to **BIOS** :
 - To retry the boot sequence, select the **Enabled** check box.
 - Drag the items to set the boot sequence and hard drive sequence.
 - If the boot mode is set to UEFI, drag the items to set the UEFI boot sequence. If required, select the check box to enable the **Secure boot** feature.

 **NOTE:** PowerEdge 17G servers support UEFI option only.

- iii. Click **Networking**. All the networks that are associated with the deployment template are displayed under **Network Interfaces**.
 - To associate an optional identity pool to the deployment template, select from the **Identity pool** drop-down menu. The networks that are associated with the selected identity pool are displayed. If the deployment template is edited in the Advanced view, the Identity pool selection is disabled for this deployment template.
 - To view the network properties, expand the network.
 - To edit the properties, click the corresponding pen symbol.
 - Select the protocol to be used for booting. Ensure that the network supports the protocol that is selected.
 - Select the untagged and tagged network to be associated to the network.
 - The partition, max, and min bandwidths are displayed from the deployment template (profile) that was created earlier.
 - Click **Finish**. The network settings of the deployment template are saved.
- The **Advanced view** lists all the deployment template attributes that can be changed (including the attributes that are shown in the Guided view). This view allows you to set (like the Guided view) or enable, or disable attribute values.
- Attributes are grouped functionally for display. Vendor-specific attributes are grouped under **Other Attributes**. Each individual attribute is displayed with a check box preceding its name. The check box indicates whether the attribute is included when the deployment template is deployed to a target device. Because of attribute dependencies, enabling or disabling an attribute can cause unexpected results on the target device, or cause deployment to fail. Each group also has a check box to the left of its name. The icon in group check boxes has one of three values:
 - i. **Checked** indicates that all the attributes in the group are selected for deployment.
 - ii. **Hyphen** indicates some (but not all) of the attributes are selected for deployment.
 - iii. **Clear** indicates that none of the attributes in the group are selected for deployment.

 NOTE:

- Many deployment attributes are linked to each other. When changing any attribute, ensure that any other attribute that could be impacted is also verified.
- You can click group icons to add or discard deployment settings for all the attributes in the group.
- The attributes with secure information, such as passwords, are hidden, and appear as empty when initially loaded. Changes made to secure attribute values are masked.
- If a profile is already associated to it, the identity pool that is associated with a deployment template cannot be changed .

3. In the **Edit Custom Telemetry** section, select **Enable Custom Telemetry** to activate the custom telemetry settings.

 NOTE:

- To exclude telemetry, clear the **Enable Custom Telemetry** option in the **Edit Template** wizard.

- To revert the changes made while configuring the custom telemetry settings, click **Revert Changes**.
 - The appliance does not perform a schema check on XML content within the **CustomComponents** tag. Instead, the appliance validates that the content adheres to XML standards.
4. Click **Next**.
In the **Summary** section, the attributes you edited by using the Guided and Advanced mode are displayed. You can also view the custom telemetry modification status.
 5. This section is read-only. Read through the settings and click **Finish**.
The updated template attributes are saved to the deployment template.

Edit a chassis deployment template

Editing chassis deployment templates is possible with OpenManage Enterprise. When you edit an exported template, selecting or discarding attributes does not change the template-stored attributes. It only affects what is deployed.

Prerequisites

- To edit chassis deployment templates, you must have the privileges of an Administrator, Device Manager, or a custom role user. For more details, see [Role and scope-based access](#).
- User passwords cannot be set on the MX7000 chassis and the Chassis Management Controller (CMC) deployment templates.

Steps

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

Edit IOA deployment template

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

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

 **NOTE:** The only special characters that are allowed in the **name** are alphanumeric, dash, underscore, and space.

Edit network properties of a deployment template

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

About this task

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

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

Steps

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

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

3. In the **VLANs** section (applicable only for the modular systems):

 **NOTE:** VLAN settings are not supported for PowerEdge 17G servers with iDRAC 10.

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

 NOTE:

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

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

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

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

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

Deploy device deployment templates

Device deployment templates include configuration attributes. When deployed, they ensure that the target device is uniformly configured.

Prerequisites

- Ensure you have the necessary privileges, as described in [Role and scope-based access](#).
- Ensure that you have either created a device deployment template, or cloned a sample deployment template, as described in [Create a deployment template from a reference device](#).
- Ensure that the target devices meet the requirements that are specified in [Host system requirements](#).
- Ensure that the OpenManage Enterprise Advanced or Advanced+ license is installed on the target devices.
- Ensure that only alphanumeric, dash, underscore, and space are used as special characters in the **Template Name**. To edit the template name see [Edit a server deployment template](#).
- To deploy a template with custom telemetry configuration, ensure that the server has a valid iDRAC DataCenter license and the iDRAC firmware is 4.40 and above.
- Ensure you use the correct template for your devices, as iDRAC 10 templates cannot be used with iDRAC 9 or earlier versions, and vice versa.

About this task

- Due to an iDRAC limitation, iDRAC operator users cannot deploy user attributes to the target. Only iDRAC users with administrator privileges can deploy all the user attributes.

NOTE: In a template deployment with external CyberArk Integration enabled in OpenManage Enterprise, where CyberArk manages target device credentials, the process excludes deploying user attributes. This exclusion is to prevent disrupting the connection between the target device and the CyberArk vault instance managing the device.

- If a device manager or a custom role user is deploying templates, only eligible target groups and devices are displayed. To be eligible, the devices and groups have to be within the scope of the user.
- For iDRAC devices and templates with multiple users, ensure that the source and target servers are discovered using a common user or share common credentials.
- During deployment of an MX7000 chassis template:
 - The target device can only be the lead MX7000 chassis.
 - If an MX7000 chassis is removed from the group, it has to be rediscovered in OpenManage Enterprise.
 - Users that are configured in the template replace the users on the MX7000 chassis.
 - Imported Active Directory settings are replaced with the values in the chassis profile.

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

Steps

1. From the list of deployment templates on the **Configuration > Templates** screen, choose the deployment template that you want, check the corresponding box, and click **Deploy Template**.
2. In the **Deploy Template: <template_name>** dialog box, under **Target**:
 - a. Click **Select**, and then select devices in the **Job Target** dialog box. See [Select target devices and device groups](#).
 - b. During deployment of the device deployment template, the configuration changes might require a forceful reboot of the server. If you do not want to reboot the server, select the **Do not forcefully reboot the host OS** option. A graceful reboot of the server is attempted when the **Do not forcefully reboot the host OS** option is selected. If the reboot fails, you must rerun the template deployment task.
 - c. Select the **Use strict checking** check box to match the VLANs with like characteristics. If cleared, only VLAN name and QoS are used for matching.

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

- d. Click **Next**.
3. If the target device is a server, follow these steps:
 - a. To install an operating system remotely, enable **Boot to Network ISO**.
 - b. Select **Share Type**.
Choose either **CIFS** or **NFS**.

Table 41. Details for share type

Share Type	Field
CIFS	Under ISO Information, enter the following details. • ISO Path: sharename\path\filename.iso Under Share information, enter the following details. • Share IP Address: The IP address of the share. • Workgroup (optional) : The domain name if your network uses a domain. • Password: The user's password.
NFS	Under ISO Information, enter the following details. • ISO Path: NFSsharefoldername/path/ filename.iso Under Share information, enter the following details. • Share IP Address: The IP address of the share. • Password: The user's password.

- c. Set **Time to Attach ISO**.

Enter the duration in minutes in the Time to Attach ISO field (default is 240 minutes).

d. Optional: **Test Connection**.

Click Test Connection to verify the entered information and establish a connection.

NOTE: You must have the Job management privilege to verify the test connection. However, you can proceed to the next step without verifying the test connection.

e. Proceed or cancel.

Click **Next** to proceed.

Click **Cancel** to abort the configuration.

4. In the **iDRAC Management IP** section, change the target device IP settings if required, and then click **Next**.

NOTE:

- Template deployment fails if DHCP settings are assigned during template deployment to a target device that was originally discovered using a static IP.
- If the IP settings are not configured on the discovered MX7000 sled or PowerEdge 17G (iDRAC 10) server, the **Boot to Network ISO** operation does not execute during the deployment of the device template.
- If the deployed template is created from a reference device, verify whether the template contains user password information. If the template contains user password information, the appliance reverts to the discovery credentials for device communication. This change can be verified post deployment by checking the **Credential Type** of the target device (It displays **Discovery**). If using the service account for communication is preferred or the device is using password rotation, trigger the onboarding task for this device. This task either updates the password on the existing service account in iDRAC or, if user slots are available, generates a new service account.

5. Before deploying the template, modify nonvirtual identity attributes unique to each selected target device, such as location and IP address in the **Target Attributes** section. When the template is deployed, these changed target attributes are implemented on only the specific devices. To change the device-specific, nonvirtual identity attributes:

- a. Select a target device from the list displaying the previously selected target devices.
- b. Expand the attribute categories and then select or clear the attributes that must be included or excluded during template deployment on the target device.
- c. Click **Next**.

6. In the **Virtual Identities** section, click **Reserve identities**.

The assigned virtual identities of the NIC cards of the selected target device are displayed. To view all the assigned identities of the identity pool of the selected target device, click **View all NIC details**.

NOTE: If identities are already assigned outside of the appliance, then a new deployment does not use those identities unless they are cleared. For more information, see [Identity pools](#).

7. In the **Schedule** section, run the job immediately or schedule for a later time. See [Schedule job field definitions](#).

8. Click **Finish**. Review the warning message and click **YES**.

Results

A device configuration job is created.

After submitting a job, the console verifies the service tag of the target to ensure that the operation is performed on the correct system. If the verification fails, the job completes with errors. The task execution history detail shows the following:

```
Running
Verifying if the device Service Tag is valid.
The device Service Tag could not be verified.
Task Failed. Completed With Errors.
Check the system to ensure that the IP address has not changed since the last discovery
was completed. Remediate by discovering the system with the updated IP address, and
retrying the operation.
```

NOTE:

- If the job fails with an authentication error, update the discovery configuration with the new password and rediscover the device on the appliance.
- For templates with custom telemetry configuration, ensure that the device has a valid iDRAC DataCenter license. Otherwise, the job fails, and the task execution history shows the following:

```
#Attributes Failed to apply
CustomComponents - required license is missin or expired.
```

- For templates that modify the TLS configuration of the iDRAC, the deployment job may fail due to a change in the initial negotiated TLS handshake. While the settings are deployed successfully, the overall deployment job shows a **Failed** status. Redeploying the template a second time results in a **Completed** status.

```
# Initiated System Configuration Job
....Running : 10%
....The operation cannot be completed because the connection with the target
device is not authenticated.
```

Next steps

- See [Using jobs for device control](#).

Deploy IOA deployment templates

If they are supported, IOA templates can be deployed to any target device. If the target device is repurposed or bare-metal, configurations cannot be reverted.

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](#).

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

- You have created an IOA deployment template for deployment. See [Create a deployment template from a reference device](#).
- The target devices meet the requirements that are specified in [Host system requirements](#).
- The firmware version of the target device should be the same as the IOA deployment template.
- Only alphanumeric, dash, underscore, and space are used as special characters in the **Template Name**. To edit the template name see [Edit IOA deployment template](#).
- Only the following cross-template deployments are supported:

Table 42. Supported cross-template deployments

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

- After job submission, the console validates the service tag of the target system to ensure that the operation is performed on the correct system. If the verification fails, the job completes with errors, and the task execution history detail shows the following:

```
Running
Verifying if the device Service Tag is valid.
The device Service Tag could not be verified.
Task Failed With Errors.
Check the system to ensure that the IP address has not changed since the last
discovery was completed. Remediate by discovering the system with the updated IP
address, and retrying the operation.
```

About this task

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

Steps

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

Clone deployment templates

Create a deployment template by cloning an existing deployment template.

Steps

1. Under **Configuration**, click **Templates**.
A list of available deployment templates is displayed.
2. Select the check box corresponding to the template that you want to clone.
 **NOTE:** A cloned iDRAC 10 template cannot be used on iDRAC 9 or earlier versions, and vice versa.
3. Click **Clone**.
The custom telemetry configuration is cloned along with the template attributes during template clone operation.
4. Enter the name of the new deployment template, and then click **Finish**.
The cloned deployment template is created and displayed in the list of deployment templates.

Export a deployment template

Export a deployment template in .xml format.

Steps

1. Go to **Configuration > Templates**.
2. Select the template that you want to export and click **Export**.
 - a. In the wizard, select **Export Entire Template** to include all the attributes and component that are in the template or select **Export Selected Template Components and Attributes** to include only selected attributes and components while excluding others.
The template is exported in .xml format.

Delete deployment templates

Delete custom templates from OpenManage Enterprise.

Prerequisites

To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See [Role-based access privileges](#)

Steps

1. Go to **Configuration > Templates**.
2. Select the templates you want to delete and click **Delete**.
Only Custom templates can be deleted.

Results

Custom telemetry configuration are deleted permanently when associated templates are deleted.

Auto deploy device configuration before discovery

Automatically assign deployment templates to devices (server or chassis) before they are discovered by the appliance.

Overview

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

Prerequisites

- Only administrators can perform the create, delete, and export tasks on the auto-deployment templates. The device managers can only 'export' the auto-deployment templates. For more information, see [Role and scope-based access](#).
- Ensure you use the correct template for your devices, as iDRAC 10 templates cannot be used with iDRAC9 or earlier versions, and the same applies in the opposite direction.

Actions

From the **Auto Deploy** screen (**Configuration > Auto Deploy**), you can:

- **Create** auto deployment targets: Assign templates to undiscovered devices. See [Create auto deployment targets](#)
- **Delete** templates that are no longer required. See [Delete auto deployment targets](#)
- **Export** the auto deployment templates to different formats. See [Export auto deployed target details](#)

Auto deploy interface

- Advanced Filters: Customize the auto deploy targets list using fields like Identifier, Template Name, Template Type, Status, or Boot to Network ISO.
- Details Panel: Displays **Created On** and **Created By** for the selected auto deployment target. When multiple auto deployment targets are selected, details of the last selected item are displayed in the section.

Post-discovery behavior

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

Create auto deployment targets

Assign one or more target devices so the appliance automatically deploys templates on them. Target devices can be specified by using their Service Tag, IDs, or importing a CSV file.

Prerequisites

- You must be a Super Administrator, Administrator, or Custom Role user with auto-deploy management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- To auto deploy a template with custom telemetry configuration, ensure that the server has a valid iDRAC DataCenter license and the iDRAC firmware is 4.40 and above.
- Ensure you use the correct template for your devices, as iDRAC 10 templates cannot be used with iDRAC9 or earlier versions, and the same applies in the opposite direction.

Steps

1. Click **Configuration > Auto Deploy > Create**
The Auto Deploy Template wizard is displayed.
2. On the **Template Information** screen, select the deployment template type (Server or Chassis).
3. From the **Select Template** drop-down menu, select an appropriate template. If the selected template has identity attributes which are not associated with any virtual identity pool, the following message is displayed: `The selected template has identity attributes, but it has not been associated with a virtual identity pool. Deploying this template will not change virtual network addresses on the target devices.`
4. Click **Next**.
The **Target Information** screen is displayed.
5. On the **Target Information** screen, target devices can be selected in one of the following methods:
 - **Enter Manually** : Enter the Service Tag or node IDs to identify the target devices. The identifiers can be entered in any order, however, identifiers must be comma-separated. Click **Validate** to verify the accuracy of the values. It is mandatory to validate the identifiers.
 - **Import CSV**: Click **Import CSV** to browse the folders and select the respective .csv file with the target device details. A summary of the number of successfully imported and invalid entries is displayed. For a more detailed view of the import result, click **View details**. The entries in the CSV file must have the following format: The identifiers must be listed in the first column, one per row, starting from the second row. For a template CSV file, click **Download sample CSV file**.
6. Click **Next**.
7. On the **Target Group Information** screen, specify a subgroup under the **Static group** if available. For more information about grouping of devices, see [Create and manage custom groups](#). The target devices would be placed under the specified target group on their discovery.
8. Click **Next**.
9. To install an operating system remotely, enable **Boot to Network ISO**.
 - a. Select **Share Type**.
Choose either **CIFS** or **NFS**.

Table 43. Details for share type

Share Type	Field
CIFS	Under ISO Information, enter the following details. • ISO Path: sharename\path\filename.iso Under Share information, enter the following details. • Share IP Address: The IP address of the share. • Workgroup (optional) : The domain name if your network uses a domain. • Password: The user's password.
NFS	Under ISO Information, enter the following details. • ISO Path: NFSsharefoldername/path/ filename.iso Under Share information, enter the following details.

Table 43. Details for share type (continued)

Share Type	Field
	• Share IP Address: The IP address of the share. • Password: The user's password.

- b. Set **Time to Attach ISO**.
Enter the duration in minutes in the Time to Attach ISO field (default is 240 minutes).
 - c. Proceed or cancel.
Click **Next** to proceed.
Click **Cancel** to abort the configuration.
10. On the **Virtual Identities** screen, click **Reserve identities**.
The assigned virtual identities of the NIC cards of the selected target device are displayed. To view all the assigned identities of the identity pool of the selected target device, click **View all NIC details**.
 11. In the **Target Attributes** section, the non-virtual identity attributes specific to each of the selected target devices, such as the location attributes and IP address, can be changed before deploying the deployment template. When the template is deployed, these changed target attributes are implemented on only the specific devices. To change the device-specific, non-virtual identity attributes:
 - a. Select a target device from the list displaying the previously-selected target devices.
 - b. Expand the attribute categories and then select or clear the attributes that must be included or excluded during template deployment on the target device.
 - c. Click **Next**.
 12. Click **Finish**.
An alert message Deploying a template can cause data loss and can cause a restart of the device. Are you sure you want to deploy the template? is displayed.
 13. Click **Yes**.
A new Auto Deploy target is created and listed on the **Auto Deploy** screen.
- i NOTE:** For templates with custom telemetry configuration, ensure that the device has a valid iDRAC DataCenter license. Otherwise, the job fails, and the task execution history shows the following:

```
#Attributes Failed to apply
CustomComponents - required license is missin or expired.
```

Delete auto deployment targets

Delete one or more targets that are associated with a deployment template.

Prerequisites

- You must be a Super Administrator, Administrator, or Custom Role user with auto-deploy management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- If a template that is associated with auto deployment targets is deleted from the **Configuration > Templates** screen, the associated auto deploy entries would also get deleted irrespective of their current state.

Steps

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

Export auto deployed target details

Export data about targets to a HTML, CSV, or PDF file.

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with auto-deploy management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

1. Go to the **Auto Deploy** screen by clicking **Configuration > Auto Deploy**.
2. Select the auto deploy target from the list and click **Export**.
3. In the **Export All** dialog box, select format as either HTML, or CSV, or PDF. Click **Finish**.

Results

A job is created and the auto deploy target data is exported in the selected format.

Overview of stateless deployment

Stateless deployments enable you to create a server environment that is dynamic and flexible. For example, deploying a server with virtual I/O identities in a boot-from-SAN environment enables you to quickly replace a failing server or deploy additional servers.

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

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

Managing identity pools for stateless deployment

Servers deployed using a device deployment template that contains virtual I/O identities are known as 'stateless'. Stateless deployments enable you to create dynamic and flexible server environments.

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

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

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

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

NOTE:

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

- Scope based restrictions don't apply to identity pools, therefore, all identity pools can be viewed and used by all user types. However, once the identities are assigned by a device manager or a custom role user, then only those identities can be viewed and used by that user.

Creating identity pools

Create identity pools to virtualize network identities for Ethernet, iSCSI, FCoE, or FC.

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

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

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

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

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

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

Pool Name	Enter a name of the identity pool. The pool name can have a maximum length of 255 characters.
Description	Enter a description for the identity pool. The maximum length of the description is 255 characters.
The following actions are available:	
Next	Displays the Ethernet tab.
Finish	Saves the changes and displays the Identity Pools screen.
Cancel	Closes the Create Identity Pool wizard without saving the changes.

Identity pools

Use virtual identity types to form identity pools for network communication. Sample virtual identity types are Ethernet iSCSI, FC, and FCoE.

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

- **Ethernet identities:** The Identities which are defined by the Media Access Control (MAC) address. MAC addresses are required for Ethernet (LAN) communications.
- **iSCSI identities:** The Identities which are defined by the iSCSI Qualified Name (IQN). IQN identities are required to support boot-from-SAN by using the iSCSI protocol.
- **Fibre Channel (FC) identities:** The Identities which are defined by the World Wide Node Name (WWNN) and World Wide Port Name (WWPN). A WWNN identity is assigned to a node (device) in an FC fabric and may be shared by some or all ports of a device. A WWPN identity is assigned to each port in an FC fabric and is unique to each port. WWNN and WWPN identities are required to support boot-from-SAN and for data access using FC and Fibre Channel over Ethernet (FCoE) protocols.
- **Fibre Channel over Ethernet (FCoE) identities:** Identities that provide a unique virtual identity for FCoE operations. These identities are defined by both MAC address and the FC addresses (that is WWNN and WWPN). WWNN and WWPN identities are required to support boot-from-SAN and for data access using FC and Fibre Channel over Ethernet (FCoE) protocols.

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

NOTE:

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

Create identity pools

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

About this task

To create a pool of virtual identity types:

Steps

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

 **NOTE:** The iSCSI Initiator IP Pool does not support IPv6 addresses.
6. In the **FCoE** section:
 - a. Select the **Include FCoE Identity** check box to include FCoE identities.
 - b. Enter the starting MAC address and specify the number of FCoE identities to be created.

The WWPN and WWNN addresses are generated by prefixing 0x2001 and 0x2000 respectively to the MAC addresses.
7. In the **Fibre Channel** section:
 - a. Select the **Include FC Identity** check box to include FC identities.
 - b. Enter the postfix octets (six octets) and the number of WWPN and WWNN addresses to be created.

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

Results

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

Create FC identity pool

Create an identity pool of Fibre Channels (FCs) using WWPN or WWNN addresses.

You can add FC addresses to the identity pool. The FC is comprised of WWPN / WWNN addresses.

Include FC Identity Select the check box to add FC addresses to the identity pool.

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

Actions

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

Create iSCSI identity pool

Create an identity pool of iSCSIs by using MAC addresses.

Configure the required number of iSCSI MAC addresses in the iSCSI tab.

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

Include virtual iSCSI MAC Addresses	Select the check box to add the iSCSI MAC addresses to the identity pool.
Starting virtual MAC Address	Enter the starting MAC address of the identity pool in one of the following formats: • AA:BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF The maximum length of a MAC address is 50 characters. This option is displayed only if the Include iSCSI MAC Addresses check box is selected.
Number of iSCSI MAC addresses	Enter the number of iSCSI MAC addresses. The MAC address can be between 1 and 5000. This option is displayed only if the Include iSCSI MAC Addresses check box is selected.
Configure iSCSI Initiator	Select the check box to configure the iSCSI initiator. This option is displayed only if the Include iSCSI MAC Addresses check box is selected.
IQN Prefix	Enter the IQN prefix of iSCSI identity pool. The length of the IQN prefix is a maximum of 200 characters. The system generates the pool of IQN addresses automatically by appending the generated number to the prefix. For example: <IQN Prefix>.<number>. This option is displayed only if the Configure iSCSI Initiator check box is selected.  NOTE: • The IQN configured with identity pools is not deployed on the target system if the boot mode is "BIOS". • If the iSCSI initiator name is displayed in a separate line in the Identity Pools > Usage > iSCSI IQN field, then, it indicates that the iSCSI IQN is enabled only on that NIC partition.
Enable iSCSI Initiator IP Pool	Select the check box to configure a pool of iSCSI initiator identities. This option is displayed only if the Include iSCSI MAC Addresses check box is selected.
IP Address Range	Enter the IP address range for the iSCSI initiator pool in one of the following formats: • A.B.C.D - W.X.Y.Z • A.B.C.D/E

Subnet mask	Select the subnet mask address of the iSCSI pool from the drop-down.
Gateway	Enter the gateway address of the iSCSI pool.
Primary DNS Server	Enter the primary DNS server address.
Secondary DNS Server	Enter the secondary DNS server address.

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

The following actions are available:

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

Create FCoE identity pool

Create an identity pool of Fibre Channels over ethernet (FCoE)s by using FIP MAC addresses.

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

Include FCoE Identity	Select the check box to include the FCoE MAC addresses to the identity pool.
FIP MAC Address	Enter the starting FCoE Initialization Protocol (FIP) MAC address of the identity pool in one of the following formats: - AA:BB:CC:DD:EE:FF - AA-BB-CC-DD-EE-FF - AABB.CCDD.EEFF The maximum length of a MAC address is 50 characters. This option is displayed only if the Include FCoE Identity check box is selected. The WWPN/WWNN values are generated from the MAC address.
Number of FCoE Identities	Select the required number of FCoE identities. The identities can be between 1 and 5000.

The following actions are available:

Previous	Displays the iSCSI tab.
Next	Displays the Fibre Channel tab.
Finish	Saves the changes and displays the Identity Pools screen.
Cancel	Closes the Create Identity Pool wizard without saving the changes.

Create ethernet identity pool

Create an identity pool of Ethernet by using MAC addresses.

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

Include ethernet virtual MAC addresses	Select the check box to add the virtual MAC addresses to the identity pool.
Starting virtual MAC Address	Enter the starting virtual MAC address in one of the following formats: • AA:BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF The maximum length of a MAC address is 50 characters. This option is displayed only if the Include ethernet virtual MAC addresses check box is selected.
Number of virtual MAC Identities	Select the number of virtual MAC identities. The identities can be 1 to 50. This option is displayed only if the Include ethernet virtual MAC addresses check box is selected.
The following actions are available:	
Previous	Displays the Pool Information tab.
Next	Displays the iSCSI tab.
Finish	Saves the changes and displays the Identity Pools screen.
Cancel	Closes the Create Identity Pool wizard without saving the changes.

View definitions of identity pools

View identity definitions of an identity pool.

Steps

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

Edit identity pools

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

Steps

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

Results

The identity pool is now modified.

Delete identity pools

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

Steps

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

Results

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

Define networks

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

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with network management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

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

Results

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

 **NOTE:** Scope-based restrictions do not apply to VLANs as they are common resource pools. Once an administrator defines a VLAN, it is available to all the device managers for use.

Network types

Assign network types for the traffic managed by the MX7000 chassis in your environment.

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

Table 44. Network types

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

Edit or delete a configured network

Edit or delete the properties of a virtual network.

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with network management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

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

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

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

Export VLAN definitions

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

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with network management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

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

Import network definitions

The following options are available to import the network definitions:

Prerequisites

You must be a Super Administrator, Administrator, or Custom Role user with network management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

 **NOTE:** Import VLAN definitions is not supported on iDRAC 10-based PowerEdge 17G server.

Steps

1. **Import VLAN definitions from a file**

To import VLAN definitions from a file:

 - a. Click **Configuration > VLANs**.
 - b. Click **Import** and select **Import from File**.
 - c. Open the file location and select an existing .json or .csv file containing the VLAN definitions, and click **Open**.
 - Invalid entries or content types in the files are identified and are not imported.
 - VLAN definitions in the .csv and .json files must be entered in the following formats:

Table 45. VLAN definition format for CSV file

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

VLAN definition format for JSON files				
<pre>[{"Name": "VLAN1", "Description": "VLAN with single ID", "VlanMinimum": 1, "VlanMaximum": 1, "Type": 1}, {"Name": "VLAN2 (Range)", "Description": "VLAN with an ID Range", "VlanMinimum": 2, "VlanMaximum": 10, "Type": 2}]</pre>				

- d. Click **Finish**. A job that is named **ImportVLANDefinitionsTask** is created to import the networks from the selected file.
2. **Import VLAN definitions from a chassis**

To import VLAN definitions from an existing MX7000 chassis:

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

- Click **Configuration > VLANs**.
- Click **Import** and select **Import VLANs from Chassis**.
- On the **Job Target** screen, select the chassis from where the VLAN definitions must be imported and click **OK**. A job that is named **ImportVLANDefinitionsTask** is created to import the networks from the selected chassis.

 **NOTE:** Chassis with iDRAC firmware 2.50.50.50 and lower is not supported for import.

Results

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

To view the execution details of the job and for the status of each network that was imported from the chassis: Click **Monitor > Jobs**, select the job, and click **View Details**.

Managing device warranty

Display the warranty statuses of all the devices in your scope that are monitored.

You must be a Super Administrator, Administrator, or Custom Role user with appliance management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#). An administrator with access to all device groups sees the warranty details of all the devices. A device manager or custom role user only sees the warranty details of the devices in their scope.

You can view and update the warranty of a device in three ways:

- Click **Devices** to select a device from the list.
- Click the **View details** button on the right, and select **Warranty**.
- Click **Devices**, select a **Name** from the device list, and click **Warranty**.
- Click **Monitor** > **Warranty**.

You can also export selected or all data to an Excel sheet for statistical and analytical purposes.

The **Warranty** screen displays the:

- **Status** of the warranty according to the settings that the administrator sets in [Manage warranty settings](#).
 -  This icon means that the warranty has expired.
 -  This icon means that the warranty is approaching expiration.
 -  This icon means that the warranty is active.
- **Service Tag**
- **Device Model**
- **Device Type**
- **Warranty State:**
 - **Initial:** The warranty that is provided with the purchase of OpenManage Enterprise.
 - **Extended:** The warranty is extended because the initial warranty duration is expired.
- **Service Level Description** lists the Service Level Agreement (SLA) associated with the device warranty.
- **Days Remaining:** The number of days left for the warranty to expire. You can set the days before which you get an alert. See [Manage warranty settings](#).

 **NOTE:** The **Service Tag**, **Device Model**, and **Device Type** are only displayed in the **Monitor** > **Warranty** screen.

OpenManage Enterprise provides a system-defined report about the warranties that expire in the next 30 days. To see the report, click **Monitor** > **Reports** > **Warranties Expiring in Next 30 days**. Click **Run**, and see [Run reports](#) for more information.

To filter the data displayed in the table, click **Advanced Filters**, and see [The OpenManage Enterprise GUI](#) for more information.

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

To export all or selected warranty data, click **Export**, and see [Export data](#) for more information.

Topics:

- [View and renew device warranty](#)
- [Internal warranty alerts](#)

View and renew device warranty

View and renew the warranty status of devices that are monitored and managed by OpenManage Enterprise.

Click **Monitor** > **Warranty** to get a list of device warranty statuses along with their details. For field descriptions, see [Managing device warranty](#).

The warranty key is valid for one year from the date it is issued. Ensure you renew and update the key to avoid disruption in warranty data retrieval.

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

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

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

Internal warranty alerts

OpenManage Enterprise generates an internal, critical alert (CWAR0001) notifying users that a specified number of device warranties have expired. This alert is generated after the warranty retrieval is completed, either after the built-in weekly warranty job or manual retrieval through the warranty view.

This internal alert is generated regardless of how the **Hide expired warranties** configuration for the **Manage warranty settings** is configured. To suppress these alert, configure an Ignore alerts policy as described in the [Manage alert logs](#) section.

Managing alerts

Click **Alerts** to view and manage alerts that devices generate in the management system environment.

The **Alerts** screen has the following tabs displayed:

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

NOTE:

- In the OpenManage Enterprise console, when duplicate alerts are received from the same source within a 60-second interval, only one of them is displayed on the **Alerts** page and considered for alert actions.
- To manage and monitor device alerts on OpenManage Enterprise, you must have [Role and scope-based access](#).
- The scope-based access that you have governs alert policies and alert logs. For example, an administrator can view and manage all the alert policies. However, device managers can only view and manage the default alert policies and the policies that they create and own. Also, the device managers can only view the alerts for the devices that are in their scope.
- SNMPv3 support is not provided on the MX5016s models.
- OpenManage Enterprise provides a system-defined report to view the list of monitored devices and the alerts that are generated for each device. Click **Monitor > Reports > Alert Counts per Device Report**. Click **Run**. See [Run reports](#)

Topics:

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

View alert logs

View alert logs that are unacknowledged and acknowledge if necessary.

The **Alerts Log** screen displays the list of alert logs for events occurring in the devices. Click **Alerts > Alert Log**. The **Alerts Log** screen is displayed.

By default, only the unacknowledged alerts are displayed. You can customize the list of alerts using either **Advanced Filters** (on the upper left side of the alert list) or by changing the **Alert Display Settings** on the **Application Settings** screen. You can use the following **Advanced Filters** on the **Alerts Log** screen to refine the list of displayed alerts:

- **Severity:** Filter alerts by severity level—Info, Normal, Warning, Critical, or Unknown.
- **Acknowledge:** Filter based on whether alerts are acknowledged or unacknowledged. You can click between the square brackets under **ACKNOWLEDGE** column to acknowledge or unacknowledge an alert.
- **Start Date/End date:** Specify a date range to display alerts generated within that period.
- **Source name:** Filter by the hostname of the device that generated the alert. Click the source name to view or configure device properties.

 **NOTE:** Internal alerts or alerts from undiscovered devices are excluded when filtering by IP address or source name.

- **Category:** The type of alert (Possible alert categories include audit, chassis, configuration, miscellaneous, primary loop, secondary loop, storage, system health, telemetry, updates, and work notes).
- **Subcategory:** Filter by the subcategory of the alert.
- **Message ID:** Filter by the unique alphanumeric identifier assigned to each alert.
- **Message:** Filter based on the alert message text.
- **User:** Filter by the user who acknowledged or unacknowledged the alert.

- The box on the right displays additional details and recommended actions for the selected alert.

To change the default display, see [Customize the alert display](#).

NOTE:

- In a multichassis management (MCM) environment, if several alerts occur at once in the lead chassis, the processing of the alerts may be delayed.
- Archived alerts are not saved during **Backup** operations as they are not part of the database.

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

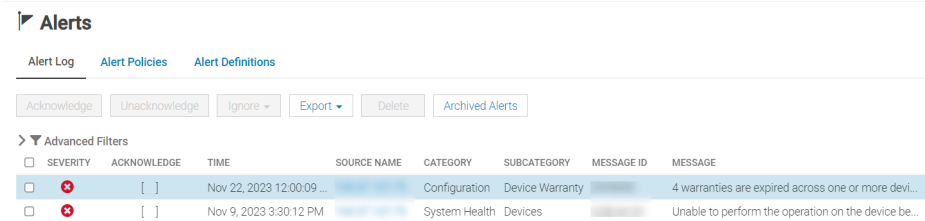
- Acknowledge alerts
- Unacknowledge alerts
- Ignore alerts
- Export alerts
- Delete alerts
- Archived alerts

Manage alert logs

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

Before you begin: You must be a Super Administrator, Administrator, or Custom Role user with alert management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

To display the **Alert log** screen, click **Alerts > Alert log**.



Acknowledge alerts

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

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

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

Unacknowledge alerts

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

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

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

Ignore alerts

Before you begin: You must be a Super Administrator, Administrator, or Custom Role user with monitoring setup management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Ignoring an alert creates an alert policy that discards all future occurrences of that alert based on the option selected. To ignore an alert, select the check box corresponding to the alert and click **Ignore**.

To stop processing alerts, choose one of the following options:

- **Ignore on Selected Device(s) Only:** This generates an ignore alert policy that ignores the specific alert message ID from the source name in the selected item.
- **Ignore All Alerts from Select Device(s):** This generates an ignore alert policy that ignores all alerts from the source name in the selected item.
- **Ignore on All Devices:** This generates an ignore alert policy that ignores the specific alert message ID in the select item for all devices.

Export alerts

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

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

Delete alerts

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

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

View archived alerts

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

Table 46. Alert purging

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

Download archived alerts

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

1. Click **Archived Alerts**. In the **Archived Alerts** dialog box, the last five purged archived alerts are displayed. File size, name, and archived date are indicated.
2. Select the check box corresponding to the alert file and click **Finish**. The .CSV file is downloaded to the location you selected.

 **NOTE:** To download archived alerts, you must have necessary privileges. See [Role and scope-based access](#).

Alert policies

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

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

Before you begin: You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with monitoring setup management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Use alert policies to perform the following actions based on certain alert characterizations:

- Send an email to a specified email address.
- Forward an alert as an SNMP trap.
- Send an alert to a syslog server.
- Ignore the alert.
- Send an alert to a phone through an SMS notification.
- Perform device power control actions such as turning on or turning off a device when an alert of a predefined category is generated.
- Run a remote script.
- Mobile push notification with a registered device through OpenManage Mobile application.

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

The alert policy details include name and description of the alert policy, status of the alert policy, email ID of the administrator, and information about syslog, SNMP Trap Forwarding, SMS, Power Control, Remote, and Mobile. A tick mark corresponding to an alert policy indicates that the alert policy is enabled.

You can perform the following tasks on the **Alert Policies** page:

- Create alert policies
- Edit alert policies
- Enable alert policies
- Disable alert policies
- Delete alert policies

Related tasks

[Create an alert policy](#)

[Forward audit logs to remote Syslog servers](#)

Configure and manage alert policies

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

Pre-requisites:

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](#).

Create an alert policy

Create alert policies to send alerts by email, phone, SNMP traps, and perform device control actions (for example, power on or off, power cycle, graceful shutdown) when an alert of a predefined category is triggered.

Steps

1. On the **Alerts > Alerts Policies** screen, click **Create**.
2. Click **Name and Description** and enter a name and description for the alert policy and click **Next**. The **Enable Policy** check-box is selected by default.
3. To activate an alert policy that is based on the category of the alerts that are received:
 - a. Click **Category**.
 - b. Select the alert category by selecting any or all the system-defined, and imported third-party Management Information Base (MIB) categories.

Select the following subcategories for viewing power-related data:

 - **Metrics**—Receive alerts on alert threshold violations.
 - **Power Configuration**—Receive alerts on policy cap violations.
 - **APC/Vertiv/Dell iPDU**—Receive specific PDU device type alerts.
 - c. Click **Next**.

You can expand each category to view and select the subcategories. To know more about categories and subcategories, see [Alert Definitions](#).
4. To activate the alert policy based on the 'Message IDs' of the alerts received, click **Message ID** to do one of the following:
 - a. Choose **File** and then upload a CSV file with the Message IDs.
 - b. Choose **Message IDs** and then enter the Message IDs separated by commas in the box. Click **Next**.

NOTE: Both Category and Message IDs cannot be used simultaneously on an alert policy. Hence, when Category is already selected, the use of Message ID is disabled.
5. In the **Target** section select the target devices on which the alert policy is applicable and click **Next**. You can choose one of the following options:
 - **Select Devices** to select device or devices.
 - **Select Groups** to select a group or groups.
 - **Specific Undiscovered Devices** to specify undiscovered devices by entering their IP address .

NOTE: When configuring alert policies for Specified Undiscovered Devices in OpenManage Enterprise, use only IP addresses as valid targets. Do not use hostnames or FQDNs, as they are not supported and may cause the policy configuration to fail.

 - **Any Undiscovered Devices** to specify all the undiscovered devices.

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

 - **All Devices** to select all the 'discovered' and the 'undiscovered' devices.
6. (Optional) Specify the duration for when the alert policy is applicable by selecting the required values for **Date Range**, **Time Interval** and **Days**, and then click **Next**.
7. In the **Severity** section, select the severity of the alert and click **Next**.

To apply the alert policy on all the severity categories, select the **All** checkbox.
8. In the **Actions** section, select one or more alert actions and click **Next**. The available options are:
 - Email: Choose Email to send information to a designated recipient by specifying details for each field and use tokens (if needed) for the subject and message. See [Token substitution in remote scripts and alert policy](#)

NOTE: Multiple alerts with the same category, message ID, and content trigger Emails only once every 2 minutes to prevent inbox clutter with redundant messages.

 - SNMP Trap Forwarding (Enable): Click **Enable** to view the SNMP Configuration window where you can configure the SNMP settings for the alert. See [Configure SMTP, SNMP, and Syslog alerts](#).

- Syslog (Enable): Click **Enable** to view the Syslog Configuration window where you can configure the system log settings for the alert. See [Configure SMTP, SNMP, and Syslog alerts](#).
- Select the **Ignore** checkbox to ignore the alert message and not activate the alert policy.

When an alert policy is configured to ignore all messages with the target set to **Any Undiscovered Devices**, audit logs generated by OpenManage Enterprise are not forwarded to alert destinations such as Syslog or SMTP. Avoid applying ignore alert policies to **Any Undiscovered Devices** if audit log forwarding is needed.

- Send an SMS to a specified phone number with the alert message containing the system hostname or IP address.

NOTE: This feature is supported only if the telecom carriers support the sending of Emails as SMS.

- Power Control: Select **Power Control** to view the actions where you can turn on, turn off, power cycle, or gracefully shutdown a device.

NOTE: Power control action is not supported on CDU devices.

- Remote Script Execution (Enable): Click **Enable** to view the Remote Command Setting window where you can add and run remote commands on remote nodes. For more information about adding remote commands, see [Executing remote commands and scripts](#).

From the drop-down menu, select the script that you want to run when this alert policy is run. You can set up running the remote command also as described in [Managing OME settings](#).

NOTE: Remote script execution on certain device types is not supported. Although alert jobs are created for these devices, they fail during execution with the following error: Unable to process action because the operation is not supported by the target device.

- Send a notification to the mobile phone registered with OpenManage Enterprise. See [OpenManage Mobile \(OMM\) Settings](#).

NOTE: In the OpenManage Enterprise console, when duplicate alerts are received from the same source within a 60-second interval, only one of them is displayed on the **Alerts** page and considered for alert actions.

9. In the **Summary** section, review the details of the created alert policy and click **Finish**.
The alert policy is successfully created and listed in the **Alert Policies** section.

Related concepts

[Alert policies](#)

Manage alert policies

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

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

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

- **Edit an alert policy:** Select an alert policy and click **Edit** to edit the required information in the [Create an alert policy](#) dialog box.

NOTE:

- Only one alert policy can be edited at a time.
- The **Time Interval** check box is disabled by default for alert policies on OpenManage Enterprise versions before version 3.3.1. After upgrading, enable the **Time Interval** and update the fields to reactivate the policies.
- Ensure that the timezone configured on both the client and appliance devices are the same. This way the schedule provided for the policy is within the configured range.
- Emails for alert policies do not work when the same events generated twice within 2 minutes. Email action for alerts containing the same message ID and content are triggered every 2 minutes to avoid many repeated/redundant alert messages in the inbox.

- o The **Emergency Power Reduction - Liquid Cooling System Alerts** policy enables EPR on the server whenever a leakage is detected in the liquid cooling system. Throttle EPR is enabled for small leaks while Shut down EPR is enabled for large leaks. EPR is disabled when the leakage is rectified.
- **Enable alert policies:** Select the alert policy and click **Enable**. A check mark appears under the **Enabled** column when an alert policy is enabled. The **Enable** button of an alert policy that is already enabled appears grayed-out.
- **Disable alert policies:** Select the alert policy and click **Disable**. The alert policy is disabled and the tick mark in the **ENABLED** column is removed. You can also disable an alert policy while creating the alert policy by clearing the **Enable Policy** check box in the Name and Description section.
- **Delete alert policies:** Select the alert policy and click **Delete**. You can delete multiple alert policies at a time by selecting the respective check boxes. To select or clear all the check boxes, select the check box in the header row next to **ENABLED**.

Forward audit logs to remote Syslog servers

To monitor all the audit logs of OpenManage Enterprise from Syslog servers, you can create an alert policy. All audit logs such as user login attempts, creation of alert policies, and running different jobs can be forwarded to Syslog servers. If a server specifies the OpenManage Enterprise as a Syslog target, traps triggered on the server will be forwarded to the OpenManage Enterprise's destination Syslog server as well. To forward audit logs to an SNMP destination, set the trap-forwarding format to **Normalized** in the Console Settings.

Steps

1. Select **Alerts > Alert Policies > Create**.
2. In the **Create Alert Policy** dialog box, in the **Name and Description** section, enter a name and description of the alert policy.
 - a. The **Enable Policy** check box is selected by default to indicate that the alert policy will be enabled once it is created. To disable the alert policy, clear the check box. For more information about enabling alert policies at a later time, see [Create an alert policy](#).
 - b. Click **Next**.
3. In the **Category** section, expand **Application** and select the categories and subcategories of the appliance logs. Alternatively, in the **Message ID** section, indicate a list of messages to be sent to the Syslog by either:
 - a. Uploading a .csv file listing the messages to be filtered. (Sample available on the UI)
 - b. Entering a list of message IDs separated by commas.
4. Click **Next**.
5. In the **Target** section, the **Select Devices** option is selected by default. Click **Select Devices** and select devices from the left pane. Click **Next**.

NOTE:

 - Selecting target devices or groups is not applicable while forwarding the audit logs to the Syslog server.
 - To forward audit logs to an SNMP destination, set the trap-forwarding format to **Normalized** in the Console Settings. See, 'Configure trap forwarding format' in [Manage console settings](#) for more details.
6. (Optional) By default, the alert policies are always active. To limit activity, in the **Date and Time** section, select the 'from' and 'to' dates, and then select the time frame.
 - a. Select the check boxes corresponding to the days on which the alert policies must be run.
 - b. Click **Next**.
7. In the **Severity** section, select the severity level of the alerts for which this policy must be activated.
 - a. To select all the severity categories, select the **All** check box.
 - b. Click **Next**.
8. In the **Actions** section, select **Syslog**.

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

Results

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

Related concepts

[Alert policies](#)

Configure remote commands and scripts

Configure remote commands and scripts on the appliance that can be executed by an alert policy Remote Script Execution action.

About this task

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

NOTE:

- The use of the following special characters as RACADM, script, and IPMI CLI parameters is not supported: `[, ;, |, $, >, <, &, ', ], ., *, and '.`
- Remote script execution is not supported on certain device types. Although alert jobs are created for these devices, they fail during execution with the following error: `Unable to process action because the operation is not supported by the target device.`

Steps

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

Automatic alerts on the MX7000 chassis

When a sled is inserted or taken off from an MX7000 chassis, OpenManage Enterprise instantly alerts and indicates it on its dashboard.

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

When a stand-alone or a lead MX7000 chassis is discovered or onboarded, an alert policy is created on the MX7000 chassis. For more information about discovering and onboarding devices in OpenManage Enterprise, see [Create a device discovery job](#) and [Onboarding devices](#).

The MX7000 auto-alert policy on OpenManage Enterprise-Modular initiates a chassis inventory refresh, labeled **Refresh Inventory of Chassis** whenever a sled is changed in the MX7000 chassis.

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

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

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

NOTE:

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

Alert definitions

Click **Alerts > Alert Definitions** to view OpenManage Enterprise alerts.

In OpenManage Enterprise:

- Alerts are displayed as *events* and *error messages*.
- Alerts are displayed on the Graphical User Interface (UI), the Command Line Interface (CLI) for RACADM and WS-Man.
- Alerts are saved in the log files (for information purposes only).
- Alerts are numbered and clearly defined to enable you to implement corrective and preventive actions.

Each event and error message includes:

- **Message ID:** Messages are classified based on components such as BIOS, power source (PSU), storage (STR), log data (LOG), and Chassis Management Controller (CMC).
- **Message** includes the cause of the event. Events are triggered for information purposes only, or when there is an error in performing tasks.
- **Category** specifies the class to which the error message belongs. For information about categories, see the *Event and Error Message Reference Guide for Dell PowerEdge Servers* available on the support site.
- **Recommended Action** lists potential resolutions to the error including UI, RACADM, or WS-Man commands. Where necessary, see documents on the support site for more information.
- **Detailed Description** includes more information about the issue for quick resolution.

You can view more information about an alert by using filters such as message ID, message text, category, and subcategory.

To view alert definitions:

1. Click **Alerts > Alert Definitions**. A list of all the standard alert messages is displayed.
2. To quickly search for an error message, click **Advanced Filters**.

The right pane displays the message information of the message ID that was selected in the table.

Managing MIB files

OpenManage Enterprise enables you to manage MIBs that are not preinstalled by default.

Before you begin: You must be a Super Administrator, Administrator, or Custom Role user with trap management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Third-party tools in your data center may generate alerts that are vital for your operations. Such alerts are stored in the Management Information Base (MIB) files defined and understood by respective vendor tools. However, OpenManage Enterprise allows managing these MIBs, enabling the import, parsing, and utilization of non-Dell MIBs for device management. OpenManage Enterprise supports SMI1 and SMI2. OpenManage Enterprise provides integrated MIB files that can be used for Dell devices. These files are read-only and cannot be edited.

 **NOTE:** OpenManage Enterprise only handles valid MIBs with traps.

You manage MIBs by:

- [Import MIB files](#)
- [Remove MIB files](#)
- [Resolve MIB types](#)

Manage the MIB files by clicking **Monitor > MIB**. A table lists the available MIB files with the following properties. Click the column heading to sort data.

Table 47. Role-based access for MIB files

OpenManage Enterprise features	Role-based access control for MIB files		
	Administrator or Custom role user	Device Manager	Viewer
View traps or MIBs	Y	Y	Y
Import MIB/Edit traps	Y	N	N
Remove MIB	Y	N	N
Edit traps	Y	N	N

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

Topics:

- [Import MIB files](#)
- [Edit MIB traps](#)
- [Remove MIB files](#)
- [Resolve MIB types](#)
- [Download an OpenManage Enterprise MIB](#)

Import MIB files

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

Prerequisites

- 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](#)

- Import only one MIB file at a time.

Steps

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

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

Results

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

Edit MIB traps

Edit the properties of a MIB trap.

Steps

1. Select the report and click **Edit**.
2. In the **Edit MIB Traps** dialog box:
 - a. Select or type data in the fields:
 - Select the new alert category to be assigned to the alert. By default, OpenManage Enterprise displays a few system-defined alert categories.
 - Type the alert component.
 - Since third party tools generate trap names, the trap name is read-only.
 - Select the severity to be assigned to the alert. By default, OpenManage Enterprise displays a few system-defined alert severities.
 - A message that describes the alert.
 - b. Click **Finish**.
The trap is edited, and the updated trap list is displayed.

 **NOTE:** You cannot edit more than one alert at a time. The traps imported to OpenManage Enterprise cannot be edited.
3. In the **Report Definition** dialog box, edit the settings. See [Creating reports](#).
4. Click **Save**.

Results

The updated information is saved.

Remove MIB files

Remove MIB files that are not associated with any alert policies.

Prerequisites

Ensure the MIB you want to remove does not contain trap definitions used in your alert policies. See [Alert policies](#)

Steps

1. In the **MIB FILENAME** column, expand the folder, and select the MIB files.
2. Click **Remove MIB**.
3. In the **Remove MIB** dialog box, select the check boxes of the MIBs to be removed.
4. Click **Remove**.

Events that are received before removing a MIB will not be affected by the associated MIB removal. However, events generated after the removal will have unformatted traps.

Results

The MIB files are removed and the MIB table is updated.

Resolve MIB types

When importing MIB files, resolve if there are any unresolved MIB types.

Steps

1. Import the MIB files. See [Import MIB files](#).
If the MIB type is unresolved, the **Unresolved Types** dialog box lists MIB type(s) indicating that the MIB type(s) will be imported only if resolved.
2. Click **Resolve Types**.
3. In the **Resolve Types** dialog box, click **Select Files**, and then select the missing file(s).
4. In the **Import MIB** dialog box, click **Next**. If there are still missing MIB types, the **Unresolved Types** dialog box again lists the missing MIB types. Repeat steps 1-3.
5. After all the unresolved MIB types are resolved, click **Finish**. Complete the importing process. See [Import MIB files](#).

Download an OpenManage Enterprise MIB

Download OpenManage Enterprise MIBs to set up traps on the appliance. You can download only the OpenManage Enterprise-related MIB files.

Steps

1. On the **Monitor** screen, click **MIB**.
2. Expand and select an OpenManage Enterprise MIB file, and then click **Download MIB**.

Configuring profiles

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

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

The following details of the listed profiles are displayed:

Table 48. Profile settings

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

Advanced Filters can be used to customize the profile list.

When a profile is selected the profile **Description**, **Last deployed time**, **Last modified time**, **Created on**, and **Created by** fields are displayed on the right side. Click **View Identities** to view the NIC configuration and virtual identities that are tagged to the profile.

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

NOTE:

- If target iDRACs are running firmware version 4.40.10.00 and above, the appliance uses Redfish for profile related tasks. If Redfish fails, the task is re-tried using WSMAN. For iDRACs running versions earlier than 4.40.10.00, the appliance uses WSMAN for template related tasks.
- Create and Delete operations are not listed as part of the table.

Table 49. Profile states and permissions

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

- Create profiles and pre-reserve virtual identities. See, [Create profiles](#)
- View profile details. See, [View a profiles details](#)
- Edit profile attributes and settings. See, [Edit a profile](#)
- Assign a profile to a device or service tag (through auto-deploy). See, [Assign a profile](#)
- Unassign a profile from a device or service tag. See, [Unassign profiles](#)
- Redeploy profile changes to the associated target device. See, [Redeploy profiles](#)
- Migrate profile from one target (device or service tag) to another.
- Delete profiles. See, [Delete profiles](#)

Topics:

- [Create profiles](#)
- [View a profiles details](#)
- [View a profiles network](#)
- [Edit a profile](#)
- [Assign a profile](#)
- [Unassign profiles](#)
- [Redeploy profiles](#)
- [Migrate a profile](#)
- [Delete profiles](#)

Create profiles

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

Prerequisites

Administrator, Device Manager, or custom role user with required privileges are allowed to perform the Profile Management tasks. See [Role and scope-based access](#).

Steps

1. Go to the **Profiles** screen by clicking **Configuration > Profiles**.
2. Click **Create** to activate the **Create Profiles** wizard.
3. In the Template section, select the **Template Type** as either Server or Chassis and then select a deployment template in the **Select Template** drop-down list. Click **Next**.
4. In the **Details** screen, modify the **Name Prefix** and provide a description in the **Description** box if needed. In the **Profile Count** box, enter the number of profiles. Click **Next**.



NOTE: The only special characters that are allowed in the profile name are alphanumeric, dash, underscore, and space.
5. If the target device is a server, follow these steps:
 - a. To install an operating system remotely, enable **Boot to Network ISO**.
 - b. Select **Share Type**.
Choose either **CIFS** or **NFS**.

Table 50. Details for share type

Share Type	Field
CIFS	Under ISO Information , enter the following details. • ISO Path: sharename\path\filename.iso Under Share information , enter the following details. • Share IP Address: The IP address of the share. • Workgroup (optional) : The domain name if your network uses a domain. • Password: The user's password.

Table 50. Details for share type (continued)

Share Type	Field
NFS	Under ISO Information, enter the following details. • ISO Path: NFSsharefoldername/path/ filename.iso Under Share information, enter the following details. • Share IP Address: The IP address of the share. • Password: The user's password.

c. Set **Time to Attach ISO**.

Enter the duration in minutes in the Time to Attach ISO field (default is 240 minutes).

d. Proceed or cancel.

Click **Next** to proceed.

Click **Cancel** to abort the configuration.

6. Click **Finish**.

Results

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

View a profiles details

Use the **Configurations > Profiles** screen to view the details of an existing profile without editing.

Steps

1. Select a profile from the list of profiles on the **Configurations > Profiles** screen.
2. Click **View** to activate the **View Profile** wizard.
3. On the **Details** screen of the wizard, source template, name, description, and target information are displayed.
4. Click **Next**.

Results

On the **Boot to Network ISO** screen. The ISO image file path, the share location of the ISO image file, and the time to attach ISO are displayed if the profile was initially set with that preference.

View a profiles network

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

Steps

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

Results

The **View Network** wizard is viewed and closed.

Edit a profile

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

Prerequisites

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](#)

About this task

To rename, edit network, or edit the attributes of an existing profile, select the profile on the **Profiles** screen and click **Edit**.

Steps

1. Select **Rename** and in the **Rename Profile** wizard edit the profile name in the **Name** box. Click **Finish** to save the changes.
- 

NOTE: The only special characters that are allowed in the profile **Name** are alphanumeric, dash, underscore and space.
2. Select **Edit Profile** to activate the **Edit Profile** wizard and edit the following:
- a. On the **Details** screen, you can edit the **Name** and **Description**. Click **Next**.

b. On the **Boot to Network ISO** screen, select the **Boot to Network ISO** check box to specify the full ISO path and the share location and do the following:

• Select **Share Type** as either **CIFS** or **NFS**.

Table 51. Details for share type

Share Type	Field
CIFS	Under ISO Information, enter the following details. ◦ ISO Path: sharename\path\filename.iso Under Share information, enter the following details. ◦ Share IP Address: The IP address of the share. ◦ Workgroup (optional) : The domain name if your network uses a domain. ◦ Password: The user's password.
NFS	Under ISO Information, enter the following details. ◦ ISO Path: NFSsharefoldername/path/ filename.iso Under Share information, enter the following details. ◦ Share IP Address: The IP address of the share. ◦ Password: The user's password.

- Set **Time to Attach ISO**. Enter the duration in minutes in the Time to Attach ISO field (default is 240 minutes).

• Click **Next** to proceed or Click **Cancel** to abort the configuration.
- c. On the **iDRAC Management IP** screen, select from one of the following :
- Don't change IP settings.

• Set as DHCP

• Set static IP and provide the relevant Management IP, Subnet Mask, and Gateway details.
- d. On the **Target Attributes** screen, you can select and edit the BIOS, System, NIC, iDRAC, and virtual identity attributes of the profile.
- e. Click **Finish** to save the changes.

Results

Existing profiles are edited.

Assign a profile

An unassigned profile can be either deployed on an existing server or can be reserved for auto deployment on an undiscovered server.

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](#).
- The existing attributes, if any, of the target server would be overwritten when a profile is deployed on it.
- Only the devices that are not associated with any profiles are available for deployment or auto deployment.
- Ensure that only alphanumeric, dash, underscore, and space are used as special characters in the **Name**. To edit the profile name see [Edit a profile](#).
- To deploy a profile with custom telemetry configuration, ensure that the server has a valid iDRAC DataCenter license and the iDRAC firmware is 4.40 and above.

Steps

1. To **Deploy a profile**:
 - a. Select an unassigned profile on the **Configuration > Profiles** screen. Then click **Assign > Deploy** to activate the **Deploy Profile** wizard.
 - b. The **Details** screen displays the source template, profile name, and description. Click **Next**.
 - c. On the **Target** screen:
 - Click **Select** and from the list of devices, select a target device. Devices that are already assigned a profile are not selectable in the target list.
 - If a reboot is required after the deployment, select the **Do not forcefully reboot the host operating system if the graceful reboot fails** check box.
 - Click **Next**.
 - d. (Optional) On the **Boot to Network ISO** screen:
 - i. Select the **Boot to Network ISO** check box.
 - ii. Provide the relevant ISO path, share location details, and the Time to Attach ISO value.
 - iii. Click **Next**.
 - e. On the **iDRAC Management IP** screen, select from one of the following options and provide further relevant details.
 - Do not change IP settings.
 - Enable DHCP.
 - Set a static IP.
 - f. On the **Target Attributes** screen, the attributes are displayed under the BIOS, System, NIC, and iDRAC sections. You can select, clear, or edit the attributes before deployment.
 - g. On the **Virtual Identities** screen, click **Reserve identities**. The assigned virtual identities of the NIC cards of the selected target device are displayed. To view all the assigned identities of the identity pool of the selected target device, click **View all NIC details**.
 - h. On the **Schedule** screen, choose:
 - **Run Now** immediately deploys the profile.
 - **Enable Schedule** allows you to set an appropriate Date and Time for the profile deployment.
 - i. Click **Finish**.
 - If identities are already assigned outside of the appliance, then a new deployment does not use those identities unless they are cleared. For more information, see [Identity pools](#).
 - Profiles that change network settings (such as changing the device from the IPV4 to the IPV6 network) can cause the target device to be unreachable. In such a situation, the SCP job appears to fail and the device goes to the **Unknown** state.
 - If the template deployed with custom telemetry settings, does not have a valid iDRAC DataCenter license, the job, and the **CustomComponentets** attributes fail in the **Job details**. You get an error message stating that A required license is missing or expired.
2. To **Autodeploy a profile**:

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

- a. Select an unassigned profile on the **Configuration > Profiles** screen, click **Assign > Auto Deploy** to activate the **Auto Deploy** wizard.
- b. The **Details** screen displays the Source Template, Name, and Description (if any) of the profile. Click **Next**.
- c. On the **Target** screen, specify the service tag or node ID of the undiscovered device in the **Identifier** box. Click **Next**.
- d. (Optional) On the **Boot to Network ISO** screen, select the **Boot to Network ISO** check box to specify the full ISO path and the share location:
 - Select **Share Type** as either **CIFS** or **NFS**.

Table 52. Details for share type

Share Type	Field
CIFS	Under ISO Information, enter the following details. ◦ ISO Path: sharename\path\filename.iso Under Share information, enter the following details. ◦ Share IP Address: The IP address of the share. ◦ Workgroup (optional) : The domain name if your network uses a domain. ◦ Password: The user's password.
NFS	Under ISO Information, enter the following details. ◦ ISO Path: NFSsharefoldername/path/filename.iso Under Share information, enter the following details. ◦ Share IP Address: The IP address of the share. ◦ Password: The user's password.

- Set **Time to Attach ISO**. Enter the duration in minutes in the Time to Attach ISO field (default is 240 minutes).
- e. Click **Finish**.

Results

For profiles with custom telemetry configuration, ensure that the device has a valid iDRAC DataCenter license. Otherwise, the job fails, and the task execution history shows the following:

```
#Attributes Failed to apply
CustomComponents - required license is missin or expired.
```

Unassign profiles

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

Steps

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

Results

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

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

Redeploy profiles

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

Prerequisites

If the attributes were not initially deployed using the **Propagate VLAN settings immediately** in the template deployment, VLAN attribute changes on target MX7000 sleds fail during profile redeployment.

Steps

1. On the **Configuration > Profiles** screen, select the profiles that are **Deployed** or **Modified** () and click **Redeploy** . The **Redeploy** wizard opens.
2. On the **Attribute Deploy Options** dialog, choose one of the following deploy options and click **Next**:
 - **Modified attributes only**: To redeploy only the modified attributes on the target device.

 **NOTE:** When you redeploy a profile on a server using the **Modified attributes only** option by changing the ISO file share type (for example, from CIFS to NFS or from NFS to CIFS), the server will not boot from the network ISO file.
 - **All Attributes**: To redeploy all the attributes, along with any modified attributes, on the target device.
3. On the **Schedule** dialog, choose from one of the following options:
 - **Run Now** to implement the changes immediately.
 - **Enable Schedule** and select a date and time to schedule the redeployment.
4. Click **Finish** to proceed.

Results

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

Migrate a profile

A deployed or autodeployed profile can be migrated from an existing target device or service tag to an identical target device or service tag.

Prerequisites

- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See [Role and scope-based access](#).
- To migrate a profile with custom telemetry configuration, ensure that it has a valid iDRAC DataCenter license and the iDRAC firmware is 4.40 and above.

About this task

When a migration is successful, the profile target assignment reflects the new target. If the migration is from a target device to an undiscovered service tag, then the state of the profile is changed to **Assigned**.

- Migrating a profile moves settings that the profile defined (including deployed virtual identities) from the source to the target.
- You can force the migration of a profile even if the source device cannot be contacted. In this case, the user must ensure that there are no virtual identity conflicts.
- True target-specific attributes are not reclaimed from the 'source' server as part of migration. Therefore, the same inventory details can be present on two servers post migration.

Steps

1. On the **Configuration > Profiles** screen, select a profile and click **Migrate** to activate the **Migrate Profile** wizard.
2. On the **Selection** dialog:

- a. From the **Select source profile** drop-down, select the profile that you want to migrate.
- b. Click **Select Target** and from the **Job target** dialog box, select a target device and click **Ok**.
- c. If needed, select the **Force the migration even if the source device cannot be contacted** check box.

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

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

Results

- A job is created to migrate the settings of a profile to the new target device. You can view the status of the job on the **Monitor > Jobs** screen.
- For profiles with custom telemetry configuration, ensure that the device has a valid iDRAC DataCenter license. Otherwise, the job fails, and the task execution history shows the following:

```
#Attributes Failed to apply
CustomComponents - required license is missin or expired.
```

Delete profiles

The existing unassigned profiles can be deleted from the **Configuration > Profiles** screen:

About this task

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

Steps

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

Results

The existing unassigned profiles are deleted.

Configuration compliance

Create and manage configuration compliance baselines using deployment templates, templates that are created from a device, or imported templates from a file.

Overview

By selecting **Configuration > Configuration Compliance**, you can create and manage compliance baselines using deployment templates, device-created templates, or imported templates to ensure device settings align with approved configurations. The compliance baseline table displays the compliance status for each baseline, including compliant, not compliant, and compliance incomplete, and a doughnut chart summarizes overall compliance. Users can monitor and correct discrepancies by creating a compliance template, baseline, and remediating noncompliant devices

Prerequisites

- To perform this task, you must have one of the following roles: Super Administrator, Administrator, Device Manager, or a Custom Role. Device Manager and Custom Role users must also have scope-based operational access to the devices. In addition, Custom Role users must have the Template Management privilege, which allows them to create and manage templates and configuration baselines.
- For servers, you must have the Enterprise-level license for OpenManage Enterprise and iDRAC.
- For Chassis Management Controller (CMC), no license is required to use this feature.

View configuration compliance baseline

After creating a configuration baseline using a compliance template, a table displays the compliance status for each baseline, and a doughnut chart summarizes the overall compliance across all baselines. The baseline status is determined by a rollup mechanism, where the lowest compliance level of any associated device (such as Critical) is applied to the entire baseline.

The configuration baseline table includes the following fields for each baseline:

- **Compliance:** Displays the rollup compliance level of devices attached to the configuration compliance baseline. The overall status of the baseline is determined by the device with the highest severity or least compliance, such as Critical. The status includes:
 - **Compliant:** All device attributes match the compliance template, indicating full compliance with the baseline.
 - Not compliant: One or more device attributes do not match the compliance template.
-  **NOTE:** A baseline may remain permanently noncompliant if configuration attribute values differ across devices. For example, Boot Control attributes such as iSCSI Target IQN and LUN ID may vary by device, resulting in lasting noncompliance.
- Compliance Incomplete: Device inventory is missing, or the compliance check is not complete.
 - **Name:** Displays the user-defined name of the configuration baseline.
 - **Template:** Lists the compliance template used by the baseline.
 - **Baseline Last Edited:** Indicates the most recent date and time the baseline was run.

Workflow summary

The workflow for configuration compliance involves a series of steps, from defining your desired configuration state to monitoring and correcting any discrepancies. Here is a summary of the configuration compliance workflow:

1. [Create a compliance template](#) : You can create a template from an existing deployment template, a reference device, or an imported configuration file.
2. [Create a configuration compliance baseline](#): After preparing your compliance templates, create configuration compliance baselines. A baseline is a list of devices or device groups associated with a specific compliance template. You can associate a device with up to 10 baselines.
 - When creating a baseline, selecting a template automatically includes its linked attributes, which can be edited later.
3. [Monitor and check compliance](#): After creating a configuration baseline, OpenManage Enterprise provides a compliance summary for each baseline in a table on the **Configuration > Configuration Compliance** screen. An overall compliance summary of all baselines is also displayed on a doughnut chart. To view detailed reports for a specific baseline, select it and click **View Report** in the right pane. You can also use the query builder feature to generate device level compliance with the selected baseline. See [Select a query criteria](#).
4. [Remediate noncompliant devices](#) : From the **Compliance Report** screen of a baseline, select noncompliant devices and click **Make Compliant** to initiate remediation.
5. Manage baselines and templates: From the **Configuration Compliance** screen, you can perform various management actions, including:
 - [Editing a configuration compliance baseline](#).
 - [Deleting configuration compliance baselines](#).
 - [Exporting baseline compliance reports](#).
 - [Managing compliance templates](#), which includes creating, cloning, editing, exporting, and deleting them.

Run predefined report

OpenManage Enterprise provides a system-defined report to view the list of monitored devices and their compliance with the configuration compliance baseline. Select **Monitor > Reports > Devices per Template Compliance Baseline**, and then click **Run**. See [Run reports](#).

Topics:

- [Manage compliance templates](#)
- [Create a configuration compliance baseline](#)
- [Edit a configuration compliance baseline](#)
- [Delete configuration compliance baselines](#)
- [Refresh compliance of the configuration compliance baselines](#)
- [Remediate noncompliant devices](#)
- [Remove a configuration compliance baseline](#)

Manage compliance templates

You can create, edit, clone, and manage compliance templates in OpenManage Enterprise to enforce configuration compliance across devices. A compliance template defines the desired configuration state for devices and is used to generate compliance baselines.

Use a compliance template to create compliance baselines and then periodically check device compliance against those baselines. See [Configuration compliance](#).

Ways to create compliance templates

You can create compliance templates using the following methods:

- Using a deployment template. See [Create a compliance template from deployment template](#).
- Using a reference device. See [Create a compliance template from reference device](#).
- Importing from a template file. See [Create a compliance template by importing from a file](#).

i NOTE: Custom telemetry attributes are only available for template deployment. They are not supported for configuration compliance. If you use a deployment template to create a compliance template, custom telemetry attributes and telemetry report definitions are ignored during compliance checks.

Prerequisites

You must have one of the following roles to manage compliance templates: Super Administrator, Administrator, Device Manager, or Custom Role with template management privileges. As a custom role or device manager, you must have scope-based operational access to the devices you manage. See [Role and scope-based access](#).

Best practices

- To ensure successful template deployment, use identical hardware and configuration for source and target devices. Otherwise, attributes not available on the target may cause a compliance deployment failure.
- Be aware that compliance templates are static and do not automatically update when new hardware or firmware introduces new attributes. To include new attributes, create a new compliance template and associate it with a new baseline.

View and manage templates

To manage compliance templates: Go to **Configuration > Configuration Compliance > Template Management**. View the list of templates based on your role and access scope. Administrators can view and manage all templates. Device Managers can view and manage only the templates they created.

You can perform the following actions:

- Create a compliance template from a deployment template, from a reference device, or by importing a file. See [Create a compliance template from deployment template](#).
- [Clone an existing template](#) to create a new one with similar attributes.
- [Edit a template](#) to update configuration parameters.
- Export a template for backup. On the **Compliance Templates** screen, select the corresponding checkbox, and then click **Export**.
- Delete templates that are no longer required. On the **Compliance Templates** screen, select the corresponding checkbox, and then click **Delete**.

Scalability guidelines

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

- Disable the default configuration inventory task that is triggered automatically and run it manually when needed.
 - Create compliance baselines with a lesser number of devices. For example, split 6,000 devices into four baselines with 1,500 devices each.
 - Stagger compliance checks across baselines instead of checking all baselines simultaneously.
-  **NOTE:** When editing a compliance template, configuration compliance is automatically triggered for all associated baselines. However, frequent template edits in a scale environment are not supported. For optimal performance, it is recommended to associate a maximum of 100 devices per baseline. This ensures efficient operation and minimizes potential issues.

Related information

[Configuration compliance](#)

Create a compliance template from deployment template

Create a baseline compliance template by using an existing deployment template.

Steps

1. Click **Configuration > Configuration Compliance > Template Management > Create > From Deploy Template**.
2. In the **Clone Deployment Template** dialog box, from the **Template** drop-down menu, select a deployment template that must be used as the reference for the new template.
3. Enter a name and description for the compliance template.

 **NOTE:** The only special characters that are allowed in the deployment template name are alphanumeric, dash, underscore and space.

4. Click **Finish**.

Results

A compliance template is created and listed in the list of compliance templates.

Create a compliance template from reference device

Create a baseline compliance template by using an existing reference device.

Prerequisites

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

Steps

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

Results

The newly-created compliance template is listed on the **Compliance Templates** screen.

Create a compliance template by importing from a file

Create a baseline compliance template by importing from an existing compliance template.

Steps

1. Click **Configuration > Configuration Compliance > Template Management > Create > Import from File**.
2. In the **Import Compliance Template** dialog box, enter a name for the compliance template.
 **NOTE:** The only special characters that are allowed in the **Template Name** are alphanumeric, dash, underscore, and space.
3. Select either the server or chassis template type, and then click **Select a file** to browse through to the file and select.
4. Click **Finish**.

Results

The compliance template is created and listed.

Clone a compliance template

Use an existing baseline compliance template to create a compliance template.

Steps

1. Click **Configuration > Configuration Compliance > Template Management**.
2. Select the compliance template to be cloned, and then click **Clone**.
3. In the **Clone Template** dialog box, enter the name of new compliance template.
4. Click **Finish**.

Results

The new compliance template is created and listed under **Compliance Templates**.

Edit a compliance template

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

Prerequisites

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

Steps

1. On the **Compliance Templates** screen, select the corresponding check box, and then click **Edit**.
2. On the **Template Details** screen, the configuration attributes of the compliance template are listed.
3. Expand the attribute that you want to edit, and then enter or select data in the fields. To enable the attribute, select the checkbox.

 **NOTE:** Attributes that are preceded by  are not editable and are not considered for compliance.

4. Click **Save** or **Discard** to implement or to reject the changes.

Results

The compliance template is edited, and the updated information is saved.

Create a configuration compliance baseline

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

Prerequisites

Ensure that you have created the appropriate compliance template.

About this task

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

The list of compliance baselines available to you depends on your role and scope-based access privileges in OpenManage Enterprise. For example, an administrator can oversee and manage all compliance baselines, while a device manager can only handle baselines that they have created and own. Also, the devices/device groups in the scope of the device manager decide the target devices available to the device manager.

You can create a configuration compliance baseline by:

- Using an existing deployment template. See [Configuration compliance](#).
- Using a template captured from a support device. See [Create a compliance template from reference device](#).
- Using a template imported from a file. See [Create a compliance template by importing from a file](#).

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

 **CAUTION:** Editing properties of a compliance template that is already associated with another baseline alters the baseline compliance levels of devices that are linked to it. Read through the Error and Event message that is displayed and act accordingly. For more information about error and event messages, see the *Error and Event Message Reference Guide* available on the support site.

Steps

1. Select **Configuration > Configuration Compliance > Create Compliance Baseline**
2. In the **Baseline Information** Section:
 - a. From the **Template** drop-down menu, select a compliance template. For more information about templates, see: [Configuration Compliance](#).
 - b. Enter a compliance baseline name and description.
 - c. Click **Next**.
3. In the **Target** section:
 - a. Select devices or device groups. Only compatible devices are displayed. See: [Select target devices and device groups](#).
 **NOTE:** Only compatible devices are listed. Selecting a group exclusively identifies devices incompatible with the compliance template or lacking support for the configuration compliance baseline feature.
4. (Optional) In the **Schedule and Options** section:
 - a. Check the **Schedule** box and specify when the notification would be triggered by selecting either **Notify any time the baseline becomes non-compliant** or **Notify on Schedule**.
 - b. To schedule the notification later and time, select **Run Later** and select the **Date and Time**. Alternatively, to trigger the notification on a weekly or daily basis, select **Run On Schedule**. Select **Daily** or **Weekly** from the drop-down list and specify a time in the 12-hour format.
 - c. From the **Format** menu select one of the following formats for the Configuration Compliance report: HTML, CSV, PDF, XLS.
 - d. In the **Email Recipient** box, enter the email address that must receive the notification. If email is not configured, you must configure the email (SMTP) address. For more information, see: [Configure SMTP, SNMP, and Syslog](#)
5. Click **Finish**

Results

Whenever a configuration baseline is created, the appliance creates a configuration inventory job. This job collects an inventory of the devices that are associated with the baseline for which the inventory data is unavailable. This newly created Configuration inventory job has the same name as the baseline for which the inventory is collected. Also, on the **Configuration Compliance** screen, a progress bar indicating the progress of Inventory job appears alongside the respective baseline.

Related information

[Configuration compliance](#)

Edit a configuration compliance baseline

Edit the devices, name, and other properties associated with a configuration baseline.

About this task

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

Steps

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

Results

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

Delete configuration compliance baselines

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

Prerequisites

To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See [Role and scope-based access](#)

About this task

To delete the configuration compliance baselines:

Steps

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

Results

The deleted configuration baselines are removed from the **Configuration Compliance** screen.

Refresh compliance of the configuration compliance baselines

Configuration compliance is used to indicate the overall compliance status of the configuration baseline. The roll-up status can show critical or non-compliant even if a single device is non-compliant and all other associated devices have a compliant status.

About this task

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

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

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

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

NOTE:

- When the configuration compliance is in 'Running' status, initiating new jobs that impact baselines, such as editing of a compliance template or baseline, is not allowed.
- Clicking on the **Refresh Compliance Summary** only refreshes the overall compliance chart and not every individual baseline. To update individual baselines, trigger an edit baseline job:
 1. Select the baseline.
 2. Click on **Edit**.
 3. On the dialog box, click on **Finish**.

Steps

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

Results

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

Remediate noncompliant devices

On the **Compliance Report** screen of a baseline, devices that do not comply with the baseline can be remediated by updating their attributes.

About this task

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

- **COMPLIANCE** is the status of the device with least compliance (for example, critical) is indicated as the status of the device.
- **DEVICE NAME** is the Name of the target device that is associated with the baseline.
- **IP ADDRESS** is the IP address of the target device.
- **TYPE** is the type of the target device associated.
- **MODEL** is the model name of the target device.
- **SERVICE TAG** is the service tag of the target device.
- **LAST SUCCESSFUL INVENTORY TIME** is the most recent date and time that a successful inventory job was run. To initiate a new default inventory job, click **Monitor > Jobs** and run the **Default Inventory Task**.

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

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

Steps

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

NOTE:

- All attributes that are part of the template are applied on the target device irrespective of the compliance status. A reboot may be required to apply the changes.
- If the deployed template is created from a reference device, verify whether the template contains user password information. If the template contains user password information, the appliance reverts to the discovery credentials for device communication. This change can be verified post deployment by checking the **Credential Type** of the target device (It displays **Discovery**). If using the service account for communication is preferred or the device is using password rotation, trigger the onboarding task for this device. This task either updates the password on the existing service account in iDRAC or, if user slots are available, generates a new service account.

4. Schedule the configuration changes to run immediately or later, and then click **Finish**.

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

Results

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

Related information

[Configuration compliance](#)

Export a compliance baseline report

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

Steps

1. Click **Configuration > Configuration Compliance > View Report**.
The **Compliance Report** screen is displayed.
2. Select the devices whose compliance is to be saved in the report:
 - Click **Export All** to export details of all the devices in the compliance baseline.
 - Click **Export Selected** after selecting the individual devices from the report.

Results

The compliance baseline report is exported.

Related information

[Configuration compliance](#)

Remove a configuration compliance baseline

Compliance data and configuration inventory of target devices can be deleted from the appliance.

About this task

You can remove the configuration compliance level of devices associated with a configuration baseline. For field descriptions displayed in the list, see [Configuration compliance](#).

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

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

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

Steps

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

Results

The compliance baseline is deleted and the **Overall Compliance Summary** table of baselines is updated.

Managing licenses

View unbound licenses and bind entitlements with devices to generate licenses using the **Configuration > Entitlements** screen. View, import, export, and deploy licenses using the **Configuration > Licenses** screen.

You can manage the following types of licenses on the **Licenses** page:

- iDRAC licenses on all PowerEdge servers that are equipped with an iDRAC9 and iDRAC10 Dell Remote Access controller.
- iDRAC Secure Enterprise Key Manager (SEKM).
- OpenManage Enterprise Advanced licenses.
- OpenManage Enterprise Advanced+ licenses for 14G and later PowerEdge servers.
- Management Module Advanced License.

For a complete list of all supported licenses, see the *OpenManage Portfolio Software Licensing Guide*.

View licenses

The **License** tab displays the following attributes of imported licenses:

- The **Status** field indicates whether the license is deployed or deployable.
 - A green icon indicates that the license is deployed on the target device.
 - A blue icon indicates that the license is deployable but yet to be deployed on the target device.
 - A yellow icon indicates that the license is not deployable. Highlight the license or hover over the yellow icon to view the **Rejection Reason**.
- The **Deployable** field indicates whether the license can be deployed on any target devices.
- The **Description** field is the type of license.
- The **Term** field denotes the validity duration and scope of the license. Possible values are **Perpetual**, **Leased**, **Evaluation**, and **Site**.
- The **Bound Service Tag** field lists the service tag of the device to which the license is bound. You can only deploy the license on this device.
- The **Entitlement ID** field is a unique license identifier.
- The **Matching Device** field indicates whether the appliance has discovered the device that is associated with the license.
- The **Deployed** field indicates whether the license is deployed to any server.
- The **Date Purchased** field lists the timestamp at which the license was purchased.
- The **Date Imported** field lists the timestamp at which the license was onboarded to the appliance.

Highlight any of the licenses listed to get further information about the license.

View license report

Use the **Monitor > Reports** page to generate the system-defined **License Report**. To create and manage reports, see [Monitoring reports](#). This report lists the following attributes:

- **Device Name**: The name of the device to which the license is assigned.
- **Device Type**: The type of the device (Server or Chassis) to which the license is assigned.
- **Device Model**: The model of the device.
- **Device Identifier**: The unique identifier of the device.
- **License Description**: A description of the license.
- **License Status**: The current status of the evaluation license is OK, Warning, or Available. OK indicates that the license is installed and not expired. Warning indicates that the license is installed and expired or nearing expiration. Available indicates that the license is bound but not installed.
- **License Type**: The type of license.
- **License Expiration Date**: The date on which the license will expire.

View entitlements

The **Entitlement** tab, when connected to Dell online, displays the following attributes of unbound licenses:

- The **License Name** indicates the license name.
- The **Type** indicates type of licenses.
- The **License Description** indicates the description of the type of license.
- The **Term** indicates the duration of the validity of the license. Perpetual licenses have no expiration date.
- The **Count** indicates the number of unbound entitlements available for binding.

Topics:

- [Obtain licenses by connecting to Dell Digital Locker account](#)
- [Import licenses](#)
- [Bind licenses](#)
- [Deploy licenses](#)
- [Export licenses](#)
- [Disconnect from Dell online](#)
- [Delete licenses from OpenManage Enterprise](#)

Obtain licenses by connecting to Dell Digital Locker account

Connect OpenManage Enterprise to Dell Digital Locker to view unbound licenses and bind entitlements with devices to generate licenses. To connect to Dell Digital Locker, launch the URL from the Connect to Dell Online window and enter the authentication code. You can disconnect from the Dell Digital Locker at any time.

Prerequisites

- Ensure that the appliance has Internet access to reach Dell Digital Locker.
- You must have an active Dell account.
- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with license management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

Steps

1. In OpenManage Enterprise, go to **Configuration > Entitlements > Connect to Dell Online**.
2. In the **Connect to Dell Digital Locker** window, an activation code is displayed for authentication with Dell Digital Locker. Click the verification link to access the Dell Digital Locker in a new browser tab. You can also copy the link and open it in a new browser tab.
3. On the **Dell Digital Locker** login page, enter the credentials, and then click **Sign In**.
4. The activation code is autopopulated from OpenManage Enterprise. Verify that the code matches with the one shown in the OpenManage Enterprise, and then click **Activate Device**.

 **NOTE:** The activation code is valid for 5 minutes. If the code is not used within 5 minutes, obtain a new code by clicking Connect to Dell Online again.

5. After successful authentication, a grid displays a summary of all unbound entitlements from Dell Digital Locker. The grid includes the following columns:

 **NOTE:** If no supported or unbound entitlements are found, this screen will be blank.

LICENSE NAME	License name.
TYPE	The type of license.
LICENSE DESCRIPTION	Description of the type of license; Enterprise License, bound, unbound, or upgraded.
TERM	The license term. Perpetual licenses have no expiration date.
COUNT	The count of unbound entitlements is available for binding.

Results

- The summary of the downloaded entitlements can be viewed in the **Entitlements** section. To bind licenses to the discovered and inventoried devices, see [Binding licenses](#).
- The connection, once established, remains active for 24 hours. After that, the connection is terminated.
- While the connection is active, logging out of OpenManage Enterprise does not end the connection with Dell Digital Locker. The connection remains active for administrators or device managers to access the available unbound entitlements from the **Entitlements** page and perform the license binding. For disconnecting, see [Disconnect from Dell online](#).
- The email address associated with the Dell Digital Locker account, used for connection, is displayed above the entitlements grid.

Next steps

If the appliance cannot connect to Dell Digital Locker due to an invalid code or incorrect proxy settings, click **Close** to exit the connection attempt. Retry the connection by going to **Connect to Dell Online** or verifying the proxy settings on the appliance under **Application Settings > Network**.

Import licenses

To import licenses, you must first download them. You can import archived licenses with perpetual term, but expired and evaluation licenses cannot be imported.

Prerequisites

Before importing a license, ensure that it meets the following prerequisites:

- The license is a valid license with Perpetual term. Licenses with evaluation terms are rejected.
- The license has a bound service tag.
- The license has a proper signature and entitlement ID.
- You must have an Administrator role, Device Manager role, or a custom user role with the License Management privilege. For more information about privileges, see [Role and scope-based access](#).

Steps

1. Click **Configuration > Licenses**, and then click **Import**.
2. Click **Import Licenses** to upload the license files from your local file system. You can import around 1,000 licenses at a time.

 **NOTE:** Only XML, ZIP, and TAR formats are accepted.

3. An import license task job is created where you can track the job progress.

Results

Once the job completes, the license is imported if it meets all the prerequisites. You can find the imported licenses on the **License** page and on the bound device's **Licensing** tab. If a license does not meet any prerequisites, it is rejected, and you can find the reason from the import license task from the **Jobs** page. If a license is bound to a discovered server, it is eligible for deployment.

Bind licenses

Bind all the unbound licenses (entitlements) to the inventoried systems by using the OpenManage Enterprise to generate deployable licenses.

Prerequisites

- Discover and inventory the licensable systems.
- Ensure that the appliance is connected to Dell Online and entitlements are available in your Dell Digital Locker account. See [Obtain licenses by connecting to Dell Digital Locker account](#).
- You must have an Administrator role, Device Manager role with scope to the device, or a custom user role with the License Management privilege and scope to the device is available. For more information about privileges, see [Role and scope-based access](#).

Steps

1. On the appliance, click **Configuration > Entitlements**.
2. Select the license to be bound and click **Bind**. Only perpetual licenses are available for binding operation. The license binding wizard is displayed.
3. Click **Select Devices** to see the devices eligible for license deployment. Select the devices and click **OK**.
Selecting all devices across pages is not supported. However, you can select all devices within each page by clicking **This page**. The total number of devices you can select is limited by the available license count for the selected licenses.
4. From the **Bind Options**, select one of the following and click **Finish**:

Option	Description
Bind	Bind the entitlements to device service tags to generate deployable licenses. A Bind Entitlements Task is created on the Jobs page. Once the job is complete, the newly bound licenses are available on the License page for deployment.
Bind and Deploy	Bind the licenses to target device service tags and then deploy the licenses on the target devices. A Bind Entitlements and Deploy Licenses task is created on the Jobs page. After successful license deployment, the device inventory is refreshed automatically, and the license is displayed on the License page.

To learn more about the jobs, go to the **Monitor > Jobs** page, select the task, and then click **View Details**.

Deploy licenses

Use OpenManage Enterprise to deploy all available licenses to discovered systems either system-by-system or all-at-once.

Prerequisites

- Discover and onboard systems to which the licenses are bound.
- Confirm that the devices in the inventory are licensable.
- Obtain and import licenses by doing one of the following:
 - Connecting to Dell Online to automatically import the unbound licenses from the Dell Online account and bind the licenses. For more information, see [Obtain licenses by connecting to Dell Digital Locker](#).
 - Downloading the license archives from Dell Online Licensing Portal and importing the licenses into OpenManage Enterprise. For more information, see [Import licenses](#).
- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with license deployment privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).

About this task

Licenses can be deployed one-to-many fashions using a single job from the **Configuration > Licenses** page or system-by-system by going to the device view details page and selecting the **Licensing** tab.

Steps

1. Click **Configuration > Licenses**, and then select the licenses to be deployed.
Verify that the licenses selected can be deployed by checking the **Deployable** field against each license. The **Deployable** status with the yellow icon indicates that the license is not deployable. Select the non deployable licenses to check the **Rejection Reason** on the right of the screen. Use this reason to make the license deployable.
2. If the selected licenses are deployable, the **Deploy** button is enabled. Click **Deploy**.
3. An Install license task job is created where you can track the job progress.

Results

After the license is deployed on the target device, the device inventory is automatically refreshed to update the license capability for the device in the appliance.

Next steps

If license deployment fails, review the task logs in the **Task Execution Details** on the **Jobs** page. Use these details to correct errors and deploy the license again.

Export licenses

Export an archive of some or all licenses on the appliance. This archive can be used as a backup when an appliance is repaired or upgraded and the Dell Licensing Portal is not accessible. Archived licenses can also be used to transfer licenses among appliance installations.

Prerequisites

Ensure that a local fileshare is reachable to the appliance over CIFS, NFS, or HTTPs.

- Ensure that the appliance has Internet access to reach Dell Digital Locker.
- You must have an active Dell account.
- You must have an Administrator role, Device Manager role, or a custom user role with the License Management privilege. For more information about privileges, see [Role and scope-based access](#).

Steps

1. Click **Configuration > Licenses**, and then select the licenses to be exported.
2. Click **Export**.
3. Select the target **Archive File Format**. Available options are ZIP or TAR.
4. Select the **Share Type**. Available options are **NFS**, **CIFS**, or **HTTPS**.
5. Enter the **Share Information**:

- **Share IP Address**: The IP address at which the share is reachable.
- **Share Path**: The file path on the server where the exported licenses are saved.

 **NOTE:** No special characters are supported in the **Share Path** field.

- **Workgroup**: The group name tag that identifies devices and their resources in the SMB domain. If **Share Type** is set to CIFS, this field is required.
 - **Username**: The username of a user that can write to the CIFS or HTTPS share. If **Share Type** is set to CIFS or HTTPS, this field is required.
 - **Password**: The password of a user that can write to the CIFS or HTTPS share. If **Share Type** is set to CIFS or HTTPS, this field is required.
6. Optional: Click **Test Connection** to verify that the appliance can reach the share.

 **NOTE:** You must have the Job management privilege to verify the test connection. However, you can proceed to the next step without verifying the test connection.

7. Click **Export** to create the file.

An export license task job is created where you can track the job progress.

Results

An archive of the exported licenses is saved to the fileshare.

Disconnect from Dell online

The appliance can be disconnected from Dell Online after all licensing tasks are complete. If the connection is not terminated by the user, the appliance will terminate the connection within 24 hours using a system-defined scheduled task.

Steps

1. In the OpenManage Enterprise, click **Configuration > Entitlements**, and then click **Disconnect from Dell Online**.

 **NOTE:** Disconnecting from Dell Online is disabled if any license binding tasks are active or the connection is inactive.

2. A confirmation box is displayed. Click **Yes**.

User authentication need to be performed again for reconnecting to the Dell Online account.

Results

Once the appliance is disconnected from Dell online, the entitlement information captured during the connection process is removed, resulting in an empty entitlements grid.

Delete licenses from OpenManage Enterprise

Remove licenses from the appliance.

Prerequisites

- You must have an Administrator role, Device Manager role, or a custom user role with the License Management privilege. For more information about privileges, see [Role and scope-based access](#).

Steps

1. Click **Configuration > Licenses**.
2. Select the licenses to be deleted.
3. Click **Delete**.

Results

The licenses are deleted from the OpenManage Enterprise appliance. Deleting licenses from the appliance does not remove them from the devices they are deployed on. To remove licenses from a device, see [View installed and available licenses on a device](#).

Using jobs for device control

A job is a set of instructions for performing a task on one or more devices. The jobs include discovery, firmware update, inventory refresh for devices, warranty, and so on. OpenManage Enterprise performs discovery, inventory, and health tasks asynchronously, improving performance and scalability in large environments. You can view the status and details of jobs that are initiated in the devices and its components, on the **Jobs** screen. OpenManage Enterprise has many internal maintenance jobs which are triggered on a set schedule automatically by the appliance. For more information on the 'default' jobs and their schedule, see [Default jobs and job schedules](#).

Topics:

- [Create and manage jobs](#)
- [View job lists](#)
- [View job details](#)
- [Create a job to blink device LEDs](#)
- [Create a job for controlling device power](#)
- [Create a remote command job for managing devices](#)
- [Create a job to change the virtual console plugin type](#)
- [Select target devices and device groups](#)
- [Manage jobs](#)

Create and manage jobs

How to create and manage jobs such as blink, power control, managing firmware baselines, or any other job where the device selection task is involved.

Prerequisites

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with job management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- Each job type is limited to devices that you have permission to access.

About this task

From OpenManage Enterprise, click **Monitor** > **Jobs** to create and manage jobs.

Steps

1. Select **Monitor** > **Jobs**.
You can perform the following tasks on the **Jobs** screen:
 - [View job lists](#) to check if jobs are running, failed, or successfully completed.
 - Create jobs to blink device LEDs, control the device power, and run remote commands on devices as described in [Create a remote command job for managing devices](#), and [Create a job to blink device LEDs](#). You can perform similar actions on a server on the **Device Details** screen, as described in [View and configure individual devices](#).
 - [Manage jobs](#) such as run, stop, enable, disable, or delete jobs.
2. To view more information about a job, select the check box corresponding to a job, and then click **View Details** to [View job details](#).

View job lists

View the status of jobs that are run on OpenManage Enterprise for device monitoring and management.

Click **Monitor** > **Jobs** to view the list of existing jobs. Information about jobs is provided in the following columns:

- **Job Status** provides the execution status of a job. When you view the job list using the **Scheduled** status filter, unscheduled **Report_Task** jobs from previous versions of the appliance are incorrectly listed. This issue does not affect unscheduled jobs created in version 4.5 of the appliance. See Jobs status and Jobs type description See [Jobs status and Jobs type description](#).
- **State** provides the state of a job. The available options are Enabled or Disabled.
- **Job Name** provides the name of a job.
- **Job Type** provides the type of a job. See [Jobs status and Jobs type description](#).
- **Description** provides a detailed description of a job.
- **Last Run** provides the timestamp at which the job was last initiated.

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

- **Last run start date:** provides the timestamp at which the job was last initiated.
- **Last run end date** provides the timestamp at which the job was last completed.
- **Source:** The available options are All, User Generated (Default), and System.

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

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

NOTE:

- On the **Discovery and Inventory Schedules** screen, the status of a scheduled job is listed as **Queued** in the **STATUS** column. However, the same status is indicated as **Scheduled** on the **Jobs** screen.
- Users are allowed to select multiple jobs either individually, or by selecting all on the current screen or across all screen, and click **Run Now**. If any of the selected jobs contain a device reboot (example: Device action or firmware update job), target devices could be adversely impacted. Exercise extreme caution when using this feature.

Jobs status and Jobs type description

Statuses of a job indicate its completion state. Jobs can be run for device discovery, health status upgrade, updating OpenManage Enterprise version and so on.

Table 53. Job status and description

Job Status	Description
Scheduled	Job is scheduled to run later.
Queued	Jobs that are waiting to be run.
Starting	Job that are in a transitional stage to run.
Running	Job is triggered using Run Now .
Completed	Job has run.
Failed	Job run was unsuccessful.
New	Job is created but not run.
Completed with errors	Job run was partially successful and was completed with errors.
Aborted	The user stopped the job.
Paused	The user paused the job.
Stopped	The user interrupted the job.
Canceled	The system forcibly stopped the job.
Not run	The job is either queued or scheduled and is yet to run.

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

Table 54. Job Types and description

Job Type	Description
Health	This job checks the health status of the devices. See Device health statuses .
Inventory	This job creates inventory report of the devices. See Managing device inventory .
Device Config	This job creates device configuration compliance baseline. See Configuration compliance .
Report_Task	This job creates reports about devices by using integrated or customized data fields. See Monitoring reports .
Warranty	This job generates data about the warranty status of target devices. See Managing device warranty .
Onboarding_Task	This job onboards discovered devices. See Onboarding devices .
Discovery	This job discovers devices. See Discovering devices .
Console Update Execution Task	This job tracks console upgrade jobs. This task helps to identify if the upgrade has completed or failed
BR_Plugin_Synchronisation_Task	This job synchronizes plugins on the target appliance according to the backup file being restored. It involves installing any missing plugins and enabling any plugins that are disabled on the target appliance.
BR_Backup_Task	This job creates a file backup of the appliance and deposits it in a secure location.
Chassis Profiles	This job creates and export profile of the chassis.
Debug Logs	This job collects Debug logs of the application monitoring tasks, events, and the task execution history.
Device Action	This job creates actions on devices such as Turn LED On, Turn LED Off, IPMI CLI, RACADM CLI, and so on.
Diagnostic_Task	This job tracks diagnostic tasks like download or running TSR or services (SupportAssist). See Run and download Diagnostic reports .
Import VLAN Definition	This job imports VLAN definitions from excel or from MSM.
OpenID Connect Provider	This job configures OpenID connections. See OpenManage Enterprise login using OpenID Connect providers .
PluginDownload_Task	This job tracks plug-in downloads and helps to identify whether the plug-in RPMs are downloaded and ready for installation. See Check and update the version of the OpenManage Enterprise and the available plugins .
Post_Upgrade_Task	This job sets the appliance settings performed in N-1 or N-2 Version. Also, this task runs the discovery task which were created in the previous version to ensure all devices are being listed.
Report_Task	This job initiates and tracks reports. (for Canned as well for Custom).
Settings Update	This job modifies console settings.
Software Rollback	This job rolls back the current software version running on OpenManage Enterprise
Update	This job updates firmware or drivers on target devices.
Upgrade_Bundle_Download_Task	This job downloads the OpenManage Enterprise upgrade bundle and identifies whether the downloading of OpenManage Enterprise RPM are completed and ready for installation.

Default jobs and job schedules

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

Table 55. Default jobs and job schedules

Job Name	Cron Expression	Cron Expression Description	Example
Alert Correlation ^a	0 0/3 * 1/1 * ? *	Every 3 minutes	- Mon May 17 19:30:00 UTC 2021 - Mon May 17 19:33:00 UTC 2021 - Mon May 17 19:36:00 UTC 2021
Configuration Inventory ^a	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the First, every month	- Tue May 18 00:00:00 UTC 2021 - Wed May 19 00:00:00 UTC 2021
Default Console Update Task	0 0 12 ? * MON * *	At 12:00:00pm, on every Monday, every month	- Mon May 24 12:00:00 UTC 2021 - Mon May 31 12:00:00 UTC 2021
Default Inventory Task ^a	0 0 5 * * ? *	At 05:00:00am every day	- Tue May 18 05:00:00 UTC 2021 - Wed May 19 05:00:00 UTC 2021
Device Config Purge Task for cleanup	0 0/1 * * * ? *	At second :00, every minute starting at minute :00, of every hour	- Mon May 17 18:39:00 UTC 2021 - Mon May 17 18:40:00 UTC 2021
File Purge Task for Share Utilization	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the First, every month	- Tue May 18 00:00:00 UTC 2021 - Wed May 19 00:00:00 UTC 2021
File Purge Task for Single DUP Files	0 0 0/4 1/1 * ? *	At second :00, at minute :00, every 4 hours starting at 00am, every day starting on the First, every month	- Mon May 17 20:00:00 UTC 2021 - Tue May 18 00:00:00 UTC 2021 - Tue May 18 04:00:00 UTC 2021 - Tue May 18 04:00:00 UTC 2021
Global Health Task ^a	0 0 0/1 1/1 * ? *	At second :00, at minute :00, every hour starting at 00am, every day starting on the First, every month	- Mon May 17 19:00:00 UTC 2021 - Mon May 17 20:00:00 UTC 2021
iDRAC Password Rotation Task ^a	0 0 0 * * ? *	Runs at midnight (00:00) every night.	- Mon May 17 00:00:00 UTC 2023 - Mon May 18 00:00:00 UTC 2023
Internal Sync Task	0 0/5 * 1/1 * ? *	At second :00, every 5 minutes starting at minute :00, every hour, every day starting on the First, every month.	- Mon May 17 18:45:00 UTC 2021 - Mon May 17 18:50:00 UTC 2021

Table 55. Default jobs and job schedules (continued)

Job Name	Cron Expression	Cron Expression Description	Example
Metrics Purge Task ^a	0 0 * ? * *	At second :00 of minute :00 of every hour	- Mon May 17 19:00:00 UTC 2021 - Mon May 17 20:00:00 UTC 2021 - Mon May 17 21:00:00 UTC 2021
Metrics Task	0 0/15 * 1/1 * ? *	At second :00, every 15 minutes starting at minute :00, every hour, every day starting on the First, every month.	- Mon May 17 18:45:00 UTC 2021 - Mon May 17 19:00:00 UTC 2021
Mobile Subscription Task	0 0/2 * 1/1 * ? *	At second :00, every 2 minutes starting at minute :00, every hour, every day starting on the First, every month.	- Mon May 17 18:54:00 UTC 2021 - Mon May 17 18:56:00 UTC 2021
Node Initiated Discovery Task	0 0/10 * 1/1 * ? *	At second :00, every 10 minutes starting at minute :00, every hour, every day starting on the First, every month.	- Mon May 17 19:00:00 UTC 2021 - Mon May 17 19:10:00 UTC 2021
Password Rotation Task ^a	0 0 0/6 1/1 * ? *	At second :00, at minute :00, every 6 hours starting at 00am, every day starting on the First, every month.	- Tue May 18 00:00:00 UTC 2021 - Tue May 18 06:00:00 UTC 2021 - Tue May 18 12:00:00 UTC 2021
Periodic Metrics Registration	0 0 3 * * ?	At 03:00:00am every day	- Tue May 18 03:00:00 UTC 2021 - Wed May 19 03:00:00 UTC 2021
Purge On Demand Health Task for Table: Task	0 0 0/5 1/1 * ? *	At second : 00, at minute : 00, every 5 hours starting at 00am, every day starting on the first, every month.	- Tue May 18 00: 00: 00 UTC 2021 - Tue May 18 05: 00: 00 UTC 2021 - Tue May 18 10: 00: 00 UTC 2021
Purge Task for Table: Core Application Log	0 0 0/5 1/1 * ? *	At second : 00, at minute : 00, every 5 hours starting at 00am, every day starting on the First, every month.	- Tue May 18 00: 00: 00 UTC 2021 - Tue May 18 05: 00: 00 UTC 2021
Purge Task for Table: Event	0 0/30 * 1/1 * ? *	At second : 00, every 30 minutes starting at minute : 00, every hour, every day starting on the First, every month	- Mon May 17 19: 30: 00 UTC 2021 - Mon May 17 20: 00: 00 UTC 2021 - Mon May 17 20: 30: 00 UTC 2021
Purge Task for Table: Infrastructure Device	0 0/30 * 1/1 * ? *	At second : 00, every 30 minutes starting at minute : 00, every hour, every day starting on the First, every month.	- Mon May 17 19: 30: 00 UTC 2021 - Mon May 17 20: 00: 00 UTC 2021 - Mon May 17 20: 30: 00 UTC 2021

Table 55. Default jobs and job schedules (continued)

Job Name	Cron Expression	Cron Expression Description	Example
Purge Task Table : announced_target	0 0 0 1/1 * ? *	At 00: 00: 00am, every day starting on the First, every month	• Tue May 18 00: 00: 00 UTC 2021 • Wed May 19 00: 00: 00 UTC 2021 • Thu May 20 00: 00: 00 UTC 2021
Purge Task Table : Event_Archive	0 0 18/12 ? * * *	At second : 00, at minute : 00, every 12 hours starting at 18pm, of every day	• Tue May 18 18: 00: 00 UTC 2021 • Wed May 19 18: 00: 00 UTC 2021 • Thu May 20 18: 00: 00 UTC 2021
Purge Task Table : Group_Audit	0 0 0 1/1 * ? *	At 00: 00: 00am, every day starting on the First, every month	• Tue May 18 00: 00: 00 UTC 2021 • Wed May 19 00: 00: 00 UTC 2021 • Thu May 20 00: 00: 00 UTC 2021
Purge Task Table : Task	0 0 0 1/1 * ? *	At 00: 00: 00am, every day starting on the First, every month	• Tue May 18 00: 00: 00 UTC 2021 • Wed May 19 00: 00: 00 UTC 2021 • Thu May 20 00: 00: 00 UTC 2021
Subscription poller task	0 0/30 * 1/1 * ? *	At second : 00, every 30 minutes starting at minute : 00, every hour, every day starting on the First, every month.	• Mon May 17 19: 30: 00 UTC 2021 • Mon May 17 20: 00: 00 UTC 2021 • Mon May 17 20: 30: 00 UTC 2021

a. This job can be scheduled using [Manage console settings](#).

View job details

View job status, execution history, and metadata. Restart jobs if needed and export job data as a CSV file.

Steps

1. In the **Jobs** screen, select the checkbox corresponding to a job.
2. In the right pane, review the job summary and click **View Details**.

Results

The right pane displays key metadata, such as Detailed Description, Created By, Updated By (if applicable), Last Run Date/Time, Next Run Date/Time (if applicable).

The **Updated By** field appears in the right pane of the **Jobs** screen when a job is selected. It shows the user who last modified the job. If ownership has been transferred, this field may still display the original user unless the new owner edits the job. This behavior is by design to preserves audit history.

In the **Job Details** screen:

- The **Execution History** section lists each time the job ran.
- The **Execution Details** section lists the devices targeted by the job and the time taken to complete it.

 **NOTE:** If a job's start, end or elapsed time is incorrect, update your local time zone and settings in the **Application Settings > Network > Time Configuration** screen.

- Click **Restart Job** if the status of a job is: *Stopped*, *Failed*, or *New*. A confirmation message appears when the job restarts.
- To export job data as a CSV file, select the relevant job checkboxes, and click **Export** to [Export data](#).

Create a job to blink device LEDs

The following steps describe how you can blink the LEDs of the specified devices using the Blink Devices Wizard.

Prerequisites

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See [Role and scope-based access](#)
- After submitting this job for execution the console will first try and verify the service tag of the intended target to ensure the operation is performed on the correct system. If the verification fails the job will complete with errors, and the task execution history detail will show the following:

```
Running
Verifying if the device Service Tag is valid.
The device Service Tag could not be verified.
Task Failed. Completed With Errors.
Please check the system to ensure the IP address has not changed since the last
discovery was completed. Remediate by discovering the system with the updated IP
address, and retrying the operation.
```

Steps

1. The **Blink Devices** wizard can be activated in the following ways:
 - a. From the **Jobs** screen (**Monitor > Jobs**) click **Create**, and then select **Blink Devices**.
 - b. From the **All Devices** screen (**Devices**), select the devices and click the **More Actions** drop-down and then either click **Turn LED On** or **Turn LED Off**.
2. In the **Blink Devices** wizard dialog box:
 - a. In the **Options** section:
 - i. In the **Job Name** box, enter a job name.
 - ii. From the **Blink LED Duration** drop-down menu, select options to blink the LED for a set duration, turn on, or to turn off.
 - iii. Click **Next**.
 - b. In the **Target** section, select the target devices or target groups and click **Next**. See [Select target devices and device groups](#).
 - c. In the **Schedule** drop-down, select **Run Now**, **Run Later**, or **Run on Schedule**. See [Schedule job field definitions](#).
3. Click **Finish**.

Results

A Blink LED job is created and listed in the **Jobs** screen (**Monitor > Jobs**) **JOB STATUS** column.

Create a job for controlling device power

Create a job to perform a power control action on a device.

Prerequisites

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

About this task

 **NOTE:** Power control actions are not supported on CDU devices.

Steps

1. Click **Create**, and then select **Power Control Devices**.
2. In the **Power Control Devices** wizard dialog box:
 - a. In the **Options** section:
 - i. Enter the job name in **Job Name**.
 - ii. From the **Power Options** drop-down menu, select any one of the tasks: **Power on**, **Power off**, **Graceful Shutdown**, **Power Cycle System (Cold Boot)**, or **System Reset (Warm Boot)**.
 - iii. Click **Next**.
 - b. In the **Target** section, select the target devices and click **Next**. See [Select target devices and device groups](#).
 - c. In the **Schedule** section, run the job immediately or schedule for a later point of time. See [Schedule job field definitions](#).
3. Click **Finish**.

Results

The job is created and listed in the Jobs list and identified by an appropriate status in the **JOB STATUS** column.

If the job is scheduled for a later point of time, but you want to run the job immediately:

- On the **Jobs** screen, select the check box corresponding to the Scheduled job.
- Click **Run Now**. The job is run, and the status is updated.
- To view the job data, click **View Details** in the right pane. See [View job details](#).

Create a remote command job for managing devices

Create a job to remotely run a command and control devices.

About this task

Use the **Command Line Job** wizard to create command jobs to manage target devices remotely.

 **NOTE:** After job submission, the console verifies the service tag of the target to ensure that the operation is performed on the correct system. If the verification fails, the job completes with errors, and the task execution history detail logs the following: Running Verifying if the device Service Tag is valid. The device Service Tag could not be verified. Task Failed. Completed With Errors. Please check the system to ensure the IP address has not changed since the last discovery was completed. Remediate by discovering the system with the updated IP address, and retrying the operation.

Steps

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

 **NOTE:** The commands in the Arguments box are run one at a time.
 - d. Click **Next**.
A green tick mark next to **Options** indicates that the necessary data is provided.
3. In the **Target** section, select the target devices and click **Next**. See [Select target devices and device groups](#).
4. In the **Schedule** section, run the job immediately or schedule for a later time. See [Schedule job field definitions](#).
5. Click **Finish**.

Results

The job is created and listed in the jobs list and identified by an appropriate status in the **Job Status** column.

If the job is scheduled for a later point, but you want to run the job immediately:

1. On the **Jobs** screen, select the check box corresponding to the Scheduled job.
2. Click **Run Now**. The job is run, and the status is updated.
3. To view the job data, click **View Details** in the right pane. See [View job details](#).

Create a job to change the virtual console plugin type

Create a job to change the plugin type of a virtual console of devices to HTML5.

About this task

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

 **NOTE:** The **Change Virtual Console Plugin on Devices** action is not supported on PowerEdge 17G servers (iDRAC10). This is because these servers are hardcoded to use the enhanced HTML5 (eHTML5) interface.

Steps

1. Click **Monitor > Jobs**
2. Click **Create**, and then select **Change Virtual Console Plugin on Devices**.
3. In the **Change Virtual Console Plugin** wizard dialog box, in the **Options** section:
 - a. Enter the job name in **Job Name**. By default, the plugin type is displayed as HTML5.
 - b. Click **Next**.
4. In the **Job Target** section, select the target devices and click **Next**. See [Select target devices and device groups](#).
 - a. Click **Next**.
5. In the **Schedule** section, run the job immediately or schedule for a later point of time. See [Schedule job field definitions](#).
6. Click **Finish**.

Results

The job is created and listed in the Jobs list and identified by an appropriate status in the **JOB STATUS** column.

If the job is scheduled for a later point of time, but you want to run the job immediately:

- On the **Jobs** screen, select the check box corresponding to the Scheduled job.
- Click **Run Now**. The job is run and the status is updated.
- To view the job data, click **View Details** in the right pane. See [View job details](#).

Next steps

After the job completes, launch the virtual console for any updated device. The HTML5 interface now provides an improved browser experience.

Select target devices and device groups

Select target devices or device groups to perform jobs.

About this task

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

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

Steps

1. Click **Select Devices**.

In the **Job Target** dialog box, the left pane lists the devices monitored by OpenManage Enterprise. In the working pane, list of devices associated with each group, and device details are displayed. For field descriptions, see [All Devices screen device list](#). For information about device groups, see [Create and manage custom groups](#).

2. Select the check box corresponding to a device and click **OK**.

Results

The selected devices are displayed in the **All Selected Devices** section of the selected group.

Manage jobs

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

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

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

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

Monitoring audit logs

OpenManage Enterprise captures and displays audit logs to help you track and understand tasks performed using OpenManage Enterprise. These logs include events such as user login attempts, creation of alert policies, and execution of various jobs.

Prerequisites

To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See [Role and scope-based access](#).

About this task

The **Monitor > Audit logs** screen lists log data to help you or Dell Support teams in troubleshooting and analysis. Audit logs are recorded for events such as:

- Group assignments or changes in access permissions.
- Modifications to user roles.
- Actions performed on devices monitored by OpenManage Enterprise.
- Changes to console settings.
- Plugin management actions (install, uninstall, etc.).

 **NOTE:** Scope-based restrictions are not applicable to the Audit logs.

Audit log retention behavior: A purge task runs automatically every 5 hours and removes all entries beyond the latest 5,000 records. This means OpenManage Enterprise retains only the most recent 5,000 audit log messages at any given time.

Steps

1. To view the audit logs, select **Monitor > Audit Logs**.
The appliance displays audit logs for tasks such as user login attempts, creation of alert policies, and execution of various jobs.
2. To sort the log data, select the header of the column you want to sort by.

Topics:

- [Filtering audit logs](#)
- [Exporting audit logs](#)
- [Forward audit logs to remote Syslog servers](#)

Filtering audit logs

Steps

1. To quickly search for information about an audit log, click **Advanced Filters**.
2. Enter or select data in the following fields:
 - **Severity:** Select the severity level of a log data. The available options are info, warning, and critical.
 - Critical: Any unusual action happened. Immediate attention is needed.
 - Warning: The event is significant, but does not need immediate attention.
 - Info: Any action performed with success.
 - **Start Time and End Time:** To view audit logs of a specified period.
 - **User:** To view audit logs from a specific user. For example, admin, system, device manager, and viewer.
 - **Source Address:** To view audit logs from a specific system. For example, the system where you have logged in to the OpenManage Enterprise.
 - **Category:** To view audit logs of audit or configuration type.
 - Audit: Logged when a user logs in or out of the OpenManage Enterprise appliance.
 - Configuration: Logged when a configuration action is performed on a target device.
 - Miscellaneous

- Updates: Logged for both successful and failed update operations involving repositories and catalogs.
- System Health: Logged to capture the status and performance metrics of system components and processes.
- **Description Contains:** Enter the text or phrase contained in the log data that you are searching for. All logs with the selected text are displayed. For example, if you enter `warningSizeLimit`, all the logs with this text are displayed.
- **Message ID:** Enter the message ID. If the search criteria matches, only the items with the matching message ID are displayed.

3. To clear all applied filters, select **Clear All Filters**.

Exporting audit logs

Steps

To export an audit log or all the audit logs, select **Export > Export Selected**, or **Export > Export All Audit Logs** respectively.

The file will not be immediately ready for download especially in cases where there is a large set of logs being collected. The collection process happens in the background, and a file save prompt is displayed when the operation is completed.

Forward audit logs to remote Syslog servers

To monitor all the audit logs of OpenManage Enterprise from Syslog servers, you can create an alert policy. All audit logs such as user login attempts, creation of alert policies, and running different jobs can be forwarded to Syslog servers. If a server specifies the OpenManage Enterprise as a Syslog target, traps triggered on the server will be forwarded to the OpenManage Enterprise's destination Syslog server as well. To forward audit logs to an SNMP destination, set the trap-forwarding format to **Normalized** in the Console Settings.

Steps

1. Select **Alerts > Alert Policies > Create**.
2. In the **Create Alert Policy** dialog box, in the **Name and Description** section, enter a name and description of the alert policy.
 - a. The **Enable Policy** check box is selected by default to indicate that the alert policy will be enabled once it is created. To disable the alert policy, clear the check box. For more information about enabling alert policies at a later time, see [Create an alert policy](#).
 - b. Click **Next**.
3. In the **Category** section, expand **Application** and select the categories and subcategories of the appliance logs. Alternatively, in the **Message ID** section, indicate a list of messages to be sent to the Syslog by either:
 - a. Uploading a .csv file listing the messages to be filtered. (Sample available on the UI)
 - b. Entering a list of message IDs separated by commas.
4. Click **Next**
5. In the **Target** section, the **Select Devices** option is selected by default. Click **Select Devices** and select devices from the left pane. Click **Next**.

NOTE:

- Selecting target devices or groups is not applicable while forwarding the audit logs to the Syslog server.
- To forward audit logs to an SNMP destination, set the trap-forwarding format to **Normalized** in the Console Settings. See, 'Configure trap forwarding format' in [Manage console settings](#) for more details.

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

If Syslog servers are not configured in OpenManage Enterprise, click **Enable** and enter the destination IP address or the hostname of Syslog servers. For more information about configuring Syslog servers, see [Configure SMTP, SNMP, and Syslog](#).

9. Click **Next**.

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

11. Click **Finish**.

Results

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

Related concepts

[Alert policies](#)

Monitoring reports

Reports enable you to collate and view data about the alerts, devices, groups, jobs, and servers.

Click **Monitor > Reports** to use the system-defined reports or create custom reports.

- You must be a Super Administrator, Administrator, Device Manager, or Custom Role user with report management privilege and scope-based operational access to the devices. For more information about privileges, see [Role and scope-based access](#).
- Definitions and criteria that is used for a system-defined report cannot be edited or deleted.
- The reports and the data that is displayed on the **Reports** screen depend on the scope-based user privileges that you have in OpenManage Enterprise. For example, Device Managers have access to only the reports that they have created in addition to the system-defined reports. Also, user-generated reports would contain data only from the devices that are in the scope for that user. For example, when administrators or 'unrestricted' device managers generate a report, all data regarding all devices and device groups is included. However, when device managers with limited scope generate a report, only data regarding devices or device groups within their scope is included.
- An audit log entry is made whenever you **Run, Edit, Delete, or Copy** a report.
- If you feel that report generation is taking time, you can stop the process.
- The reports that are generated are automatically translated to the language which is set while installing OpenManage Enterprise.
- The right pane displays the details such as:
 - Fields in the report
 - Last Run Duration
 - Last Run By
 - Last Edited By
 - Schedule
 - Format
 - Delivery Options: Email recipients or network share.

The OpenManage Enterprise reports feature enables you to:

- Create a report using up to 20 filters. See [Create a report](#).
- Run and download the report. See [Run reports](#).
- Run and Email the report to up to 20-30 recipients at a time. See [Run and email reports](#).
- Edit the Custom reports. See [Edit reports](#).
- Use Schedule and Options to automatically run a report at a selected date and time. You can also select whether the report is emailed or saved to the internal share. See [Schedule and delivery options for reports](#).
- Copy an existing custom report to create and customize a new report. See [Copy reports](#).
- Delete the custom reports from the **Reports** screen. See [Delete reports](#).
- Export the content of the selected reports to HTML, CSV, or PDF. See [Export selected reports](#).
- View the scheduled date and time of the Scheduled reports or to delete the scheduling. See [Schedule and delivery options for reports](#).
- Use the **Advanced Filters** to list the reports as required.

Table 56. Privileges for managing reports

User role	Permissions
Administrator, Custom role user, and Device Manager	• Run a report. • Create a report. • Copy a report. • Email a report. • Download a report. • Export a report.
Viewer	• Run a report. • Email a report. • Download a report.

Table 56. Privileges for managing reports (continued)

User role	Permissions
	Export a report.

Related tasks[Run reports](#)[Run and email reports](#)[Edit reports](#)[Delete reports](#)**Topics:**

- [Run reports](#)
- [Run and email reports](#)
- [Edit reports](#)
- [Schedule and delivery options for reports](#)
- [Copy reports](#)
- [Delete reports](#)
- [Create a report](#)
- [Export selected reports](#)
- [View and remove report schedule details](#)

Run reports

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

About this task

When you run a report, the first 20 rows are displayed. Scroll to the bottom of the table to display the number of pages and to navigate from one page to another. To view all the rows at one time, download the report. To edit this value, see [Export data](#). Data displayed in the output cannot be sorted because it is defined in the query that is used to build a report. To sort data, edit the report query or export it to an Excel sheet. It is recommended to not run more than five (5) reports at a time because reporting consumes system resources. However, this value of five reports depends on the devices discovered, fields used, and number of tables joined to generate report. A Reports job is created and run when a report generation is requested. For role-based privileges to generate reports, see [Create a report](#).

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](#).
- Reports generated by device managers will only have data pertaining to the devices that are in their scope.
- It is not recommended to frequently run a report because it consumes processing and data resources.
- For a report whose category is 'Device', the first columns by default are Device name, Device model, and Device Service Tag. You may exclude columns while customizing your report.
- If the generated file corresponding to a report run is larger than 5MB, an internal alert will be logged.
- If you are downloading or running a report that is already generated, and another user tries to delete that report simultaneously, both the tasks are successfully completed.
- For the power headroom report, the power value that is considered for the calculation of stranded power is the maximum power value for the selected report duration.

Steps

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

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

Related concepts

[Monitoring reports](#)

Run and email reports

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

Prerequisites

- If an Admin has not set up SMTP on the appliance, users with DM privileges cannot use this feature.
- If the message size exceeds the fixed message size set on the SMTP server, email operations may fail with large reports. In such instances, consider resetting the message size limit on the SMTP server and try again.

Steps

1. Select the report and click **Run and Email**.
2. In the **Email Report** dialog box:
 - a. From the **Format** drop-down menu, select one of the file formats in which the report must be generated: HTML, CSV, PDF, or XLSX.
 - b. In the **To** box, enter the email address of the recipient. If the email address is not configured, click **Go to SMTP Settings**. For more information about setting SMTP properties, see [Configure SMTP, SNMP, and Syslog](#).
 - c. Click **Finish**.

Results

The report is emailed and recorded in the Audit logs.

Related concepts

[Monitoring reports](#)

Edit reports

Only user-created reports can be edited.

Steps

1. Select the report and click **Edit**.
2. In the **Report Definition** dialog box, edit the settings. See [Creating reports](#).
3. Click **Save**.
 **NOTE:** While editing a customized-report, changing a category results in the removal of any associated fields.

Results

The updated information is saved. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Related concepts

[Monitoring reports](#)

Schedule and delivery options for reports

For the reports on the **Reports** screen, you can schedule their automatic execution and choose the delivery options (email recipients/network share).

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](#).
- Report results depend on the scope that is assigned to the user.

Steps

1. On the **Monitor > Reports** screen, select the report(s) for which you want to set the execution schedule and click **Schedule and Options**.
2. In the Schedule and Options wizard, select the **Schedule** check box and do one of the following:
 - a. Select **Run Later** and select the **Date** and **Time**.
 - b. Select **Run On Schedule** and select **Daily** or **Weekly** from the drop-down list and specify a time in the 12-hour format.
3. From the **Report Format** list, select one of the following report delivery formats: HTML (default), CSV, PDF, XLS.
4. To set the report delivery option, do one of the following:
 - a. Select the **Email Report** check box and fill the **Email Recipient** box to email the report. A list of email recipients (comma-separated list) can be specified to a max of 512 characters.
If the email configuration is not set or if you want to change the existing email setup, click **Go to SMTP Settings**. For more information see, [Configure SMTP, SNMP, and Syslog](#).
 - b. Select the **Save Report to Share** check box and select the **Share Type** as CIFS or NFS share and enter the respective Share Information such as **Share IP Address**, **Share Path**, **Workgroup**, **Username**, and **Password**. Once the details are entered, you can test the connection by clicking **Test now**.

 **NOTE:** Special characters are not supported in the CIFS **Share Path** field.

5. Click **Finish**.

Results

The respective report(s) will run and deliver the report(s) based on the Schedule and Options settings. The schedules of these reports can be viewed, deleted, or edited by clicking View Schedules. See, [View and remove report schedule details](#).

Copy reports

Create a new report by copying from an existing report.

About this task

Only user-created reports can be copied.

Steps

1. Select the report, click **More Actions**, and then click **Copy**.
2. In the **Copy Report Definition** dialog box, enter a new name for the copied report.
3. Click **Save**.

Results

The updated information is saved. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Delete reports

Delete user-created reports.

About this task

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

Steps

1. Click **Monitor > Reports**.

A list of devices available reports is displayed.

2. Select the report, click **More Actions**, and then click **Delete**.

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

3. In the **Delete Report Definition** dialog box, when prompted whether or not the report must be deleted, click **Yes**.

Results

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

Related concepts

[Monitoring reports](#)

Create a report

User-defined reports are used to customize criteria and get tailor-made information.

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](#).
- When device managers generate reports, the reports only contain data that pertains to the device groups which are in their scope.
- Some tables contain device-type-specific data which locks the report to that device type. Mixing columns from multiple device-specific tables of different types (for example servers and chassis) results in an invalid report with no entries.

About this task

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

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

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

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

Table 57. Role-based access privileges for reports

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

Steps

1. Click **Reports > Create**.
2. In the **Report Definition** dialog box:
 - a. Type the name and description of the new report to be defined.
 - b. Click **Next**.
3. In the **Report Builder** section:
 - a. From the **Category** drop-down menu, select the report category.
 - If you select Device as the category, select the device group also.
 - If necessary, edit the filter criteria. See [Select a query criteria](#).
 - b. Under the **Select Columns** section, select the check boxes of the fields that must appear as the report columns. Selected field names are displayed in the **Column Order** section.
 - c. You can customize the report by:
 - Using the **Sort by** and **Direction** boxes.
 - Dragging the fields either up or down in the **Column Order** section.
4. Click **Finish**.

Results

The report is generated and listed in the list of reports. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Next steps

To export a report for analytical purposes, see [Export data](#).

Select the query criteria

Use the system defined queries to create reports about devices monitored by OpenManage Enterprise.

About this task

Define filters while creating query criteria for:

- Generating customized reports. See [Creating the reports](#).
- Creating Query-based device groups under the **CUSTOM GROUPS**. See [Creating a Query \(Dynamic\) device group](#).

Define the query criteria by using two options:

- **Select existing query to copy:** By default, OpenManage Enterprise provides a list of system-defined query templates that you can copy and build your own query criteria. A maximum of 20 criteria (filters) can be used while defining a query. To add filters, you must select from the **Select Type** drop-down menu.
- **Select type:** Build query criteria from scratch using attributes listed in this drop-down menu. Items in the menu depend on the devices monitored by OpenManage Enterprise. When a query type is selected, only appropriate operators such as =, >, <, and null are displayed based on the query type. This method is recommended for defining query criteria in building customized reports.

NOTE:

- When a query is evaluated with multiple conditions, the order of evaluation is the same as SQL. To specify a particular order for the evaluation of the conditions, add or take off parenthesis when defining the query.
- When selected, the filters of an existing query criteria are copied only virtually to build a new query criteria. The default filters associated with an existing query criteria are not changed. The definition (filters) of a system-defined query criteria is used as a starting point for building a customized query criteria. For example:
 1. *Query1* is a system-defined query criterion that has the following predefined filter: `Task Enabled=Yes`.

2. Copy the filter properties of *Query1*, create *Query2*, and then customize the query criterion by adding another filter:
`Task Enabled=Yes AND (Task Type=Discovery)`.
3. Open *Query1*. Its filter criteria should still contain `Task Enabled=Yes`.

Steps

1. In the **Query Criteria Selection** dialog box, select whether you want to create a query criteria for Query groups or for report generation.
2. Add or take off a filter by clicking the plus or dustbin symbol respectively.
3. Click **Finish**.

Results

A query criterion is generated and saved in the list of existing queries. An audit log entry is made and displayed in the Audit logs list. See [Managing the audit logs](#).

Export selected reports

Reports generated by the appliance can be exported to local files.

Steps

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

 **NOTE:** Reports exported to the CSV or PDF format that have been generated in Japanese or Chinese may contain incorrectly encoded characters. To display the data correctly, import the file to a spreadsheet program with the encoding **Unicode (UTF-8)**. Save the resulting sheets using the native format of the program or PDF to retain encoding information.

3. Click **Finish**.

Results

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

View and remove report schedule details

You can view the details of the scheduled reports and remove them from their schedules.

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](#).
- The user accessing the UI can only view reports that they have created. For a list of all reports the user may have access to, click **More Actions > All Report Schedules**.

Steps

1. On the **Monitor > Reports** screen, select the report from which you must remove the schedule.
2. Click **More Actions > View Schedule**.
3. Select the schedules that you want to delete based on details such as Username, Schedule, Format, Recipient associated with a report.
4. Click **Delete**.

Results

The associated schedules with that report are deleted.

Manage the Power Management features

Configure the Power Management settings, manage licensed devices and groups, and policies. Also, you can view a summary of the power data.

Topics:

- [Monitor and manage devices for power](#)
- [Overview](#)
- [View devices and groups added for power management and monitoring](#)
- [View details of Unmonitored Devices](#)
- [Policies](#)
- [Manage data center during power reduction](#)
- [View racks of physical groups](#)
- [Compare server usage metrics](#)
- [Analyze multivariate metrics using parallel coordinates](#)
- [Set preferences](#)
- [View metrics, and monitor devices and groups history](#)
- [Monitor Graphics Processing Unit \(GPU\)](#)
- [Monitor Power Supply Unit \(PSU\)](#)
- [Monitor Central Processing Unit \(CPU\)](#)
- [Thresholds](#)
- [Create alert thresholds](#)
- [View alert thresholds](#)
- [Edit alert thresholds](#)
- [Delete alert thresholds](#)

Monitor and manage devices for power

This section provides high-level information to help administrators get started with using the Power Management feature.

Prerequisites

Ensure that the following prerequisites are met:

- The devices are compatible for power management and monitoring. For more information, see the *OpenManage Enterprise Support Matrix*.
- Discover the devices in OpenManage Enterprise.
- For more information about creating static groups, see OpenManage Enterprise User's Guide.
- Add the **OpenManage Enterprise Advanced or Advanced+** and the management console licenses on the target devices. For more information about adding a license, see the respective management console guide.

To monitor the data of devices and groups, perform the following steps:

Steps

1. Create static custom groups or physical groups in OpenManage Enterprise.

For more information about creating physical groups under **PHYSICAL HIERARCHY**, see [Create physical groups in OpenManage Enterprise](#).

For more information about system profile groups under **SYSTEM GROUPS**, see [View devices associated with system and workload profiles](#).

The physical groups that are created or deleted in OpenManage Enterprise are automatically added or removed from power management and monitoring.

If you have created a physical group:

- a. Add the [unmonitored devices](#) for power management and monitoring.
 - b. Add the [individual devices and unmonitored devices](#) in physical groups.
2. Add the [individual devices](#), or [static groups](#) for power management and monitoring.
 3. Configure your preferences in Power Management using the **Settings** page. For more information, see [Setting preferences](#).
 4. After adding devices and groups for power management and monitoring, you can perform the following tasks:
 - View all the groups or device [metric details](#) using **Metrics**.
 - Create and apply [Power policies](#) to regulate the power consumption on devices or groups.
 - Create and apply [Temperature-triggered policies](#) to regulate device temperature.
 - During a power emergency, reduce power consumption using the [Emergency Power Reduction](#) feature.
 - Create [alert thresholds](#) by configuring the warning and critical values for devices or groups that are monitored for power management and monitoring.
 - View and monitor virtual machines. For more information, see [Virtual machines](#).
 - View generic logs generated in OpenManage Enterprise through **Monitor > Audit Logs** tabs.

Overview

This page provides a quick summary of the devices and groups that are monitored for power.

View top ten power offenders

Prerequisites

Ensure that you have configured the power and temperature thresholds in the **Alert Thresholds** tab under the **Monitoring Metrics** tab for devices, or under **Group Details** for groups.

About this task

To view a list of devices and groups that have violated the defined threshold values of power, run the in-built report for **Metric Thresholds Report for Devices**, **Metric Thresholds Report for Groups**, and **Metric Thresholds Report for GPU Cards**. The total violation count for power is the sum of upper warning and upper critical violation counts. The total violation count for temperature is the sum of upper warning, upper critical, lower warning, and lower critical violation counts.

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

If you are logging in as a Device Manager DM1 user, the top 10 devices that is assigned to the Device Manager DM1 user and that have violated the defined threshold values for the maximum number of times are displayed.

Steps

1. Start OpenManage Enterprise and click **Power Management > Overview**.
The **Overview** tab is displayed.
2. View the **Top 10 Power Offenders** section.
The details that are displayed are: Device name, service tag, number of times the device has violated the defined power threshold, and the nature of violations based on the alert threshold values.
3. To view the groups or GPU cards that have violated the power threshold, select **Groups** or **GPUs** from the **Entity Type** menu.
The details that are displayed are: Group or GPU name, number of times the group or GPU has violated the power threshold, location, and the nature of violations based on alert threshold values. For GPU devices, the identifier and FQDD data are also displayed.
4. To view devices, groups, or GPUs in a particular violation state, select an option from the **State** drop-down menu.
5. Optional: To refresh the data, click the refresh option.

View top ten temperature offenders

Prerequisites

Ensure that you have configured the power and temperature thresholds in the **Alert Thresholds** tab under the **Monitoring Metrics** tab for devices, or under **Group Details** for groups.

About this task

To view a list of devices and groups that have violated the defined threshold values of temperature, run the in-built report for **Metric Thresholds Report for Devices**, **Metric Thresholds Report for Groups**, **Metric Thresholds Report for GPU Cards**, and **Temperature Threshold Metric Report for CPUs**. The total violation count for temperature is the sum of upper warning, upper critical, lower warning, and lower critical violation counts.

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

If you are logging in as a Device Manager DM1 user, all the devices that have violated the temperature maximum number of times within the Device Manager DM1 user scope are displayed.

Steps

1. Start OpenManage Enterprise and click **Power Management > Overview**.
The **Overview** tab is displayed.
2. To view the devices that have violated the temperature threshold go to the **Top 10 Temperature Offenders** section.
The details that are displayed are: Device name, service tag, the number of times the device has violated the temperature threshold, and the nature of violations based on the alert threshold values.
3. To view the groups, GPU cards, or CPUs that have violated the temperature threshold, select **Groups, GPUs**, or **CPUs** from the **Entity Type** menu.
The details that are displayed are: Group, GPU, or CPU name, number of times the group, GPU, or CPU has violated the temperature threshold, location, and the nature of violations based on alert threshold values. For GPUs and CPUs, the identifier and FQDD data are also displayed.
4. To view devices, groups, GPUs, or CPUs in a particular violation state, select an option from the **State** drop-down menu.
5. Optional: To refresh the data, click the refresh option.

View top ten underutilized racks for power and space

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

If you are logging in as a Device Manager DM1, the top 10 underutilized racks in the physical groups that are assigned to DM1 are displayed.

To view the top 10 underutilized racks, perform the following steps:

Steps

1. Start OpenManage Enterprise and click **Power Management > Overview**.
The **Overview** tab is displayed.
2. To view the racks for unused power, go to the **Top 10 Underutilized Racks (Power)** graph.
By default, the **Actual** view is displayed.
To change the scale to the percentage, click the **View** drop-down menu and select the **Percentage** option.
3. To view the top 10 racks for unused space, go to the **Top 10 Underutilized Racks (Space)** graph.
By default, the **Actual** view is displayed.
To change the scale to the percentage, click the **View** drop-down menu and select the **Percentage** option.
4. To view the information in tabular format, click the tabular image.
The respective table is displayed.

5. To refresh the data, click the **Refresh** option.

View power and space headroom

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

If you are logging in as a Device Manager DM1, the power and space headroom for the physical groups that are assigned to DM1 are displayed.

To view the consumption of power in a group, perform the following steps:

Steps

1. Start OpenManage Enterprise and click **Power Management > Overview**.
The **Overview** tab is displayed.
2. Go to the **Headroom** section.
The power headroom and the space headroom graphs are displayed. For power shelves, the power headroom data is not applicable.
3. To change the group name, provide the group name in the **Physical Hierarchy Group** field and press the **Enter** key.
Details of power and space headroom are displayed.
4. Optional: To refresh the data, click the refresh option.

View power history of virtual machines and virtual machine groups

View the maximum and minimum power consumption of virtual machines and virtual machine groups.

Steps

1. Start OpenManage Enterprise and click **Power Management > Overview**.
The **Overview** tab is displayed.
2. View the **Virtual Machines** and **Virtual Machines Groups** sections.
Maximum Power Consumption displays the top 10 VMs consuming maximum power and **Minimum Power Consumption** displays the top 10 VMs consuming minimum power. Hover over each of the bars in the graph to view the VM name, VM group name, and hostname.
3. Optional: To change the duration, select an option from the **Duration** drop-down menu.
4. Optional: To refresh the data, click the refresh icon.

View idle servers

Prerequisites

Idle server detection feature is supported only on servers having the iDRAC Datacenter License.

Steps

1. Start OpenManage Enterprise and click **Power Management > Overview**.
The **Overview** tab is displayed.
2. To view the idle servers, go to the **Idle Servers** section in the right pane.
3. To view a list of all the servers, click the numerical symbol that is displayed in the **Idle Servers** section.
4. Optional: To refresh the data, click the refresh option.

View devices and groups added for power management and monitoring

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view only the groups that are assigned to the Device Manager DM1 user.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. To refresh the list of devices and groups that are added, click **Refresh Power Management**.
3. To view a device or a group that is added for power management and monitoring, perform one of the following:
 - To view a static group, click **Static Groups**.
 - To view a physical group, click **Physical Groups**.

 **NOTE:** The location of the physical group is displayed based on the hierarchy that is selected for this particular group at the time of creation.

- To view a system profile group, click **System Profile Settings**.
 - To view a device, click the **Individual Devices** tab.
 - To view all capable devices being monitored, including those that are a part of individual devices, physical groups, and system profile groups, click the **All Monitored Devices** tab.
4. Optional: To filter and view the data on any of the tabs:
 - a. Click a tab.
 - b. Click **Advanced Filters**.
 - c. Select a filter category.

The following filters are displayed for the **Static Groups**, **Physical Groups**, and **System Profile Settings** tabs:

- Group Name

The following filters are displayed for the **Individual Devices** tab:

- Health State
- Power State
- Connection State
- Name
- Identifier
- Model
- Type
- Managed State

The following filters are displayed for the **All Monitored Devices** tab:

- Health State
- Power State
- Connection State
- Name
- Identifier
- Model
- Type
- Managed State
- Part of Group

5. Optional: To clear the filters, click **Clear All Filters**.
6. Optional: To sort any column alphabetically, click the column name so that an arrow is displayed with the column name.

Add devices for power management and monitoring

To collect and monitor power and thermal utilization, and airflow data of devices, add the devices for power management and monitoring.

Prerequisites

Ensure that the following prerequisites are met:

- The devices have **OpenManage Enterprise Advanced or Advanced+** and the required management console licenses.
- The devices are discovered in OpenManage Enterprise. For information about discovering devices, see OpenManage Enterprise User's Guide.
- The modular server is not in a **Proxied** state in OpenManage Enterprise.

About this task

If no devices are available for power management and monitoring, a banner is displayed to automatically add the capable devices for monitoring. If you click **Dismiss**, the banner reappears when the page is refreshed.

To view the list of devices that are compatible with for power management and monitoring, before running the inventory in OpenManage Enterprise and immediately after the installation, perform the following steps:

1. In OpenManage Enterprise, click **Devices > Run Inventory** option.
2. Click **Power Management > Power Managed Devices > Refresh Power Management** option. The list of devices compatible for power management and monitoring is displayed when you start to add the devices from OpenManage Enterprise.

To add devices, perform the following steps:

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. Click **Individual Devices > Add device(s)**.
The **Add Devices to Power Management** page is displayed.
3. View all the devices that are discovered in OpenManage Enterprise by expanding the **SYSTEM GROUPS** section on the left side and in the **All Devices** tab. Select the devices that you want to add.
You can also add non-Dell servers.
4. Optional: To filter and view the data:
 - a. Click **Advanced Filters**.
The following filters are displayed:
 - **Health State**
 - **Power State**
 - **Connection State**
 - **Name**
 - **Identifier**
 - **Model**
 - **Type**
 - **Managed State**
5. Optional: To clear the filters, click **Clear All Filters**.
6. To view the selected devices, click the **Selected Devices** tab.
7. To add the devices, click **Add Selected**.
All the devices added individually are displayed on the **Individual Devices** tab along with the total count of devices that are added for power management and monitoring.

All the individual devices and devices that are part of the selected group are added and are displayed on the **All Monitored Devices** tab along with the total count of devices.

Results

The following changes are added after adding the devices and groups for power management and monitoring:

- After adding the devices or groups, if the server is running iDRAC firmware version 4.40.10.0 or later (and is a supported device), Power Management automatically enables the iDRAC Telemetry Streaming configuration and creates a custom

Metric Report Definition for collecting data from servers. For the list of supported models, see OpenManage Enterprise User's Guide.

- If the added device host VMs and the hypervisors are compatible for power management and monitoring, the VMs are listed in the **Power Managed Devices** tab. For information about viewing VMs, see [View virtual machines](#). For a list of compatible operating systems for monitoring VMs, see OpenManage Enterprise User's Guide.

License behavior in the Power Management feature

Use OpenManage Enterprise Advanced or Advanced+ license together with your iDRAC license to work with all the features of Power Management.

The following table provides the license combinations that are required to add and monitor servers for power management and monitoring. For example, if servers have only the iDRAC Base license, iDRAC Express license, or iDRAC Enterprise license, they cannot be monitored or managed.

Table 58. License capability with servers

OpenManage Enterprise Advanced or Advanced+ license	iDRAC Base license	iDRAC Express license	iDRAC Enterprise license	iDRAC Data Center license	Device and group monitoring	Device and group management
Not added	Added	Not added	Not added	Not added	No	No
Not added	Not added	Added	Not added	Not added	No	No
Not added	Not added	Not added	Added	Not added	No	No
Not added	Not added	Not added	Not added	Added	No	No
Added	Added	Not added	Not added	Not added	Yes	No
Added	Not added	Added	Not added	Not added	Yes	No
Added	Not added	Not added	Added	Not added	Yes	Yes
Added	Not added	Not added	Not added	Added	Yes	Yes

The following table provides license information that is required to add chassis for power management.

Table 59. License capability with chassis

Chassis models	CMC Enterprise license	Monitoring	Power policy	Emergency Power Reduction (EPR)
PowerEdge VRTX	Not added	Yes	No	Yes
PowerEdge VRTX	Added	Yes	Yes	Yes
PowerEdge FX2 or PowerEdge FX2s	Not added	Yes	No	Yes
PowerEdge FX2 or PowerEdge FX2s	Added	Yes	Yes	Yes
PowerEdge M1000e	N/A	Yes	Yes	Yes
PowerEdge MX7000	N/A	Yes	Yes	Yes

Licensing behavior in Power Management for devices:

- If the OpenManage Enterprise Advanced or Advanced+ license on the target devices is expired or deleted, the devices are removed. You must readd the devices after adding the license.
- Enabling EPR on a device, if its license expires, deleted, or removed, restricts device access. To disable EPR, go to the iDRAC or CMC page of the device and remove the EPR.
- If policy and alert thresholds are set on a device, and the device is removed because of an expired or deleted license, then the policy and alert thresholds are removed from the device.

Licensing behavior in Power Management for groups:

- For a group, only the devices that have a valid license are added as part of the group for power management and monitoring. Metrics are collected only for these devices in the group.
- If the OpenManage Enterprise Advanced or Advanced+ license is expired or deleted from the target devices that are part of a group, the devices are removed. After the license is updated, these devices are automatically added in the next inventory cycle.
- If EPR is enabled on a group, and if the license is expired or deleted for any device in a group, the device is not removed.
- If EPR is enabled on a group, you cannot remove the group or any device that is part of the group from power management and monitoring. However, the device can be removed from the group and EPR will be disabled from the removed device.

Remove devices

To stop monitoring the devices for power, remove them from power management and monitoring.

Prerequisites

Ensure that Emergency Power Reduction (EPR) is not enabled on the device.

About this task

NOTE: If a device is removed in **OpenManage Enterprise**, then that device is automatically removed from power management and monitoring.

NOTE: When a device is added individually and as part of a group for power management and monitoring, ensure that all the instances of the device are removed to stop monitoring the devices for power.

For example, if you are logging in as a Device Manager user, you can delete the devices from the physical groups that are assigned to you from the **Individual Devices** tab. However, after removing the device from power management and monitoring, you cannot readd the device to the Power Management feature when logged in as a Device Manager user.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. Click the **Individual Devices** tab.
The **Individual Devices** tab is displayed.
3. Select the devices that you want to remove and click **Remove Device(s)**.
The **Remove Device** confirmation window is displayed.
4. To confirm removal, click **Remove**.
The devices are removed.

NOTE: For PowerEdge servers 14G and later with OpenManage Enterprise Advanced or Advanced+ license, the devices continue to be monitored for power even though they are removed because they are associated with the system and workload profile groups.

Add static groups for power management and monitoring

To collect and monitor custom static group data, add the groups for power management and monitoring.

Prerequisites

Ensure that the following prerequisites are met:

- Static groups are created in OpenManage Enterprise.
- The servers that are part of a group must have an OpenManage Enterprise Advanced or Advanced+ license.
- Modular servers that are part of the group are not in a **Proxied** state in OpenManage Enterprise.
- It is recommended that each group contains less than or equal to 40 devices.
- The maximum number of groups that you can add for power management and monitoring is 500.
- The maximum level of group nesting is 5.

About this task

NOTE: Query groups that are created in OpenManage Enterprise are not supported for power management and monitoring.

NOTE: After you add a group for power management and monitoring, only devices that are compatible for power management and monitoring are added as part of the group. Hence, the data is collected only for these devices in a group. For example, if a group you have added for power management and monitoring consists of five devices, but only three devices have valid licenses, only three devices are added as part of the group.

NOTE: If a device discovered through in-band method (operating system) or a compute without OpenManage Enterprise Advanced or Advanced license is added to a device group monitored by Power Management, and later out-of-band discovery is performed or required license is deployed, the device will automatically start monitoring metrics within 12 hours and contribute to group level metrics.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. On the **Static Groups** tab, click **Add Group(s)**.
The **Add Groups to Power Management** page is displayed.
3. On the left pane, select a group from the **Static Groups** category and click **Add Selected**.
The groups added for power management and monitoring are displayed on the **Groups** page along with the total count of groups added.

All the individual devices and devices that are part of the selected group are added and are displayed on the **All Monitored Devices** tab along with the total count of devices.

Results

If you have created static groups and added devices to OpenManage Enterprise groups, the total number of servers available in the groups is displayed as zero, after adding the groups for power management and monitoring. Hence, click the **Refresh Power Management** option on the **Power Managed Devices** tab after running an inventory in OpenManage Enterprise.

Remove groups

To stop monitoring the groups, remove them from power management and monitoring.

Prerequisites

Ensure that the following prerequisite is met:

- The Emergency Power Reduction (EPR) option is not enabled on the specific devices that are part of the group.

About this task

To remove a group, perform the following steps:

NOTE: If a group or a specific device in a group is removed from OpenManage Enterprise, then the changes are automatically reflected in Power Management.

NOTE: After you apply a policy to a group, if you delete the group, the policy is also removed from power management and monitoring.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. Click the **Static Groups** tab.
The **Static Groups** tab is displayed.
3. Select the groups and click **Remove Group(s)**.
The **Remove Group** confirmation window is displayed.
4. To confirm the removal, click **Remove**.
The groups are removed from power management and monitoring.

Create physical groups through CSV file

Create physical groups and add devices to rack slots by importing new or existing physical group details through a CSV file.

About this task

Consider the following points before creating and importing the CSV file:

- Only Administrators can import the CSV files.
- The script checks if the devices are discovered in OpenManage Enterprise.
- Ensure that the physical group you are creating adheres to the hierarchy as follows:

Table 60. Supported hierarchy format

Physical group	Supported hierarchies
Data Center	Room, Aisle, Rack
Room	Aisle, Rack
Aisle	Rack
Rack	Not applicable

- When creating a rack in a physical group, ensure that you provide the rack name, power capacity of the rack, and space capacity of the rack.
- A unique name is used to identify each physical group and their siblings in a physical group hierarchy.
- To add a device in the physical group:
 - Ensure that only one device detail is entered in each row. A unique identifier is used to identify a device. The identical devices are ignored while importing, and only the unique devices are added in a rack slot.
 - To place the device in a particular slot, ensure that you provide the rack slot information.
- When you are considering multiple device allocations on the same physical group hierarchy, you can duplicate the fields. However, only the rack slot and device identifier are unique fields.
- View details about the import job by selecting the **Physical Group CSV Import Task** job on the **Jobs** page. You can view the status about each row that is added in the file on the **Execution Details** page.
- Only valid group data from the CSV file is considered for group creation and device placement. Groups with invalid or incomplete data are not considered during processing.
- If no valid groups are identified, an empty message is displayed indicating there is nothing to validate.
- If at least one group is valid, the job is successful, and the job status is displayed as success.
- If a group has valid data but an issue is identified during the creation, a message about the issue is displayed.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. Click **Physical Groups** and then click **Import**.
The **Import physical groups from CSV file** page is displayed.
3. Optional: To view the format of the CSV file, click **Download sample file**.
A sample CSV file is downloaded which you can use as a reference for adding the group information.
4. To upload the CSV file and create the physical groups, click **Import CSV file**.
The groups are created successfully after importing the CSV file for valid entries.

Virtual machines

Discovery feature discovers the hypervisors hosting virtual machines (VM) along with host servers. The virtual machines are listed in **Guest Information** section in OpenManage Enterprise. After servers are added for power management and monitoring, the required hypervisor settings are automatically enabled to retrieve data that is related to virtual machines from the servers and the virtual machines are listed on the **Power Managed Devices** tab.

Hypervisors do not directly provide the power and energy consumption details of the VMs. Hence, OpenManage Enterprise collects the CPU usage data for each VM in the host and calculates approximately the power and energy consumption of servers to the individual VMs in the host. Use this feature to view resource consumption of each VM and to monitor and manage the servers hosting the VMs.

Information of VMs hosted on Hyper-V hypervisors is visible only if the host is discovered in OpenManage Enterprise using credentials having administrator privilege. For ESXi hypervisors, VM information is visible even for hosts discovered using credentials having read-only privilege.

A VM is identified using a unique identifier, UUID for each VM. The list of VMs and their information is refreshed with each metric collection. If a new VM is created, or deleted, this information is reviewed in the next cycle. If the VM is migrated to another server, and if this new server is added for power management and monitoring, the VM is identified using the UUID and the metrics collection continues for the VM. In case the UUIDs do not match and the VM is detected as a new VM, OpenManage Enterprise collects the data as a new VM.

A VM cannot be added or removed manually from OpenManage Enterprise. Only if the host server is added for power management and monitoring, the VMs are automatically added for power management and monitoring. And, if the host server is removed from power management and monitoring or deleted from OpenManage Enterprise, the VM is automatically removed for power management and monitoring.

View virtual machines and virtual machine groups

View all the virtual machines (VM) added for power management and monitoring.

Prerequisites

Before viewing the virtual machines, ensure the following:

- The server (iDRAC) and the hypervisor (host operating system) are discovered in OpenManage Enterprise.
- The correlation of the discovered server and the hypervisor is successful.
- The credentials provided to discover the hypervisor have Administrator privileges.
- The server is added for power management and monitoring.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, and a group G1 is assigned to the Device Manager DM1 user, you can view only the virtual machines that the devices host in the G1 group.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. To view virtual machines monitored for power management and monitoring, expand the Virtual Machines section in the left pane.
3. To view all VMs added for power management and monitoring, click **All Virtual Machines**.
A section with all the VM details is displayed on the right pane.
4. To view the power, virtual machine energy, total facility energy, overhead energy, and associated cost of a VM, click **View Metrics**.
The power metrics of a VM are displayed.
5. To change the duration, expand and select the required duration from the **Duration** drop-down menu.
Hover your mouse pointer over the graph to view the device and VM power at a certain time. For an enlarged view of a graph, select a section of the graph to zoom.
6. To view the latest metrics, click the refresh icon.
7. To view VMs in VM groups, click a group name.
8. To view power, virtual machine energy, total facility energy, overhead energy, and associated cost of groups, right-click a VM group name and click **View Metrics**.
The power that is displayed is the sum of the power that is consumed by the VMs in the group.

Next steps

After you migrate VMs from source to target server, if you create a VM on the source server, then the same UUID that was allotted to the migrated VM may get assigned to the new VM. If both the source and target servers are monitored, you may not see the VMs displayed in the All Virtual machines section. To view and monitor all the VMs hosted on servers that are power managed and monitored, check and delete the VMs with conflicting UUIDs.

To view the UUIDs of VMs, perform the following steps:

1. Start OpenManage Enterprise and click **Devices**.
2. Click a device name. The device **Overview** page is displayed.
3. Click the **Hardware** tab and then click **Guest Information**. The VM guest information is displayed.

Create virtual machine groups

Create new virtual machine (VM) group on **Power Managed Devices** page to monitor power consumed by VMs in a group.

About this task

Every group lists the VMs that are added to the group. However, a parent group lists all the VMs added in child groups. It is recommended to create a maximum of five child groups.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. Right-click **Virtual Machine Groups** and click **Create Group**.
Create Virtual Machine Group wizard is displayed.
3. Enter a group name and description. From the drop-down menu, select a parent group.
4. Click **Next**.
5. Select VMs and click **Finish**.

To view the selected VMs, click the **Selected Virtual Machines** tab.

You can add a VM to multiple groups.

Edit virtual machine groups

Edit an existing virtual machine group.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. Expand **Virtual Machine Groups**.
3. Right-click a virtual machine group and click **Edit Group**.
Update Virtual Machine Group wizard is displayed.
4. Make the changes and click **Next**.
5. Add or remove VMs from the group and click **Finish**.

You can remove VMs only from the group where this VM is originally added. For example, If VM1 is added to G1, VM1 can be removed only from G1.

Delete virtual machine groups

Delete virtual machine groups that are no longer required.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices** tab.
2. Expand **Virtual Machine Groups**.
3. Right-click a virtual machine group and click **Delete Group**.
4. To confirm, click **Yes**.

View details of Unmonitored Devices

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view the unmonitored devices that are part of the group in your scope.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices > UNMONITORED > Unmonitored Devices** tab.
2. After you add the unmonitored devices in a physical group under a rack, the location and rack slot columns are populated for this device. To view the devices associated with an unmonitored chassis, click the value under the **ASSOCIATED DEVICES** column for the corresponding chassis.

Add unmonitored device details

Unmonitored devices are user-defined or noncompatible devices that must be considered for accurate rack management. The unmonitored devices are not monitored for power capabilities such as power, thermal monitoring, power policy and EPR, and alert thresholds.

About this task

Add the information of the unmonitored devices for power management and monitoring to replicate the physical group hierarchy present in your data center and manage the racks.

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can only view and cannot edit the unmonitored devices information that is part of the group in Device Manager DM1 user scope.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices > UNMONITORED > Unmonitored Devices** tab.
2. To add the Unmonitored Devices, click **Add**.
The **Add Unmonitored Devices** page is displayed. An unmonitored chassis is automatically added or deleted from this page when a half-width compute sled is discovered or removed.
You cannot perform any operations—add, edit, or delete—on an unmonitored chassis.
3. Provide the device details and click **Finish**.
For information about each field, see the following table.

Table 61. Details for Unmonitored Devices

Field	Description	Mandatory	Value Ranges
Device Name	Provide a unique device name.	Yes	Combination of characters, special characters, and numbers. Limit: 1–255 characters
Description	Provide brief information about the device that you are adding.	No	Combination of characters, special characters, and numbers. Limit: 0–255 characters
Hostname	Provide a hostname.	No	Combination of characters, special characters, and

Table 61. Details for Unmonitored Devices (continued)

Field	Description	Mandatory	Value Ranges
			numbers. Limit: 1–255 characters
Identifier	Provide a unique identifier for the device.	Yes	Combination of characters, special characters, and numbers. Limit: 1–255 characters
Model	Provide the model name.	No	Combination of characters, special characters, and numbers. Limit: 0–255 characters
Size of Device (U)	Provide the space occupied on the rack.	Yes	Numbers only. Limit: 1-80
Estimated Max Power (W)	Provide the defined maximum power that the device can consume.	No	Numbers only. Limit: 1–629365631

Edit Unmonitored Devices details

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can only view and cannot edit the unmonitored devices information that is part of the group in Device Manager DM1 user scope.

To edit the details of a device, perform the following steps:

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices > UNMONITORED > Unmonitored Devices** tab.
2. Select a device and click **Edit**.
For information about the values of fields, see the **Details for Unmonitored Devices** table in [Add Unmonitored Devices details](#).
3. Provide the data and click **Finish**.

Delete Unmonitored Devices

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can only view and cannot edit the unmonitored devices information that is part of the group in Device Manager DM1 user scope.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Power Managed Devices > UNMONITORED > Unmonitored Devices** tab.
2. Select the devices and click **Delete**.
3. In the confirmation screen, click **Yes**.

Policies

The Power Management feature supports two types of policies that you can use to monitor the power and temperature of your data center devices.

Static policy

A static policy contains various settings that help regulate the power consumption of a specific device or a group. A power management policy is useful in different situations. For example, you can create a policy to:

- Ensure that power consumption does not exceed the capacity of the circuit.
- Schedule power usage according to the workload of the device or group. For example, to reduce the overall power use in your data center, apply an aggressive power cap policy when the workload is low.
- Increase rack density. For example, to increase the rack density or number of devices in a group you can set a power cap limit at a group level and add more servers. The policy cap keeps the power within the defined limit.

Temperature-triggered policy

If the cooling infrastructure does not work, a temperature-triggered policy is used to prevent damage to devices due to overheating. It limits the processing capability of the devices in the group, hence reducing the heat generation. The policy helps in maintaining the data center temperature to align to the standards defined by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). Create a temperature-triggered policy on a group of devices by defining a temperature threshold value. After defining the threshold value and enabling the policy, if the average inlet temperature of the group crosses the temperature threshold value, EPR—Throttle on the group—is enabled. On the EPR page, the source of EPR is displayed as Temperature-triggered—Throttle on the group.

NOTE: Temperature-triggered policies are applicable only for groups, and only one temperature-triggered policy is supported for a group.

NOTE: After applying a policy on a group, if you add more devices to the group and the power consumption exceeds the power cap limit, then you receive alerts in **Alert Log** with the recommended action.

In a multiple policies scenario, an active policy with a power cap limit of 1000 Watts is applied on a device, and then another active policy with a power cap limit of 1500 Watts is applied on the same device, the policy with power cap limit of 1000 Watts is applied on the device as this policy is the most restrictive policy.

Create static or temperature-triggered policy

Create a static policy to limit the power consumption for devices and groups or apply EPR on devices in a group when the average inlet temperature exceeds the temperature threshold.

Prerequisites

Ensure that the following prerequisites are met:

- Devices or groups are added for power management and monitoring.
- Devices are PowerEdge servers because this feature is not supported on non-Dell servers.
- Servers have the iDRAC and OpenManage Enterprise Advanced or Advanced+ licenses.
 - If a device is a PowerEdge VRTX or PowerEdge FX2 chassis, it has a Chassis Management Controller (CMC) Enterprise license.

About this task

NOTE: If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can create policies on devices and groups that are in the Device Manager DM1 user scope.

When Device Manager users have common groups or devices in their scope, Device Manager DM1 user creates a policy on any of these groups or devices:

- All the policies that are created by Device Manager DM1 user are not listed for other Device Manager users.
- If the Device Manager DM1 user creates a temperature-triggered policy on a group, the Device Manager DM2 user cannot create a temperature-triggered policy on the same group since only one temperature-triggered policy is supported on a group. And, the temperature-triggered policy is not visible or listed for Device Manager DM2 user. If the Device Manager DM2 user has to create a temperature-triggered policy on this group, ensure that the DM1 user, or the Administrator deletes the existing temperature-triggered policy.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Policies** tab.

2. Click **Create**.

The **Create Policy** wizard is displayed.

3. In the **General** section, provide the following information and click **Next**.

a. In **Type**, select the type of policy.

- **Static policy**—Applies a cap on the power consumption of a device or group.
- **Temperature-triggered policy**—Applies Emergency Power Reduction (EPR) on a group of devices when its temperature equals or exceeds a specified value.

 **NOTE:** After a policy is created, you cannot change the type of policy.

The **Enable** option is selected by default for activating the policy after creation.

When a policy is activated, an alert is generated for power policy—warning—and temperature-triggered policy—critical.

b. Provide a policy name and description.

4. In the **Devices/Groups** section, select the required option:

- To add a device:

a. Select the **Device** option and click **Select Device**.

The **Select Device** page is displayed.

b. Click **Advanced Filters**.

The following filters are displayed:

- **Health State**
- **Power State**
- **Connection State**
- **Name**
- **Identifier**
- **Model**
- **Type**
- **Managed State**
- **Part of Group**

c. Select the device, and click **OK**.

- To add a group:

a. Select the **Group** option and click **Select Group**.

The **Select Group** page is displayed.

b. Click **Advanced Filters**.

The following filters are displayed:

- **Name**
- **Type**

c. To clear the filters, click **Clear All filters**.

d. Select the group and click **OK**.

 **NOTE:** You can select only one device or group when creating a policy.

 **NOTE:** After you create a policy for a device, you cannot apply the policy to a group. Similarly, after creating a policy for a group, you cannot apply the policy to a device.

5. Click **Next**.

6. For a static policy:

In the **Settings** section, provide the **Power cap Limit**, and then click **Next**.

Use the **Power Data** section as a reference to set the power cap limit.

- **Power Data** for a device—displays minimum, average, and maximum power consumption with the lower and upper bound values. The values change as you change the duration.
- **Power Data** for a group—displays minimum, average, and maximum power consumption with lower and upper bound values. The minimum, average, and maximum power history of the group is the sum of all the minimum, average, and maximum power consumption of individual devices in the group. The values change as you change the duration. The upper and lower bound value for a group is the sum of upper bound and lower bound values for all devices part of the group. The **Power Cap Limit** displayed is the sum of all the power cap values of the devices in the group.

The power cap violation is measured against the maximum power consumption.

Guidance for providing a power cap limit:

- The default **Power Cap Limit** displayed is the upper bound value of the device. You can change the **Power Cap Limit** value, and the **Power Cap Limit** percentage gets populated automatically.
- If you change the percentage of **Power Cap Limit**, the **Power Cap Limit** value gets populated automatically.
- For groups, provide the power cap limit or percentage of consumption at the group level or at every device level.
- Provide the power cap limit that ranges between the lower and upper bounds of the device.

NOTE: For the following list of PowerEdge servers, the **Lower Bound** and **Upper Bound** threshold range values are always static.

Table 62. Power cap range for servers

Generation of servers	Models	Value Range (Watts)
14 th generation	• PowerEdge XE7440 • PowerEdge XE7420 • VxRail G560 • VxRail G560F • PowerEdge C6420 • PowerEdge R6415 • PowerEdge R7415 • PowerEdge R7425	Zero to 32767

For a temperature-triggered policy:

In the **Settings** section, select or provide the **Temperature Threshold** value, and then click **Next**.

Use the **Temperature data** section as a reference to set the temperature threshold value. Based on your selection of the **Duration** value, the temperature summary details are displayed.

- The values change as you change the duration.
- Select your preferred American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) temperature threshold from the **Temperature Threshold** drop-down menu. Based on your ASHRAE class selection, the temperature value is populated. Select the ASHRAE standard relevant in your region or provide a custom value in Celsius only.
 - **ASHRAE Class H1 Recommended: 22°C (71.6°F)**
 - **ASHRAE Class H1 Allowable: 25°C (77°F)**
 - **ASHRAE Recommended: 27°C (81°F)**
 - **ASHRAE Class A1 Allowable: 32°C (90°F)**
 - **ASHRAE Class A2 Allowable: 35°C (95°F)**
 - **ASHRAE Class A3 Allowable: 40°C (104°F)**
 - **ASHRAE Class A4 Allowable: 45°C (113°F)**
- You can also provide a custom temperature threshold value.

7. In the **Schedule** section, provide the following information and click **Next**.

You can create and apply multiple policies on a specific device or group. In any instance, if multiple policies are active on a device, either by policies set on the device or by policies set on the group the device is a part of, the most restrictive power cap among the policies is applied on the device.

- a. For the **Time Span** option, select **Always** for the policy to be active from the time of creation. If the policy does not have to be active always when enabled, click **Range** and provide a time range during which the policy must be active when it is enabled.
- b. For the **Day(s)** option, select **Always** for the policy to be active from the time of creation. If the policy does not have to be active always when enabled, click **Daily**, to select specific days on which the policy must be active when it is enabled.

c. For the **Active Date** option, select the date range during which the policy must be active when enabled.

i **NOTE:** A temperature-triggered policy cannot be scheduled.

8. In the **Summary** section, view the policy details and click **Finish**.

The policy is created successfully.

The following table provides more information about all the fields in the policy wizard.

Table 63. Policy wizard details

Field	Mandatory	Value Range
Type	Yes. By default, the type is selected as Static .	• Static policy • Temperature-triggered policy
Name	Yes	Combination of characters, special characters, and numbers. Limit: 1–255 characters
Description	No	Combination of characters, special characters, and numbers. Limit: 0–255 characters
Enable	No. By default, the check box is selected.	• Select • Clear
Duration	Yes. By default, the time period is selected as 1 Day .	• 1 Day • 7 Days • 1 Month • 3 Months
For static policy		
Power cap Limit	Yes. By default, the power cap is populated with the Upper Bound value and a hundred percent.	Recommended limit: Lower Bound-Upper Bound
Time Span	Yes. By default, the option is selected as Always .	Range Limit: 12 hours format
Day(s)	Yes. By default, the option is selected as Always .	Daily Select at least one day.
Active Date	Yes. By default, the option is selected as Always .	Range • From • To Limit: Current and future dates
For temperature-triggered policy		
Temperature Threshold	Yes. By default, the option that is selected is ASHRAE Recommended .	• Custom value range: -10 to 60 degrees • ASHRAE Recommended • ASHRAE Class A1 • ASHRAE Class A2 • ASHRAE Class A3 • ASHRAE Class A4 • ASHRAE Class H1

View policy

View all the policies that are created for devices and groups.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view only the policies that are created by Device Manager DM1 user and apply these policies only on the groups in the Device Manager DM1 user scope. However, the Administrator has access to all the policies created by all the Device Manager users.

Steps

1. To view all the policies created using the Power Management feature:
 - Click **Power Management > Policies**. The **Policies** tab is displayed.
 - Select your category of filters, and view the data. The following is a list of categories available:
 - **State**—Filters the policies that are based on the state of the policy. The supported filters are **All**, **Enabled**, **Disabled**.
 - **Name**—Filters the policies that are based on the name of the policy.
 - **Description**—Filters the policies that are based on the description of the policy.
 - **Type**—Filters the policies that are based on the type of policy. The supported filters are, **All**, **Static**, and **Temperature-Triggered**.
 - **Assigned To**—Filters policies that are based on the device or group it is assigned to.
 - **User**—Filters based on user groups.
 - To filter and view the data, click **Advanced Filters**.
 - To clear the filters, click **Clear All filters**.
 - To sort any column alphabetically, click a column name so that an arrow is displayed with the column name.
2. To view all the policies created for a device—Click **Devices > Monitoring Metrics > Policies**. All the policies applied to the device are displayed with the details.
3. To view all the policies created for a group—click **Devices**, click a custom group with static membership, click **Group Details**, and then click **Policies**. The policies applied to the group are displayed with the details.

Edit policy

Update a policy based on the changes in power consumption history or average inlet temperature that is generated by the devices or groups.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can edit only the policies that are created by a Device Manager DM1 user.

When there are changes to group membership and the group has an active policy, then you are notified to reevaluate the policy associated with the group.

 **NOTE:** After you create a policy for a device, you cannot apply the policy to a group. Similarly, after creating a policy for a group, you cannot apply the policy to a device.

 **NOTE:** For a temperature-triggered policy, if the temperature threshold value is increased after the EPR is applied, then Power Management automatically removes the EPR if the updated temperature threshold value is greater than the average temperature of the group.

To edit a policy, perform the following steps:

Steps

1. Start OpenManage Enterprise and click the **Power Management > Policies** tab.

2. Select a policy and click **Edit**.
The power policy wizard is displayed.
For more information about each field in the wizard, see [Create power or temperature-triggered policy](#).
3. To save your changes, click **Finish**.
The changes are saved successfully.

Disable policy

To remove power consumption or temperature policy limits, disable the relevant policy.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can disable only the policies that are created by a Device Manager DM1 user.

To disable a policy, perform one of the following steps:

Steps

1. Start OpenManage Enterprise and click the **Power Management > Policies** tab.
2. Perform one of the following methods:
 - a. Select the policy that you want to disable, and click **Disable**.
 - b. In the confirmation window, click **Yes**.OR
 - a. Select the policy that you want to disable, and click **Edit**. The Create Policy wizard is displayed.
 - b. In the **General** section, clear the **Enable** check-box and click **Next** until you reach the **Summary** section, and then click **Finish**. The policy is successfully disabled.

Enable policy

On enabling a policy, the power or temperature cap is activated on the devices and groups.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can enable only the policies that are created by a Device Manager DM1 user.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Policies** tab.
2. Enable a policy using one of the following methods:
 - Select the policy that you want to enable, and click **Enable**.
 - At the time of creation or when editing the policy, select the **Enable** option from **Create Power Policy** wizard.
3. In the confirmation window, click **Yes**.
The policy is enabled successfully, and a tick mark is displayed against the policy.

Delete policy

Delete policies that are no longer required.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can delete only the policies that are created by the Device Manager DM1 user.

When an active policy is deleted, any power consumption restrictions or temperature thresholds that are applied by the policy are also deleted.

 **NOTE:** If you delete an active temperature-triggered policy, the Emergency Power Reduction (EPR) is automatically removed from the group.

Steps

1. Start OpenManage Enterprise and click the **Power Management > Policies** tab.
2. Select a policy that you want to delete, and click **Delete**.
3. In the confirmation window, click **Yes**.
The policy is deleted successfully.

Manage data center during power reduction

The Emergency Power Reduction (EPR) feature helps reduce power consumption of devices immediately during a power emergency. For example, if a power failure occurs and your devices are running on a UPS, apply EPR to reduce the power consumption of your managed devices.

EPR also helps in preventing device damage due to overheating in an event of cooling infrastructure failure. Use temperature-triggered policies for enabling EPR on a group of devices when its average inlet temperature crosses a defined threshold value.

 **NOTE:** Applying EPR on the devices throttles down the power to a low level, impacting performance, or shuts down the devices completely. All devices on which an EPR is applied are affected. Use this feature only in an emergency situation.

This feature is not supported on non-Dell servers.

Following are the EPR options available for servers, chassis, and groups:

- **Throttle**—Set to a minimal power consumption state

 **NOTE:** Only the **Throttle** option is supported for a chassis.

- **Shut down**—Shut down the server

When EPR is applied on devices and groups, they are marked as **EPR Enabled (Throttle)** or **EPR Enabled (Shut down)** on the **Power Managed Devices** tab. The summary of devices and groups on which EPR is applied is displayed on the **Emergency Power Reduction** tab in **Power Management**.

Enable Emergency Power Reduction

During a power shortage, enable the Emergency Power Reduction (EPR) on devices so that they run on minimal power.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager, you can enable EPR on a device or group that is defined in the Device Manager user scope. And, only the Device Manager DM1 user or the Administrator can disable the EPR, if it is applied manually.

When Device Manager users have common groups or devices in their scope, and Device Manager DM1 user applies EPR on any of these groups or devices:

- Other Device Manager users, administrators, and viewers can see the red color banner. However, the active EPR is listed on **Emergency Power Reduction** and **Policies and EPR** tabs only for Device Manager DM1 user and not for any other Device Manager users since it is not a shared resource.
- If temperature-triggered EPR is applied on a group or device, due to a temperature-triggered policy created by Device Manager DM1 user, then all the other Device Manager users can see the red color banner with the source of EPR.

NOTE:

- Temperature-triggered EPR cannot be activated manually. When a temperature-triggered policy is active and the group temperature is equal to or exceeds the threshold value, Power Management automatically applies the EPR.
- LCS Event-triggered EPR cannot be activated manually. When a leak alert is generated from the device, EPR is applied. EPR is deactivated automatically when the event is rectified. However, an administrator can manually deactivate the EPR .

:

Steps

1. From OpenManage Enterprise, perform one of the following steps:
 - For a device:
 - a. Click the **Devices** tab. All the devices that are discovered in OpenManage Enterprise are displayed.
 - b. From the list of devices, click a device name. The details of the device are displayed on the **Overview** page.
 - c. To view power-related information, click the **Monitoring Metrics** tab.
 - For a static group:
 - a. Click **Devices > Static Groups > Group name**. All the devices that are part of the static group are displayed.
 - b. To view group information, click **Group Details**.
 - For a physical group, perform one of the following steps:
 - a. Click **Devices > Physical Hierarchy > Group name**. All the devices that are part of the physical group are displayed.
 - b. To view group information, click **Group Details**. To view the rack groups, click **Rack Details**.
 - a. Or, launch OpenManage Enterprise, and then click **Power Management > Rack View**. The **Rack View** tab is displayed. Optional: To filter and view the data, expand the Advanced Filters option. The following is a list of categories available:
 - **Group Name**
 - **Health State**
 - **Power State**
 - **Connection State**
 - **Type**Select the categories of your choice and view the filtered data.
 - b. Click the device name or IP address.
2. To enable EPR, click the **Policies and EPR** tab, and then click **Apply EPR**.
In the confirmation screen, select one of the options and click **Apply EPR**.
 - **Throttle**—All selected devices and groups are allowed to consume an extremely low level of power. This setting affects performance.

NOTE: The throttle option is supported for servers with iDRAC DC or iDRAC Enterprise licenses and chassis.

 - **Shut down**—All selected devices or devices part of the selected group are shut down gracefully. If graceful shutdown is unsuccessful, force shutdown is applied if it is configured in **Settings**.

NOTE: If a group consists of servers and chassis, and you select the **Shut down** option, then only the servers in the group are shut down. The shut-down option applies only to servers.
3. Click **Yes** on the confirmation screen.
EPR is enabled on the selected device or group. A red color bar indicator is displayed on the **Policies and EPR** tab along with the type of EPR option applied.

View active Emergency Power Reduction

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

If you are logging in as a Device Manager DM1 user, you can view only the EPRs applied by DM1 on the assigned devices and groups.

When Device Manager users have common groups or devices in their scope, and Device Manager DM1 user applies EPR on any of these groups or devices:

To view the list of devices and groups to which Emergency Power Reduction (EPR) is applied, perform the following:

Steps

From OpenManage Enterprise, perform any of the following:

- To view an EPR applied on a device or a group, click **Devices > Device name > Monitoring Metrics > Policies and EPR**.
- To view EPRs applied on all devices and groups in Power Management:

a. Click **Power Management > Emergency Power Reduction**.

The following fields are displayed:

- **ASSIGNED TO**—Device name or service tag to which the EPR is applied.
- **ENTITY TYPE**—Specifies the type of the device and the supported entity types are, devices, and groups.
- **EPR TYPE**—Type of EPR applied. The EPR types are **Throttle** and **Shut down**.
- **EPR SOURCE**—Specifies the source of an EPR trigger. You can apply an EPR manually or automatically.
- **CREATED ON**—Time the EPR was applied.

b. To filter and view the data, click **Advanced Filters**.

You can filter your data using the following components:

- **Assigned To**—Filters the EPRs based on the device name or service tag.
- **EPR Source**—Filters the EPR source. The supported filters are **All**, **Manual**, **Temperature-triggered**, **LCS Event**.

 **NOTE:** An EPR activated because of an LCS Event is deactivated automatically when the event is rectified. An administrator can also manually deactivate an EPR.

c. To sort any column alphabetically, click a column name so that an arrow is displayed with the column name.

Disable Emergency Power Reduction

To restore the devices or groups to their normal state, disable the Emergency Power Reduction (EPR).

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1, you can disable only the EPRs that DM1 has applied, and on the devices and groups that DM1 has access to.

 **NOTE:**

- An EPR activated because of a temperature-triggered event cannot be disabled manually. After the temperature reduces to the normal value, EPR is automatically removed.
- Enable the **Staggered EPR Removal** setting to stagger the powering on of devices when EPR is disabled. For more information about the setting, see [Set preferences](#).

Steps

1. Start OpenManage Enterprise and click the **Power Management > Emergency Power Reduction** tab.
2. Select the devices or groups, and click **Disable**.

On the confirmation page, click **Yes**.

EPR is disabled successfully.

View racks of physical groups

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view only the devices from groups that are assigned to a Device Manager DM1 user in rack view.

Steps

1. Start OpenManage Enterprise, and then click **Power Management > Rack View**.

Optional: To filter and view the data, expand the **Advanced Filters** option. The following is a list of categories available:

- **Group Name**
- **Health State**
- **Power State**
- **Connection State**
- **Type**

Select the categories of your choice and view the filtered data.

2. To view the **Monitoring Metrics** details of a device that is monitored for power, click the device name.

 **NOTE:** Some devices that are part of a physical group do not have a link because the device is not Power Management capable.

The **Monitoring Metrics** details for the device are displayed.

3. To manage racks, view group details, and create policies, click the vertical ellipses for each rack, and select the appropriate option.

Compare server usage metrics

Compare the usage metrics—CPU, I/O, memory bandwidth, and system usage—of a maximum of four servers.

About this task

The metric usage is displayed as a percentage based on the number of metric collection cycles for a specific time. For example, for a specific duration, CPU usage is between 0% and 10% based on three metric collection cycles.

This feature is not supported on non-Dell servers.

To view the graphs of the metrics, you have to do the following each time. The graphs are unavailable when you go to another page.

Steps

1. Start OpenManage Enterprise and click **Power Management > Analyze Usage Metrics**.

2. To add servers to view and compare the metric data, click **Add Servers**.

3. Select the servers for which you want to view and compare the metrics.

4. Click **Apply**.

The **Analyze Usage Metrics** page displays the server usage metric data. You can compare each of the metrics for a server and compare the metrics against different servers.

5. Optional: To change the duration, select an option from the **Duration** list.

Analyze multivariate metrics using parallel coordinates

Visualize multivariate device metrics in OpenManage Enterprise using a parallel coordinate graph. Analyze and evaluate complex and multidimensional time-series metrics.

Prerequisites

Ensure that the devices are added in the rack physical group.

About this task

All metrics are displayed as a vertical axis. For more information about the supported metrics, see [View metrics, and monitor devices and groups history](#).

Steps

1. In OpenManage Enterprise, click **Power Management > Analyze Multivariate Metrics**.
2. To add the groups for which you want to view the graphs, click **Add Groups**.
Only the rack physical groups are listed on this page. If there are no devices that are monitored in the rack, you cannot select the group.
3. Select a maximum of four groups and click **Apply**.
4. To set the parameters to view the graph, do the following:
 - Optional: To change the duration, select an option from the **Duration** list.
 - To set the smoothness of the graph, click, hold, and drag the button.
 - In the left pane under metric sources, the group and device—server and chassis—names are displayed. Search by a group or device name to view a particular device or group. Hover over a metric data—Date and timestamp—under the device name to view the metrics for that device on the graph.
 - To view the different measures of metric, in visual controls, select the summary statistics—**Min**, **Avg**, **Max**, and **Instant**.
 - To view the different metric types, select the appropriate metric.
 - On the graph, drag any metric name to rearrange the order.
 - To view a metric about a device, pause the pointer over the vertical axis corresponding to the attribute you want to measure. The pointer changes to a cross-wire symbol.
 - a. Click and hold the mouse button, and drag the cross-wire to select the date and time range.
 - b. Click the same vertical axis to remove the filter.
 - Optional: To refresh, remove the search, and remove the filtered data, click the refresh option.If a metric is not supported for a device, the plot for the unsupported metric is on the **Unsupported** axis.

Set preferences

The settings on the page enable you to collect data for the devices and groups added for power management and monitoring. Set the **Sampling Intervals** according to your data center recommendations and monitor your devices.

About this task

If you are logging in as a Device Manager, you can only view the preferences that an Administrator has configured in Power Management.

To set the units and sampling intervals, perform the following steps:

Steps

1. Launch OpenManage Enterprise, and then click **Power Management > Settings**.
The Settings tab is displayed.
2. Click **Edit**.
The **Edit Power Management Preferences** window is displayed.
3. To reset to the default value, click **Reset to Default > Yes**.
4. Select the values for the listed options, and then click **Apply**.

The following table provides more information about the attributes that are displayed in Power Management.

Table 64. Power Management Settings

Field	Description
Data Gathering	Enable this setting to collect metrics from the monitored devices periodically.
Data Gathering Interval	Select the frequency to collect data from devices or groups. Use your data center requirements such as network traffic, and criticality of data to set the data gathering interval. If the data gathering interval is 5 minutes, and when the number of devices: - Excluding VMs that are added for power management and monitoring exceeds 1000, the interval automatically changes to 15 minutes. You cannot return this 15 minutes setting to 5 minutes. - Including VMs exceeds 1000, the interval should be manually changed to 15 minutes. If the number of devices in PMP is less than 1000 but the device count exceeds 1000 in other plug-ins—discovered before or after PMP device discovery—and the data gathering interval is 5 minutes, the metric collection in PMP might not happen for the second and third 5 minute interval. Because the total number of devices exceeds 1000, metric collection might take more than 5 minutes. The metric graphs might have gaps at regular intervals, and the aggregations are not displayed.
Duration of top energy consumers	Select the duration to view the list of devices or groups that consume maximum energy on the OpenManage Enterprise dashboard for the selected duration. Only the top five energy consumers are displayed.
Report Duration	View data for the selected duration.
Aggregation Period	Select the frequency of the level of detailed information that has to be displayed in reports. NOTE: If you select a Report Duration other than 1 Day, the Aggregation Period is automatically set to 1 Day.
Delete Power Management data	Based on your data requirements, select one of the options: Yes—To delete configured alert thresholds and metric data that is collected from devices and groups when they are removed from power management and monitoring. No—To retain the configured alert thresholds and metric data that is collected from devices and groups when they are removed from power management and monitoring. NOTE: When you set Delete Power Management data to No and delete devices or groups, all power-related data for that device or group is removed from view but not deleted. When you add the device or group again, data for that device or group is available again.
Automatic Physical Hierarchy: Enable Automatic Physical Hierarchy Creation	If the location data is available on the device and the device is not part of any rack physical group, then after the discovery and inventory of the device, it is automatically placed in the physical hierarchy. To enable this setting, select Yes . Else, manually create the physical hierarchy or initiate the creation using the Automatically create physical hierarchy feature.

Table 64. Power Management Settings (continued)

Field	Description
Automatic Physical Hierarchy: Space Capacity	Select the rack height for automatic creation of physical groups. The location information of devices is automatically populated.
Automatic Physical Hierarchy: Power Capacity	Power capacity of racks.
Power Operations: Server Power On Delay	Set a delay for the Power On operation that is performed in a staggered and sequential approach among the servers in a rack.
Power Operations: Server Power Off Delay	Set a delay for the Power Off operation that is performed in a staggered and sequential approach among the servers in a rack.
Power Cap Threshold: Enable	Enable the setting to generate alerts for devices and groups when power consumption approaches the power cap limit that is defined in the policy.
Power Cap Threshold: Threshold	A value less than or equal to the power cap to generate alerts for devices and groups when power exceeds the threshold. The threshold violation is measured against the average power consumption.
Idle Server Detection: Threshold	Set the server utilization threshold.
Idle Server Detection: Scan Interval	A time interval to collect server utilization information.
Idle Server Detection: Utilization Percentile	The threshold value is compared with utilization percentile to determine the underutilized servers. Ensure that you do not: - Frequently modify the idle server detection parameters. A job is run for every 24 hours to update any change in the settings. - Use the iDRAC interface to modify the configurations. For example: Consider the default values for the threshold (20%), scan interval (240 hours), and utilization percentile (80%). If in the last 240 hours, the system utilization has been less than or equal to 20% for 80% of the time then a server is considered as idle.
Force shutdown: Enforce	Enable this setting to force shutdown devices when graceful shutdown fails while enabling EPR.
Staggered EPR Removal: Enforce	Enable staggering of device power-on capability when EPR is disabled to prevent a surge in power.
Staggered EPR Removal: Time Delay	Specify a time that would introduce a delay between devices to power on after EPR is disabled.
Flat Rate /kWh	Specify a fixed cost of energy consumed per kWh.
Power Usage Effectiveness (PUE)	A value that is a multiplier of the data center energy which estimates the cooling energy.
Currency	Select a currency that is used to calculate the energy-consumed cost.
Emission Conversion Factor	Set a factor to determine the carbon emissions for a unit of energy consumed.

NOTE: To delete the data after a specific duration, configure the **Data purge interval** option present in the following location: **OpenManage Enterprise > Application Settings > Console Preferences > Metrics Collection Settings**.

The following table provides further information about the mandatory fields and the value range for each field.

Table 65. Details about mandatory data intervals and duration

Field	Mandatory	Value Range
Power Unit	Yes, Watt is the default unit.	Watt and BTU/Hr
Temperature Unit	Yes, Celsius is the default unit.	Celsius and Fahrenheit
Data gathering	Yes, Default value: Yes	Yes and No
Data gathering interval	Yes. Default value: 5 minutes	5, 15, and 30 minutes
Duration of top energy consumers	Yes. Default value: 3 Months	1 Day, 7 Days, 15 Days, 1 Month, 3 Months, 6 Months, and 1 Year
Report Duration	Yes. Default value: 3 Months	1 Day, 7 Days, 15 Days, 1 Month, 3 Months, 6 Months, and 1 Year
Aggregation Period	Yes. Default value: 1 Day	One Day and One Hour
Delete Power Management data	Yes. Default value: No	Yes and No
Automatic Physical Hierarchy: Enable Automatic Physical Hierarchy Creation	Yes. Default value: Yes	Yes and No
Automatic Physical Hierarchy: Space Capacity	Yes. Default value: 48 U Size	1-80 U
Automatic Physical Hierarchy: Power Capacity	Yes. Default value: 7000 Watt	1-629365631
Power Operations: Server Power On Delay	Yes. Default value: 2 Seconds	1-30 seconds
Power Operations: Server Power Off Delay	Yes. Default value: 2 Seconds	1-30 seconds
Power Cap Threshold: Enable	Yes. Default value: No	Yes and No
Power Cap Threshold: Threshold	Yes. Default value: 0 %	0% to 30%
Idle Server Detection: Threshold	Yes. Default value: 20 %	0% to 50%
Idle Server Detection: Scan Interval	Yes. Default value: 240 Hours	48 hours through 9000 hours
Idle Server Detection: Utilization Percentile	Yes. Default value: 80 %	80% to 100%
Force shutdown: Enforce	Yes. Default value: No	Yes and No
Staggered EPR Removal: Enforce	Yes. Default value: Yes	Yes and No
Staggered EPR Removal: Time Delay	Yes. Default value: 5 Seconds	5 s–20 s
Flat Rate /kWh	Yes. Default value: 0	0–629365631
Power Usage Effectiveness (PUE)	Yes. Default value: 1.5	1–629365631
Currency	Yes. Default value: US Dollar (USD)	US Dollar (USD), Canadian Dollar (CAD), Australian Dollar (AUD), Pound (GBP), Euro (EUR), Japanese Yen (JPY), Chinese Yuan (CHY), and Hong Kong Dollar (HKD)
Emission Conversion Factor	Yes. Default value as per the U.S. Environmental Protection Agency: 0.3865 kgCO ₂ e/kWh	0–1

View metrics, and monitor devices and groups history

View the visual representation of the data that is collected for all devices and groups that are added for power management and monitoring.

Prerequisites

Ensure that the devices or groups are added for power management and monitoring. For more information, see [Adding devices for power management and monitoring](#) and [Adding groups for power management and monitoring](#)

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, as a Device Manager DM1 user, you can view the device metrics only for the groups and devices in the Device Manager DM1 user scope.

Steps

1. From OpenManage Enterprise, perform one of the following steps:
 - For a device:
 - a. Click the **Devices** tab. All the devices that are discovered in OpenManage Enterprise are displayed.
 - b. From the list of devices, click a device name. The details of the device are displayed on the **Overview** page.
 - c. To view power-related information, click the **Monitoring Metrics** tab.
 - For a static group:
 - a. Click **Devices > Static Groups > Group name**. All the devices that are part of the static group are displayed.
 - b. To view group information, click **Group Details**.
 - For a physical group, perform one of the following steps:
 - a. Click **Devices > Physical Hierarchy > Group name**. All the devices that are part of the physical group are displayed.
 - b. To view group information, click **Group Details**. To view the rack groups, click **Rack Details**.
 - a. Or, launch OpenManage Enterprise, and then click **Power Management > Rack View**. The **Rack View** tab is displayed. Optional: To filter and view the data, expand the Advanced Filters option. The following is a list of categories available:
 - **Group Name**
 - **Health State**
 - **Power State**
 - **Connection State**
 - **Type**Select the categories of your choice and view the filtered data.
2. If the device location data in OpenManage Enterprise and the device is inconsistent, a message is displayed for devices and physical groups. Click **Update Device Location** and do the following.

This feature is not supported on non-Dell servers.

 **NOTE:** Before updating the location for FX2s and VRTX chassis, ensure that you provide the complete hierarchy information.

 - Select the devices.
 - Click **Update Location**.

If the update is unsuccessful, a warning alert is generated.
3. Optional: When you upgrade to Power Manager 3.5 and OpenManage Enterprise 4.5 and later, the half-width compute sleds added must be removed and the corresponding unmonitored chassis must be added to the Rack.
 - Click **Reconcile Rack**.
 - Select the unmonitored chassis, Rack, and slot number.
 - Click **Finish**.
4. View metrics and monitoring data in the **Metrics** tab.
 - For groups and PowerEdge servers that are based on AMD processors, only power, thermal, and system airflow information are displayed.

- For PowerEdge FX2 and PowerEdge FX2s chassis, view only the instant temperature .
- For non-Dell servers, view only the power—maximum, average, and minimum—and instant temperature.
- For groups, only the metrics of devices that are monitored for power are displayed.
- For the PDU group metrics, you can also view the instant PDU power.

For an enlarged view of a graph, select a section of the graph to zoom. For a simultaneous view of all the metrics at a specific time, hover over one of the graphs.

If the criteria are met and you still are not able to view power data, ensure that the **Server Power Monitoring** feature is enabled on the device you are discovering. To view the discovery log of a device:

- In OpenManage Enterprise, click **Monitor > Jobs**.
- Search for the discovery type job for the device and select the job.
- Click the **View Details** on the right side of the tab. Details about the job are displayed. In the **Messages:** section, check the status for the **Server Power Monitoring** feature.

 **NOTE:** If the **Server Power Monitoring** feature is disabled, the device is not compatible for power management.

The following metrics are displayed:

- Recent device metrics—Battery capacity, output state, and battery time remaining
 - Device metrics trend
 - Power
 - Thermal
 - System usage
 - Output energy
 - CPU utilization
 - Memory bandwidth utilization
 - I/O utilization
 - System airflow
 - Carbon emission
 - Values for the following are available only when the components are available on the monitored server:
 - Overall CPU power consumption
 - Overall memory power consumption
 - Fan power consumption
 - Storage power consumption
 - FPGA power consumption
 - Grid A current
 - Grid B current
 - System current
 - Total current
 - Overall GPU Usage
 - Overall GPU Memory Usage
 - Overall GPU Memory Bandwidth Usage
 - Overall GPU Board Temperature
 - Overall GPU Power Consumption
 - Recent virtual machine metrics—View the power and vCPU metrics of a maximum of five VMs that are available on the device.
 - Recent component metrics—View the power supply status, thermal alert state, power break state, and reset recommended state.
 - Component metrics trend
 - CPU—View the CPU thermal values.
 - Graphics Processing Unit (GPU)—View the GPU power consumption and temperature—primary and memory. For more information about the other metrics, see [Monitor GPU](#).
 - Power Supply Unit (PSU)—View the PSU current and thermal values.
- To download the metric graphs in various formats, click the following: **Download as PNG**, **Download as JPEG**, **Download as PDF**, **Download as CSV**, and **Download as XLS**.
 - To view the graphs in full screen, click **View in Full Screen**.
To exit the full-screen view, press **Esc** on the keyboard or click **Exit Full Screen**.
 - In **Energy Consumption Cost and Carbon Emission**, view the energy, cost, and carbon emission that are associated with the following:

- IT equipment—The devices in the data center.
- Total facility—Energy associated with the devices, lighting, cooling, and so on.
- Overhead—Difference of IT equipment energy and facility energy.

If the device or group is idle or running with less workload, then the energy consumption and carbon emission values report zero value for shorter intervals.

8. To change the duration, expand the metric and select a duration from the **Duration** drop-down menu. Hover your mouse pointer over the graph to view the maximum, average, and minimum values. For **Power**, view the power cap limit that is applied on the device by power policy or EPR for a specified duration.

The values are displayed according to the format that you have specified in the **Monitoring Units** and **Metric gathering interval** in the **Power Management Preferences** section.

Metric data may not be displayed for date ranges that include the current date as the latest date when the appliance is running in a time zone that lags behind the user browser time zone from which OpenManage Enterprise is accessed. In such cases, you can select a latest date that is a future date for the appliance.

It is recommended to select date ranges based on the appliance time zone to ensure that accurate metric data is displayed.

Based on your selection, details of the granular information available are as follows:

Table 66. Granularity of data

Duration	Granularity of data
1 Hour or 6 Hours or 12 Hours or 1 Day	Data is displayed based on the Metric gathering interval set in the Preferences section.
7 Days or 1 Month	Data is displayed at an interval of one hour.
3 Months or 6 Months or 1 Year	Data is displayed at an interval of one day.
Custom , Earliest Date , and Latest Date	All graphs and energy consumption data are displayed after 24 hours of adding devices for power management and monitoring. Data is displayed for one data point for each day in the selected range. The earliest date is the starting point on the graph from which historical data is displayed. The latest date is the most recent or final date, which can extend up to the current date.

9. Expand **Recent Virtual Machine Metrics** to view the power and vCPU usage of VMs.
10. To view the list of all VMs associated with the device, click the tabular view icon.
11. To view the latest metrics, click the refresh icon.

Table 67. List of Power Management metrics and supported devices

Metric	Supported devices
Power	• 14th and later generations of PowerEdge servers  NOTE: Cabled PSU servers are not supported.  NOTE: PowerEdge Fm120 aqua is not supported. • PowerEdge MX7000 • PowerEdge VRTX • PowerEdge FX2 • PowerEdge FX2s • Non-Dell servers—Most HPE servers having Integrated Lights-Out 5 (iLO 5) • Non-Dell servers—Most Lenovo servers having XClarity Controller (XCC)
Energy Consumption	• 14th and later generations of PowerEdge servers • PowerEdge MX7000 • PowerEdge VRTX

Table 67. List of Power Management metrics and supported devices (continued)

Metric	Supported devices
	- PowerEdge FX2 - PowerEdge FX2s
Thermal	14th and later generations of PowerEdge servers - PowerEdge MX7000 - PowerEdge VRTX - PowerEdge FX2 - PowerEdge FX2s - Non-Dell servers—Most HPE servers having Integrated Lights-Out 5 (iLO 5) - Non-Dell servers—Most Lenovo servers having XClarity Controller (XCC)
CPU Utilization	14th, 15th, and 16th generation of PowerEdge Intel servers 15th and 16th generation of PowerEdge AMD servers with iDRAC version 4.30.30.30 and later
I/O Utilization	14 th , 15 th , and 16 th generation of PowerEdge servers (Intel)
Memory Bandwidth Utilization	14 th , 15 th , and 16 th generations of PowerEdge servers (Intel)
System Airflow	Nonmodular PowerEdge servers. The latest generation of AMD servers with iDRAC Data Center license and iDRAC version 4.10.10.10 and later are supported.  NOTE: 14th generation AMD servers with iDRAC version 4.10.10.10 and later are supported.
Recent Virtual Machine Metrics	14 th and later generations of PowerEdge servers with a hypervisor deployed
Overall CPU Power Consumption	14 th and later generation of PowerEdge servers (Redfish)
Overall Memory Power Consumption	14 th and later generation of PowerEdge servers (Redfish)
System Usage	14 th , 15 th , and 16 th generation of PowerEdge servers (Redfish).
Fan Power Consumption	14 th and later generation of PowerEdge servers (Redfish)
Storage Power Consumption	14 th and later generation of PowerEdge servers (Redfish)
FPGA Power Consumption	14 th , 15 th , and 16 th generation of PowerEdge servers (Redfish).
Grid A Current	14 th and later generation of PowerEdge Rack and Tower servers (Redfish) and PowerEdge MX7000 chassis
Grid B Current	14 th and later generation of PowerEdge Rack and Tower servers (Redfish) and PowerEdge MX7000 chassis
System Current and Total Current	14 th and later generation of PowerEdge Rack and Tower servers (Redfish) and PowerEdge MX7000 chassis
Overall GPU Usage	14 th , 15 th , 16 th , and 17 th generation of PowerEdge servers (Redfish).
Overall GPU Memory Usage	14 th , 15 th , 16 th , and 17 th generation of PowerEdge servers (Redfish).
Overall GPU Memory Bandwidth Usage	14 th , 15 th , 16 th , and 17 th generation of PowerEdge servers (Redfish).
Overall GPU Board Temperature	14 th , 15 th , 16 th , and 17 th generation of PowerEdge servers (Redfish).

Table 67. List of Power Management metrics and supported devices (continued)

Metric	Supported devices
Overall GPU Power Consumption	14 th , 15 th , 16 th , and 17 th generation of PowerEdge servers (Redfish).

For PowerEdge 17G servers, the minimum iDRAC firmware version is 1.20.25.00.

Monitor Graphics Processing Unit (GPU)

Dell PowerEdge servers are shipped with Graphics Processing Unit (GPU). After a server with a GPU is discovered in OpenManage Enterprise, view the GPU details and metrics—power and thermal—on the server details page.

Steps

1. On the **Power Managed Devices > All Monitored Devices** page, click the server name which has a GPU card. For more information about the supported GPUs, see the *OpenManage Enterprise Support Matrix* available on the support site.
2. To view the GPUs available in the server, click **Hardware > Graphics Processor**.
3. To view the power and thermal metrics, click **Monitoring Metrics > Component Metrics Trend > GPU** and **Recent Component Metrics**.

On the metrics page, view the supported metrics—recent and historical—of GPUs. However, a GPU might support all or some of the following metrics:

Recent Component Metrics: Select a GPU from the **GPUs** list.

- Power supply status—Displays the power supply status. Possible values are enable, disable, and not applicable.
- Thermal alert state—Specifies if there is any thermal alert pending.
- Power break state—Specifies if the power brake is released or set.
- Reset recommended state—Indicates if GPU reset is recommended.

Component Metrics Trend: Select a GPU from the **GPUs** list.

- GPU Power consumption—Total GPU board power consumption
- GPU Primary temperature—Primary GPU temperature
- GPU Secondary Temperature—Secondary GPU temperature
- Board Temperature
- GPU Memory temperature—Temperature of memory monitoring sensor of GPU
- GPU Usage—GPU usage percentage
- Total SM Usage Time—Accumulated Streaming Multiprocessor (SM) utilization time
- SM Compute Ratio—The ratio of cycles an SM has at least one warp assigned. Computed from the number of cycles and elapsed cycles.
- SM Warp Ratio—The ratio of the number of warps residing on an SM. The number of resident as a ratio of the theoretical maximum number of warps per elapsed cycle.
- Tensor Core Usage—The ratio of cycles any tensor pipe is active
- Clock Frequency—GPU clock frequency
- Memory Usage—GPU memory usage percentage
- Memory Bandwidth Usage—DRAM usage as a percentage relative to the maximum theoretical bandwidth.
- HMMA Usage—The ratio of cycles the tensor Half Matrix Multiplication and Accumulation (HMMA) pipe is active
- Memory Clock Frequency—GPU memory clock frequency
- Clock Event Factors—List of factors that are reducing clock frequency. If all throttle reasons are returned as "Not Active", it means that clocks are running as high as possible.
- Throttle Duration Thermal—Total duration of throttling caused by a thermal limit of the processor since reset
- Throttle Duration Power—Total duration of throttling caused by a power limit of the processor since reset
- PCIe RX Throughput
- PCIe TX Throughput
- PCIe Link Speed—The current PCIe link speed.
- PCIe Correctable Error Count—The metric represents the count. The following errors are reported as correctable errors: Receiver error, Bad TLP, Bad DLLP, Replay rollover, Replay timeout, and Advisory non-fatal error
- DBE Retired Pages—Number of pages dynamically retired because of double-bit errors in frame buffer memory

- SBE Retired Pages—Number of pages dynamically retired because of single-bit errors in frame buffer memory
4. To create, view, and edit the GPU alert thresholds, see [Create alert thresholds](#) and [View alert thresholds](#).

Monitor Power Supply Unit (PSU)

Monitor the PSU current and thermal metrics on the server details page of OpenManage Enterprise.

Steps

1. On the **Power Management > Power Managed Devices > All Monitored Devices** page, click the server name which has a PSU.
2. To view the PSUs available in the server, click **Hardware > Power Supply Information**.
3. To view the current—grid A, grid B, system current, and total current—metrics, click **Monitoring Metrics > Device Metrics Trend** and **Component Metrics Trend**.

Device Metrics Trend:

- **Grid A Current**—Displays the current from the odd number of PSU slots. For example, PSU1, PSU3.
- **Grid B Current**—Displays the current from the even number of PSU slots. For example, PSU2, PSU4.
- **System Current**—Displays the sum of currents from all PSUs available on a device.
- **Total Current**—Displays the sum of currents from all PSUs available in a group.

Component Metrics Trend: Select a PSU from the **PSUs** list.

- **Power Supply - Current**—Displays the current value for the selected PSU.
- **Power Supply - Thermal**—Displays the thermal value for the selected PSU.

When the PSU is disconnected from the AC power supply, the metrics continue to be displayed.

Monitor Central Processing Unit (CPU)

Monitor the CPU thermal metrics on the server details page of OpenManage Enterprise.

Steps

1. On the **Power Management > Power Managed Devices > All Monitored Devices** page, click a server name.
2. To view the CPUs available in the server, click **Hardware > Processor**.
3. To view the thermal metrics, click **Monitoring Metrics > Component Metrics Trend**.

Component Metrics Trend: Select a CPU from the **CPUs** list.

CPU Socket - Thermal—Displays the thermal value for the selected CPU.

4. To create, view, and edit the CPU alert thresholds, see [Create alert thresholds](#), and [View alert thresholds](#).

Thresholds

Thresholds enable you to specify warnings and critical limits for power and temperature metrics on devices, groups, and GPU cards. OpenManage Enterprise generates alerts when the configured limits are violated. The status of power and temperature are displayed in the form of graphs on the **Monitoring Metrics** or **Group Details** tab.

Create alert thresholds

To monitor devices, groups, GPUs, and CPUs for threshold violations, define the power and temperature threshold values.

Prerequisites

- To set alert thresholds, ensure that you have added devices and groups.
- To set GPU alert thresholds, ensure that you have added servers with GPUs.

About this task

NOTE: If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can create and manage alert thresholds that are created by any other Device Manager user only for the devices in the Device Manager DM1 user scope.

To configure alert thresholds for power and temperature, perform the following steps:

Steps

- From OpenManage Enterprise, perform one of the following steps:
 - For a device:
 - Click the **Devices** tab. All the devices that are discovered in OpenManage Enterprise are displayed.
 - From the list of devices, click a device name. The details of the device are displayed on the **Overview** page.
 - To view power-related information, click the **Monitoring Metrics** tab.
 - For a static group:
 - Click **Devices > Static Groups > Group name**. All the devices that are part of the static group are displayed.
 - To view group information, click **Group Details**.
 - For a physical group, perform one of the following steps:
 - Click **Devices > Physical Hierarchy > Group name**. All the devices that are part of the physical group are displayed.
 - To view group information, click **Group Details**. To view the rack groups, click **Rack Details**.
 - Or, launch OpenManage Enterprise, and then click **Power Management > Rack View**. The **Rack View** tab is displayed. Optional: To filter and view the data, expand the Advanced Filters option. The following is a list of categories available:
 - Group Name**
 - Health State**
 - Power State**
 - Connection State**
 - Type**Select the categories of your choice and view the filtered data.
- To set the threshold, click **Alert Thresholds > Device Alert Thresholds, GPU Alert Thresholds, or CPU Alert Thresholds**, and click the edit icon.
The **Edit Alert Thresholds** page is displayed.
- Provide threshold values for **Power** and **Temperature**.

NOTE: When the alert threshold value units are set for power in **BTU/Hr** and temperature in **Fahrenheit**, ensure that you provide only the values and no other special character as the value may change after saving.

When the power or temperature values exceed the lower or upper warning values, a warning-level alert is generated and sent to OpenManage Enterprise.

When the power or temperature value exceeds the lower or upper critical values, a critical-level alert is generated and sent to OpenManage Enterprise.
- To apply the settings to all the GPUs and CPUs, select **Configure threshold values for all the GPUs** and **Configure threshold values for all the CPUs**.
- Click **Apply** to save the values.
The thresholds are saved successfully, and the scales are color-coded based on the current state of the device or group.
See the following tables for each threshold value range.

Table 68. Alert threshold range details for Watt and Celsius scale

Field	Mandatory	Device value range	GPU value range	CPU value range
Power (Watt)				
Upper Warning	No	Limit: 1–29,307,121 integers	Limit: 1-29,307,121 integers	N/A

Table 68. Alert threshold range details for Watt and Celsius scale (continued)

Field	Mandatory	Device value range	GPU value range	CPU value range
Upper Critical	No	Limit: 1–29,307,121 integers	Limit: 1-29,307,121 integers	N/A
Temperature (Celsius)				
Lower Critical	No	Limit: -10 to 60 degrees	N/A	N/A
Lower Warning	No	Limit: -10 to 60 degrees	N/A	N/A
Upper Warning	No	Limit: -10 to 60 degrees	Limit: 10–200 degrees	Limit: 10–200 degrees
Upper Critical	No	Limit: -10 to 60 degrees	Limit: 10–200 degrees	Limit: 10–200 degrees

Table 69. Alert threshold range details for BTU/hour and Fahrenheit scale

Field	Mandatory	Device value range	GPU value range	CPU value range
Power (BTU/hour)				
Upper Warning	No	Limit: 3–99,937,283 integers	Limit: 3-99,937,283 integer	N/A
Upper Critical	No	Limit: 3–99,937,283 integers	Limit: 3-99,937,283 integers	N/A
Temperature (Fahrenheit)				
Lower Critical	No	Limit: 14-140 degrees	N/A	N/A
Lower Warning	No	Limit: 14-140 degrees	N/A	N/A
Upper Warning	No	Limit: 14-140 degrees	Limit: 50-392 degrees	Limit: 50-392 degrees
Upper Critical	No	Limit: 14-140 degrees	Limit: 50-392 degrees	Limit: 50-392 degrees

View alert thresholds

View the status of the device, group, GPUs, and CPUs that is based on the configured alert thresholds.

Prerequisites

- To set alert thresholds, ensure that you have added devices and groups.
- To set GPU alert thresholds, ensure that you have added servers with GPUs.

About this task

NOTE: If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view and manage all the alert thresholds that are configured by any Device Manager user or Administrator on the groups and devices that are in Device Manager DM1 user scope.

Steps

1. From OpenManage Enterprise, perform one of the following steps:
 - For a device:
 - a. Click the **Devices** tab. All the devices that are discovered in OpenManage Enterprise are displayed.
 - b. From the list of devices, click a device name. The details of the device are displayed on the **Overview** page.
 - c. To view power-related information, click the **Monitoring Metrics** tab.
 - For a static group:
 - a. Click **Devices > Static Groups > Group name**. All the devices that are part of the static group are displayed.
 - b. To view group information, click **Group Details**.
 - For a physical group, perform one of the following steps:
 - a. Click **Devices > Physical Hierarchy > Group name**. All the devices that are part of the physical group are displayed.
 - b. To view group information, click **Group Details**. To view the rack groups, click **Rack Details**.
 - a. Or, launch OpenManage Enterprise, and then click **Power Management > Rack View**. The **Rack View** tab is displayed. Optional: To filter and view the data, expand the Advanced Filters option. The following is a list of categories available:
 - **Group Name**
 - **Health State**
 - **Power State**
 - **Connection State**
 - **Type**Select the categories of your choice and view the filtered data.
 - b. Click the device name or IP address.
2. View the power and temperature status on the **Alert Thresholds** tab.

The **Collected At** field displays the last collection time.

The pointer on the scale gives the average power and thermal data.

Power Management displays the minimum and maximum power and temperature values of the device and the previous readings that were collected. The scale is disabled if the thresholds are not set or if the threshold values are cleared off. The upper and lower warning and critical values are displayed only if the threshold values are set. To view more information about any violations, see the **Alert Log** on the **Alerts** page and the **Audit Logs** on the **Monitor** page.

Edit alert thresholds

Update alert thresholds that are based on changes to device utilization or updates in group membership.

Prerequisites

- To set alert thresholds, ensure that you have added devices and groups.
- To set GPU alert thresholds, ensure that you have added servers with GPUs.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can view and manage all the alert thresholds that are configured by any Device Manager user or Administrator on the groups and devices that are in Device Manager DM1 user scope.

To edit the threshold values for a device or a group, perform the following steps:

Steps

1. From OpenManage Enterprise, perform one of the following steps:
 - For a device:
 - a. Click the **Devices** tab. All the devices that are discovered in OpenManage Enterprise are displayed.
 - b. From the list of devices, click a device name. The details of the device are displayed on the **Overview** page.
 - c. To view power-related information, click the **Monitoring Metrics** tab.
 - For a static group:

- a. Click **Devices > Static Groups > Group name**. All the devices that are part of the static group are displayed.
 - b. To view group information, click **Group Details**.
- For a physical group, perform one of the following steps:
 - a. Click **Devices > Physical Hierarchy > Group name**. All the devices that are part of the physical group are displayed.
 - b. To view group information, click **Group Details**. To view the rack groups, click **Rack Details**.
 - a. Or, launch OpenManage Enterprise, and then click **Power Management > Rack View**. The **Rack View** tab is displayed. Optional: To filter and view the data, expand the Advanced Filters option. The following is a list of categories available:
 - **Group Name**
 - **Health State**
 - **Power State**
 - **Connection State**
 - **Type**
 Select the categories of your choice and view the filtered data.
 - b. Click the device name or IP address.
2. On the **Alert Thresholds** tab, click **Device Alert Thresholds**, **GPU Alert Thresholds**, or **CPU Alert Thresholds** and click the edit icon.
The **Edit Alert Thresholds** page is displayed.
3. Provide the values and click **Apply**.
Threshold values are updated successfully.

Delete alert thresholds

To remove the thresholds that are configured on devices or groups, clear all the thresholds.

About this task

 **NOTE:** If you are logging in as a Device Manager, only the device groups and devices that are in your scope are available for viewing and management.

For example, if you are logging in as a Device Manager DM1 user, you can create and manage alert thresholds that are created by any other Device Manager user only for the devices in the Device Manager DM1 user scope.

To delete alert thresholds, perform the following steps:

Steps

1. From OpenManage Enterprise, perform one of the following steps:
 - For a device:
 - a. Click the **Devices** tab. All the devices that are discovered in OpenManage Enterprise are displayed.
 - b. From the list of devices, click a device name. The details of the device are displayed on the **Overview** page.
 - c. To view power-related information, click the **Monitoring Metrics** tab.
 - For a static group:
 - a. Click **Devices > Static Groups > Group name**. All the devices that are part of the static group are displayed.
 - b. To view group information, click **Group Details**.
 - For a physical group, perform one of the following steps:
 - a. Click **Devices > Physical Hierarchy > Group name**. All the devices that are part of the physical group are displayed.
 - b. To view group information, click **Group Details**. To view the rack groups, click **Rack Details**.
 - a. Or, launch OpenManage Enterprise, and then click **Power Management > Rack View**. The **Rack View** tab is displayed. Optional: To filter and view the data, expand the Advanced Filters option. The following is a list of categories available:
 - **Group Name**
 - **Health State**
 - **Power State**
 - **Connection State**
 - **Type**
 Select the categories of your choice and view the filtered data.
 - b. Click the device name or IP address.

2. On the **Alert Thresholds** tab, click **Device Alert Thresholds**, **GPU Alert Thresholds**, or **CPU Alert Thresholds** and click the edit icon.
The **Edit Alert Thresholds** page is displayed.
3. To remove all the thresholds, clear all the existing threshold values, and click **Apply**.

Back up or restore

Use the **Backup And Restore** screen to create a backup of the appliance or restore an appliance from a backup.

CAUTION:

- **Appliances running on cloned VMs with OMES and AIOps Infrastructure Observability plug-in enabled do not support backup or restore operations. Perform this operation on a VM without cloning.**
- **Only one backup or restore process is supported at a time. Running more than one backup or restore process at a time can lead to unexpected system behavior.**

Before any backup or restore operation for installed plug-ins:

- Ensure you have read and complied with the limitations and requirements in the *Manage backup and restore for plug-ins* section of the *User's Guide* of every plug-in .
- Choose a low-volume time to lower the risk of critical alerts.

Table 70. Data Considered During Backup and Restore Jobs

Item	Description
Database	• Devices that are discovered and all template, profile, firmware, and configuration compliance information related with the device. • Configuration information (template, profile, firmware, configuration compliance, and so on.). • Job history and audit logs • Application settings
Configuration files	• Certificate store • Samba share files • Multifactor authentication files. • Appliance keystore used for encryption • Apache webserver configuration files • Source appliance information like RAM, CPU, storage, and device count. This information is collated into the import readiness report and deleted post restore.
Auto install plug-ins	Source plug-in details are captured to install on the target appliance automatically during the restore operation.
DCS and plug-in restore	DCS and installed plug-ins from the source appliance stores plug-in-related files and restores them on the target appliance.

Topics:

- [Appliance states](#)
- [Backup an appliance](#)
- [Restore an appliance](#)

Appliance states

Details of the appliance state during backup and restore jobs.

Table 71. Appliance states

Appliance state	Write actions: New jobs	Description
RUNNING	Enabled	In this state, all features of the appliance are accessible and fully functional. This state is the default state of the appliance.

Table 71. Appliance states (continued)

Appliance state	Write actions: New jobs	Description
MAINTENANCE_PENDING	Restricted	A banner is displayed at the top of the UI when the administrator begins a backup or restore process. The banner is also displayed when the scheduling process initiates the backup process that is based on a predefined schedule.
MAINTENANCE	Restricted	A banner appears at the top of the OpenManage Enterprise UI during backup. The migrate-out appliance must be in this state before the streaming operation can be activated.

Backup an appliance

Use backup jobs to store appliance data like application settings, device inventory, compliance, and plug-in data.

Prerequisites

- Ensure you are logged in as the default local administrator account . This is the only account that contains the super administrator role, as described in [User roles](#).
- Ensure that there is enough storage space on the target appliance.
- Ensure that all installed plugins are enabled.
- If FSD is enabled, disable FSD from the TUI using the [Enable Field Service Debug \(FSD\) mode option](#).
- Ensure the **Backup / Restore Settings** are configured, as described in [Manage console settings](#).
- If the backup location is a local network share:
 - Ensure OpenManage Enterprise has both read and write access to the share, as described in [Enable read and write access to your network share](#).
 - For backup files over 4GB, use **CIFS** or **NFS** share types, as HTTPS shares have a 4GB limit.

About this task

- During a backup:
 - The appliance is in *Maintenance* state. During this time, all new task scheduling is suspended. Only administrators can log in and all write operations targeting the appliance return an error. No operations can be performed on the console during this time.
 - All other users are logged off and unable to take action until the backup is complete.
 - Emergency Power Reduction (EPR) remains in an active state.
 - Scheduled policy activation and automatic group creation jobs that are running are ended.
 - All static policies (power) are disabled before starting backup and restore and the policies are enabled after backup and restore is completed.
- The Technical Support Report (TSR) and diagnostic reports are not included as part of the backup process.

Steps

1. Click **Backup / Restore > Backup**.
2. Select the **Backup Location**:
 - Select **HTTPS** if you have an HTTPS share, and enter the:
 - **Destination Path** to where your backup files will be stored.
 - **Username** used to authenticate the share.
 - **Password** used to authenticate the share.
 - Select **CIFS** if you have a CIFS share, and enter the:
 - **Domain** on which the share is hosted.
 - **User** used to authenticate the share.
 - **Password** used to authenticate the share.
 - Select **NFS** if you have an NFS share, and enter the **Destination Path** to where your backup files will be stored.
3. Enable **Backup File Encryption** by entering a **Passphrase** that will be required in order to recover this backup.
4. Optionally, change the value of **Set Schedule** to configure the automatic backup process to *Run Now*, *Run Later*, *Run On Schedule*, or set it to *Off*.

 **NOTE:** The best practice is to select **Prerequisites > Running Tasks > Complete Running Tasks Before Running Backup** for scheduled backups.

5. Click **Run Backup**.

Results

A backup job is initiated. The backup is created in the specified location and can be used to [Restore an appliance](#).

Next steps

During backup, you can click **Abort Backup** to stop the backup at any time.

 **NOTE:** **Abort Backup** fails when the appliance is in *Maintenance Pending* state.

Restore an appliance

Restore an appliance from a backup to reinstate appliance data like application settings, device inventory, compliance, and plugin data.

Prerequisites

 **CAUTION:** Restoring an appliance overwrites its data, and this action cannot be undone in OpenManage Enterprise. Best practice is to take a snapshot of target appliances before you restore them.

- Ensure that you are a super administrator, as described in [User roles](#).
- Ensure that the restore location is registered.
- If FSD is enabled, disable FSD from the TUI using the [Enable Field Service Debug \(FSD\) mode](#) option.
- Ensure the **Backup / Restore Settings** are configured, as described in [Manage console settings](#).
- Ensure the OpenManage Enterprise version on the source and target appliances are identical.

 **NOTE:** The plugin manager installs the necessary plugins that are identified in the backup file being restored.

- Ensure that the target appliance resources meet or exceed the source's memory, CPU cores, and storage. Otherwise the restore readiness report indicates a problem and the restore will not continue.

About this task

After restoring backups with plugins, a plugin synchronization job may run if plugins on the source appliance are missing or disabled on the target. Since firmware bundles are not part of the backup file, any firmware update causes the redownload of catalog files for the upgrade if the task was triggered by a baseline.

Steps

1. Click **Backup / Restore > Restore**.
2. Display the list of available backups:
 - Select **HTTPS** if you have an HTTPS share, and enter the:
 - **Destination Path** to where your backup files are stored.
 - **Username** used to authenticate the share.
 - **Password** used to authenticate the share.
 - Select **CIFS** if you have a CIFS share, and enter the:
 - **Domain** on which the share is hosted.
 - **User** used to authenticate the share.
 - **Password** used to authenticate the share.
 - Select **NFS** if you have an NFS share, and enter the **Destination Path** to where your backup files are stored.
3. Click **Test** to validate the access of the appliance to the destination path.
4. Click **Apply** to display the list of backup files available on the device.
Select the checkbox to **Only show backups generated by this appliance**.

 **NOTE:** Backups that are generated from the same appliance can be deleted.

5. Select the required backup file.
6. Enter the **Passphrase** required to decrypt the backup file.
7. Click **Restore**.

 **NOTE:** If the target appliance does not meet the system requirements found in the backup file, the restore readiness report shows items that require attention. Resolve these items and then retry the restore operation.

Results

If the restore task is successful:

- A restore job is initiated on the target appliance.
- An active backup job is displayed while the restore job is running.
- The target appliance is overwritten and cannot be restored.
- Once restoration is complete:
 - The backup job is stopped.
 - The restored appliance reboots.
 - When the restored appliance is up and running, all group discovery and regular discovery jobs are initiated.

 **NOTE:** The initial group discovery and regular discovery jobs take longer than expected due to the dual group tasks triggered while initiating the appliance.

Next steps

- Check for running or failed plugin synchronization jobs in the `api/BackupRestoreService/RestoreExecutionDetails` response.
- While services are being loaded, do not trigger multiple executions of the same job through the **Jobs** screen.
- If the restore is performed on an appliance that was not the original source, restored to a new appliance, perform the following post-restore:
 - When restoration is complete, shut down the source appliance.
 - Re-create the source appliance configuration on the target appliance, as described in [Configure the system using the TUI](#).
 - Ensure that the restored appliance is registered with an FQDN in the DNS settings.
 - Update static routes to the restored appliance network.
 - Upload your custom certificate to the restored appliance.
 - If you restore a backup to an appliance with a different IP address, re-run discovery on devices that were previously in the **Managed with Alerts** state. Ensure the **Enable alert reception from discovered devices** checkbox is selected during re-discovery. This step re-subscribes devices to Redfish/SNMP events using the new IP. If the restored appliance has the same IP address as the original, no re-discovery is needed

 **NOTE:** In case the restore task fails:

1. A yellow banner is displayed, indicating the failure of the last restore job.
2. To investigate the cause of the failure, click **View logs** to access the restore activity logs.
3. Revert the appliance to a historical snapshot and then retry the restore task.

Updating the console and plugins

Use the **Application Settings > Console and Plugins** screen to view the current version of your OpenManage Enterprise software and plugins, check if updates are available, and update to a newer version.

Upgrade Paths:

- To upgrade to OpenManage Enterprise version 3.10.x, ensure that your appliance is running on version 3.9.2.
- To upgrade to OpenManage Enterprise version 4.1, perform a migration from version 3.10.x.
- If your appliance is already running version 4.0.x, you can upgrade to version 4.1 and later versions.

For detailed instructions on migrating an appliance, see the [OpenManage Enterprise 4.1.x User's Guide](#) for more information.

i NOTE:

- The OpenManage Enterprise 4.4.0 upgrade has been removed from the OpenManage Enterprise online update catalog due to a Docker interface issue that affects upgrades to this version. However, new deployments of the OpenManage Enterprise version 4.4.0 appliance are not impacted and remain available for download on [dell support](#).
- If you are upgrading from earlier versions, upgrade directly to version 4.4.1. Upgrading from version 4.4.0 to 4.4.1 is not allowed.
- Customers already on version 4.4.0 or who have successfully upgraded to 4.4.0 do not need to upgrade to 4.4.1. Version 4.4.1 includes a fix for the Docker interface issue. No other features or functionalities are impacted in either version.

For information about supported plugin versions for your OpenManage Enterprise version, see [OpenManage Enterprise 4.x.x Support Matrix](#).

Figure 2. Potential upgrade paths to 4.x.x



Click **Update Settings** to:

- Check for software version updates **Automatically** or **Manually**.

- (Best practice) Automatically update the software and plugin versions from Dell.com, as described in [Online update](#).
- When there is no connectivity to external networks, you can update the software and plugin version from a local network share, as described in [Offline update](#).

Topics:

- [Update prerequisites](#)
- [Online update](#)
- [Configuring a local network share for offline update](#)
- [Offline update](#)
- [System-generated postupgrade task](#)

Update prerequisites

Before updating to the latest version, administrators must consider the following points:

- Hardware and hypervisor:
 - Ensure that the hardware and hypervisor requirements are met for the version you are upgrading to. For more information, see the [OpenManage Enterprise 4.x.x Support Matrix](#).
- Backup and snapshot:
 - Take a VM snapshot of the console as a backup in case something unexpected occurs. Allocate more downtime for this if necessary.
- Allocate time:
 - Allocate at least an hour for the update process. Allocate more time if the update must be downloaded by using a slower network connection.
- Prepare scaled appliance:
 - Upgrade of a 'scaled' appliance may fail due to insufficient provisioning of hard drive space that is required for the data backup from a large number of devices and additional plugins.
 - It is recommended to add twice the used hard drive space before initiating the upgrade using the **Configure Appliance Disk Size** on the Text User Interface (TUI) screen. For example, consider expanding the available HD space to 1.2 TB if the initial allocation is 400 GB. For more information see, [Configure the system using the TUI](#).
- Manage tasks:
 - Ensure that no device configuration, deployment, or extension (plug-in) tasks are running or are scheduled to run during the planned downtime.
 - Any active or scheduled tasks or policies are terminated without further warning during the update.
 - Clicking **Update** would initiate an Upgrade Bundle Download job. This job finishes automatically after all the update files are downloaded and cannot be terminated by the user.
- Restart after device deletion:
 - Post deletion of devices, a restart of services using TUI is recommended before initiating a console upgrade. Otherwise, the upgrade may fail and the console would reboot with the previous working state of the appliance.
- Notify users:
 - Notify other console users of the impending scheduled update.
- Plan for upgrade failure:
 - If the upgrade fails, the appliance would restart. It is recommended to revert the VM snapshot and upgrade again.
- Time duration for large-scale upgrade:
 - When you update OpenManage Enterprise with more than 8000 discovered devices, the update task completes in two to three hours. During this time, the services might become unresponsive. It is then recommended to gracefully reboot the appliance. After the reboot, normal functionality of the appliance is restored.
- Time duration for upgrade with plug-in:
 - Upgrade time for an appliance with the Power Manager plug-in installed, might be between 1 and 10 hours depending on the number of devices being monitored by Power Manager.

NOTE: Update Compatibility:

- If your OpenManage Enterprise version is earlier than 3.10, first update it to 3.10.x, and then use Migrate an appliance to move to 4.1. For more information about migration, see the *OpenManage Enterprise 4.1.x User's Guide*.
- OpenManage Enterprise **Automatic** > **Online** method supports N-2 where N is the currently released version. For example, if the current released version is 4.1, you can update from 3.10.x or newer. For systems running on Tech Release, it is recommended to first update to either 3.0 or 3.1.

Online update

Download and update the appliance using bundles downloaded from Dell.com

Prerequisites

- Ensure you have administrator privileges for this task, as described in [Role and scope-based access](#).
- Ensure you comply with the [Update prerequisites](#).
- Ensure your appliance can connect to Dell.com.

About this task

Upgrading OpenManage Enterprise is a two-step process:

Steps

1. [Define online update settings](#) to specify the update method.
2. [Update the appliance from dell.com](#) from the **Console and Plugins** screen.
Configuring the update settings is a one-time process. Once the update settings are configured, you can click the refresh icon in the **Update** section to see if an updated version is available to download.

Define online update settings

Configure the update settings for online update from dell.com.

Steps

1. Click **Application Settings > Console and Plugins > Update Settings**.
2. In **How to check for updates**, define the appliance update method:
 - **Automatic:** The appliance checks for the availability of the updates automatically every Monday from the source specified in the **Where to check for updates**.
 - **Manual:** Manually check for the availability of the update from the source specified in the **Where to check for updates** by clicking the **Refresh** list icon in the **Updates** section on the **Console and Plugins** screen.
3. In **Where to check for updates**, select **dell.com** to specify the location from where the appliance will check for updates.
4. Select the **Automatically start the console update when downloads are complete** check box to initiate an installation of the console update immediately after the update package is downloaded. Otherwise, the update can be initiated manually.
5. Click **Apply**.

Results

The appliance checks for updates directly from https://downloads.dell.com/openmanage_enterprise.

Next steps

[Update the appliance from dell.com](#)

Update the appliance from dell.com

Download and update the appliance firmware using bundles downloaded from Dell.com.

Prerequisites

- Ensure you comply with the [Update prerequisites](#).
- Ensure you comply with the [Online update](#).
- Ensure you [Define online update settings](#).
- Take a VM snapshot of the console as a backup in case something unexpected occurs. Allocate more downtime for this if necessary.

Steps

1. Based on the update settings, the appliance checks for the availability of an update and if a new version is available, a banner with the new upgrade version information is displayed. On the banner, the administrator can choose to dismiss the notification, be reminded later, or can click **View Now** to know details such as the version and size of the update available on the **Application Settings > Console and Plugins** screen. The OpenManage Enterprise section of the **Console and Plugins** screen displays all the new features and enhancements of the available update.
2. Click **Update** and then click **Download Console** to download the package from the specified source.

NOTE:

- Clicking **Update** initiates an **Upgrade Bundle Download** job. This job finishes by itself after all the update files are downloaded and cannot be terminated.
- If the upgrade fails, the appliance will restart. In this case, it is recommended to revert the VM snapshot and upgrade again.

Results

If the **Automatically start the console update when downloads are complete** check box is selected in the Update settings, the upgrade will start automatically after the update package is downloaded. Otherwise, click **Update Console** to perform the update.

Once the console upgrade completes, multiple mandatory tasks are undertaken as part of a system-generated task named **Post upgrade Task**. For more information, see [post upgrade task](#).

Next steps

Log in after the update and confirm that the product works as expected. Check the audit log for any warnings or errors that are related to the update. If there is an error, export the audit log and contact Dell support.

After the appliance is updated:

- Clear the browser cache and cookies. If the cache or cookies are not cleared, new tasks may fail post update.
- You can log in immediately after the appliance is updated and do not have to wait till the entire inventory is discovered. Discovery tasks are triggered in the background. For more information, see [View job details](#).
- Before starting another console or plug-in update, wait until all jobs including the **Post Upgrade** task is completed.

Configuring a local network share for offline update

Best practice is to use the automatic online update and backup features whenever possible. However, if your company is in a dark site or does not have access to the Internet, you must configure a local network share.

To configure a network share for [Updating the console and plugins](#):

1. [Create the directory structure and download the update bundles](#).
2. Configure the share for offline update:
 - [Configure an NFS network share on a Windows server](#).
 - [Configure an NFS network share on a Linux server](#).
 - [Configure an HTTP network share on a Windows server](#).

Create the directory structure and download the update bundles

Create the directory structure required for offline software updates.

Prerequisites

Ensure you are a Windows user with administrator privileges.

About this task

For [Updating the console and plugins](#), your network share directory structure should be the same as the structure of the folder containing the required update files in the upgrade repository at https://downloads.dell.com/openmanage_enterprise/.

Steps

1. Open https://downloads.dell.com/openmanage_enterprise/ in a browser to display the contents of the upgrade repository.
2. Click the folder of the OpenManage Enterprise version that you want to upgrade to, and note whether the update contains a *full* or a *minimal* folder.

NOTE: Depending on the size of the update file (and subsequently, the time it would take to update the software), some OpenManage Enterprise versions will contain a **full** folder and others will contain a **minimal** folder. The *full* update bundle contains the full upgrade packages and typically takes much longer than a minimal update. The *minimal* update bundle is typically a patch release and only contains specific upgrade packages.

3. Create a folder on your local network share for **<OMEUpdates>**.
4. Copy the structure of the version folder in the upgrade repository to the **<OMEUpdates>** folder on your local network share.

In your local network share **<OMEUpdates>** folder:

- a. Create a folder for the OpenManage Enterprise software version that you want to upgrade to. Make sure your local version folder is named the same as it is in the upgrade repository. For example, to update to OpenManage Enterprise version 3.10, create ...<NetworkShare>/<OMEUpdates>/3.10/.
- b. Copy the latest `LexingtonUpdates.xml` and `LexingtonUpdates.xml.asc` files from the upgrade repository to your local software version folder.
- c. Create either a *full* or a *minimal* folder, depending on which of these folders is in the required version folder in the upgrade repository. For example, to update to OpenManage Enterprise:
 - Version **3.9.2**, create ...<NetworkShare>/<OMEUpdates>/3.9.2/minimal.
 - Version **3.10**, create ...<NetworkShare>/<OMEUpdates>/3.10/full.
- d. Copy the OpenManage Enterprise update files from the upgrade repository to your local network share *full* or *minimal* folder.

Results

Your directory is structured correctly and contains the files required for updating OpenManage Enterprise and plugin software from a local network share.

Next steps

Configure the share:

- [Configure an NFS network share on a Windows server.](#)
- [Configure an NFS network share on a Linux server.](#)
- [Configure an HTTP network share on a Windows server.](#)

Configure an NFS network share on a Windows server

When your network share is Windows-based, use Windows Server Manager for offline software update and backing up OpenManage Enterprise appliances.

Prerequisites

- Ensure you are a Windows user with administrator privileges.
- If this share contains update bundles, see [Create the directory structure and download the update bundles.](#)

Steps

1. Open **Windows Server Manager**.
2. Click **File and Storage Services > Shares**, select the share, and right-click **Properties**.
3. In the **Share Properties** screen:
 - a. In the **Authentication** screen, select **No server authentication** and **Allow unmapped user access by UID/GID**.
 - b. In the **Share Permissions** screen, click **Add**, add a **Host** (IP address) for each appliance, and provide *Read/Write* access to each appliance.
4. Click **OK**.

Results

The NFS share is ready for input or output.

Next steps

If this share contains your appliance backups, see [Enable read and write access to your network share](#).

Configure an NFS network share on a Linux server

Configure a network share on a Linux server with a Network File System (NFS) for offline software update and backing up OpenManage Enterprise appliances.

Prerequisites

- Ensure you are a Linux user with administrator privileges.
- Ensure that an NFS package is not already installed by running `rpm -qa nfs` on the server terminals. If NFS is not installed, use the below command to install it.

```
yum install nfs-utils libnfsidmap -y
```

- For offline update bundles: [Create the directory structure and download the update bundles](#).

Steps

1. Enable the NFS service by running:

```
systemctl enable rpcbind  
systemctl enable nfs-server
```

2. Start the NFS service by running:
 - a. `systemctl start rpcbind` to convert the RPC program numbers into universal addresses.
 - b. `systemctl start nfs-server` to enable the clients to access NFS shares.
 - c. `systemctl start rpc-statd` to recover locked files when the server fails and reboots.
 - d. `systemctl start nfs-idmapd` to map user and group IDs to names.
3. Create a directory under the root partition by running:

```
mkdir /NFSSHARE
```
4. Allow the client to read and write data in the directory that you created by running:

```
chmod 777 /NFSSHARE
```

Results

The NFS share is ready for input or output.

Next steps

[Enable read and write access to your network share](#)

Configure an HTTP network share on a Windows server

Configure an HTTP or HTTPS network share on a Windows server for offline software update and backing up OpenManage Enterprise appliances.

Prerequisites

- Ensure you are a Windows user with administrator privileges.
- If this share contains your update bundles, see [Create the directory structure and download the update bundles](#).

Steps

1. Open **Windows Server Manager**, and select **Add Roles and Features** to open the wizard:
 - a. On the **Before You Begin** screen, click **Next**.
 - b. On the **Installation Type** screen, select **Role-based or feature-based installation**, and click **Next**.
 - c. On the **Server Selection** screen, select **Select a server from the server pool**, select a server, and click **Next**.
 - d. On the **Server Roles** screen, select the required options, and click **Install**:
 - Common HTTP Features:
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - HTTP Redirection
 - WebDAV Publishing
 - Health And Diagnostics:
 - HTTP Logging
 - Custom Logging
 - Logging Tools
 - ODBC Logging
 - Performance (All)
 - Security
 - Request Filtering
 - Basic Authentication
 - Digest Authentication
 - IP And Domain Restrictions
 - URL Authorization
 - Windows Authentication
 - Application Development
 - .NET Extensibility
 - ASP .NET 4.8
 - ISAPI Extensions
 - ISAPI Filters
2. Once the installation is complete, restart the Windows server.
3. Set the Multipurpose Internet Mail Extensions (MIME) types in Internet Information Services (IIS):
 - a. Confirm that the default MIME types `.xml`, `.tar.gz`, and `.json` exist.
 - b. Add the `.xml.asc`, `.zip.asc`, and `.json.asc` MIME types.

Alternatively, open the Windows command prompt and run the following commands for each required MIME type:

 - i. `cd \Windows\System32\inetsrv`
 - ii. `appcmd.exe set config /section:staticContent /[fileExtension='<fileExtension>', mimeType='<mimeType>']`.

For example: `appcmd.exe set config /section:staticContent /[fileExtension='.xml', mimeType='application/xml']`.

Table 72. MIME types

fileExtension	mimeType
<code>.xml</code>	<code>application/xml</code>
<code>.zip</code>	<code>application/zip</code>
<code>.tar.gz</code>	<code>application/octet-stream</code>
<code>.json</code>	<code>application/json</code>
<code>.xml.asc</code>	<code>text/plain</code>
<code>.zip.asc</code>	<code>text/plain</code>
<code>.json.asc</code>	<code>text/plain</code>

4. Click **Add Authoring Rule** to enable read/write access to the content on the network share. In the **Add Authoring Rule** dialog box:
 - a. Set **Allow access** to **All content**.
 - b. Set **Allow access to this content** to **All users**.
 - c. Set **Permissions** to **Read/Write**.
 - d. Click **OK**.
5. Configure the user authentication method:
 - a. Click **Select Authentication**.
 - b. Enable both **Allow Basic Authentication** and **Anonymous Authentication**.

Results

Your HTTP or HTTPS network share is ready for [Updating the console and plugins](#) or to host your [appliance backups](#) .

Enable read and write access to your network share

To backup and restore appliances, you will need to enable both read and write access to a Common Internet File System (CIFS) or a Network File System (NFS) network share on a Windows server.

Prerequisites

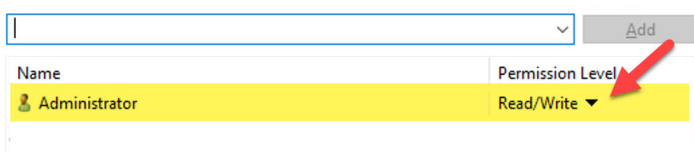
- Ensure you are a Windows user with administrator privileges.
- Configure the share:
 - [Configure an NFS network share on a Windows server](#).
 - [Configure an NFS network share on a Linux server](#).
 - [Configure an HTTP network share on a Windows server](#).

Steps

1. In Windows, right-click on your **<OMEUpdates>** folder and select **Properties**.
 - For CIFS file systems, click the **Sharing** tab.
 - For NFS file systems, click the **NFS Sharing** tab.
2. Click the **Share** button.
The **Network access** dialog box is displayed.
3. Add an **Administrator** user with *Read/Write* permissions.

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.



Name	Permission Level
Administrator	Read/Write ▼

Results

You can [Back up or restore](#) from a local offline folder when there is no external connectivity.

Offline update

If you are unable to connect to dell.com to update OpenManage Enterprise, you can update the console or the plugins from a local network file share. To do so, you must first manually download the relevant update packages and store them on your local network share. An audit log is created after every manual attempt to find an update.

Prerequisites

- Ensure you have administrator privileges as described in [Role and scope-based access](#).

- Ensure you comply with the [Update prerequisites](#).
- Take a VM snapshot of the console as a backup.
- Add a second network interface only after completion of the console update task.
- Ensure that the security certificates are trusted third-party certificate authority signed when using an HTTPS share.

About this task

Updating OpenManage Enterprise from a network share is a two-step process:

Steps

1. [Configure a local network share for offline update](#)
2. [Download update files to local network share](#)
3. [Initiate update from a network share](#)
If the update fails, the appliance restarts. In this case, revert the VM snapshot and update again.

Download update files to local network share

Download the files that are required for an offline update and place them for use in the network share.

Prerequisites

Ensure you [Configure a local network share for offline updates](#).

Steps

1. Go to [OpenManage Enterprise upgrade repository](#) and select the target revision number (x.y.z). Download the following files from the directory:
 - `LexingtonUpdates.xml`
 - `LexingtonUpdates.xml.asc`
 - `omenterprise_x.y.z.tar.gz`

NOTE:

- To install or update [OpenManage Enterprise plug-ins](#), create local copies of the following:
 - `plugins` folder
 - `spotlight` folder
 - `plugins_catalog_meta_data.json`
 - `plugin_spotlight.json`
 - `plugin_spotlight.json.asc`
- The OpenManage Enterprise catalog on downloads.dell.com is used to upgrade to the latest version available, and will not function properly when pointing to a location other than https://downloads.dell.com/openmanage_enterprise (or https://dl.dell.com/openmanage_enterprise).

2. Create a directory structure in the root directory of the share that matches the `UpdateArchivePath` from the `LexingtonUpdates.xml` file.
For target revision x.y.z, the folder structure would be `x.y.z/minimal`, `x.y.z/full`, or `x.y.z/archives` depending on the type of revision that is targeted (major, minor, or patch).

3. Copy the downloaded files to the following locations on the share.
 - `LexingtonUpdates.xml` must be placed in the root directory of the share (/).
 - `LexingtonUpdates.xml.asc` must be placed in the root directory of the share (/).
 - `omenterprise_x.y.z.tar.gz` must be placed here: `/x.y.z/<full/minimal/archives>`



CAUTION: Do not make any modifications to the above files. Since they are signed, any changes to the files will invalidate them.

4. Click **Application Settings > Console and Plugins > Update Settings**.
5. In **How to check for updates**, select one of the following options:
 - **Automatic:** The appliance checks for the availability of the updates automatically every Monday from the source specified in the **Where to check for updates**.

- **Manual:** Manually check for the availability of the update from the source specified in the **Where to check for updates** by clicking the **Refresh** list icon in the **Updates** section of the **Console and Plugins** screen.
6. In **Where to check for updates**, select **Network Share** option to specify the location from where the appliance checks for updates.
 - a. In **Local Path**, specify the NFS, HTTP, or HTTPS path that contains the downloaded files.
The format of a network share is: `nfs://<IP Address>/<Folder_Name>`, `http://<IP Address>/<Folder_Name>`, or `https://<IP Address>/<Folder_Name>`.
 - b. To verify the connection to the specified network share, click **Test Now**.
 7. Select the **Automatically start the console update when downloads are complete** check box to initiate an installation of the console update immediately after the update package is downloaded. Otherwise, the update can be initiated manually.
 8. Click **Apply**.

Next steps

[Initiate update from a network share.](#)

Initiate update from a network share

Configure the appliance to download the update files from a locally available network share.

Prerequisites

- Ensure you comply with the [Offline update](#) prerequisites.
- Ensure you [Set up an offline network share for offline updates](#).

Steps

1. Based on the update settings, the appliance checks for the availability of an update and if a new version is available, a banner with the new upgrade version information is displayed. On the banner, the administrator can choose to dismiss the notification, and be reminded later, or can click **View Now** to know details such as the version and size of the update available on the **Application Settings > Console and Plugins** screen. The OpenManage Enterprise section of the **Console and Plugins** screen displays all the new features and enhancements of the available update.
2. Click **Update** and then click **Download Console** to download the package from the specified source.

NOTE:

- Clicking **Update** initiates an *upgrade bundle download* job. This job finishes by itself after all the update files are downloaded and cannot be terminated.

Results

If you chose to start the update automatically in the update settings, the upgrade will start immediately after the update package is downloaded. Else, click **Update Console** to perform the update.

Once the console upgrade completes, multiple tasks are undertaken as part of a system-generated task named **Post upgrade Task**. For more information, see [post upgrade task](#).

Next steps

Log in after the update and confirm that the product works as expected. Check the audit log for any warnings or errors that are related to the update. If there is an error, export the audit log and contact Dell support.

After the appliance is updated:

- Clear the browser cache and cookies. If the cache or cookies are not cleared, new tasks may fail post update.
- You can log in immediately after the appliance is updated and do not have to wait till the entire inventory is discovered. Discovery tasks are triggered in the background. For more information, see [View job details](#).
- Before starting another console or plug-in update wait until all jobs including the **Post Upgrade** task is completed.

System-generated postupgrade task

Once the console upgrade completes, a series of mandatory tasks is undertaken as part of a system-generated task that is named **Post upgrade Task**. This task should be allowed to complete before installing or upgrading any available plugins. Do not manually disable or stop this task.

 **NOTE:** When the post-upgrade task is running, a warning banner is displayed asking users to avoid restarting OpenManage Enterprise services or rebooting the appliance. The banner appears on the home page each time a user logs in until the job is completed.

The **Post upgrade Task** performs the following operations:

- Restoring upgrade console settings
- Restoring logging status
- Processing configuration task parameters
- Upgrading console settings if applicable to the current release.
- Running email tasks
- Sending out a reminder to disable any incompatible plugins.
- Running catalog updates for plugins
- Running discovery tasks
- Enabling NTP services
- Updating the job completion status for the firmware update
- Updating SNMP configurations
- Setting FSD capability for the console

Check the **Job status** under the **Monitor > Jobs view** using the **Source** filter set for **System generate**.

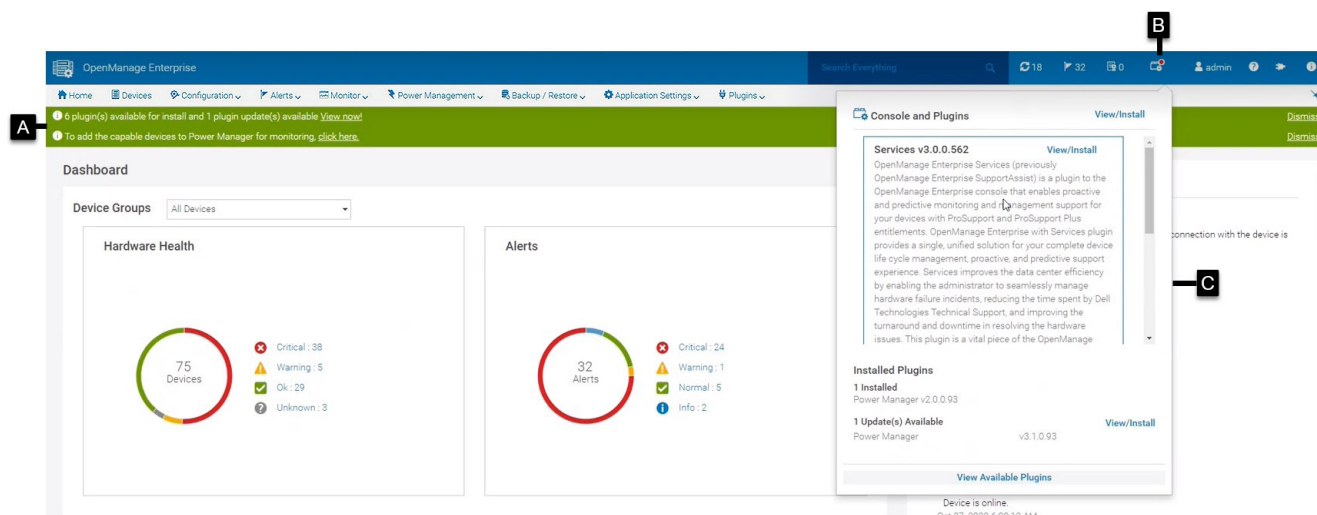
Adding a second network interface should be done only after the completion of the **Post upgrade Task**. Attempt to add a second NIC while the postupgrade task is in progress would be ineffective.

 **CAUTION:** After upgrading, you may log in and begin using the appliance once the UI becomes available. However, do not reboot the appliance or initiate operations that may trigger a reboot, such as plugin installation or upgrade, until all **Post upgrade Task**, including discovery and onboarding tasks, are complete. Interrupting these background tasks can result in an unstable appliance state. Allow sufficient time for these operations to finish before performing administrative actions to ensure system integrity.

Managing plugins

Use the **Application Settings > Console and Plugins** screen to manage one or more OpenManage Enterprise plugins.

- By default, no plugins are installed on a fresh appliance. Installing a plugin both installs and enables the plugin.
- When a plugin is disabled or uninstalled using REST API, refresh the browser for the change to be reflected in the **Plugins** menu.



- **A** - The banner displays the number of plugins currently available for installation or update. Click on **View now** to open the **Console and Plugins** screen.
- **B** - The **software status button** displays a red dot when a plugin is not installed, and the plugin catalog contains a compatible install version or the plugin is installed, and the plugin catalog contains a compatible upgrade version.

NOTE: Clicking this icon opens a dialog box.

- **C** - The **software status dialog** is displayed, listing all installed and update-able plugins. Click **View/Install** or **View Available Plugins** to open the **Console and Plugins** screen and update the plugin.

Click **Update Settings** to:

- Check for software version updates **Automatically** or **Manually**.
- Update the software version from Dell.com, as described in [Online update](#).
- Update the software version from a network share, as described in [Offline update](#).

Topics:

- [Install plugins](#)
- [Enable plugins](#)
- [Update plugins](#)
- [Disable plug-ins](#)
- [Uninstall plugins](#)

Install plugins

Enhance the functionality of OpenManage Enterprise by installing OpenManage Enterprise plugins.

Prerequisites

- The OpenManage Enterprise Advanced or Advanced+ license is required for some of the OpenManage Enterprise plugins features to be fully functional. For more in-depth information about OpenManage Enterprise plugins, see the respective documentation on the Dell Support site.
- To install OpenManage Enterprise plugins from Dell.com, ensure that the OpenManage Enterprise appliance can access downloads.dell.com.
- To install OpenManage Enterprise plugins from a local network share, manually download the package to your network share. Update the location on the **Update Settings** screen of OpenManage Enterprise. For more information about configuring your **Update Settings**, see [Offline update](#) and [Define online update settings](#).

About this task

 **NOTE:** Installing OpenManage Enterprise plugins on OpenManage Enterprise restarts the appliance services.

Steps

1. Click **Application Settings > Console and Plugins**.
The **Console and Plugins** screen is displayed.
2. In the **Plugins** section, click **Install** for the plug-in you want to install.
The **Install and update multiple plugins** wizard is displayed.
3. From the **Plugins available for install** list, select the plug-ins that you want to install, and then click **Next**.
4. View the progress of the plug-in that you selected to install under the **Download** section, and then click **Next** on completion.

 **NOTE:** If you leave the wizard, the download continues.

5. The **Review License Agreement** section displays the consent form listing the necessary **End User License Agreement** and other required license agreements for plug-in installation. Click **Accept** and then click **Next** to continue.

 **NOTE:** All agreements must be read and accepted before continuing.

The **Review and confirm Backup** section lists the number of logged-in users, tasks in progress, and scheduled jobs.

6. Confirm that you have taken a backup of the appliance and then click **Finish**.
The status of installation operation is displayed. After the successful installation of the plug-in, the status that appears on the top of the plug-in section changes from **Available** or **Downloaded** to **Installed**.

Results

The specified plug-ins are installed in OpenManage Enterprise.

Next steps

Plug-ins like AI Ops Infrastructure Observability and OMES must be activated before being used. See the respective plug-in documentation for information about how to activate the plug-in.

Enable plugins

OpenManage Enterprise plugins screens are displayed and their functionality is enabled in OpenManage Enterprise. The REST APIs specific to OpenManage Enterprise plugins are also enabled in **OpenManage Enterprise**.

About this task

 **NOTE:** Enabling OpenManage Enterprise plugins restarts the appliance services.

Steps

1. Click **Application Settings > Console and Plugins**.
The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Enable** for one or more plugins.
The **Enable multiple plugins** wizard is displayed.
3. Select the plugins that you want to enable from the **Select Plugin** section, and click **Next**.
The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirm Backup** section.
4. To confirm, select the **I agree that I have captured a backup of the OpenManage Enterprise appliance prior to performing a plugin action**. option, and then click **Finish**.

Results

The specified OpenManage Enterprise plugin screens are displayed and their functionality is enabled in OpenManage Enterprise.

Update plugins

Based on your **Update Settings**, the appliance checks for the availability of an update of the installed plug-ins. If a new version is available, a banner with the new upgrade version information is displayed. On the banner, the administrator can dismiss the notification, be reminded later, or can click **View Now** to display notification details. The **Plugin** section of the **Console and Plugins** screen displays new features and enhancements of all available plug-in updates.

Prerequisites

- Ensure that your **Update Settings** are configured as described in [Updating the console and plugins](#).
- Ensure that the version of OpenManage Enterprise plugins you plan to upgrade is compatible with your OpenManage Enterprise version. For more information, see *OpenManage Enterprise Support Matrix*.

Steps

1. In the **Plugin** section, click **Update Available** for the plug-ins you want to update.
The **Install and update multiple plugins** wizard is displayed.
2. Select the plug-ins that you want to update in the **Select Plugin** section and click **Next**.
Note the update progress in the **Download** section, and click **Next** on completion .
 **NOTE:** The download continues even if you leave the wizard.
3. A consent form is displayed under the **Review license agreement** section to inform you about the **End User License Agreement** . Click **Accept** and then click **Next** to continue.
 **NOTE:**
 - All agreements must be read and accepted before continuing.
 - The **Review and confirm action** lists the number of logged in users, tasks in progress, and scheduled jobs are displayed in .
4. Confirm that you have taken a backup by enabling the checkbox and then click **Finish**.
5. To view the list of devices and groups that are Redfish capable: Click **Run Inventory** on the appliance, and then click the **Refresh Power Manager capabilities** option on the **Power Manager Devices** page.
If Redfish is enabled on the device post upgrade, discover the device again in OpenManage Enterprise.

Results

The new software version is displayed in the **Plugin** section of OpenManage Enterprise plugins.

Next steps

After the plug-in is updated:

- Clear the browser cache and cookies. Not clearing them may cause failing of new tasks post update.
- You can log in immediately after the appliance is updated and do not have to wait till the entire inventory is discovered. Discovery tasks are triggered in the background. For more information about the task, click [View job details](#).
- Before starting another console or plug-in update, wait until all jobs including the **Post Upgrade** task is completed.

Disable plug-ins

Disables the functionality of OpenManage Enterprise plugins. The REST APIs specific to Power Manager are also disabled.

Prerequisites

- The Emergency Power Reduction (EPR) is not enabled on the device. View the EPR status of all devices and groups on the **Emergency Power Reduction** page.
- There are no active policies.

About this task

 **NOTE:** Disabling OpenManage Enterprise plugins restarts the appliance services.

Steps

1. Click **Application Settings > Console and Plugins**.
The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Disable** for the plug-ins you want to disable.
The **Disable multiple plugins** wizard is displayed.
3. Select the plug-ins that you want to disable from the **Select plugins** section, and click **Next**.
The details of the number of users logged into OpenManage Enterprise, tasks in progress, and scheduled jobs are displayed in the **Confirmation** dialog box.
4. Confirm that you have taken a backup by enabling the checkbox and then click **Finish**.

Results

All disabled plug-in screens and information are hidden, and plug-in groups with disabled plug-ins are hidden from all group actions. However, if the actions were previously added, they remain members of features (firmware and configuration baselines, alert actions, and so on.).

 **NOTE:** If a group is modified while a plug-in is disabled, hidden groups are removed as members of the feature. To retain these memberships, enable the plug-in before editing group actions for various features.

Uninstall plugins

Uninstalls OpenManage Enterprise plugins, and deletes any collected data.

Prerequisites

- The Emergency Power Reduction (EPR) is not enabled on the device. View the EPR status of all devices and groups on the **Emergency Power Reduction** page.
- There are no active policies.

About this task

After you uninstall Power Manager, the iDRAC telemetry configuration is still enabled on the target servers. For a list of telemetry services enabled by Power Manager, see the Supported Protocols section.

To disable these configurations, perform one of the following actions:

- Create a server configuration template with a disabled telemetry streaming configuration in OpenManage Enterprise and deploy the template across all target devices.
- Manually disable the telemetry services in iDRAC on each device.

Steps

1. Click **Application Settings > Console and Plugins**.
The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Uninstall** for the plug-in you want to uninstall.
The **Uninstall multiple plugins** wizard is displayed.
3. Select the plug-ins that you want to uninstall from the **Select Plugin** section and then click **Next**.

The **Confirm Backup** section lists the number of logged-in users, tasks in progress, and scheduled jobs.

4. To confirm the uninstall, confirm that you have captured a backup of the appliance, and click **Finish**.

Results

The specified plug-ins are uninstalled, and the data that has been collected is deleted.

Troubleshooting

Definitions about some of the commonly displayed fields in OpenManage Enterprise are listed and defined here as well as other useful information.

Topics:

- [Devices](#)
- [Discovery](#)
- [Alerts](#)
- [Configurations](#)
- [Monitor](#)
- [Plugins](#)
- [Application Settings](#)
- [Upgrade](#)
- [Troubleshooting the Power Management features](#)
- [The Power Management feature Frequently asked questions](#)

Devices

Troubleshooting device issues includes resolving problems with inventory, health status, grouping, firmware updates, or remote actions like power control and iDRAC access.

Supported and unsupported actions on proxied sleds

Some device actions are not available for sleds in a proxied state. The following table shows supported and unsupported Redfish: actions on the proxied sleds.

Table 73. Supported and unsupported actions on proxied sleds

ID	Action	Description	RedFish
1	POWER_CONTROL_ON	Power up	YES
2	POWER_CONTROL_OFF	Power Down hard or graceful	YES
3	POWER_CONTROL_RESET	Power reset hard or graceful	YES
4	SENSOR_DETAILS	Get sensor info, subsystem health details.	No
5	POWER_MONITOR	Power statistics retrieval	YES
6	TEMPERATURE_MONITOR	Temp statistics retrieval	YES
8	FW_UPDATE	Update the firmware remotely.	YES
9	BLINK_LED	Identify function on the server.	YES
11	HW_LOGS	System Hardware logs	YES
12	DIAGS	Diagnostics	No
13	TSR	Tech Support Report	No
16	VIRTUAL_CONSOLE	Ability to run RACADM tasks	No
30	REMOTE_RACADM	14G specific features	No

Table 73. Supported and unsupported actions on proxied sleds (continued)

ID	Action	Description	RedFish
31	REMOTE_IPMI	14G specific features	No
32	REMOTE_SSH	14G specific features	No

Devices with unknown compliance status

The firmware or driver compliance status of the following devices in the firmware or driver baseline compliance reports is displayed as `Unknown` as the Dell firmware or driver catalog does not support firmware or software updates for these devices.

Table 74. False compliant devices

Device Category	Device List
Storage	• SC Series • MD Series • ME Series
Network devices in the FX2, M1000e, and VRTX chassis	• F10 switch • Input or Output Aggregators (IOAs) • Input or Output Modules (IOMs)
Hyperconverged Appliances (HCI)	• VxRail • XC Series
Devices that can be updated using the Dell Update Packages (DUP) of individual devices but not directly supported on Dell catalog	• MX9116n Fabric Engine • MX5108 n Ethernet Switch • PowerEdge MX5000s
Devices that cannot be updated using the Dell catalog or the individual DUP  NOTE: For firmware/driver update of these devices, see the Installation Guide of the individual devices.	• MX7116n Fabric Expander Module • PowerEdge MX 25 GbE PTM

 **NOTE:** For a complete list of devices in the SC, MD, ME, and XC series, see the *OpenManage Enterprise Support Matrix* on the support site.

Decommissioned or duplicate device entries in the discovery job

Reason: Frequent changes in device IP addresses result in duplicate and decommissioned device entries in the discovery job.

Resolution: To prevent the decommissioned or duplicate device entries that are caused due to frequently changing iDRAC or device IP addresses, configure the Fully Qualified Domain Name (FQDN) hostname on the devices. Then, discover the devices using their hostnames.

PowerEdge server displays multiple iDRAC management IPs in OpenManage Enterprise

Issue: The device details page of a PowerEdge server shows multiple IP addresses for the iDRAC management IP. Typically, a managed device should have only one iDRAC management IP. However, in some cases, multiple IP addresses may be associated with the device.

Cause:

- After a motherboard replacement, the system's service tag remains the same, but the iDRAC details change (new MAC address and new IP address).
- iDRACs use DHCP leases for their IP addresses. Upon renewal, a new IP address may be assigned.

Workaround: To resolve this issue, follow these steps:

1. Delete the device from OpenManage Enterprise.

 **NOTE:** Any associated profile must be unassigned first.

2. Rediscover the device using the new management IP address. This ensures that only the current IP address is retained in OpenManage Enterprise.

Devices not getting removed from nested static groups after deleting from the parent group

Reason: Parent groups list all devices that are in their child and nested groups.

Resolution: When removing devices from nested groups, you must initiate removal from child and nested groups and then from the parent group if needed..

Discovery

Troubleshooting discovery involves fixing failed discovery and onboarding of devices due to unreachable IPs, unsupported protocols, authentication issues, or misconfigured job settings.

Device rediscovery running for a long time after deleting iDRAC service account

When a device is managed using a service account and IP blocking is enabled in iDRAC, deleting the service account (local user) on iDRAC may cause OpenManage Enterprise to become locked out as it attempts to reconnect the device multiple times. In this case, the appliance deletes its credentials for the device, and the device becomes invisible within the 'All Device' page. When this occurs, the device must be rediscovered by re-running the original discovery job or creating a new one.

If the service account is deleted on the iDRAC and a rediscovery job is started before the appliance recognizes the device as unreachable, the rediscovery job may fail as the appliance continues to connect with the device using invalid credentials. When this occurs, re-run the discovery job once the device is no longer visible on the 'All Devices' page.

Troubleshooting power shelf onboarding failures

If an onboarding task fails for a power shelf, consider the following possible causes:

- Ensure that the target device is reachable over the network.
- Verify that there are no duplicate Redfish alert subscriptions on the target device for the same OpenManage Enterprise IP address.
- Confirm that the target device has not exceeded the maximum number of allowed Redfish alert subscriptions. For example, the Delta 21" power shelf supports a maximum of 15 Redfish subscriptions.

SONiC switch discovery or inventory fails

If discovery or inventory fails for a Dell SONiC switch, the issue might be related to the size or complexity of the configuration data on the switch. To resolve this issue:

1. Open the **Discovery** wizard.
2. Select the SONiC switch discovery task, and select **Edit**.
3. In the **Create Discovery Job** window, click **Additional Settings**.
4. Set the **Timeout** value to 300 seconds.
5. Re-run the discovery task.

Increasing the timeout allows OpenManage Enterprise to process large configuration responses.

Onboarding job fails with error CUSR6004

The onboarding job for newly discovered servers in OpenManage Enterprise may fail with the following error message: CUSR6004 - Unable to complete the operation because either user name or password is not correct. This issue can occur even when the discovery job completes successfully and the credentials that are used are valid. The onboarding job typically fails on the first attempt.

Recommended action: Re-run the discovery job for the affected devices. If the issue persists, verify and re-enter the credential profile that is used for discovery.

Alerts

Troubleshooting alerts focuses on misconfigured alert policies, missing or duplicate alert logs, SNMP/Syslog issues, or problems with alert categories and automatic alerting.

Alert categories after EEMI relocation

Provides a list of previous alert categories and subcategories and their corresponding new categories and subcategories after EEMI relocation.

Table 75. Alert categories

Previous Category	Previous Subcategory	New Category	New Subcategory
Audit	Devices	System Health	Devices
Audit	Devices	Configuration	Devices
Audit	Devices	Configuration	Devices
Audit	Devices	Configuration	Devices
Audit	Devices	Configuration	Devices
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Devices	Audit	Users
Audit	Templates	Configuration	Templates
Audit	Templates	Configuration	Templates
Audit	Templates	Configuration	Templates
Audit	Templates	Configuration	Templates
Audit	Templates	Configuration	Templates
Configuration	Inventory	Configuration	Job
Configuration	Inventory	Configuration	Job
Configuration	Inventory	Configuration	Job
Configuration	Inventory	Configuration	Devices
Configuration	Inventory	Configuration	Devices
Configuration	Inventory	Configuration	Devices
Configuration	Firmware	Configuration	Jobs
Configuration	Firmware	Configuration	Jobs

Table 75. Alert categories (continued)

Previous Category	Previous Subcategory	New Category	New Subcategory
Miscellaneous	Jobs	Configuration	Jobs
Miscellaneous	Jobs	Configuration	Jobs
Miscellaneous	Jobs	Configuration	Jobs
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Devices	Configuration	Devices
Miscellaneous	Devices	Configuration	Devices
Audit	Security	Configuration	Security
Audit	Security	Configuration	Security
Audit	Security	Configuration	Security

Token substitution in alert policy actions

OpenManage Enterprise supports token substitution for customizing remote scripts and email messages triggered by alert policies. This topic includes tables detailing the supported tokens for both email notifications and remote script execution.

Remote script tokens

Table 76. Tokens supported for remote script in OpenManage Enterprise

Tokens	Description
\$IP	IP address of the device.
\$HOSTNAME	FQDN or Hostname (if FQDN is not present).
\$SERVICETAG	Service tag.
\$ASSETTAG	Asset tag.
\$MODEL	Model name.
\$MSG	Alert message.
\$DATE	Date when the alert was received.
\$TIME	Time when the alert was received.
\$CATEGORY	Category of the alert.
\$SEVERITY	Severity level of the alert.
\$RESOLUTION	Recommended resolution action.

Email message tokens

Table 77. Tokens supported for email message in OpenManage Enterprise

Tokens	Description
\$ip	IP address of the device.
\$hostname	Hostname of the device.
\$name	Name of the device.
\$identifier	Identifier of the device.
\$assetTag	Asset tag of the device.
\$mac	MAC address of the device.
\$model	Model of the device.
\$id	ID of the alert.
\$severity	Severity level of the alert.
\$definition	Definition ID of the alert.
\$category	Category of the alert.
\$subcategory	Subcategory of the alert.
\$status	Acknowledgement status of the alert.
\$time	Timestamp of the alert.
\$message	Alert message.
\$eemiMessage	EEMI message of the alert.
\$action	Recommended resolution action.
\$messageId	Message ID of the alert.
\$catalogName	Catalog name of the alert.
\$msg	Alert message.

Configurations

Troubleshooting configurations involves addressing issues with profile creation, assignment, or redeployment, and resolving compliance mismatches caused by incorrect or outdated templates and baselines.

Firmware and DSU requirements for HTTPS

If HTTPS is enabled for network share operations, ensure that servers have the required minimum firmware and DSU to support HTTPS-enabled device operations.

Table 78. HTTPS Operations and minimum firmware and DELL EMC System Update (DSU) version requirements

Use Case or Operation.	14G servers and above
Firmware Update	Firmware v3.00.00.00
Driver Update	DSU v2.0.2
Server Configuration Profile (SCP) for template capture, deployment, configuration inventory, and remediation)	Firmware v3.00.00.00
Technical Support Report (TSR)	Firmware v3.21.21.21

Table 78. HTTPS Operations and minimum firmware and DELL EMC System Update (DSU) version requirements (continued)

Use Case or Operation.	14G servers and above
Remote Diagnostics	Firmware v3.00.00.00

Firmware schedule reference

Schedule a firmware update to run immediately or at a later point of time.

- **Update Now:** The firmware version is updated and matched to the version available in the associated catalog. To make the update become effective during the next device restart, select the **Stage for next server reboot** check box.
- **Schedule Later:** Select to specify a date and time when the firmware version must be updated.

Firmware baseline field definitions

The fields that are used while creating an OpenManage Enterprise firmware baseline.

- **COMPLIANCE** The rollup health status determines the health status of the firmware baseline. If any device associated with the baseline is in critical health, the baseline is considered critical. The rollup health status aligns with the highest severity within the baseline. For additional details, see the *Managing The Rollup Health Status By Using iDRAC On The Dell 14th Generation And Later PowerEdge Servers white paper* on the Dell TechCenter.
- **NAME** is the firmware baseline name. Click to view the baseline compliance report on the **Compliance Report** screen. For more information about creating a firmware baseline, see [Create a baseline](#).
- **CATALOG:** The firmware catalog to which the baseline belongs. See [Manage firmware and driver catalogs](#).
- **LAST RUN TIME:** The time when the baseline compliance report is last run. See [Check the compliance of firmware and drivers](#).

Schedule job field definitions

Defines the fields that are used to create a job.

- **Run now** to start the job immediately.
- **Run Later** to specify a later date and time.
- **Run On Schedule** to run repeatedly based on a selected frequency. Select **Daily**, and then select the frequency appropriately.

NOTE:

- When a Job is created to run later or scheduled for a different time, the job scheduler clock uses the local system or browser time for job execution, rather than the time specified in the appliance.
- By default, the job scheduler clock is reset at 12:00 A.M. everyday. The cron format does not consider the job creation time while calculating the job frequency. For example, if a job is started at 10:00 A.M. to run after every 10 hours, the next time the job runs is at 08:00 P.M.. However, the subsequent time is not 06:00 A.M. next day but 12:00 A.M.. This is because the scheduler clock is reset at 12:00 A.M. everyday.
- Post deleting and re-creating a specific user, scheduled jobs that are created with the user may fail due to changes in the internal identification of the user. Re-create the recurring task from the active user to avoid failure.

Monitor

Troubleshoot issues due to connectivity loss, disabled tasks, or appliance service errors affecting health polling, inventory refresh, warranty sync, and job executions.

Misleading global health task status

Misleading global health task status for DM or custom role users with access scope.

The Global Health Task status reflects the status of all devices, including those devices outside the user's access scope. The task may display `Completed with Error` even if all devices within the user's scope completed successfully.

If you see a `Completed with Error` status, verify with an administrator user to check if the errors are on devices outside your access scope. The task may have completed successfully for all devices within your scope.

Troubleshooting connectivity

From the **Monitor > Troubleshoot** screen, you can perform various device connectivity tests, test appliance connectivity to external Dell resources, restart the appliance, test accessibility to network shares, generate a console log bundle, and enable/disable field service debug (FSD).

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](#).

Test protocol availability for any undiscovered device

Verify if the following protocols are available for an undiscovered device: SNMP, WS-Man, Redfish, IPMI, SSH, VMware, or Rest_Storage.

Steps

1. On the **Monitor > Troubleshoot** screen click **Device**.
2. Select **Test Protocol Connection**.
3. In the **IP Address/HostName box**, enter the IP address or the hostname of the device.
4. From the **Additional Settings > Protocol** list, select one of the following: SNMP, WSMAN, REDFISH, IPMI, SSH, VMWARE, REST_STORAGE. If no protocol is selected under Additional Settings, ICMP is used by default..
 - a. Enter the other additional settings such as username and password, retries, timeout, port, and certificate validation, depending on the protocol.

 **NOTE:** SNMP testing can take longer to complete than other protocols due to the number of internal tests required.

5. Click **Test**.

Results

- The result is displayed as 'Success' or 'Failed' with the details of the attempt.
- If you select the Redfish protocol for chassis device, the **Test Protocol Connection** may return a successful result even when the credentials are incorrect for the target device. This occurs because the test validates network connectivity and protocol availability, but does not verify authentication.

Test protocol availability for a discovered device

Verify if the following protocols are available for a discovered device: SNMP, WS-Man, Redfish, IPMI, SSH, VMware, or Rest_Storage.

Steps

1. On the **Monitor > Troubleshoot** screen click on **Device**.
2. Select **Test Protocol Connection**.
3. In the **IP Address/HostName box**, enter the IP address or the hostname of the device.
4. Click **Test**.

Results

The result is displayed as 'Success' or 'Failed' with the details of the attempt.

Ping any device

Ping a device to see if it is accessible.

Steps

1. On the **Monitor > Troubleshoot** screen click on **Device**.
2. Select **Ping Device**.
3. Under **Additional Settings**, select values for **Retries** (1-31) and **Timeout** in seconds (1-100). The default value for **Retries** is 3 s and for **Timeout** is 60 s.
4. Click **Test**.

Results

The appliance sends data packets to the device and records any response that is received.

Test appliance connectivity

Verify that the appliance is connected to all web resources required to download MIBs, upgrade bundles, and so on.

Steps

1. On the **Monitor > Troubleshoot** screen, click **Appliance**.
2. From the **Sites** list:
 - Select **Select All Sites** to check connectivity with both Dell Online and Dell Warranty sites.
 - Select **Dell Online** to check connectivity with Dell Online.
 - Select **Dell Warranty Information** to check connectivity with the Dell Warranty site.
3. Choose the number of **Retries** (1-31). The default value is three.
4. Choose the **Timeout** seconds (1-100). The default is set at 60 s.
5. Click **Test**.

Restart the appliance

Restart the appliance from within the user interface without using the Text User Interface (TUI).

Steps

1. On the **Monitor > Troubleshoot** screen, click **Appliance**.
2. Select **Restart**.
3. Click **Restart**.

Results

The user logs out, and the appliance restarts.

Test connection with network share

Verify that the appliance is connected to all network shares and can access their contents.

Steps

1. On the **Monitor > Troubleshoot** screen click on **Network Share**.
2. Select **Share Type** as **CIFS** or **NFS**.
3. Enter the **Share Path** linked to the Network drive to be tested.
4. Enter the **Share IP Address**. If you are using CIFS, enter the **Workgroup**, **Username**, and **Password**.
5. Optional: Click on **Test Connection** to verify the connection to the share location.

 **NOTE:** You must have the Job management privilege to verify the test connection.

Results

The appliance attempts to reach the share and returns whether the share contents are accessible.

Generate and download console log archive

Generate archived console log data and download to a specified location.

Steps

On the **Monitor > Troubleshoot** screen click on **Logs**.

- a. To generate the console log archive file, click **Generate Log**.
A job is initiated to generate the log file.
- b. To download the generated console log archive file, click **Download Log**.

Results

The common dialog box lets the user specify the drive, directory, and name of the console log archive file to save to the local system.

Field service debug

Field service debug is exclusively for internal debugging within the OpenManage Enterprise appliance. It can only be activated with assistance from a certified Dell support representative.

Steps

1. Click **Monitor > Troubleshoot > FSD**.
2. Click the action that you want to perform.

Option	Description
Download dat.ini File	Download the dat.ini file.
Upload Signed dat.ini File, SSH Public Key	Upload the signed dat.ini file or SSH Public Key.
Invoke Debug Capability	Enable debug capability on the console.
Disable FSD	Disable the debug capability on the console.

 **NOTE:**

- When the debug capability is invoked, a Warning banner (Debug log collection is activated) is displayed. This warning banner is removed only when you disable FSD.
- Before you invoke the debug capability, ensure that the DAT.ini file is signed, returned by a certified Dell support representative, and uploaded to OpenManage Enterprise.
- Once you disable FSD, ensure that you stop any SSH daemon or SSH sessions that are using the debug capability.

Plugins

Troubleshooting plugin issues includes resolving failed installations, update errors, unmet system requirements, or plugin behavior conflicts with appliance resource limits.

Plugin does not meet minimum requirements

The most common cause for this error is inadequate memory assigned to the OpenManage Enterprise virtual machine (VM). Each plugin has specific memory requirements, and if the VM does not have enough allocated memory, the plugin may fail to install. Review the memory requirements for the plugin you are trying to install from the OME user's guide *OpenManage Enterprise hardware requirements* section. After increasing the memory, attempt to reinstall the plugin.

Application Settings

Troubleshooting application settings includes fixing misconfigured SNMP, SMTP, or Syslog settings, directory service issues, certificate mismatches, or alert display errors.

Unable to create new users or edit existing users

You may encounter the following error when trying to create or edit a user: `An unknown error has occurred. Please try again.`

This issue happens if you open the user creation or edit wizard immediately after logging in.

To avoid this issue, refresh your browser before performing any user management actions.

Catalog Management field definitions

Defines the fields on the **Catalog Management** screen.

CATALOG NAME: Name of the catalog. Built-in catalogs cannot be edited.

DOWNLOAD: Indicates the download status of catalogs from its repository folder. The statuses are: Completed, Running, and Failed.

REPOSITORY: Repository types such as Dell.com, CIFS, and NFS.

REPOSITORY LOCATION: Location where the catalogs are saved. Examples are Dell.com, CIFS, and NFS. Also, indicate the completion status of a job running on the catalog.

CATALOG FILE: Type of catalog file.

CREATED DATE: Date when the catalog file was created.

iDRAC virtual console fails to launch in OpenManage Enterprise

When attempting to **Launch Virtual Console** from OpenManage Enterprise, the console fails to open and displays an unknown error.

This issue may occur if the network subnet where the appliance is deployed is not excluded from proxy routing. Proxy interference can prevent the virtual console from establishing a direct connection.

To resolve this, go to **Application Settings > Network > Proxy Configuration**, and then update the **Proxy Exclusion List** to include the subnet IP of the network where OpenManage Enterprise is deployed.

Upgrade

Upgrade-related troubleshooting involves resolving upgrade failures, unmet prerequisites, or issues like loss of user roles and appliance settings post-upgrade.

User roles lost during upgrade

When upgrading to OpenManage Enterprise version 4.3.2, you may encounter issues with user roles being lost for custom role users. This issue can prevent users from logging in and result in the following error message: `Critical Error: The user name or password you entered is incorrect`. The system logs also show errors related to missing roles for the affected users. To manually restore user roles, see the [OpenManage Enterprise 4.3.2 API guide](#).

Troubleshooting the Power Management features

Data purge interval not reset

Scenario:

After reinstalling or updating to the latest version of OpenManage Enterprise, the data purge interval is not reset to the default value.

Resolution:

Reset the data purge value at the following location after you reinstall or update to the latest version of OpenManage Enterprise: **OpenManage Enterprise > Application Settings > Console Preferences > Metrics Collection Settings**

Failure to add devices for power management and monitoring

Scenario:

When you rediscover a device or an inventory job is in progress in OpenManage Enterprise, the following error message is displayed: `Value entered for id is invalid`

Resolution:

Add the devices for power management and monitoring after the discovery or inventory job is completed.

Why cannot I apply Emergency Power Reduction (EPR) on a target device or a group?

Scenario:

When you are trying to apply EPR on a device, the EPR operation may fail and there is an entry in the Audit Logs.

When you are trying to apply the EPR option on a group, the EPR operation may fail with the following error message: `The Emergency Power Reduction feature cannot be enabled on the group <group name> because either the member devices of the group cannot be accessed, do not have necessary license, or the Emergency Power Reduction (EPR) feature is already enabled.`

Resolution:

Ensure that all the following conditions are met:

- There is at least one device in the group that is eligible for applying EPR.
- **Throttle** option is applicable for the following devices:
 - Server with iDRAC Enterprise license

- PowerEdge M1000e or PowerEdge MX7000 chassis
- **Shutdown** option is applicable only for servers.

Power and temperature units are not updated on the UI

Scenario:

When you change the power and temperature units through REST APIs and check for the unit change updates in the UI, the updates are not reflected on the UI.

Resolution:

To view the updates on the UI after changing the power and temperature units through REST APIs, refresh the browser.

Why is OpenManage Enterprise unresponsive when I try to perform plug-in lifecycle-related actions?

Scenario:

The life cycle actions are install, uninstall, enable, or disable plug-ins.

After you reboot the OpenManage Enterprise appliance, if you try to perform any plug-in lifecycle-related actions for Power Management, the job is initiated in the back-end but you still see the Console and Plugins page. And, the following message is displayed after some time: `This page isn't working`

Resolution:

Wait for some time, and view the status. The plug-in lifecycle-related action is completed successfully.

The power cap limit or the percentage for the MX7000 chassis is not updated when either entry is changed

Scenario:

For an MX7000 chassis, the power cap limit is displayed as same as the upper bound value. When you manually change the power cap percentage, the value is not updated and even if you change the value, the percentage is not updated.

Resolution:

Provide the power cap limit, and save the policy. The policy imposes the specified power cap limit on the selected devices or groups.

Events not generated for alert thresholds

Scenario:

Events are not generated for the following combination of temperature threshold violations:

- Lower Warning to Upper Warning
- Lower Critical to Upper Critical
- Upper Warning to Lower Warning
- Upper Critical to Lower Critical

Resolution:

Provide realistic warning and critical values so that there are no immediate alert generating temperature changes.

Error when removing a device from a group using REST API

Scenario:

When you try to remove a device that is part of multiple groups using the REST API, then an error message is displayed.

Resolution:

To remove a device that is part of multiple groups, remove the device from the group in OpenManage Enterprise. The changes are automatically reflected in Power Management.

Multiple alerts for group membership changes in Audit Logs

Scenario:

Multiple entries on group membership changes in **Audit Logs**.

Resolution:

When devices are simultaneously added to and removed from a static group through OpenManage Enterprise, there are multiple entries of this update in the **Audit Logs** and **Alert Log**.

All options for managing physical groups are not displayed

Scenario:

After creating a physical group, you may not see **Create New Physical Group**, **Edit Group**, **Manage Rack**, **Delete Group**, or **Attributes** options when you right-click any group.

Resolution:

As a workaround, wait for some time or refresh the page, and then right-click the group. All the relevant options are displayed.

The Power Management feature Frequently asked questions

Why am I not able to view the metrics?

Cause: After you remove the required iDRAC or DC License, or the OpenManage Enterprise Advanced or Advanced+ Feature license, the license-dependent features are not available on the User Interface (UI). The metric is not available, and Power Management does not collect the values from the next inventory cycle.

Why do I see two entries with the same date in the graph when the time duration chosen for showing the graph is changed?

Cause: When you view the **Metrics** graph for 3 months, 6 months, or 1 year, the data is autoconverted from the UTC time zone to your current time zone and displayed. Due to the time zone differences, there are two entries for the same day on the graph. The last entry is for the current day, and the last but one entry is for the previous day.

Why do I see two entries with the same date in a graph?

Cause: After upgrading to OpenManage Enterprise 3.9, all the graphs might have multiple entries with the same date for a metric. After a maximum of 24 hours, the correct data points are displayed.

Why do I see slight variations in values of power and temperature in the Alert Thresholds section?

Cause: When the power and temperature values are provided in BTU/Hour and Fahrenheit, they are converted to Watt and Celsius. When the values are displayed, they are reconverted and rounded off to the next highest numbers. The values are slightly higher when displayed in BTU/Hour and Fahrenheit scale.

Why are there the same number of power cap limit or threshold violations for all the entries in my report?

Cause: For an in-built or custom report which consists of a violation attribute along with a timestamp attribute, the violation count that is displayed for all the entries is always for the latest value.

Why do I see blank entries for total energy consumed in reports or metrics graphs?

Cause: The **Total Energy Consumed** field has no entry for servers and PowerEdge MX7000 devices due to the following reasons:

- The energy consumption value is not available until the second metric collection is taken.
- If you change the **Data gathering interval** to 60 minutes, and then for a 60 minutes time period the **Energy Consumption** value cannot be calculated. This happens when data is collected for a day with hourly granularity for reports.
- If the power metric in iDRAC is reset during the interval that is chosen, and the latest reading has a lower value than the oldest reading.

Why do I see a failure of EPR in the audit log but EPR is applied successfully for the device?

Cause: Applying EPR on the target device may fail due to the following reasons:

- Connectivity issues between the appliance and the target device.
- If the target device is part of Power Management with an expired license.

Why do I see a failure of EPR in the audit log but EPR is applied successfully for the group?

Cause: When EPR is applied for a group, and if EPR is applied successfully for at least one device in the group, the EPR banner is displayed at the group level. However, the EPR option may fail on other devices within the group due to connectivity issues or license expiry and so on. Therefore, use the EPR audit logs for successful and failure scenarios for all devices of the group.

Why are devices not listed for addition to Power Management?

Cause: You cannot view certain devices in Power Management because of the following reasons:

- If devices do not have OpenManage Enterprise Advanced or Advanced+ license.
- If the devices are discovered in OpenManage Enterprise, and then Power Management is installed, then the devices are not displayed in Power Management until you **Run Inventory** on OpenManage Enterprise.
- Devices like switches, storage sleds, I/O modules are not supported in Power Management.
- Servers that are discovered through the operating system(in-band) are not supported in Power Management.

 **NOTE:** When OpenManage Enterprise and Power Manager are upgraded to the latest version 4.4 and 3.5 respectively, an inventory job must be manually initiated for PowerEdge 17G servers that are discovered in OpenManage Enterprise 4.3 and Power Manager 3.4 so that the PowerEdge 17G servers can be added to the Power Manager 3.5 monitoring list.

Why are policies being disabled when too many policies are selected for deletion or disable or enable?

Cause: When you select multiple policies for enabling or disabling or deleting, the job is initiated. However, the policies are disabled on the user interface (UI) until the action is complete. After the job is completed, there are entries to the audit logs for these actions.

Why cannot I remove some devices or groups from Power Management?

Cause: If you have applied an Emergency Power Reduction (EPR) option on the device or a group, then you cannot remove the device or group from Power Management.

Resolution: Disable the EPR option on the device or group, and then remove them from Power Management.

Why am I not able to apply policies on some devices or groups?

Cause: You can apply a policy only on devices that are supported on Power Management, having a valid license, and that are added to Power Management.

You can apply policies on supported PowerEdge servers with iDRAC Enterprise, PowerEdge FX2, FX2s, and VRTX chassis with CMC Enterprise license.

 **NOTE:** PowerEdge M1000e and PowerEdge MX7000 chassis do not require a CMC Enterprise license.

Why are some alerts not being forwarded using SNMP?

Cause: The following events are not forwarded as SNMP alerts:

- Device membership or group membership changes
- Device management such as change in license status

Alerts are generated in OpenManage Enterprise or Power Management that is displayed in the `system health` category and `metric/power configuration` subcategory the SNMP trap forwarding is not supported.

Why some email alerts are not getting forwarded?

Cause: The following events are not forwarded as SNMP alerts:

- Device membership or group membership changes
- Device management such as change in license status

SNMP trap forwarding is not supported.

Why are some devices automatically removed from Power Management?

Cause: If the OpenManage Enterprise Advanced or Advanced+ license has expired or is removed from a target node, then the device is removed from Power Management after the device capability check is run.

Why do I not see temperature metrics for some devices?

Cause: If the devices are powered off, the temperature metric is not visible.

Why can I not select a particular child group?

Cause: When you select a group, all the child groups within this group are also selected. When you clear a child group, the selection gets cleared at the main group level.

Why am I seeing No Data Available or No Information available message for some devices metrics?

Cause: When the first metric collection has not yet happened or if the device is not reachable, the following message is displayed: `No Data Available`

When a device is not added to Power Management even though it is a supported device, the following message is displayed: No Information available.

Why are some of the fields in reports empty?

Cause: The fields may be empty in a report due to the following reasons:

- The device was not reachable for that duration.
- That category is not applicable for that device.
- The values are not defined for certain fields in Power Management and these fields are part of the report. For example, when you have not configured the power and temperature threshold values for a device, the following fields are added to the report, but the values are not populated:
 - Upper Warning Power
 - Upper Critical Power
 - Lower Critical Temperature
 - Lower Warning Temperature
 - Upper Warning Temperature
 - Upper Critical Temperature

If you have configured the above threshold values and only when the threshold values are violated, the following fields are populated and displayed in the report:

- Lower Critical Violation Count
- Lower Warning Violation Count
- Upper Critical Violation Count
- Upper Warning Violation Count

Why do I not see regular metric data points in the metric graphs?

Cause: A metric graph having irregular metric points indicate that data was not collected for that device at that duration of time.

Why can I not clear the checkbox for policies?

Cause: If the policy is being enabled, disabled, or edited, the check box for policies in the **Power Policies** page is disabled . After the job is completed, you can clear the policy.

How do I see the old metric data?

Cause: The old metric data is not available after a few days because the data is deleted. This configuration depends on the selection of the **Delete Power Management data** available in the **Power Management Preferences** section.

Why are the values that I set using threshold REST API not configured?

Cause: If you use threshold REST API before installing and adding the devices to Power Management, the values are not retained.

Resolution: Install and add the devices to Power Management, and then use the threshold REST APIs.

How to delete power cap limits from devices when they are removed from power management and monitoring?

Cause: When a power policy is applied on a static group and a member device is removed from that static group in OpenManage Enterprise, and the policy is active, and then the power cap limit on the device is retained on the management console of the device.

Resolution: To remove the power cap limit on the device, login to the respective management console and disable the power cap policy.

How to remove EPR on a device that was part of the deleted physical group?

Cause:

Resolution: If one of the devices part of a physical group, have an Emergency Power Reduction (EPR) applied on them, and you delete the physical group from OpenManage Enterprise, the EPR is still active on the device.

Resolution: Though the device being a part of a physical group is deleted in OpenManage Enterprise, the device is available for power management and monitoring. To remove EPR on the device:

1. Click **Power Management > Emergency Power Reduction**. The **Emergency Power Reduction** tab is displayed.
2. Select the device and click **Disable**.

Why is the Metric Report Definition not updated for some devices when added for power management and monitoring?

Cause: If you add a device to the latest version of OpenManage Enterprise that has an older version of the Metric Report Definition, OpenManage Enterprise does not update the Metric Report Definition.

Resolution: Manually delete the old Metric Report Definition from the device.

Why an incorrect accelerator count is displayed?

When you upgrade to OpenManage Enterprise 4.5, an incorrect accelerator count is displayed until the first inventory of all the devices that are placed in the rack is completed. The compute must be discovered Out-of-Band using iDRAC for accurate reporting of accelerator count.

Appendix

Here are the details about all the filters that are used in the **Individual Devices** tab of Power Management.

- **Health State** indicates the working state of the device. The color symbols represent the corresponding health status—Ok, critical, and warning.

Table 79. Device health statuses in OpenManage Enterprise

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

- **Power State** indicates that the device is turned on or off.
- **Connection State** indicates whether the device is connected to OpenManage Enterprise.
- **Name** indicates the device name.
- **Service Tag/Identifier** indicates the unique code for the device.
- **Model** indicates the device model.
- **TYPE** indicates the type of devices—Server chassis, storage, and networking switch.
- **Managed State** indicates the onboarding status of the device.
 - **Error**—Device cannot be onboarded. Try by logging in by using the recommended privileges in the OpenManage Enterprise User's Guide.
 - **Managed**—Device is successfully onboarded and OpenManage Enterprise can manage the device.
 - **Monitored**—Device does not have management option (devices that are discovered by using SNMP).
 - **Managed with alerts**—Device is successfully onboarded, and OpenManage Enterprise has successfully registered its IP address with the device as a trap destination during discovery.
 - **Proxied**—It is available only for the MX7000 chassis. It indicates that the device is discovered through an MX7000 chassis and not directly.
- **Part of Group** indicates if the device is part of any group that is monitored for power.
- **State** indicates that the Power Management policy is enabled or disabled.
- **Description** indicates the device, policy, or job description.
- **Hostname** indicates the unique name of the device.
- **Type** indicates static power or temperature-triggered policy.
- **Assigned To** indicates to which device that the policy is assigned to.
- **EPR Source** indicates if the policy is applied manually or a system-triggered policy.
- **Size of Device (U)** indicates the rack space that the device consumes.
- **Estimated Max Power (W)** indicates the maximum power that is defined for the device.