OpenManage Enterprise 4.0.x

User's Guide

April 2024
Rev. A06

DELL Technologies

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.

© 2023-2024 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Revision history

The following table shows the revision history of this document:

Table 1. Revision history in OpenManage Enterprise 4.0.1

Revision	Date	Description
A06	April 2024	Updated Managing alerts chapter for appliance alert policy skipping multiple repeated alerts.
A05	April 2024	Added troubleshooting information for Dell Connectivity Service access token error.
A04	March 2024	Updated the prerequisite for internal iDRAC credential management.
A03	February 2024	Updated for OpenManage Enterprise 4.0.1 release: • Proxy requirements for Migrate an appliance.
A02	January 2024	Updated the certificate requirements for migration operation.
A01	December 2023	Updated disk requirements for deploying OpenManage Enterprise on KVM.
A00	October 2023	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 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 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.
Italic	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
Monospace italic	Variables.
`Monospace bold`	User input.
[ ]	Square brackets enclose optional values.
|	Vertical bars indicate different selections - the bar means "or".

Table 2. Typographical conventions (continued)

Typographical conventions	Description
{ }	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 (01:44 min)
- Creating a firmware baseline in OpenManage Enterprise (01:22 min)
- OpenManage Enterprise systems management console (02:02 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 Power Manager plugin: Click **OpenManage Enterprise Power Manager** > **OpenManage Enterprise Power Manager** > **Documentation**.
  - OpenManage Enterprise Update Manager plugin: Click **OpenManage Enterprise Update Manager** > **OpenManage Enterprise Update Manager** > **Documentation**.
  - OpenManage Enterprise CloudIQ plugin: Click **OpenManage Enterprise Connected Services** > **OpenManage Enterprise CloudIQ** > **Documentation**.
- For **OpenManage Enterprise APIs**, go to Dell Technologies developers portal. To display the API documentation of:
  - OpenManage Enterprise: Click **Servers** > **OpenManage Enterprise API**
  - OpenManage Enterprise Modular Edition: Click **Servers** > **OpenManage Enterprise Modular API**
  - OpenManage Enterprise Services plugin: Click **Servers** > **OpenManage Enterprise Services API**.
  - OpenManage Enterprise Update Manager plugin: Click **Servers** > **OpenManage Enterprise Update Manager API**
  - OpenManage Enterprise Power Manager plugin: Click **Servers** > **OpenManage Enterprise Power Manager API**
  - OpenManage Enterprise CloudIQ plugin: Click **CloudIQ Public API**

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.

Contents

Revision history....3
Preface....4

Chapter 1: Overview....13
New features....14
Licensing....15
Security....16
User roles....17
Role and scope-based access....17
Scalability and performance....21
OpenManage Enterprise plug-ins....21

Chapter 2: Deployment....23
Host system requirements....23
Deployment best practices....24
Deployment prerequisites....24
OpenManage Enterprise hardware requirements....24
Management ports and protocols....26
Device ports and protocols....28
Firewall exceptions....28
Deploy in VMware vSphere....29
Deploy in Microsoft Hyper-V....30
Deploy in KVM....30
Deploy in KVM using virt-install....31
Deploy programmatically....32
Configure the system using the TUI....34

Chapter 3: Getting started....38
Log in to an appliance....38
Initial onboarding....39
The Welcome to OpenManage Enterprise dialog....39
The OpenManage Enterprise GUI....40
The OpenManage Enterprise menu bar....42
The OpenManage Enterprise dashboard....43
Doughnut charts....44
Device health statuses....45
The OpenManage Enterprise home screen....45

Chapter 4: System configuration....46
Configure network settings....46
Manage users, roles, and scopes....47
User roles....48
Role and scope-based access....49
Add or edit local users....52
Edit OpenManage Enterprise user properties....53

Enable OpenManage Enterprise users... 53
Disable OpenManage Enterprise users... 53
Delete OpenManage Enterprise users... 54
Import Active Directory and LDAP groups... 54
Transfer of ownership of device manager entities... 55
Ending user sessions... 56
Directory services integration... 56
Add or edit the Active Directory connection... 56
Add or edit LDAP connection... 57
Delete Directory services... 59
Login using OIDC providers... 59
Add an OIDC provider... 60
Configure OIDC login using PingFederate... 61
Configure OIDC login using Keycloak... 61
Test OIDC registration... 62
Edit an OIDC providers details... 62
Enable OIDC providers... 63
Delete OIDC providers... 63
Disable OIDC providers... 63
Security certificates... 63
Generate and download a certificate signing request... 64
Assign a web server certificate to an appliance... 64
Manage console settings... 65
Internal iDRAC credential management... 68
Enable internal OME password rotation feature... 69
Enable CyberArk integration for password management... 69
Set the login security properties... 70
Customize the alert display... 72
Configure SMTP, SNMP, and Syslog... 72
Manage incoming alerts... 73
Set SNMP Credentials... 74
Manage warranty settings... 74
Configure remote commands and scripts... 75
OpenManage Mobile settings... 75
Enable or disable alert notifications for OpenManage Mobile... 76
Enable or disable OpenManage Mobile subscribers... 76
Delete an OpenManage Mobile subscriber... 77
View the alert notification service status... 77
Notification service status... 77
View information about OpenManage Mobile subscribers... 78
OpenManage Mobile subscriber information... 78
Troubleshooting OpenManage Mobile... 79

Chapter 5: Discovering devices... 80
Server-initiated discovery ... 81
Create a device discovery job... 83
Onboarding devices... 84
Protocol support matrix for discovering devices... 85
View device discovery job details... 87
Edit a device discovery job... 87

Run a device discovery job....87
Stop a device discovery job....87
Discover multiple devices by .csv import....88
Global exclusion of ranges....88
Specify a discovery mode for server discovery....89
Create a custom discovery job for servers....89
Specify discovery mode for chassis discovery....91
Create a custom discovery job for the chassis....91
Specify discovery mode for Dell storage discovery....92
Specify discovery mode for network switch discovery....93
Create a custom discovery job for HTTPS storage devices....93
Create a custom discovery job for SSH devices....93
Create a custom discovery job for SNMP devices....94
Specify the discovery mode for multiple discovery jobs....94
Delete a device discovery job....95

Chapter 6: Managing devices and device groups....96
Organize devices into groups....96
Create a custom static or query group....98
Create a static device group....99
Create a query device group....99
Edit a static group....100
Edit a query group....101
Rename a static or query group....101
Delete a static or query device group....101
Clone a static or query group....102
Add devices to a new group....102
Add devices to existing group....103
Refresh health on group....103
All Devices screen device list....104
All Devices screen actions....104
Delete devices from OpenManage Enterprise....105
Exclude devices from OpenManage Enterprise....106
Run inventory on devices....106
Update the device firmware and drivers by using baselines....107
Refresh the device health of a device group....108
Refresh health on devices....108
Roll back an individual device's firmware version....109
Export the single device inventory....109
Performing more actions on chassis and servers....110
Hardware information displayed for MX7000 chassis....110
Export data....110
View and configure individual devices....111
Device Details....111
Device hardware information....112
Run and download diagnostic reports....112
Extract and download a Services report....113
Managing individual device hardware logs....113
Run remote commands on managed devices....114
Launch the iDRAC device management application....114

Launch the virtual console ... 114
Attaching iDRAC virtual media ... 115
Refresh device inventory of a single device ... 115

Chapter 7: Managing device inventory ... 116
Create an inventory job ... 116
Run an inventory job now ... 117
Stop an inventory job ... 118
Delete an inventory job ... 118
Edit an inventory schedule job ... 118

Chapter 8: Managing device firmware and drivers ... 119
Manage firmware and driver catalogs ... 120
Add a catalog by using Dell.com ... 120
Add a catalog to the local network ... 121
SSL Certificate Information ... 122
Update a catalog ... 122
Edit a catalog ... 123
Delete a catalog ... 123
Create a baseline ... 123
Edit a baseline ... 124
Delete a baseline ... 124
Check the compliance of firmware and drivers ... 125
View the baseline compliance report ... 125
Update the device firmware and drivers ... 126

Chapter 9: Managing device deployment templates ... 129
Create a deployment template from a reference device ... 130
Create a deployment template by importing a template file ... 131
View a deployment template information ... 131
Edit a server deployment template ... 131
Edit a chassis deployment template ... 133
Edit IOA deployment template ... 133
Edit network properties of a deployment template ... 133
Deploy device deployment templates ... 134
Deploy IOA deployment templates ... 136
Clone deployment templates ... 137
Auto deploy device configuration before discovery ... 137
Create auto deployment targets ... 137
Delete auto deployment targets ... 138
Export auto deployed target details ... 139
Overview of stateless deployment ... 139
Managing identity pools for stateless deployment ... 139
Creating identity pools ... 140
Define networks ... 145
Network types ... 145
Edit or delete a configured network ... 146
Export VLAN definitions ... 146
Import network definitions ... 146

Chapter 10: Managing device warranty....148
View and renew device warranty....148
Internal warranty alerts....149

Chapter 11: Managing alerts....150
View alert logs....150
Manage alert logs....151
Alert policies....153
Configure and manage alert policies....153
Automatic alerts on the MX7000 chassis....157
Alert definitions....157

Chapter 12: Managing MIB files....159
Import MIB files....159
Edit MIB traps....160
Remove MIB files....161
Resolve MIB types....161
Download an OpenManage Enterprise MIB....161

Chapter 13: Configuring profiles....162
Create profiles....163
View a profiles details....163
View a profiles network....164
Edit a profile....164
Assign a profile....165
Unassign profiles....166
Redeploy profiles....166
Migrate a profile....167
Delete profiles....167

Chapter 14: Configuration compliance....168
Manage compliance templates....169
Create a compliance template from deployment template....169
Create a compliance template from reference device....170
Create a compliance template by importing from a file....170
Clone a compliance template....170
Edit a compliance template....171
Create a configuration compliance baseline....171
Edit a configuration compliance baseline....172
Delete configuration compliance baselines....173
Refresh compliance of the configuration compliance baselines....173
Remediate noncompliant devices....174
Export a compliance baseline report....175
Remove a configuration compliance baseline....175

Chapter 15: Using jobs for device control....176
Create and manage jobs....176
View job lists....176

Jobs status and Jobs type description ... 177
Default jobs and job schedules ... 178
Create a job to blink device LEDs ... 181
View job details ... 182
Create a job for managing power devices ... 182
Create a remote command job for managing devices ... 183
Create a job to change the virtual console plugin type ... 183
Select target devices and device groups ... 184
Manage jobs ... 184

Chapter 16: Monitoring audit logs ... 185
Forward audit logs to remote Syslog servers ... 186

Chapter 17: Monitoring reports ... 187
Run reports ... 188
Run and email reports ... 189
Edit reports ... 189
Schedule and delivery options for reports ... 190
Copy reports ... 190
Delete reports ... 191
Create a report ... 191
Select the query criteria ... 192
Export selected reports ... 193
View and remove report schedule details ... 193

Chapter 18: Back up, restore, or migrate ... 195
Appliance states ... 196
Backup an appliance ... 196
Restore an appliance ... 197
Migrate an appliance ... 199
Migrate out an appliance ... 199
Migrate in an appliance ... 201

Chapter 19: Updating the console and plugins ... 204
Update prerequisites ... 204
Online update ... 205
Define online update settings ... 206
Update the appliance from dell.com ... 206
Configuring a local network share for offline update ... 207
Create the directory structure and download the update bundles ... 207
Configure an NFS network share on a Windows server ... 208
Configure an NFS network share on a Linux server ... 208
Configure an HTTP network share on a Windows server ... 209
Enable read and write access to your network share ... 211
Offline update ... 211
Download update files to local network share ... 212
Initiate update from a network share ... 213
System-generated postupgrade task ... 213

Chapter 20: Managing plugins....215
Install plugins....216
Enable plugins....216
Update plugins....217
Disable plug-ins....218
Uninstall plugins....218

Appendix A: Troubleshooting....219
Troubleshooting connectivity....219
Test protocol availability for any undiscovered device....219
Test protocol availability for a discovered device....220
Ping any device....220
Test appliance connectivity....220
Restart the appliance....220
Test connection with network share....221
Generate and download console log archive....221
Field service debug....221
Firmware and DSU requirements for HTTPS....222
Firmware schedule reference....222
Firmware baseline field definitions....222
Supported and unsupported actions on proxied sleds....222
Schedule job field definitions....223
Alert categories after EEMI relocation....223
Token substitution in remote scripts and alert policy....225
Catalog Management field definitions....225
Devices with unknown compliance status....225
Device rediscovery running for a long time after deleting iDRAC service account....226
Dell Connectivity Service : Failed with exception: Unable to get access token from DCS....226

1

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.
- Manage virtual identity settings across devices using intelligent 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.

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 GUI, where the navigation is designed by considering the sequence of tasks that are predominately used by an administrator and device manager. 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.

The typical sequence of tasks that are performed by OpenManage Enterprise users is:

1. Deployment
2. Configure the system using the TUI
3. Discovering devices
4. Managing devices and device groups
5. The OpenManage Enterprise dashboard
6. Organize devices into 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
- User roles
- Role and scope-based access
- Scalability and performance
- OpenManage Enterprise plug-ins

New features

The new features introduced in this major version of OpenManage Enterprise.

Table 3. New features in OpenManage Enterprise 4.0.1

Functional area	Feature description	Summary of benefits
Migration	Enhancements and Fixes: • Fixed migration issue observed in a proxy enabled setup. Therefore, a 3.10.x source appliance using proxy for Internet can communicate with a target appliance version 4.0.1 during migration. • Fixed hash comparison failure that results in decryption error on target appliance.	Customers using proxy for Internet can migrate to 4.0.1 from 3.10.x.

Table 4. New features in OpenManage Enterprise 4.0

Functional area	Feature description	Summary of benefits
Back up, restore, and migration.	VM to VM streaming using Migrate In.	• Stream backup data from a source appliance to a target appliance. • This feature only supports migrations from OpenManage Enterprise 3.10.x to OpenManage Enterprise 4.0.
Initial onboarding	Default plug-in (CloudIQ and Service Plug-ins) installation.	• Services and CloudIQ plug-ins are automatically installed when you download and install OpenManage Enterprise. • You can also defer default plug-in installation during appliance setup and install them later.
Device management	The iDRAC Password Management feature allows password management solutions to manage passwords of supported iDRACs.	• With the **Internal iDRAC credential management** option, OpenManage Enterprise creates encrypted credentials to access iDRAC, along with

Table 4. New features in OpenManage Enterprise 4.0 (continued)

Functional area	Feature description	Summary of benefits
		an option to rotate them at regular intervals. • With the **CyberArk Integration** option, OpenManage Enterprise supports customers who use the CyberArk identity security platform. OpenManage Enterprise can now access iDRAC passwords from the CyberArk vault.
Appliance communication	Redfish support	Added Redfish protocol support for onboarding, offboarding, template, and profile management.
Security enhancements	SMB 1 deprecated	SMB 1 is no longer supported on appliance shares: • SMB 1 support is removed. • Only SMB 2 is supported for CIFS, enhancing security for the appliance share.
	TLS1.3 and cipher suite support	Network security is enhanced with TLS 1.3 and cipher suite support.
	Secure boot	The preboot environment is now protected by ensuring that only trusted software is allowed to run during appliance startup.
	RSA SecurID authentication	Administrators can select which appliance users, including other administrators, require multifactor authentication to log in to the appliance.
	OpenManage Enterprise is now based on the common operating system SLES 15 SP4.	OpenManage Enterprise is now based on the common operating system SLES 15 SP4.

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

The Advanced license is required to use the following features of OpenManage Enterprise:

- Bare metal server deployment and cloning
- Deploy automatically with service tag or node IDs.
- Editable chassis templates
- Power Manager plugin
- Monitor and enforce configuration compliance.
- Virtual address management and stateless provisioning

- IOA provisioning and VLAN management
- MX platform profile management
- Boot to ISO
- Server configuration deployment
- Server configuration compliance baseline creation and remediation.
- iDRAC password management

The Advanced+ license is required to use the following features of OpenManage Enterprise:

- Support for all partner plugins - when available:
  - VMware vCenter plugin
  - Microsoft System Center plugins
- Support for partner integration - when available:
  - ServiceNow integration
  - CyberArk integration

NOTE:

- To access features of the 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.
- The *OpenManage Advanced+* license contains all the features of *OpenManage Advanced license*

Supported servers

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

- 13G servers that have the iDRAC8 2.50.50.50 or later firmware versions.
- 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 by using features such as Role-based access control (RBAC), scope-based access, SELinux, encryption, and 256-bit encrypted browsers.

Some of the security features of OpenManage Enterprise are:

- Role-based access control allows different device management functionality for different user roles (Administrator, Device Manager, Viewer).
- Scope-based access control allows an administrator to determine the device groups that the device managers 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 (Admin, DeviceManager, or Viewer).
- Running device management actions requires an account with appropriate privileges on the device.

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 5. User roles

Role	Privileges
Backup Administrator	The ability to perform all actions on the console by UI or REST API, including backup, restore, and migration. ● Users cannot manage or edit this role as it is internal and predefined. ● This role is only assigned to the preconfigured **admin** user.
Administrator	The ability to perform all actions on the console by UI or REST API except backup, restore, and migration. 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, Microsoft Active Directory (AD), and LDAP users and assign roles. ● Enable and disable users. ● Modify the roles of existing users. ● Delete the users. ● Change the user password.
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.

- 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 table below lists the privileges of each role.

Table 6. Privileges of OpenManage Enterprise roles

Privilege	Description	User roles			
		Backup Administrator	Administrator	Device Manager	Viewer
Backup, restore, and migration	Back up, restore, and migrate appliance.	**Y**	N	N	N
Appliance setup	Global appliance settings involving the setting up of the appliance	**Y**	**Y**	N	N
Security setup	Appliance security settings	**Y**	**Y**	N	N
Alert management	Alerts actions or management	**Y**	**Y**	N	N
Fabric management	Fabric actions or management	**Y**	**Y**	N	N
Network management	Network actions or management	**Y**	**Y**	N	N
Group management	Create, read, update, and delete for static and dynamic groups.	**Y**	**Y**	N	N
Discovery management	Create, read, update, and delete for discovery tasks and run discovery tasks.	**Y**	**Y**	N	N
Inventory management	Create, read, update, and delete for inventory tasks and run inventory tasks.	**Y**	**Y**	N	N
Trap management	Import MIB, Edit trap	**Y**	**Y**	N	N
Auto-deploy management	Manage auto-deploy configuration operations.	**Y**	**Y**	N	N
Monitoring setup	Alerting policies, forwarding, Services (formerly SupportAssist), and so on.	**Y**	**Y**	**Y**	N
Power control	Reboot or cycle device power	**Y**	**Y**	**Y**	N
Device configuration	Device configuration, application of templates, manage or migrate I/O identity, storage mapping (for storage devices), and so on.	**Y**	**Y**	**Y**	N
Operating system deployment	Deploy the operating system, map to LUN, and so on.	**Y**	**Y**	**Y**	N
Device update	Device firmware update, application of updated baselines, and so on	**Y**	**Y**	**Y**	N
Template management	Create or manage templates.	**Y**	**Y**	**Y**	N

Table 6. Privileges of OpenManage Enterprise roles (continued)

Privilege	Description	User roles			
		Backup Administrator	Administrator	Device Manager	Viewer
Baseline management	Create, manage firmware, and configuration baseline policies.	**Y**	**Y**	**Y**	N
Power management	Set power budgets	**Y**	**Y**	**Y**	N
Job management	Job execution or management.	**Y**	**Y**	**Y**	N
Report management	Create, read, update, and delete operations on reports.	**Y**	**Y**	**Y**	N
Report run	Run reports	**Y**	**Y**	**Y**	**Y**
View	View all data, report execution or management, and so on.	**Y**	**Y**	**Y**	**Y**

Scope-based access control (SBAC)

Using Role-Based Access Control (RBAC) administrators can assign roles while creating users. Roles determine their level of access to the appliance settings and device management features. Scope-based Access Control (SBAC) is an extension of the RBAC feature that allows an administrator to restrict a Device Manager role to a subset of device groups called scope.

While creating or updating a device manager, administrators can assign scope to restrict operational access of Device Manager to one or more system groups, custom groups, and plug-in groups.

Administrator and Viewer roles have unrestricted scope. That means they have operational access as specified by RBAC privileges to all devices and groups entities.

The scope can be implemented as follows:

1. Click **Create** or **Edit User**.
2. Assign a Device Manager role.
3. Assign scope to restrict operational access.

For more information about managing users, see Manage users, roles, and scopes.

Using SBAC administrators can implement an Restricted View feature. With Restricted View, the Device Managers only see the following:

- 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 the scope of a Device Manager is 'unrestricted', then that Device Manager can view all the devices and groups, however, would only be able to see the entities owned by the user such as jobs, alert policies, baselines, and so on along with the community and built-in entities of any kind.

When a Device Manager with an assigned scope logs in, the Device Manager can see and manage scoped devices only. Also, the Device Manager can see and manage entities such as jobs, firmware templates, configuration templates and baselines, alert policies, profiles, and so on, associated with scoped devices, only if the Device Manager owns the entity (Device Manager has created that entity or is assigned ownership of that entity). For more information about the entities a Device Manager can create, see Role-Based Access Control (RBAC) privileges in *OpenManage Enterprise User's Guide*.

For example, by clicking **Configuration** > **Templates**, a Device Manager user can view the default and custom templates owned by the Device Manager user. Also, the Device Manager user can perform other tasks as privileged by RBAC on owned templates.

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

Similarly, by clicking **Configuration** > **VLANs Pools**, the Device Manager can see all the VLANs created by the admin and export them. The Device Manager cannot perform any other operations. If the Device Manager has a template, it 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 or importing AD or LDAP user. Scope assignment for OIDC users can be done only on Open ID Connect (OIDC) providers.

SBAC for local users

- While creating or editing a local user with Device Manager role, admin can select one or more device groups that defines the scope for the Device Manager. For example, you (as an administrator) create a Device Manager user with a name dm1 and assign group *g1* present under custom groups. Then dm1 will have operational access to all devices in *g1* only. The user dm1 cannot access any other groups or entities that are related to any other devices.
- Furthermore, with SBAC, dm1 cannot view the entities created by other Device Managers (say dm2) on the same group *g1*. That means a Device Manager user can view the entities that are owned by the user. 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 can 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 Device Manager the 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 are 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, Device Manager, 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 EMC OpenManage Enterprise support site.

: The administrator can transfer owned resources from a device manager (source) to another device manager. For example, an administrator can transfer all the resources assigned from a source dm1 to dm2. A device manager with owned entities such as firmware and configuration baselines, configuration templates, alert policies, and profiles are considered an eligible source user. Transfer of ownership transfers only the entities and not the device groups (scope) owned by a device manager to another. For more information see, Transfer of ownership of device manager entities.

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 8. 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.
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.

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 9. OpenManage Enterprise plug-ins

Plugin name	Description
Services	Enables proactive and predictive monitoring and management support for your devices with ProSupport and ProSupport Plus.
Power Manager	Provides visibility to power consumption, system anomalies, and resource utilization on servers.
Update Manager	Enables managing custom Repositories and Catalogs of firmware and Windows Driver updates available for Dell PowerEdge servers.
CloudIQ	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, Windows Server HCI cluster creation, hardware patching, firmware update, and Dell servers and modular system maintenance.

Table 9. OpenManage Enterprise plug-ins (continued)

Plugin name	Description
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.

2

Deployment

OpenManage Enterprise is provided as an appliance deployed on a hypervisor. The virtual appliance can be configured from the application web client after initial network provisioning in the Text User Interface (TUI).

To view and update the current OpenManage Enterprise version, see Updating the console and plugins.

Topics:

- Host system requirements
- Deployment best practices
- Deployment prerequisites
- 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 10. Minimum host system requirements

System components	Minimum requirements
Hypervisors	• VMware vSphere supported on ESXi 6.7 or higher. **NOTE:** ○ Secure boot requires firmware boot option as Extensible Firmware Interface, and is only supported on ESXi 6.7 or higher. ○ Ensure that any ESXi to be deployed is disconnected from vCenter. • Microsoft Hyper-V Generation 2 virtual machines supported on Windows Server 2019 or later. • KVM supported on Red Hat Enterprise Linux 6.5 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

Deployment best practices

Consider the following best practices when deploying OpenManage Enterprise.

Table 11. 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.	• 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.

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.

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

Starting from the OpenManage Enterprise 4.0 version, the appliance is shipped with the maximum recommended hardware requirements to provide you 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 hardware requirements to determine the appropriate hardware resources required for your specific requirements. The following table lists recommended hardware requirements for installing OpenManage Enterprise and all of its plugins.

Table 12. Appliance default hardware configuration

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

Table 12. Appliance default hardware configuration

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 VHDX.
- 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 13. Large deployment where the maximum number of devices managed by OpenManage Enterprise is up to 8,000

OpenManage Enterprise appliance and plugins	Minimum RAM [a]	Minimum cores
OpenManage Enterprise	32 GB	8
Additional requirements for each plug-in		
CloudIQ plug-in (Default plug-in)	+4 GB	
Services (Default plug-in)	+8 GB	
Power Manager	+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	64 GB	8 CPU cores

a. **NOTE:** If you want to migrate from an OpenManage Enterprise 3.10.x appliance to a later version, while deploying the OpenManage Enterprise 4.0.x version, ensure that you allocate the minimum required memory (required for the migration of both OpenManage Enterprise and its plug-ins from 3.10.x) even if you plan to decline the installation of default plug-ins during the migration process. Else, migration will not be allowed.

Table 14. Small deployment where the maximum number of devices managed by OpenManage Enterprise is up to 1,000

OpenManage Enterprise appliance and plugins	Minimum RAM [a]	Minimum cores
OpenManage Enterprise	16 GB	4
Additional requirements for each plug-in		
CloudIQ plug-in (Default plug-in)	+2 GB	
Services (Default plug-in)	+8 GB	
Power Manager	+3 GB	

Table 14. Small deployment where the maximum number of devices managed by OpenManage Enterprise is up to 1,000 (continued)

OpenManage Enterprise appliance and plugins	Minimum RAM [a]	Minimum cores
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 istalled	40 GB	4 CPU cores

a. **NOTE:** If you want to migrate from an OpenManage Enterprise 3.10.x appliance to a later version, while deploying the OpenManage Enterprise 4.0.x version, ensure that you allocate the minimum required memory (required for the migration of both OpenManage Enterprise and its plug-ins from 3.10.x) even if you plan to decline the installation of default plug-ins during the migration process. Else, migration will not be allowed.

Management ports and protocols

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

Table 15. 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)

Table 15. Ports and protocols on management stations (continued)

Port	Protocol	Type	Encryption	Source	Direction	Destination	Usage
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.
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

Table 15. Ports and protocols on management stations

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.

Device ports and protocols

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

Table 16. 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.
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 iDRAC7 and later versions. • Manage CMC. • To download firmware or driver DUPs • To upload or download deployment templates
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.

Firewall exceptions

Some OpenManage Enterprise features require access to external resource URLs.

Table 17. 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

Table 17. External resources (continued)

Feature	External resource URL [a]
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

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

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 ESXi 6.7 or later versions.
- 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.
- Ensure that any ESXi to be deployed is disconnected from vCenter.

NOTE: 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.

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 or OVA 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 on 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 pre-allocate 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 completes, the VM will be booted up.

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).

Deploy in Microsoft Hyper-V

Deploy OpenManage Enterprise on Hyper-V 2016 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 **New 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.

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 4.0 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

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 18. Parameters and Descriptions

Parameter	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.
memory	Memory to allocate for guest instance in megabytes.
vcpus	The number of virtual processors that are assigned to the VM
disk	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 `bus=sata` after the image file names as shown in the example below.
os-variant	For OpenManage Enterprise 4.0 and later, the operating system is *SUSE Linux Enterprise 15 SP4 (15.4)*. **NOTE:** Use the below command to find a list of accepted `os-variant` values for your version of virt-install: `virt-install --os-variant list`
network	Connect the VM to the host network.
graphics	When set to true, a graphical console is allocated to the VM.
listen	When set to 0.0.0.0, a VNC display is used.
noautoconsole	If this modifier is provided, the VM does not automatically try to connect to the guest console.
boot	[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 4.0_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

Deploy programmatically

OpenManage Enterprise can be deployed programmatically (using a script) on VMware ESXi version 6.5 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 and extract the `openmanage_enterprise_ovf_format.zip` file or download the following OVF files individually from the Dell support site:
   - `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`

   Place the files in the same folder where the OVF tool is installed (The default location is `C:\Program Files\VMware\VMware OVF Tool`).

2. Open the `ovf_properties.config` and set the following parameters:

Table 19. Parameters in `ovf_properties.config`

Parameter	Accepted Values	Description
bEULATxt	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 ovf_properties.config file.
adminPassword	• 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.
bEnableDHCP	true or false	Set to true if you want the appliance to enable IPv4 DHCP and to ignore the static IPv4.
bEnableIpv6AutoConfig	true or false	Set to true if you want the appliance to enable IPv6 auto configuration and to ignore the static IPv6.
staticIP	static IP in CIDR format	IP addresses can be IPv4 or IPv6. (You cannot set both the IPv4 and IPv6 types at a time.)
gateway	IPv4 or IPv6	You cannot set static Gateway as IPv4 and IPv6 types at a time.

3. 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, OVA, 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

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 20. 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, Tomcat, Database, and Monitoring 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.

Table 20. Text User Interface options (continued)

Options	Descriptions
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. • **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:** • 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 *Multihoming on OpenManage Enterprise technical white paper* 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.

Table 20. Text User Interface options (continued)

Options	Descriptions
	NOTE: If multihoming is enabled, the appliance can be accessed from two 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 *Multihoming on OpenManage Enterprise technical white paper* 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 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.

Table 20. Text User Interface options (continued)

Options	Descriptions
	○ Use the **Options** menu to select all services, clear all selections, or restore state before you make changes. ● **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. **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: `NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439].` ● 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.

3

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 4.0 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 to 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. Choose whether you are migrating from a 3.10.x appliance or setting up a new appliance.

   The default TLS protocol for a migration destination is **TLS 1.2 only**. For new appliances, the default TLS protocol is **TLS 1.2 and higher**.
   - To proceed with default plug-in (CloudIQ and Service plug-ins) installation, select the **End User License Agreement** and the **Infrastructure Telemetry Notice** 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 this appliance is a migration destination, the **Migrate In** screen appears. To complete the migration process on the 4.0 or later target appliance, see Migrate in an appliance.
   - For a fresh installation with all required agreements, 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 OpenManage Enterprise 4.0.x.

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.

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 **Primary NTP Server Address** and **Secondary NTP Server Address** (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 and does not use a trusted third-party certificate. Using this option ignores the system-defined certificate checks used for the warranty and catalog synchronization.
   - Enter IPv4, IPv6 addresses, or domain names of devices exempt from the proxy server in the **Proxy Exclusion list** field.

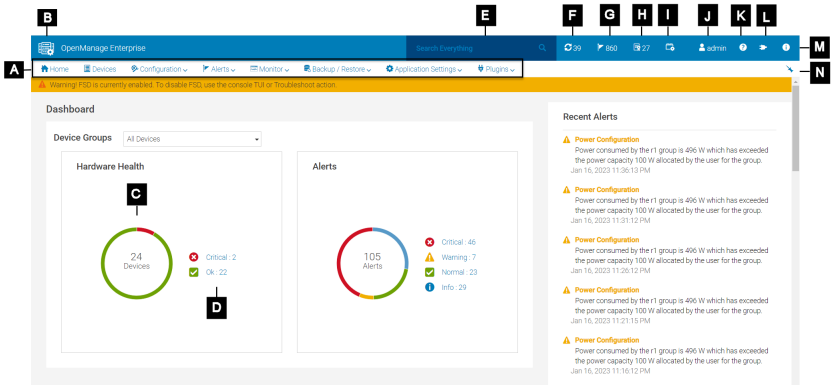
4. Click **Apply** to save the settings.

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.



- **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 ".**
- **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.

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 privileges (Administrator, Device Manager, and Viewer) can view the message, but only an Administrator can update the version. An Administrator can choose to get reminded later or dismiss the message. For more information about updating the OpenManage Enterprise version, see 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

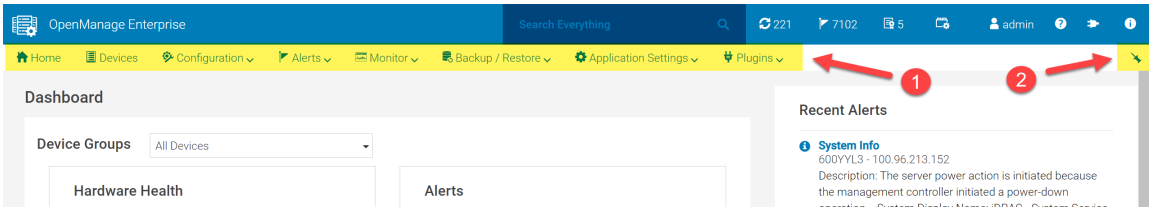
The OpenManage Enterprise menu bar

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

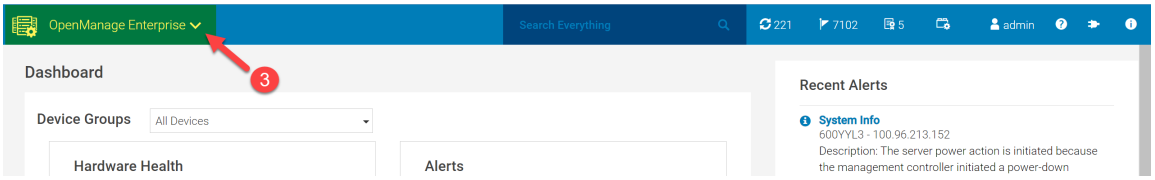
NOTE: The state of the **Menu bar** (pinned or unpinned) is saved for each user role. This means that if the **Administrator** unpins the **Menu bar**, it will remain unpinned with every subsequent **Administrator** log-in, until the **Administrator** pins it again.

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

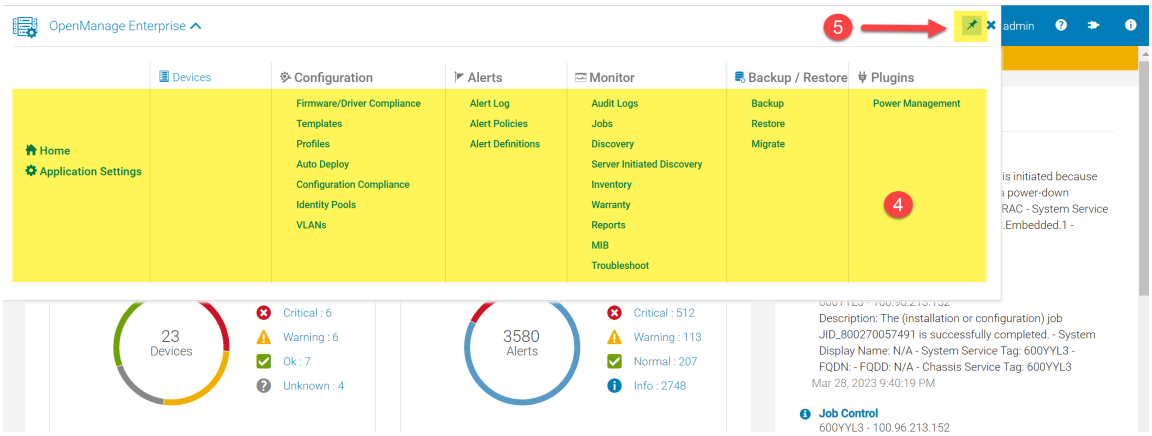
(2) Click the **pin** to the far right of the **Menu bar** to hide it.



(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 Organize devices into 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.

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 indicates 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 in indicated by a doughnut chart. Compliance levels can be:

Table 21. 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 Poweredge 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 in indicated by a doughnut chart. Compliance levels can be:

Table 22. Device configuration compliance

Icon	Health status
	Compliant
	Not compliant

Device health statuses

Describes the statuses of monitored devices.

Table 23. 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, roles, and scopes.

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 rollup 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.
- The **Recent Alerts** section lists the most recent alerts generated by devices that are monitored by OpenManage Enterprise. Click the alert title to view in-depth information about the alert. See Managing 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, the **Home** screen displays information related to the device/device group the DM owns. Also, the Device Groups dropdown lists only the device groups that the device manager has operational access to. See Role and scope-based access.

Related tasks

The Welcome to OpenManage Enterprise dialog

4

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 users, roles, 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

Log into OpenManage Enterprise as an **Administrator**, as described in 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** check box 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 100 respectively.
   d. Click **Apply** to save the settings or click **Discard** to retain the default values.

   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** check box, 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**.

4. Configure the OpenManage Enterprise proxy settings by expanding **Proxy Configuration**.
   a. Select the **Enable HTTP Proxy Settings** check box to configure the HTTP proxy, and then enter HTTP proxy address and HTTP port number.
   b. Select the **Enable Proxy Authentication** check box to enable proxy credentials, and then enter the username and password.
   c. Select the **Ignore Certificate Validation** check box if the configured proxy intercepts SSL traffic and does not use a trusted third-party certificate. Using this option will ignore the built-in certificate checks used for the warranty and catalog updates.
   d. In the **Proxy Exclusion List** box, enter the IPv4, IPv6 addresses or the domain names of devices that can bypass the proxy server to directly access the appliance.
   e. Click **Apply**.
   f. To reset the settings to default attributes, click **Discard**.

Results

To understand all the tasks that you can perform by using the Application Settings feature, see System configuration.

Manage users, roles, 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 an Admin, Device Manager, or Viewer role 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 following default user roles that cannot be edited or deleted: *admin*, *system*, and *root*. 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

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 24. User roles

Role	Privileges
Backup Administrator	The ability to perform all actions on the console by UI or REST API, including backup, restore, and migration. ● Users cannot manage or edit this role as it is internal and predefined. ● This role is only assigned to the preconfigured **admin** user.
Administrator	The ability to perform all actions on the console by UI or REST API except backup, restore, and migration. 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, Microsoft Active Directory (AD), and LDAP users and assign roles. ● Enable and disable users. ● Modify the roles of existing users. ● Delete the users. ● Change the user password.
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.

- 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 table below lists the privileges of each role.

Table 25. Privileges of OpenManage Enterprise roles

Privilege	Description	User roles			
		Backup Administrator	Administrator	Device Manager	Viewer
Backup, restore, and migration	Back up, restore, and migrate appliance.	**Y**	N	N	N
Appliance setup	Global appliance settings involving the setting up of the appliance	**Y**	**Y**	N	N
Security setup	Appliance security settings	**Y**	**Y**	N	N
Alert management	Alerts actions or management	**Y**	**Y**	N	N
Fabric management	Fabric actions or management	**Y**	**Y**	N	N
Network management	Network actions or management	**Y**	**Y**	N	N
Group management	Create, read, update, and delete for static and dynamic groups.	**Y**	**Y**	N	N
Discovery management	Create, read, update, and delete for discovery tasks and run discovery tasks.	**Y**	**Y**	N	N
Inventory management	Create, read, update, and delete for inventory tasks and run inventory tasks.	**Y**	**Y**	N	N
Trap management	Import MIB, Edit trap	**Y**	**Y**	N	N
Auto-deploy management	Manage auto-deploy configuration operations.	**Y**	**Y**	N	N
Monitoring setup	Alerting policies, forwarding, Services (formerly SupportAssist), and so on.	**Y**	**Y**	**Y**	N
Power control	Reboot or cycle device power	**Y**	**Y**	**Y**	N
Device configuration	Device configuration, application of templates,	**Y**	**Y**	**Y**	N

Table 25. Privileges of OpenManage Enterprise roles (continued)

Privilege	Description	User roles			
		Backup Administrator	Administrator	Device Manager	Viewer
	manage or migrate I/O identity, storage mapping (for storage devices), and so on.				
Operating system deployment	Deploy the operating system, map to LUN, and so on.	**Y**	**Y**	**Y**	N
Device update	Device firmware update, application of updated baselines, and so on	**Y**	**Y**	**Y**	N
Template management	Create or manage templates.	**Y**	**Y**	**Y**	N
Baseline management	Create, manage firmware, and configuration baseline policies.	**Y**	**Y**	**Y**	N
Power management	Set power budgets	**Y**	**Y**	**Y**	N
Job management	Job execution or management.	**Y**	**Y**	**Y**	N
Report management	Create, read, update, and delete operations on reports.	**Y**	**Y**	**Y**	N
Report run	Run reports	**Y**	**Y**	**Y**	**Y**
View	View all data, report execution or management, and so on.	**Y**	**Y**	**Y**	**Y**

Scope-based access control (SBAC)

Using Role-Based Access Control (RBAC) administrators can assign roles while creating users. Roles determine their level of access to the appliance settings and device management features. Scope-based Access Control (SBAC) is an extension of the RBAC feature that allows an administrator to restrict a Device Manager role to a subset of device groups called scope.

While creating or updating a device manager, administrators can assign scope to restrict operational access of Device Manager to one or more system groups, custom groups, and plug-in groups.

Administrator and Viewer roles have unrestricted scope. That means they have operational access as specified by RBAC privileges to all devices and groups entities.

The scope can be implemented as follows:

1. Click **Create** or **Edit User**.
2. Assign a Device Manager role.
3. Assign scope to restrict operational access.

For more information about managing users, see Manage users, roles, and scopes.

Using SBAC administrators can implement an Restricted View feature. With Restricted View, the Device Managers only see the following:

- 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 the scope of a Device Manager is 'unrestricted', then that Device Manager can view all the devices and groups, however, would only be able to see the entities owned by the user such as jobs, alert policies, baselines, and so on along with the community and built-in entities of any kind.

When a Device Manager with an assigned scope logs in, the Device Manager can see and manage scoped devices only. Also, the Device Manager can see and manage entities such as jobs, firmware templates, configuration templates and baselines, alert policies, profiles, and so on, associated with scoped devices, only if the Device Manager owns the entity (Device Manager has created that entity or is assigned ownership of that entity). For more information about the entities a Device Manager can create, see Role-Based Access Control (RBAC) privileges in *OpenManage Enterprise User's Guide*.

For example, by clicking **Configuration** > **Templates**, a Device Manager user can view the default and custom templates owned by the Device Manager user. Also, the Device Manager user can perform other tasks as privileged by RBAC on owned templates.

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

Similarly, by clicking **Configuration** > **VLANs Pools**, the Device Manager can see all the VLANs created by the admin and export them. The Device Manager cannot perform any other operations. If the Device Manager has a template, it 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 or importing AD or LDAP user. Scope assignment for OIDC users can be done only on Open ID Connect (OIDC) providers.

SBAC for local users

- While creating or editing a local user with Device Manager role, admin can select one or more device groups that defines the scope for the Device Manager. For example, you (as an administrator) create a Device Manager user with a name dm1 and assign group *g1* present under custom groups. Then dm1 will have operational access to all devices in *g1* only. The user dm1 cannot access any other groups or entities that are related to any other devices.
- Furthermore, with SBAC, dm1 cannot view the entities created by other Device Managers (say dm2) on the same group *g1*. That means a Device Manager user can view the entities that are owned by the user. 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 can 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 Device Manager the 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 are 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, Device Manager, 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 EMC OpenManage Enterprise support site.

: The administrator can transfer owned resources from a device manager (source) to another device manager. For example, an administrator can transfer all the resources assigned from a source dm1 to dm2. A device manager with owned entities such as firmware and configuration baselines, configuration templates, alert policies, and profiles are considered an eligible source user. Transfer of ownership transfers only the entities and not the device groups (scope) owned by a device manager to another. For more information see, Transfer of ownership of device manager entities.

Add or edit local users

Create and edit properties of local users based on the role 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 needs to 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 only adding and editing the local users. While editing local users, you can edit all the user properties. However, you can only edit the role and device groups (in the case of a Device Manager) for Directory users. 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 the password by clicking **Edit** in the right pane.

Steps

1. Select **Application Settings** > **Users** > **Users** > **Add**.
2. In the **Add New User** dialog box:
   a. Under **User Details**, select Administrator, Device Manager, or Viewer from the **User Role** drop-down menu.
      For more information, see Role and scope-based access.
      By default, the user is enabled to indicate that the user privileges set up are enabled for a user.
   b. For the Device Manager roles, the scope is defaulted to **All Devices** (unrestricted scope), however, the administrator can restrict the scope by choosing the **Select Groups** option followed by selecting the device group(s).
   c. Under **User Credentials**, enter **Username**, **Password**, and reenter the password in the **Confirm Password** fields.
      The username must contain only alphanumeric characters (but underscore is allowed) and the password must contain at least one character in: uppercase, lowercase, digit, and special character.
   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 **Backup Administrator** accounts can enable or disable multifactor authentication on themselves.
      - Every time an **RSA SecurID** enabled user logs in, the appliance reaches out to the RSA Authentication server. If a proxy is introduced, 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 casing are considered to be different accounts on the appliance. For example, while 'test' and 'TEST' are considered the same account on RSA, they will be treated as two different accounts on OpenManage Enterprise.
      - Accounts that have **RSA SecurID** enabled will not be able to 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 new 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 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.

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, roles, 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. Click **Input Credentials**.
   c. 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.
   d. 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 device manager 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 one device manager to another device manager. Administrators can initiate a 'transfer of ownership' when a device manager leaves the organization.

Prerequisites

- Ensure you are logged into OpenManage Enterprise as an **Administrator**, as described in User roles.
- Reassign the device groups owned by the former device manager to the device manager who will be taking over.

About this task

- **Transfer of ownership** transfers only the entities and not the device groups (scope) owned by a device manager 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 account from where the ownership of entities must be transferred.

   NOTE: The **Source User** drop-down list will only list local, active directory, OIDC, or deleted device managers that have entities such as jobs, firmware or configuration templates, alerts policies and profiles associated with them.

3. From the **Target User** drop-down list, select the device manager account to which the entities will be transferred.
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 device manager to the target device manager.

Next steps

The new device manager must reschedule any tasks that were scheduled by the former device manager, such as the tasks for 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, roles, 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 either the UPN (username@domain) or in the NetBIOS (domain\username) format.
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.

   d. In the **Attribute of Group Membership** box, enter the attribute that stores the groups and member information in the directory.
   e. 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.

   f. 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.
4. 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.
5. Click **Test connection**.
   In the **Directory Service Information** dialog box, a message is displayed to indicate a successful connection.
6. Click **OK**.
7. 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

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.

Delete Directory services

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

Steps

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

Related references

System configuration
Disable OpenManage Enterprise users
Enable OpenManage Enterprise users
Manage users, roles, 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 nonadmin 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.**

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope-based access.
- Only a maximum of four OpenID Connect provider IDs can be added in the appliance.

Prerequisites:

Before enabling an OpenID Connect provider login, you must:

1. **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.
2. **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, or Viewer) by adding and mapping the scope that is called **dxcua** (Dell extended claim for user authentication). For more information, see:
   - Configure OIDC login using PingFederate
   - Configure OIDC login using Keycloak

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

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. (Example: https://xx.xx.xx.xx:9301)
   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 **dxcua** (Dell extended claim for user authentication) to the Client ID and define the user privileges.

About this task

CAUTION: User roles and scopes are reset to 'default' on client re-registration with the OIDC provider PingFederate (PingIdentity). This issue might reset the privileges and scope of nonadmin roles (DM and Viewer) to that of the Administrator. Re-registration of the appliance console with the 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.

NOTE: The default assigning algorithm should be RS256 (RSA Signature with SHA-256).

Steps

1. Add an 'exclusive' or 'default' scope called **dxcua** 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 **dxcua**.
   c. In Contract fulfillment, add `dxcua` and select the type as 'Text'. Then, define the user privileges for OpenManage Enterprise OpenID Connect provider login using one of the following attributes:
      i. Administrator: `dxcua : [{"Role": "AD"}]`
      ii. Device Manager: `dxcua : [{"Role": "DM"}]`
      NOTE: To restrict access of the device manager to select device groups, say G1 and G2, in OpenManage Enterprise use `dxcua : [{"Role": "DM", "Entity":"G1, G2"}]`.
      iii. Viewer: `dxcua : [{"Role": "VE"}]`
   d. If an 'exclusive' scope is configured after the client registration in OpenManage Enterprise, edit the configured client in PingFederate and enable the created 'dxcua' 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 **dxcua** 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.

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 : `dxcua : [{"Role": "AD"}]`
   - Device Manager: `dxcua : [{"Role": "DM"}]`

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

- Viewer: `dxcua : [{"Role": "VE"}]`

2. Once the client is registered in Keycloak, in the Mappers section, add a "User Attribute" mapper type with the below values:
   - Name: dxcua
   - Mapper Type: User Attribute
   - User Attribute: dxcua
   - Token Claim Name: dxcua
   - 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 **Appication 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.
4. Click **Generate**.
   A CSR is created and displayed in the **Certificate Signing Request** dialog box. A copy of the CSR is also sent to the email address you provided in your request.
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.

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 cerficate 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 **Dowload certificate chain**.

   NOTE: If you intend to perform a migration, ensure to download the certificate chain. The certificate chain must include all certificates from the root to the host certificate. For more information about the full certificate requirements, see Migrate out and Migrate in sections.

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.

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 will automatically replace 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 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 easy 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: The device naming choices in the General Device Naming and the Server Device Naming are independent of each other and they 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 by the appliance on the target devices. By default, this is set as 3 attempts.

- In the **Timeout** box, specify the duration that the appliance must wait for a response before the next attempt. By default, this is 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 any of the discovered devices do not have the DNS name or the NetBIOS name to satisfy the setting, then the appliance identifies such devices with their IP addresses.
   - 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 any of the iDRACs do not have the iDRAC hostname or the System hostname to satisfy the setting, then the appliance identifies such iDRACs using their IP addresses.
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**: To allow servers with iDRAC Firmware version 4.00.00.00, which are on the same network as the console, to be discovered automatically by the console.
- **Manual**: For the servers to be discovered by the user manually.
- 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 allows users to select whether managed devices access the appliance's internal share using the IP or FQDN:

- **IP** [default]: Requires all communication to happen using IP address.
- **FQDN** : Allows iDRACs to communicate with appliances in an environment where access is controlled via Domain Naming Services 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 one of the following external network share options that the appliance must access to complete operations such as updating of the device firmware and/or drivers, extraction, and deployment of templates and profiles, and for downloading of the diagnostic and technical 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.

- **CIFS v2**(Default): To enable SMBv2.
  NOTE: On OpenManage Enterprise 4.0 and later, 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 FX2 and FX2s sleds	2.21
iDRAC7, iDRAC8 and iDRAC9	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, and VRTX chassis.
  - The credentials to the HTTPS share are automatically rotated every 6 hours.

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 internal alerts, select **Normalized (Valid for all events)**. By default **Original Format (Valid for SNMP traps only)** is selected that does not forward internal alerts 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 Sessions** (Max: 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.
   NOTE: The default value is 3 minutes.
2. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.

Power Manager metric collection settings

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

1. In the **Data purge interval** box, enter the frequency to delete the Power Manager 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/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.
- 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. For more information about Password Strength Policy, see the *iDRAC user's guide*.

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.
- 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

- To perform any tasks on OpenManage Enterprise, ensure necessary user privileges. See Role and scope-based access
- AD and LDAP directory users can be imported and assigned to one of the OpenManage Enterprise roles (Admin, DeviceManager, or Viewer).

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** :
   a. Select the **By User Name** check box to prevent a specific username from logging in to OpenManage Enterprise.
   b. Select the **By IP address** check box to prevent a specific IP address from logging in to OpenManage Enterprise.
   c. 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.
   d. In the **Lockout Fail Window** box, enter the duration for which OpenManage Enterprise must display information about a failed attempt.
   e. In the **Lockout Penalty Time** box, enter the duration for which the user is prevented from making any login attempt after multiple unsuccessful attempts.
   f. Click **Apply**. To reset the settings to default attributes, click **Discard**.
3. Expand **TLS Protocol Configuration**:
   a. Set the **TLS Protocol** to **TLS 1.2 and Higher**, **TLS 1.2**, or **TLS 1.3**.

      NOTE: Ensure that the appliance has the TLS 1.2 protocol set up for migration.

   b. Enter a **Custom TLS 1.2 Cipher String** to customize the types of encryption supported by the appliance while using TLS 1.2.
   c. 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 multi-factor authentication to log in to the appliance:
   a. To enable **RSA SecurID**, check the **Enabled** checkbox.
   b. Log in to the RSA Authentication Server and download the RSA Server Certificate required.
   c. Click **Upload** to upload the downloaded certificate and **View** to see the details of the certificate.
   d. Enter the **RSA SecurID Authentication Server** URL and **Port #** for HTTPS access.
   e. Enter the **RSA SecurID Client ID**. The ClientID is the hostname/ IP address of the system on which the RSA Authentication Agent application (RSASecurIDSoftwareToken) 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.
   f. 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. In case of a suspected security breach, regenerate the access key twice on the RSA authentication server before entering the key on the appliance.

   g. Enter the **Connection Timeout**. This is the time period for which the RSA authentication server waits for a response from identity routers.
   h. 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.
   i. Use the **Test Connection** button to verify whether the appliance is able to reach the RSA authentication server via the port provided. If a proxy is introduced, 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`.

j. Click **Apply** to initiate registration to the RSA authentication server. If a proxy is introduced, ensure that the appliance can still communicate with the RSA Authentication server to avoid service disruption. To discard the changes made, click **Cancel**.

NOTE: After 3 invalid passcode entries, the RSA account goes into 'next token mode'. You will be 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 will fail. 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 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**.
2. 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.
3. Select the **Enabled** check box to enable the respective SNMP traps to send alerts if there is predefined events.
4. 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.
5. From the **SNMP Version** menu select the SNMP version type as SNMPv1, SNMPv2, or SNMPv3 and fill the following fields:
   a. In the **Community String** box, enter the SNMP community string of the device that must receive the alert.
   b. Edit the **Port Number** if needed. Default port number for SNMP traps=162.

      See Management ports and protocols.

   c. 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.
6. To test an SNMP message, click the **Send** button of the corresponding trap.
7. 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:

1. Expand **Syslog Forwarding Configuration**.
2. Select the check box to enable the Syslog feature on the respective server in the **Server** column.
3. In the **Destination Address / Host Name** field, enter the IP address of the device that receives the Syslog messages.
4. Default port number by using UDP=514. Edit if necessary by entering or selecting from the box.

   See Management ports and protocols.
5. Click **Apply**.
6. To reset the settings to default attributes, click **Discard**.

Manage incoming alerts

Set TrapForward properties and define users who receive incoming SNMPv3 alerts.

Prerequisites

To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access.

About this task

By clicking **Application Settings** > **Incoming Alerts**, you can set TrapForward properties and define the user who receives the incoming SNMPv3 alerts.

Steps

1. Select the **SNMPV3 Enable** check box.
2. Click **Credentials**.
3. In the **SNMP Credentials** dialog box:
   a. In the **User Name** box, enter the login ID of the user who manages the OpenManage Enterprise settings.
   b. From the **Authentication Type** drop-down menu, select either the **SHA** or **MD_5** algorithm as the authentication type.
   c. In the **Authentication Passphrase** box, enter the passphrase pertaining to SHA or MD_5 based on your selection.

d. From the **Privacy Type** drop-down menu, select either DES or AES_128 as your encryption standard.
e. In the **Privacy Passphrase** box, enter the passphrase based on your privacy type.
f. Click **Save**.

4. In the **Community** box, enter the community string to receive the SNMP traps.
5. By default, the SNMP port number for the incoming traps is 162. Edit to change the port number.
6. Click **Apply**.
   The SNMP credentials and settings are saved.
7. To reset the settings to default attributes, click **Discard**.

   NOTE: If SNMPv3 alert settings are configured before upgrading the appliance, you have to reconfigure the settings by providing the username, authentication passphrase, and privacy passphrase to continue receiving the alerts. If the issues persists, restart the services using the Text User Interface (TUI).

8. Click **Apply** to save the changes or click **Discard** to reset to cancel.

Set SNMP Credentials

Use SNMP Credentials to secure SNMP communication on the appliance.

Steps

1. Click **Credentials**.
2. In the **SNMP Credentials** dialog box:
   a. In the **User Name** box, enter the login ID of the user managing the OpenManage Enterprise settings.
   b. From the **Authentication Type** drop-down menu, select either the **SHA** or **MD_5** algorithm as the authentication type.
   c. In the **Authentication Passphrase** box, enter the passphrase pertaining to SHA or MD_5 based on your selection.
   d. From the **Privacy Type** drop-down menu, select either DES or AES_128 as your encryption standard.
   e. In the **Privacy Passphrase** box, enter the passphrase based on your privacy type.
3. Click **Save**.

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 and IPMI CLI parameters is not supported: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, *, and **'**.

Steps

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

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.
- 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:

- The administrator rights are required for enabling or disabling OpenManage Mobile subscribers.
- 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

Administrator rights are required for deleting an OpenManage Mobile subscriber.

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.

Table 28. Notification service status (continued)

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

Table 29. OpenManage Mobile subscriber information (continued)

Field	Description
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 *OpenManage Mobile User's Guide* 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

5

Discovering devices

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

By clicking **Monitor** > **Discovery**, you can discover devices in your data center environment to manage them, improve their usability, and improve resource availability for your business-critical operations. The **Discovery** screen displays the number of devices that are discovered in the task and information about the status of discovery job for that device. The job statuses are `Queued`, `Completed`, and `Stopped`. The right pane displays task information such as:

- Total possible devices
- Whether the device is discovered with device types (and their respective count)
- Next run time (for scheduled discovery tasks)
- Last discovered time

View Details in the right pane displays individual discovery job details.

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices as described in Role and scope-based access.
- In order 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 have to be deleted and rediscovered using their OpenSSH credentials. See the Microsoft documentation to enable OpenSSH on Windows and Hyper-V.
- On the **Discovery** and **Inventory** screen, the status of a scheduled job is indicated as `Queued` in the **STATUS** column. However, the same status is indicated as `Scheduled` on the **Jobs** screen.
- By default, the last discovered IP of a device is used by OpenManage Enterprise for performing all operations. To make any IP change effective, you must rediscover the device.
- For third party devices, you might see duplicate entries if they are discovered using multiple protocols. This duplication can be corrected by deleting the entries and rediscovering the device(s) using only the IPMI protocol.

By using the **Discovery** feature, you can:

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

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 servers
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
- Create a device discovery job
- Protocol support matrix for discovering devices
- View device discovery job details
- Edit a device discovery job
- Run a device discovery job
- Stop a device discovery job
- Discover multiple devices by .csv import

- Global exclusion of ranges
- Specify a discovery mode for server discovery
- Create a custom discovery job for servers
- Specify discovery mode for chassis discovery
- Create a custom discovery job for the chassis
- Specify discovery mode for Dell storage discovery
- Specify discovery mode for network switch discovery
- Create a custom discovery job for HTTPS storage devices
- Create a custom discovery job for SSH devices
- Create a custom discovery job for SNMP devices
- Specify the discovery mode for multiple discovery jobs
- Delete a device discovery job

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.

   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.

Create a device discovery job

Create a job to discover either server, chassis, storage, or network devices.

Prerequisites

Ensure you have the necessary user privileges as described in Role and scope-based access.

Steps

1. Click **Monitor** > **Discovery** > **Create**.
2. In the **Create Discovery Job** dialog box, a default job name is populated. To change it, enter the discovery job name.

   By default, the dialog box enables you to define properties of similar devices at a time.

   - To include more devices or ranges to the current discovery job, click **Add**. Another set of the following fields is displayed where you can specify the device properties: Type, IP/Hostname/Range, and Settings.

     CAUTION: A maximum of 8,000 devices can be managed by OpenManage Enterprise. Hence, do not specify large networks that have devices more than the maximum number of devices supported by OpenManage Enterprise. It may cause the system to abruptly stop responding.
   - When discovering a large number of devices, avoid creating multiple discovery jobs using individual IP address and instead use IP range of the devices.
   - To discover devices by importing ranges from the .csv file. See Discover multiple devices by .csv import.
   - To exclude certain devices, remove devices from being excluded, or to view the list of devices excluded from being discovered, see Global exclusion of ranges.
3. From the **Device Type** drop-down menu, to discover:
   - A server, select **Server**. See Specify a discovery mode for server discovery.
   - A chassis, select **CHASSIS**. See Specify discovery mode for chassis discovery.
   - A Dell storage device, or network switch, select **DELL STORAGE**, or **NETWORKING SWITCH**. See Specify discovery mode for Dell storage discovery.
   - To discover devices by using multiple protocols, select **MULTIPLE**. See Specify the discovery mode for multiple discovery jobs.
4. In the **IP/Hostname/Range** box, enter the IP address, host name, or the range of IP address to be discovered or included. For more information about the data you can enter in this field, click the **i** symbol.

   NOTE:
   - The range size is limited to 16,385 (0x4001).
   - IPv6 and IPv6 CIDR formats too are supported.
5. In the **Settings** section, enter the username and password of the protocol that is used for discovering the ranges.
6. Click **Additional Settings**, to select a different protocol, and change the settings.

   NOTE: To reduce the run time of the discovery job, ensure that:
   - Only the required protocols are selected.
   - Separate ranges for specific protocols are created.
   - Timeout values and retries are reduced.
7. In the **Scheduling Discovery Job** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions.
8. Select **Enable trap reception from discovered iDRAC servers and MX7000 chassis** to enable the OpenManage Enterprise receive the incoming traps from the discovered servers and MX7000 chassis.

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

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

Results

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

NOTE:

- During CMC discovery, the servers, and IOM and storage modules (configured with IP and SNMP set to "public" as community string), residing on CMC are also discovered and are onboarded. If you enable trap reception during CMC discovery, the OpenManage Enterprise is set as the trap destination on all the servers and not on the chassis.
- During CMC discovery, FN I/O Aggregators in Programmable MUX (PMUX) mode are not discovered.

Onboarding devices

Upon device discovery, iDRAC based PowerEdge servers and MX7000 chassis are automatically onboarded. 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.

About this task

Onboarding enables servers to be managed, rather than monitored.

- Onboarding tasks only support iDRAC, and MX7000 chassis-based devices that are not in a managed state of proxy.
- If administrator-level credentials are provided during discovery, the servers are onboarded (the device status is displayed as **Managed** in the All Devices view).
- If lower privileged credentials are provided during discovery, the servers are not onboarded (the status is displayed as **Monitored** in the All Devices view).
- If the console is also set as a trap receiver on the servers, then their Onboarding status is indicated as **Managed with Alerts**.
- **Error** indicates an issue in onboarding the device.
- 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.
- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope-based access.

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 check box 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: 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. 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.
      NOTE: If the timeout value entered is greater than the current session expiry time, you are automatically logged out of OpenManage Enterprise. However, if the value is within the current session expiration timeout window, the session is continued and not logged out.
   c. In the **Port** box, enter the port number that the job must use to discover.
   d. [Optional field] Select **Enable Common Name (CN) check**.
   e. [Optional field] Select **Enable Certificate Authority (CA) check** and browse to the certificate file.
5. Click **Finish**.
   NOTE: The **Enable trap reception from the discovered** check box is effective only for servers that are discovered by using their iDRAC interface. Trap reception does not impact other servers like operating system-discovered servers.

Protocol support matrix for discovering devices

Discover devices 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 provides information about the supported protocols for discovering devices.

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.

Table 31. Protocol support matrix for discovery

Device/ Operating System	Protocols						
	Web Services-Management (WS-Man)	**Redfish**	**Simple Network Management Protocol (SNMP)**	**Secure Shell (SSH)**	**Intelligent Platform Management Interface (IPMI)**	**ESXi (VMWare)**	**HTTPS**
iDRAC6 and later	**Supported**	**Supported** Only for iDRAC9 Version 4.40.10.00 and later.	Not supported	Not supported	Not supported	Not supported	Not supported
PowerEdge C- Series	**Supported**	Not Supported	Not supported	Not supported	Not supported	Not supported	Not supported
PowerEdge chassis (CMC)	**Supported**	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
PowerEdge MX7000 chassis	Not supported	**Supported**	Not supported	Not supported	Not supported	Not supported	Not supported
Storage devices	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported	Not supported
Ethernet switches	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported	Not supported
ESXi	Not supported	Not supported	Not supported	Not supported	Not supported	**Supported**	Not supported
Linux	Not supported	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported
Windows	Not Supported	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported
Hyper-V	Not Supported	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported
Non-Dell servers	Not supported	Not supported	Not supported	Not supported	**Supported**	Not supported	Not supported
PowerVault ME	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	**Supported**
HP iLO Remote Server Management	Not supported	**Supported** [a]	Not supported	Not supported	Not supported	Not supported	Not supported
Lenovo Xclarity Controller	Not supported	**Supported** [b]	Not supported	Not supported	Not supported	Not supported	Not supported

a. During discovery, select the protocol 'HP Redfish'
b. During discovery, select the protocol 'Lenovo Redfish'

View device discovery job details

View information about a device discovery job.

Steps

1. Click **Monitor** > **Discovery**.
2. Select the row corresponding to the discovery job name, and then click **View Details** in the right pane.
   The **Job Details** screen displays the respective discovery job information.
3. 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

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 Enteprise** > **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 servers.
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 servers

Use the **Additional Settings** dialog box to enter the details for the protocol with which you want to discover servers. The appropriate protocols are automatically pre-selected based on your initial inputs.

Steps

1. To **Discover using WS-Man/Redfish (iDRAC, Server, and/or Chassis)**:

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 hardcoded number of retries. If a target iDRAC is slow to respond or there are network delays, it is recommended to increase the timeout value higher than the default to avoid connection failures. The console will generate CDEV6131 alerts in the event of a device connection failure.
   - 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.
   - Select the **Enable Certificate Authority (CA)** check box, if needed.

   NOTE:
   - If you disable the protocol on a device after its discovery or enable a different protocol on a device post-discovery, the device must be re-discovered with valid credentials. This ensures the correct protocol is used for all operations. This applies to both enabling and disabling protocols post-discovery.
   - For in-band device discovery to be successful, ensure that the firewall on the target server allows **Echo Request - ICMPv4-In** and **Echo Request - ICMPv6-In** under **Windows Firewall with Advanced Security** > **File and Printer Sharing**.
   - When a certificate is used to discover a device and CA entries are used, the DNS name is used to identify the device and not the IP.

2. To **Discover Non Dell devices (OOB)** via Redfish:
   a. Select **HP iLO** or **Lenovo XClarity** to discover and monitor servers.
   b. In the **Credentials** section, enter a **User Name** and **Password**.
3. 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.
4. 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 via the `/DeviceService/HostKeys` REST API service. Please 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 server(s) `/etc/sudoer` file must be configured to use `NOPASSWD`.

5. 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.

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

- 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 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.

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. If OpenManage Enterprise plug-in services are installed, use either SNMP or SSH protocols.

Steps

1. From the **Device Type** drop-down menu, select **NETWORK SWITCH**.
2. Enter the IP address, hostname, or IP range in **IP/Hostname/Range**.
3. If the OpenManage Enterprise Services plug-in is installed on OpenManage Enterprise, select the protocol that is used to discover the switch.
   - SSH
   - SNMP v1/v2

   To ensure that OpenManage Enterprise plug-in services can interact with your network switch, fill out:
   - SNMP public string
   - SSH Username (Available under **Additional Settings**)
   - SSH Password (Available under **Additional Settings**)
   - SSH Enable Password (Available under **Additional Settings**)
4. 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.
5. 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 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 servers.

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

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

6

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.

Click **Devices** to view and manage the device groups and devices that are discovered in OpenManage Enterprise. Device managers can only view or manage the device groups and its associated trees that are in their scope.

The left pane displays the device groups as follows:

- All Devices: The top-level root group contains all groups.
- System groups: Default groups created by OpenManage Enterprise when shipped.
- Custom groups: User-defined groups that administrators or device managers create. Create 'query' groups or 'static' groups under custom groups.
- Plug-in groups: Groups that plug-ins create.

You can create child groups under these parent groups. For more information, see Device Groups.

On top of the working pane, doughnut charts display the health state and alerts of all devices by default. However, when a group is selected on the left pane these doughnut charts would display the health state and alerts of the group that is selected. 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.

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

Use **Advanced Filters** to narrow down displayed devices in the **Device List** based on criteria such as Name, IP Address, Identifier, and more.

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

NOTE:

- After you upgrade OpenManage Enterprise to the latest version, the devices list will be updated after the discovery jobs are rerun.
- In the **All Devices** table, select a maximum of 25 devices per page and navigate the pages to select more devices and perform tasks.
- Tasks that are related to devices that are performed on the **All Devices** screen can also be performed individually from their respective **Device Details** screens.

Topics:

- Organize devices into groups
- All Devices screen device list
- All Devices screen actions
- View and configure individual devices

Organize devices into groups

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

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

- Group the devices. For example, you can group devices by functions, operating systems, user profiles, location, jobs run, and then run queries to manage devices.
- Filter the device-related data while managing devices, updating firmware, discovering devices, and managing alert policies and reports.

- You can manage the properties of a device in a group. See View and configure individual devices.

OpenManage Enterprise provides a system-defined report to get an overview of the OpenManage Enterprise monitored devices. Click **Monitor** > **Reports** > **Devices Overview Report**. Click **Run**. See Run reports.

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.

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

NOTE: The symbols on the UI indicate the health status of a device or group. The health status of a group is the health of a device in a group that has the most critical health status. For example, among many devices in a group, if the health of a server is Warning then the group health is also 'Warning'. The rollup status is equal to the status of the device that has high severity. For more information about Rollup Health status, see the *Managing The Rollup Health Status By Using iDRAC On The Dell 14th Generation And Later PowerEdge Servers technical white paper* on the Dell TechCenter.

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

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

- **HCI Appliances** includes Hyperconverged devices such as VxRAIL, Dell XC series, and AX devices.

NOTE:
- For HCI devices, a discovery job that is undertaken after Cluster IP or port changes might result in a new cluster group.
- Depending on the configuration of the target system, discovered HCI devices may display their virtual management address.

- **Hypervisor Systems** includes Hyper-V servers, and VMware ESXi servers.
- **Modular Systems** includes PowerEdge Chassis, PowerEdge FX2, PowerEdge 1000e chassis, PowerEdge MX7000 chassis, and PowerEdge VRTX chassis.

  NOTE: An MX7000 chassis can be a lead, stand-alone, or member chassis. If an MX7000 chassis is a lead chassis and has a member chassis, the latter is discovered by using the IP of its lead chassis. An MX7000 chassis is identified by using one of the following syntaxes:
  - **MCM group** indicates the Multi-Chassis Management (MCM) group that has more than one chassis identified by the following syntax: `Group_<MCM group name>_<Lead_Chassis_Svctag>` where:
    - `<MCM group name>` is the name of the MCM group.
    - `<Lead_Chassis_Svctag>` is the Service Tag of the lead chassis. The chassis sleds, and network IOMs form this group.
  - **Stand-alone Chassis groups** are identified by using the `<Chassis_Svctag>` syntax. The chassis, sleds, and network IOMs form this group.
- **Network Devices** includes Dell Force10 networking switches, and Fibre Channel switches.
- **Servers**: Dell iDRAC servers, Linux servers, Non-Dell servers, OEM servers, and Windows servers
- **Storage Devices**: Dell Compellent storage Arrays, PowerVault MD storage arrays, and PowerVault ME storage arrays
- **Discovery Groups**: Groups that map to the range of a discovery task. They cannot be edited or deleted because the discovery job controls the group where the include or exclude condition is applied. See Discovering devices.

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

Administrators create **Custom Groups** for specific requirements. For example, servers that host email services are grouped. Users can view, edit, and delete based on user privileges and group types.

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

NOTE:
- Static and Query groups cannot have more than one parent group. Meaning, a group cannot be added as a 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.
- Creating more Custom (Query) groups in the device group hierarchy 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.

On the **All Devices** screen, in the left pane, you can create child groups under the parent Static and Query group. See Create a static device group and Create a query device group.

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.

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

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

Plugin Groups: Plug-in groups are created when plug-ins such as Services, Power Manager plug-in are installed. Plug-ins, when installed, have their own system groups and some plug-ins such as the Power Manager plug-in allows users to create Custom groups under them.

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 Enteprise** > **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.

Related concepts

Configuration compliance

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.
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**).

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

NOTE:

- Before performing any action, ensure you have the necessary user privileges as described in Role and scope-based access.
  - All tasks that require OpenManage Enterprise to communicate with an iDRAC causes a log entry 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 occur for a short period of time during the discovery or inventory task. Also, when you click the **Devices** > **NAME** > **Device Details** screen, OpenManage Enterprise

generates repeated, live requests to the iDRAC to maintain up-to-date data for display. Various factors can increase this activity, such as multiple discovery, inventory, or compliance tasks running simultaneously for a given device. These factors can increase the number of system-related authentication entries. If needed, leverage the Lifecycle Log display filters to restrict which log entries are displayed.

- From the**Group Actions** drop-down, 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.
- From the **Discovery** drop-down, 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.
- From the **Inventory** drop-down, you can:
  - Run inventory on a device group. See Create an inventory job.
  - Run inventory on devices. See Run inventory on devices.
- From the **Refresh Health** drop-down, you can:
  - Refresh health on group. See Refresh health on group.
  - Refresh health on devices. See Refresh health on devices.
- From the **More Actions** drop-down, 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 managing power devices.
  - Power off the devices. See Create a job for managing power devices.
  - Gracefully shutting down devices. See Create a job for managing power devices.
  - Power Cycle a system (Cold Boot). See Create a job for managing power devices.
  - System reset (Warm Boot). See Create a job for managing power devices.
  - 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 not available in the drop-down menu. The UI calculates device capabilities only for those in the current view or grid (limited to 25 devices at a time).
  - 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

Delete devices from OpenManage Enterprise

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

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.

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

NOTE: Deleted devices will be rediscovered when a discovery range is re-run at any time. To permanently remove devices and prevent them from discovery, Exclude devices from OpenManage Enterprise instead.

Related concepts

Organize devices into 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

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. 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

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. 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.

- 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.
- 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. In the **Schedule** section:

   - Under **Schedule Update**, click **Additional Information** to view the important information and select one of the following:
     a. **Update Now**: To apply the firmware or driver updates immediately.
     b. **Schedule Later**: To specify a date and a time when the firmware and driver version must be updated. This mode is recommended if you do not want to disturb your current tasks.
   - Under **Server Options** select one of the following reboot options :
     a. Select **Reboot server immediately** after creating update jobs on the target device, and select an option from the drop-down menu:
        i. **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.
        ii. **Graceful Reboot with Forced Shutdown** attempts a graceful reboot of the operating system. If the operating system accepts the request, a graceful reboot is performed. If the operating system rejects the request, iDRAC forces a hard reset on the system.

iii. **PowerCycle** causes a hard reset of the device.

b. Select **Stage for next server reboot** to trigger the firmware or driver update when the next server reboot happens. If this option is selected, then the inventory and baseline check must be performed manually after the package is installed in the remote device.

3. Click **Finish**.

Results

A firmware or driver update job is created and listed in the Jobs list. See Using jobs for device control.

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.

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

Organize devices into 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

- 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. Select the devices from the Devices list on which you want to refresh the health.
3. Click the **Refresh Health** drop-down menu and then click **Refresh Health on Devices.**

Results

A Health task is initiated for the selected devices. You can view the status of the health task on the **Jobs** 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.

- 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.

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.

NOTE: In order to downgrade iDRAC9 to pre-February 2021 firmware versions, iDRAC will first require a downgrade to iDRAC9 firmware version 4.40.10.00. This firmware version supports the legacy hardware root of trust certificate and allows downgrades to earlier versions.

Steps

1. In the left pane, select the group, and then click the device name in the list.
2. On the device details screen, click **Firmware/Drivers**.
3. From the **Baseline** drop-down menu, select the baseline to which the device belongs to.
   All the devices that are associated with the selected baseline are listed. For information about field description in the table, see View the baseline compliance report.
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.

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.

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 IMPI 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

View and configure device properties. Update or roll back firmware of components in a device and associated with a baseline.

In the Device list, click the device name or IP address to view device configuration data, and then edit the device configuration.

NOTE:

- Some device actions are not available for sleds in a 'Proxied' Managed State. See, Supported and unsupported actions on proxied sleds.
- 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.

Click **Devices** > **selecting a device in the device list** > **View Details** to:

- View information about the device like health and power status, device IP, and service tag.
- Perform device control and troubleshooting tasks.
- View device component information such as RAID, PSU, operating system, NIC, memory, processor, and storage enclosure. 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.

  NOTE: Updating a device using the Individual Package workflow only supports executable (EXE) based Dell Update Packages. The executable DUP must be installed on one of the sleds in the chassis when updating an FX2 CMC.
- Acknowledge, export, delete, or ignore the alerts pertaining to a device. See Managing device alerts.

  NOTE: Alerts tab is enabled for Non-Dell servers.
- View and export hardware log data 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.

  NOTE: The configuration inventory is disabled for Non-Dell servers.
- View the compliance level of a device against the configuration compliance baseline that it is associated with. See Configuration compliance.
- View the device warranty status, warranty state, service level description, and days remaining until the warranty expires. See Managing device warranty.

  NOTE: The **Warranty** screen is not displayed for sleds in a 'Proxied' Managed State.

Device Details

View data about device hardware such as service tags, DIMMs, iDRAC, processors, operating systems, and alerts. Start iDRAC or Lifecycle Controller. Manage the power status of the device and run diagnostic reports.

- On the device details screen, under **Overview**, the health, power status, and Service Tag of the device is displayed. Click the IP address to open the iDRAC login screen. See the *iDRAC User's Guide* available on the Dell support site.
  - **Information**: Device information such as Service Tag, DIMM slots, iDRAC DNS name, processors, chassis, operating system, and data center name. Multiple management IP addresses correlated to the device are listed and can be clicked to activate the respective interfaces.
  - **Recent Alerts** lists the recent alerts that are 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.
  - **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.
  - **Server Subsystem** displays the health status of other components of the device such as PSU, fan, CPU, and battery.

    NOTE: The time taken to collect subsystem data of sensor components 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.
  - The **Last Updated** section indicates the last time when the device inventory status was updated. Click the **Refresh** button to update the status. An Inventory job is started, and the status is updated on the screen.
  - The **Discovery Job** details show the status of the completed discovery job that is used to discover the particular device.
- By using **Power Control**, turn on, turn off, power cycle, and gracefully shut down a device.

- By using **Troubleshoot**:
  - Run and download the Diagnostics report. See Run and download diagnostic reports.
  - Reset iDRAC.
  - Extract and download the Services (SupportAssist) report. See Extract and download a Services report.
- Refresh the device status.
- Refresh the device inventory.
- Export the device inventory that is collected by clicking **Refresh Inventory**. See Export data.
- Run a remote RACADM or IPMI command on the device. See Run remote commands on managed devices.

OpenManage Enterprise provides a system-defined report to get an overview of OpenManage Enterprise monitored devices . Click **Monitor** > **Reports** > **Devices Overview Report**. Click **Run**. See Run reports.

Device hardware information

Display information about hardware components of OpenManage Enterprise monitored devices.

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

- **Device Card Information** provides information about cards that are used in the device.
- **Installed Software** lists firmware and software that are installed on different components in the device.
- **Processor** provides processor information such as sockets, family, speed, cores, and model.
- **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, seeManaging the Rollup Health status by using iDRAC on the Dell 14th generation and later PowerEdge servers .
- **NIC Information** provides information about NICs used in the device.
- **Memory Information** provides data about DIMMs used in the device.
- **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.
- **Power Supply Information** provides information about the PSUs installed on the device.
- **OS** lists the operating system that is installed on the device.
- **Licenses** list the health status of different licenses that are installed on the device.
- **Storage Enclosure** provides the status of storage enclosure with their EMM version.
- **Virtual Flash**lists virtual flash drives and its technical specification.
- **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 of the iDRAC used to manage the target server.
- **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.

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

- Ensure 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 that completes at a nominal pace.
- **Long Run**: An in-depth report that completes slowly.

NOTE: See the Dell white paper on *Remotely Running Automated Diagnostics Using WS-Man and RACADM Commands technical white paper* .

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

- Ensure you have the necessary privileges and access, as described in 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: Due to limitations within iDRAC7 and 8, 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 Monitoring audit logs.
- For a chassis, the real-time data about the hardware logs are retrieved from the chassis.
- To add a comment, click **Add Comment**.
- In the dialog box, type the comment, and then click **Save**. 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.

Run remote commands on managed devices

Run remote commands to manage devices monitored by OpenManage Enterprise. RACADM and IPMI commands are supported.

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. Upto 100 commands can be entered with each command required to be on a new line. To display the results in the same dialog box, select the **Open results after sending** check box.

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

4. Click **Send**.
   A job is created and displayed in the dialog box. The job is also listed on the Job Details. See View job lists.
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.

Steps

1. Select the check box corresponding to the device.
   The device working status, name, type, IP, and Service Tag are displayed.
2. In the right pane, click **Launch Management Application**.
   The iDRAC login 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 inAll 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.

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.

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, Launch the virtual console.
2. In the top-right corner of the screen, click on **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.

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

Organize devices into groups

7

Managing device inventory

Create, edit, run, stop, or delete inventory schedules. A list of existing inventory schedule jobs is displayed.

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.
- 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.

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

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.
- 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 Organize devices into groups.
4. In the **Scheduling** section, run the job immediately or schedule for a later point of time.

   See Schedule job field definitions.
5. The following **Additional Options** can be selected while running the inventory job:
   - Select the **Collect configuration inventory** check box to generate an inventory of the configuration compliance baseline.
   - Select the **Collect driver inventory** check box to collect driver inventory information from the Windows server. Also, to install the Inventory Collector and Dell System Update on the Windows server if these components are not available on the server.

   NOTE:
   - 'Collect driver inventory' applies only to devices discovered as 64-bit Windows servers.
   - Inventory collection of Windows-based devices is supported only using OpenSSH. Other SSH implementations on Windows, like the CygWin SSH, are not supported.

   For information about configuration compliance baselines, see 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.

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.

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.

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.

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.

8

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.

NOTE:

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

By using the **Firmware/Driver** feature, you can:

- Use a firmware and driver catalog from Dell.com either directly or after saving it on a network path. See Add a catalog by using Dell.com or Creating a firmware catalog by using local network.
- Create a firmware and driver baseline by using the available catalogs. These baselines serve as benchmarks to compare the firmware and driver version on the devices against the version in the catalog. See Creating the firmware baseline.
- Run a compliance report to check if the devices associated with the baseline comply with the baseline firmware and driver versions. See Checking firmware compliance. The **COMPLIANCE** column displays:
  - **OK** : If the firmware and driver version of the target device is the same as the baseline, an OK is displayed.
  - **Upgrade**: If the target device has one or more versions earlier than the firmware or driver version of the baseline. See Updating the device firmware version
    - **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.
    - **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.
  - **Downgrade** : If the device firmware and driver is later than the baseline version.
  - Export the compliance report for statistical and analytical purposes.
  - Update device firmware and driver version by using the baseline. See Update the device firmware and drivers by using baselines.

NOTE:

- When a firmware or driver baseline with many devices is checked for compliance, only one noncompliant device warning (CDEV9000) is logged on the **Alerts** screen.
- The firmware or driver compliance status of devices that cannot be updated using the Dell catalog is displayed as **Unknown**. These devices are network switches, modular IOAs, and Dell storage devices. 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, see Devices with unknown compliance status .

You can update firmware version of a device using:

- Update the device firmware and drivers.
- The **Device Details** screen. 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.

  NOTE: Updating a device using the Individual Package workflow only supports executable (EXE) based Dell Update Packages. The executable DUP must be installed through one of the sleds in the chassis to update FX2 CMCs.

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

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 Enteprise, however, device managers 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 or the PowerEdge 13G server that have iDRAC version 2.50.50.50 and earlier. 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

- 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.
- In OpenManage Enterprise 4.0 and later, SMBv1 is not supported. iDRAC devices running below a certain firmware i.e Fx2: 2.21, and VRTX 3.21 can no longer be updated by the appliance.

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.

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.
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 have no association 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 specified in the catalog.

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.
- 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 don't require a reboot of the target devices.
      v. Click **Next**.
   b. In the **Target** section:
      - To select the target device(s):
        i. Select **Select Devices**, and then click the **Select Devices** button.
        ii. In the **Select Devices** dialog box, all the devices monitored by OpenManage Enterprise, IOMs, and devices under static or query group are displayed in respective groups.
        iii. In the left pane, click the category name. Devices in that category are displayed in the working pane.
        iv. Select the check box corresponding to the device(s). The selected devices are listed under the **Selected Devices** tab.
      - To select the target device group(s):
        i. Select **Select Groups**, and then click the **Select Groups** button.
        ii. In the **Select Groups** dialog box, all the devices monitored by OpenManage Enterprise, IOMs, and devices under static or query group are displayed in respective categories.
        iii. In the left pane, click the category name. Devices in that category are displayed in the working pane.
        iv. Select the check box corresponding to the group(s). The selected groups are listed under the **Selected Groups** tab.
3. Click **Finish**.
   A message is displayed that a job is created for creating the baseline.

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

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 to 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 to their respective catalogs. When more than one device is associated with a baseline, the status of the least compliant device to the baseline is indicated as the compliance level of that baseline. For example, the compliance level of a baseline with only one device with compliance as 'critical, is indicated as 'critical' even if most of the devices are compliant.

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

- Select the check box corresponding to the baseline and click **View Report** in the right pane. On the **Compliance Report** screen, the list of devices associated with the baseline and their compliance level is displayed. By default, the devices in **Critical** and **Warning** statuses are displayed.
  NOTE: If each device has its own status, the highest severity status is considered as the status of the group. For more information about Rollup Health status, see the *Managing The Rollup Health Status By Using iDRAC On The Dell 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 to the catalog is displayed.

NOTE: For all the devices (except the MX7000 chassis) which are fully in compliance with the associate firmware baseline, the **>** symbol is not displayed.

2. Select one or more check boxes corresponding to the devices whose firmware compliance status is 'Critical' and requires an update.
3. Click **Make Compliant**. See Update the device firmware version by using the baseline compliance report.

- **SERVICE TAG**: Click to view complete information about the device on the device details screen. For more information about tasks you can complete on this screen, see View and configure individual devices.
- **REBOOT REQ**: Indicates if the device must be restarted after updating the firmware.
- **Info** : Symbol corresponding to every device component is linked to the support site 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

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

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.
- You must create an inbound firewall rule to allow communication with port 22.
- If HTTP and HTTPS shares were configured using the proxy settings, ensure that these local URLs are included in the proxy-exception list before initiating any update tasks.
- Only one update task can be initiated on the target machine at a given time.
- Target devices with iDRAC should be running firmware versions 2.50.50.50 and above.

About this task

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

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

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

- The Reset iDRAC function is not supported for the devices under an MCM chassis that are in a 'Proxied' onboarding state and for updating only the drivers of the devices. For more information about onboarding states, see Onboarding devices.
- 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.
- 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.`

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

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

The driver updates are available only on devices 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.
- Ensure that the certificates are installed on a trusted root authority when using an HTTPS share for Built-in appliance share. For more information, see the *Dell System Update (DSU) User Guide*.

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, the 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.
3. Click **Make Compliant**.
4. In the **Devices/Components Confirmation** > **Options** section:
   - 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 mode is recommended if you do not want to disturb your current tasks.
   - Under Server Options, choose **Reboot server immediately** to reboot the server(s) immediately after the firmware/driver update job is created on the target, and select one of the following options from the dropdown menu:
     - **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 a graceful reboot is performed. If the operating system rejects the request, the iDRAC forces a hard reset on the system.
     - **PowerCycle for a hard reset of the device**

     Or, select **Stage for next server reboot** to trigger the firmware/driver update when the next server reboot happens.

     NOTE: If the firmware update/driver jobs are created with the 'Stage for next server reboot' option, to collect the latest inventory, wait till the firmware update completes on the target device (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.

NOTE: 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.

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

5. 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.

9

Managing device deployment templates

Create, deploy, and manage device deployment templates to configure configuration properties on servers and chassis.

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

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

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

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

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 recreate it.
- 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 re-tried using WSMAN. The appliance uses WSMAN to initiate template related tasks on iDRACs running versions earlier than 4.40.10.00.

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.

Topics:

- Create a deployment template from a reference device
- Create a deployment template by importing a template file
- View a deployment template information
- Edit a server deployment template
- Edit a chassis deployment template
- Edit IOA deployment template
- Edit network properties of a deployment template
- Deploy device deployment templates
- Deploy IOA deployment templates
- Clone deployment templates
- Auto deploy device configuration before discovery
- Create auto deployment targets
- Delete auto deployment targets
- Export auto deployed target details
- 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.
- Reference chassis or PowerEdge 12 and 13 generation servers should be running iDRAC firmware later than version 2.50.50.50.
- With HTTPS-enabled internal shares, deployment template creation is not supported on MX7000 sleds that are discovered using the Complete Chassis Discovery (CCD).
- With SMBv2-enabled CIFS share, deployment template creation is not supported on Fx2: 2.21 and, VRTX 3.21 devices.

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.
   b. Select the Deployment template type:
      - **Clone Reference Server**: Enables you to clone the configuration of an existing server.
      - **Clone Reference Chassis**: Enables you to clone the configuration of an existing chassis.
      - **Clone Reference IOA**: Enables you to clone the configuration of an existing M I/O aggregator.

        NOTE: The attributes in the IOA template are uneditable. Only the **name** and **description** of an IOA template can be edited.
   c. Click **Next**.
   d. In the **Reference Device** section, click **Select Device** to select the device whose configuration properties must be used for creating the 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 servers
      - 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, you can select to clone the server properties such as iDRAC, BIOS, Lifecycle Controller, and Event Filters. By default, all elements are selected.
   f. Click **Finish**.
   After successful creation, the job is displayed in the list. A deployment template creation job is started, and the status is displayed in the **STATUS** column.

   The job information is also displayed on the **Monitor** > **Jobs** screen. To view additional details of the job, select the job and click **View Details** in the working pane. On the **Job Details** screen, the execution details of the job are displayed. In the **Results** pane, click **View Details** to view detailed information of the job execution.

NOTE: Templates that are created from a reference device may contain a discovery password. When deployed on target devices, this can cause communication failure. To work around 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.
   b. Click **Select a File**, and then select a template file.
   c. Select either **Server**, **Chassis**, or **IOA**to indicate the template type.
3. Click **Finish**.
   The properties of an existing template file is imported and a new deployment template is created.

Example

- To view information about a deployment template, select the check box, and then click **View Details** in the right pane. On the **Template Details** 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

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.
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 you select BIOS as the boot mode, do the following:
          - To retry the boot sequence, select the **Enabled** check box.
          - Drag the items to set the boot sequence and hard drive sequence.
        - If you select UEFI as the boot mode, drag the items to set the UEFI boot sequence. If required, select the check box to enable the Secure boot feature.
     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. Select only if the network supports the protocol.
            - 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. Click **Next**.
   In the **Summary** section, the attributes you edited by using the Guided and Advanced mode are displayed.
4. This section is read-only. Read through the settings and click **Finish**.
   The updated template attributes are saved to the deployment template.

Edit a chassis deployment template

Editing chassis deployment templates is possible with OpenManage Enterprise. When 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 or a Device Manager. 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**.
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.

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):
   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.
- Reference chassis or PowerEdge 12 and 13-generation servers should be running iDRAC firmware later than version 2.50.50.50.
- 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.

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 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 device manager.
- 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, in the **Boot to Network ISO** section:
   a. Select the **Boot to Network ISO** check box.
   b. Choose **CIFS** or **NFS** as the share type and enter information in fields like ISO image file path and storage location. Use the tooltips to enter the correct syntax.
   c. Select the **Time to Attach ISO** dropdown menu options to set the number of hours the network ISO file remains mapped to the target devices. By default, this value is set as four hours.
   d. Click **Next**.
4. In the **iDRAC Management IP** section, change the target device IP settings if required, and then click **Next**.

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

5. 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 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 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.

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 the following cross-template deployments are supported:

Table 32. 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 new 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 you want to clone.
3. Click **Clone**.
4. Enter the name of new deployment template, and then click **Finish**.
   The cloned deployment template is created and displayed in the list of deployment templates.

Auto deploy device configuration before discovery

Even before a device (server or chassis) is discovered by the appliance, you can assign a deployment template to it so the template is automatically deployed immediately after the device is discovered by appliance.

Existing deployment templates in the OpenManage Enterprise can be assigned to the servers and chassis which are awaiting discovery. These deployment templates are automatically deployed on the respective devices when they are discovered and onboarded.

To access the **Auto Deploy** screen, click **Configuration** > **Auto Deploy**.

The auto deploy targets and their respective **Identifier** (service tag or node IDs), **Template name**, **Template type**, **Status**, and **Boot to Network ISO status** (for servers) are displayed.

The **Auto Deploy** target list can be customized using the **Advanced Filters** fields available on the top of the list.

Section on the right side of the **Auto Deploy** screen shows the **Created On** and **Created By** details of the selected auto deployment target. When multiple items are selected, details of the last selected item is displayed in the section.

Once an auto-deployment target is discovered, its entry from the **Auto-Deploy** 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.

The following actions can be performed on the **Auto Deploy** screen:

- **Create** templates for auto deployment. See Create auto deployment targets
- **Delete** templates that are not needed. See Delete auto deployment targets
- **Export** the auto deployment templates to different formats. See Export auto deployed target details

NOTE: Only administrators can perform the create, delete, and export tasks on the auto-deployment templates. The device managers can only 'export' the auto-deployment templates. For more information, see Role and scope-based access.

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

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 **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 Organize devices into groups. The target devices would be placed under the specified target group on their discovery.
8. Click **Next**.
9. If the target device is a server, on the **Boot to Network ISO** screen :
   - Select the **Boot to Network ISO** check box.
   - Select **CIFS** or **NFS**.
   - Enter the **ISO Path** of location where the ISO image file is stored. Use tool tips to enter the correct syntax.
   - Enter **Share IP Address**, **Workgroup**, **Username**, and **password**.
   - Select the **Time to Attach ISO** dropdown menu options to set the number of hours the network ISO file will remain mapped to the target device(s). By default, this value is set as four hours.
   - Click **Next**.
10. On the **Virtual Identities** 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.

Delete auto deployment targets

Delete one or more targets that are associated with a deployment template.

Prerequisites

- To perform any tasks on OpenManage Enterprise, you must have necessary user 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.

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 identify pools can viewed and used by all user types. However, once the identities are assigned by a device manager, then only those identities can be viewed and used by that device manager.

Creating identity pools

Create identify 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. Also, administrator can see all the identities under which are being used. Device managers an see all the identity pools and perform all the operations on it (as specified by RBAC), however under Usage the device managers can only see the identities that are associated to the devices under their scope.

About this task

To create a pool of virtual identity types:

Steps

1. On the **Configuration** 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.

You can configure the required number of iSCSI MAC addresses in the iSCSI tab.

NOTE: The iSCSI attributes are applied only when the DHCP option for iSCSI Initiator is disabled in the source template.

Include virtual iSCSI MAC Addresses	Select the check box to add the iSCSI MAC addresses to the identity pool.
Starting virtual MAC Address	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". **NOTE:** If the iSCSI initiator name is displayed in a separate line in the **Identity Pools** > **Usage** > **iSCSI IQN** field, then, it indicates that the iSCSI IQN is enabled only on that NIC partition.
Enable iSCSI Initiator IP Pool	Select the check box to configure a pool of iSCSI initiator identities. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.
IP Address Range	Enter the IP address range for the iSCSI initiator pool in one of the following formats: • `A.B.C.D - W.X.Y.Z` • `A.B.C.D/E`
Subnet mask	Select the subnet mask address of the iSCSI pool from the drop-down.
Gateway	Enter the gateway address of the iSCSI pool.

Primary DNS Server	Enter the primary DNS server address.
Secondary DNS Server	Enter the secondary DNS server address.

NOTE: The **IP Address Range**, **Gateway**, **Primary DNS Server**, and **Secondary DNS Server** must be valid IPv4 addresses.

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 identify 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

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. 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 33. 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.

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.
   - VLAN configuration on FX2 chassis is not supported in an IPv6 infra, as IPv6 addressing is not supported by M I/O Aggregator (IOA) and FN I/O modules.
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.

Steps

1. To download as a CSV file :
   a. Click **Configuration** > **VLANs** > **Export** and select **Export All as CSV**.
2. To download as a JSON file :
   a. Click **Configuration** > **VLANs** > **Export** and select **Export All as JSON**.

Import network definitions

The following options are available to import the network definitions:

Steps

1. **Import VLAN definitions from a file**

   To import VLAN definitions from a file:
   a. Click **Configuration** > **VLANs**.
   b. Click **Import** and select **Import from File**.
   c. 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 34. 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
`[{"Name":"VLAN1","Description":"VLAN with single ID","VlanMinimum":1,"VlanMaximum":1,"Type":1},`

VLAN definition format for JSON files
`{"Name":"VLAN2 (Range)","Description":"VLAN with an ID Range ","VlanMinimum":2,"VlanMaximum":10,"Type":2}]`

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.

   a. Click **Configuration** > **VLANs**.
   b. Click **Import** and select **Import VLANs from Chassis**.
   c. On the **Job Target** screen, select the chassis from where the VLAN definitions 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**.

10

Managing device warranty

Display the warranty statuses of all the devices in your scope that are monitored.

You must have necessary role-based user privileges and scope-based operational access to the devices, as described in Role and scope-based access. An administrator with access to all device groups sees the warranty details of all the devices. A device manager 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.

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.

11

Managing alerts

Click **Alerts** to view and manage alerts generated by the devices in the management system environment.

The **Alerts** screen has the following tabs displayed:

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

NOTE:

- In 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.
- Alert policies and alert logs are governed by the scope based access that you have in OpenManage Enterprise. For example, an administrator can view and manage all the alert policies, however, device managers can only view and manage the default alert policies and the policies that they create and own. Also, the device managers can only view the alerts for the devices that are in their scope.
- Currently, only the SNMPv1 and SNMPv2 alerts are received by OpenManage Enterprise from the following PowerEdge servers— MX840c and MX5016s.
- OpenManage Enterprise provides a built-in report to view the list of devices monitored by OpenManage Enterprise and the alerts generated for each device. Click **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. The following fields are populated by default on the Alerts screen:

- **Acknowledge**: Click between the square brackets under **ACKNOWLEDGE** to acknowledge or unacknowledge an alert.
- **Time**: Time indicates the timestamp at which the alert was generated.
- **Source name**: Operating system hostname of the device that generated the alert. Click the source name to view and configure the properties of the device.

  NOTE: If the alert is internal or generated from an undiscovered device, they do not appear when filtering by IP addresses or source name.
- **Category**: The type of alert (Possible alert categories include system health and audit).
- **Message ID**: A message ID, or message identifier, is a unique alphanumeric code that is assigned to a specific alert.
- **Message**: The message field contains the alert text.
- The box on the right provides additional information such as the detailed description and recommended action for a 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.

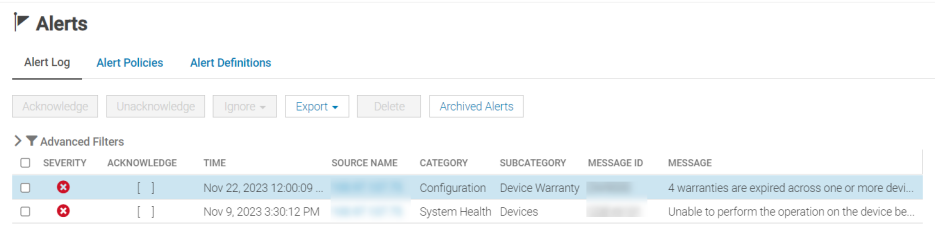
Select an alert to view the additional information such as the detailed description and recommended action on the right side of the **Alerts Log** screen. You can also perform the following tasks on the **Alerts Log** screen:

- 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.

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

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 35. 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.

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**.

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.
   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 or hostname.
   - **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.
     - The appliance recognizes all alerts that are sent by undiscovered (foreign) devices over all SNMP protocol versions.
   - **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** check box.
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** check box to ignore the alert message and not activate the alert policy.
   - 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. To shut down an operating system before performing power control actions, select the **Shut down OS First** check box.
   - Remote Script Execution (Enable): Click **Enable** to view the Remote Command Setting window where you can add and run remote commands on remote nodes. For more information about adding remote commands, see 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.
   - Send a notification to the mobile phone registered with OpenManage Enterprise. See OpenManage Mobile (OMM) Settings.

   NOTE: In 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.
- **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.

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.
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 and IPMI CLI parameters is not supported: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, *, and **'**.

Steps

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

12

Managing MIB files

OpenManage Enterprise enables you to manage MIBs that are not preinstalled by default.

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.

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 36. Role-based access for MIB files

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

To download the 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**.

13

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 37. 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 38. 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

Only users with OpenManage Enterprise Administrator or Device Manager 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**.
5. Optionally, in the **Boot to Network ISO** screen, select the **Boot to Network ISO** check box and specify the full ISO path, the file share location, and choose a **Time to Attach ISO** option to set the number of hours the network ISO file will remain mapped to the target device(s).
6. Click **Finish**.

Results

Profiles are created based on the deployment template name and the count provided. These profiles are listed on the **Profiles** 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.
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.
      - In the **ISO Path** box, enter the full ISO path. Use the tool tips to enter the correct syntax.
      - Provide details in the **Share IP Address**, **Username**, and **Password** boxes.
      - Select the **Time to Attach ISO** dropdown menu options to set the number of hours the network ISO file will remain mapped to the target device. By default, this value is set as four hours.
      - Click **Next**.
   c. On the **iDRAC Management IP** 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.

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.
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.
   - In the **ISO Path** box, enter the full ISO path. Use the tooltips to enter the correct syntax.
   - Provide details in the **Share IP Address**, **Username**, **Password** boxes.
   - Select the **Time to Attach ISO** dropdown menu options to set the number of hours the network ISO file remains mapped to the target devices. By default, this value is set as four hours.
e. Click **Finish**.

Unassign profiles

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

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.
   - **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.

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.

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.

14

Configuration compliance

Create and manage configuration compliance baselines using deployment templates, templates that are created from a device, or imported templates from a file.

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

After a configuration baseline is created by using a compliance template, the summary of compliance level of each baseline is listed in a table. Each device that is associated with the baseline has its own status, however, the highest severity status is considered as the status of the baseline. For more information, see the *Managing The Rollup Health Status By Using iDRAC On The Dell 14th Generation And Later PowerEdge Servers white paper* on the support site.

NOTE: A baseline may be permanently noncompliant when attribute values differ among multiple devices. For instance, Boot Control attributes like iSCSI Target IQN, LUN ID , may differ among targets and lead to a lasting noncompliance with the baseline.

The Overall Compliance Summary report displays the following fields:

- **COMPLIANCE**: The Rollup compliance level of devices that are attached to a configuration compliance baseline. The status of the device with least compliance (say, critical) is indicated as the status of the whole baseline.
- **NAME** lists the user-defined name of the report.
- **TEMPLATE** lists the compliance template that the baseline uses.
- **BASELINE LAST EDITED**: The most recent date and time when the compliance baseline was run.

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

Use the query builder feature to generate device level compliance with the selected baseline. See Select a query criteria.

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.

Related tasks

Create a configuration compliance baseline
Edit a configuration compliance baseline
Remove a configuration compliance baseline
Manage compliance templates
Select a query criteria

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

Create, clone, and edit compliance baseline templates using a deployment template, reference device, or importing from a file.

Use compliance template to create compliance baselines and then periodically check the configuration compliance status of devices that are associated with the baseline. See Configuration compliance.

You can create compliance templates by using deployment template, reference device, importing from a file. See Manage compliance templates.

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 best results with deploying templates ensure that your source and target are of like hardware and configurations. Otherwise, attributes that are not available on the target could cause an failure with the compliance deployment.
- The compliance templates associated to baselines are not dynamic. Newer attributes that are added by either the addition of new hardware or update firmware will not be captured in the base template. To perform compliance against any new attributes, create a new compliance template and then create a new baseline.

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

- You can create compliance template by:
  - 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.
- Edit a compliance template. See Edit a compliance template.
- Clone a compliance template. See Clone a compliance template.
- Export report about a compliance template. On the **Compliance Templates** screen, select the corresponding check box, and then click **Export**. See Export data.
- Delete a compliance template. On the **Compliance Templates** screen, select the corresponding check box, and then click **Delete**.

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

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

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

Related concepts

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.
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.
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.
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:
   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:

      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 concepts

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.

Related concepts

Configuration compliance

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, you can remediate the devices that do not match the associated baseline by changing the attribute values to match with the associated baseline attributes.

About this task

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

- **COMPLIANCE**: The status of the device with least compliance (for example, critical) is indicated as the status of the device.
- **DEVICE NAME**: The Name of the target device associated with the baseline.
- **IP ADDRESS**: The IP address of the target device.
- **TYPE**: Type of the target device associated.
- **MODEL**: Model name of the target device.
- **SERVICE TAG**: The service tag of the target device.
- **LAST SUCCESSFUL INVENTORY TIME**: The most recent date and time 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 non-compliant devices. Also, the Select All and sorting support can be used on Configuration compliance results. To undo the filters, click **Clear Filters**.

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

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, so a reboot may be required to apply the changes.

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.

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 **Complaince Report** screen is displayed.
2. Click **Export All** to export details of all the devices in the compliance baseline. Or,
3. Click **Export Selected** after selecting the individual devices from the report.

Results

The compliance baseline report is exported.

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.

Related concepts

Configuration compliance

15

Using jobs for device control

A job is a set of instructions for performing a task on one or more devices. The jobs include discovery, firmware update, inventory refresh for devices, warranty, and so on. You can view the status and details of jobs that are initiated in the devices and its components, on the **Jobs** 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
- Create a job to blink device LEDs
- View job details
- Create a job for managing power devices
- Create a remote command job for managing devices
- Create a job to change the virtual console plugin type
- Select target devices and device groups
- Manage jobs

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

- Ensure you have the necessary user privileges as described in Role and scope-based access.
- Each job type is limited to devices that you have permission to access.

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. 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 39. 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 40. 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.

Table 40. Job Types and description (continued)

Job Type	Description
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
Backup	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 peformed 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).
Restore	This job reinstates appliance data after upgrades, major configuration changes, or when migrating from VM to VM.
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 41. 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

Table 41. Default jobs and job schedules (continued)

Job Name	Cron Expression	Cron Expression Description	Example
			• 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
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

Table 41. Default jobs and job schedules (continued)

Job Name	Cron Expression	Cron Expression Description	Example
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
`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

Table 41. Default jobs and job schedules (continued)

Job Name	Cron Expression	Cron Expression Description	Example
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.

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.

View job details

View job status and restart if necessary. 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, click **View Details**.
   In the **Job Details** screen:
   - The **Execution History** contains an entry for each time the job ran.
   - The **Execution Details** section lists the devices on which the job was run, and displays the time taken to run the job.
     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 message is displayed when the job has started running.
   - To export job data as a CSV file, select the relevant job checkboxes, and click **Export** to Export data.

Create a job for managing power devices

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).

Steps

1. Click **Create**, and then select **Power Control Devices**.
2. In the **Power Control Devices** wizard dialog box:
   a. In the **Options** section:
      i. Enter the job name in **Job Name**.
      ii. From the **Power Options** drop-down menu, select any one of the tasks: **Power on**, **Power off**, or **Power cycle**.
      iii. Click **Next**.
   b. In the **Target** section, select the target devices and click **Next**. See Select target devices and device groups.
   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.

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.

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 Organize devices into 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**.

16

Monitoring audit logs

OpenManage Enterprise captures and displays audit logs to help you understand tasks performed using OpenManage Enterprise. For example, user login attempts, creation of alert policies, and running different jobs.

Prerequisites

To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access.

About this task

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

- A group is assigned or access permission is changed.
- User role is modified.
- Actions that were performed on the devices monitored by OpenManage Enterprise.
- A console setting is modified.
- A plugin management action is performed (install, uninstall, etc.).

The audit log files can be exported to the CSV file format. See Export data.

NOTE:

- Scope-based restrictions are not applicable to the Audit logs.
- 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.

Steps

1. To view the audit logs, select **Monitor** > **Audit Logs**.
   The audit logs that OpenManage Enterprise stores and displays about the tasks performed by using the appliance are displayed. For example, user login attempts, creation of alert policies, and running different jobs.
2. To sort data in any of the columns, click the column title.
3. To quickly search for information about an audit log, click **Advanced Filters**.
   The following fields are displayed that act as filters to quickly search for data.
4. Enter or select data in the following fields:
   - **Severity**: Select the severity level of a log data. The available options are info, warning, and critical.
     - Critical: Any unusual action happened. Immediate attention is needed.
     - Warning: The event is significant, but does not need immediate attention.
     - Info: Any action performed with success.
   - **Start Time** and **End Time**: To view audit logs of a specified period.
   - **User**: To view audit logs from a specific user. For example, admin, system, device manager, and viewer.
   - **Source Address**: To view audit logs from a specific system. For example, the system where you have logged in to the OpenManage Enterprise.
   - **Category**: To view audit logs of audit or configuration type.
     - Audit: Generated when a user logs in or out of the OpenManage Enterprise appliance.
     - Configuration: Generated when any action is performed on a target device.
   - **Description Contains**: Enter the text or phrase contained in the log data that you are searching for. All logs with the selected text are displayed. For example, if you enter `warningSizeLimit`, all the logs with this text are displayed.
   - **Message ID**: Enter the message ID. If the search criteria matches, only the items with the matching message ID are displayed.
5. To remove the filter, click **Clear All Filters**.
6. To export an audit log or all the audit logs, select **Export** > **Export Selected**, or **Export** > **Export All Audit Logs** respectively. For more information about exporting the audit logs, see Export data.

Topics:

- Forward audit logs to remote Syslog servers

Forward audit logs to remote Syslog servers

To monitor all the audit logs of OpenManage Enterprise from Syslog servers, you can create an alert policy. All 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.

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.

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

17

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.

- 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.
- 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 42. Privileges for managing reports

User role	Permissions
Administrator 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 42. 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.

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 Connection**.

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 43. 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.

18

Back up, restore, or migrate

Use the **Backup And Restore** screen to create a backup of the appliance, restore an appliance from a backup, or migrate an appliance.

CAUTION:

- **Appliances running on cloned VMs with OMES and CloudIQ enabled do not support backup, restore, or migrate operations. Perform this operation on a VM without cloning.**
- **Only one backup, restore, or migrate process is supported at a time. Running more than one backup, restore, or migrate process at a time can lead to unexpected system behavior.**

Before any backup, restore, or migrate 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 44. Data Considered During Backup, Restore, and Migration 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.

Related tasks

Migrate out an appliance
Migrate in an appliance

Topics:

- Appliance states
- Backup an appliance
- Restore an appliance
- Migrate an appliance

Appliance states

Details of the appliance state during backup, restore, and migration jobs.

Table 45. 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.
MAINTENANCE_PENDING	Restricted	A banner is displayed at the top of the UI when the administrator begins a backup, restore, or migration 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 or when migration data is ready on the destination appliance. The migrate-out appliance must be in this state before the streaming operation can be activated.
Streaming	Restricted	A banner is displayed at the top of the OpenManage Enterprise UI when the compressed backup file is being transferred to the migrate-in appliance. The target VM initiates the streaming operation. ● If the data is successfully transferred, the source VM enters the **STREAMING_COMPLETED** state. ● If the data transfer is not successfully transferred, the appliance reverts to the **MAINTENANCE** state.
Streaming Completed	Restricted	A banner is displayed at the top of the OpenManage Enterprise UI when the compressed backup file transfer is completed to the migrate-in appliance.
Decommission Ready	Restricted	The VM enters this state once the target VM notifies the source VM that the extraction and import of the data is successful. All the generated backup payloads that were streamed over are deleted from the appliance. The login UI color and text is modified on the migrate-out appliance once the migration is completed. **NOTE:** Only admin can log in to the console but instead of the dashboard, a message is displayed declaring that the appliance is ready to be decommissioned. The admin state can bring the appliance back to the **RUNNING** state which is highly discouraged. The administrator recommended action is to power off and archive the VM.

Backup an appliance

Use backups jobs to store appliance data like application settings, device inventory, compliance, and plugin data.

Prerequisites

- Ensure you are logged in as the default local administrator account . This is the only account that contains the backup administrator role, as described in User roles.
- Ensure there is enough storage space on the target appliance.
- Ensure 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 are able to 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.
- 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** in you have an HTTPS share, and enter the:
     - **Destination Path** to where your backup file(s) 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 file(s) 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: 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 you are a root (backup) 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 and plugin versions on the source and target appliances are identical.

About this task

To learn more about the data and settings included for migration, see Back up, restore, or migrate.

After restoring backups with plugins, a plugin synchronization job may start if there are plugins that are installed on the source appliance that are either not installed, or disabled, on the target appliance. 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 appliance's access 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**.

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.

  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.

Migrate an appliance

Migrating an OpenManage Enterprise appliance involves transferring the data, application configuration, and plugin data from a previous appliance version 3.10.x to a new appliance running version 4.0.x

- 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 4.0 or 4.0.1, perform a migration from version 3.10.x.

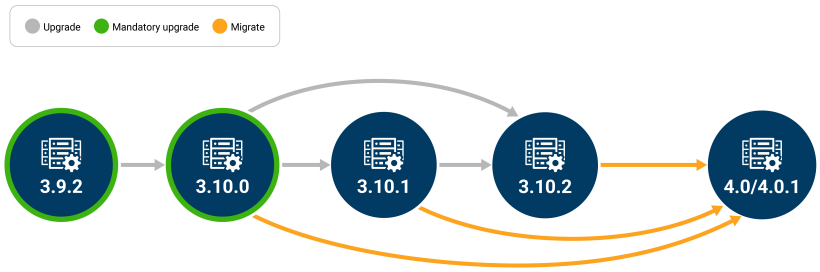


Figure 1. Potential upgrade paths to 4.0.x

Prerequisites

- Ensure you are logged in as the local admin account. See User roles for more information.
- If you are leveraging a web certificate that was signed by a Certificate Authority ensure that the certificate chain is available and uploaded to both the migrate-out and migrate-in appliances. See Assign a web server certificate to an appliance for more details.

Steps

Migrating to an appliance is a two-step process.

1. Click **Backup / Restore** > **Migrate**.
2. Create a backup of the appliance and make it ready to stream to the target appliance. See Migrate out an appliance.
3. Stream the backup data, configure it from the source appliance and restore it on a target. See Migrate in an appliance.

To learn more about the data and settings included for migration, see Back up, restore, or migrate.

Related tasks

Migrate out an appliance
Migrate in an appliance

Migrate out an appliance

Migrate out is an operation to create a backup of the appliance and make it ready to stream to the target appliance.

Prerequisites

- Ensure you are logged in as the local admin account. See User roles for more information.
- Ensure that there is enough storage space on the appliance before running the operation.
- Primary NIC must be enabled before performing a migrate out operation. To enable see Configure the system using the TUI.
- Ensure that all services are running with a stable network connection.
- If FSD is enabled, disable it from the TUI using the Enable Field Service Debug (FSD) mode option.

  NOTE: If the migrate job attempts to terminate all other running tasks when a critical task is running, the backup job fails.
- Ensure that all plugins are enabled, or uninstall any unused plugins before proceeding.
- Ensure the certificate that is used for migration meets the following requirements:
  - For migration, a certificate chain must be used.
  - The certificate chain must include all certificates from the root to the host certificate.
  - The installed certificate must be signed by the same Certificate Authority on both the source and destination consoles.

- The uploaded certificate must have both client and server authentication, and key encipherment enabled for Public Key Usage (Key Usage Extensions).
- If any of the requirements are not met, an upload error is displayed (CGEN1008).

Steps

1. Click **Backup / Restore** > **Migrate** and then select **Migrate Out**. Migrate out option is only available in OpenManage Enterprise 3.10.x.
2. In **Sign Certificate** you may choose to **Proceed with the self-signed certificate** that was shipped with the appliance or continue with a Certificate Authority (CA) signed **Upload certificate** option. If the CA signed certificate does not include the certificate chain an error will be shown. Proceed with the Upload certificate to upload the certificate that includes the chain.
   - **Proceed with self signed certificate**
   - **Upload certificate**

     For migration, use a certificate chain. Select **Upload certificate** > **Generate certificate signing request** to generate a CSR for creating a new CA signed certificate. Under **SSL Certificates**, click **Upload** > **Certificate Chain** > **Select File** to upload the CA signed certificate.

     NOTE:
     - To generate a Certificate Signing Request (CSR), see Generate and download a certificate signing request and to download a chain certificate see Assign a web server certificate to an appliance.
3. In **Setup Target Console**: If you are using proxy configurations for the Internet, before starting Step 2, ensure the proxy configuration is turned off from the **Application Settings** > **Networks**.
   a. Enter target appliance details:
      - **IP address**: Enter the IP address of the target appliance. The target IP address cannot be the same as the current OpenManage Enterprise console.
      - **User**: Enter the username used to authenticate to the target OpenManage Enterprise console.
      - **Password**: Enter the password used to authenticate to the target OpenManage Enterprise console.

   b. Click **Validate** to ensure that the source console is able to connect to the target console.

      If a self-signed certificate is used, a **Trust Certificate** dialogue box opens. Click **Yes** to trust the target and continue. On trusting the certificate, the system undergoes an Apache web server restart, and the system logs out the user. Re-login to continue the Migrate out steps from Step 2: Setup the source console.

      NOTE: Due to the Apache web server restart, you may see connectivity errors temporarily. The login screen will appear when Apache web services re-spawn on the appliance automatically.

   c. Click **Apply** to register the destination console.
4. In **Prepare for Migration**: If you are using proxy configurations for the Internet, before starting Step 3, ensure the proxy configuration is turned on.

   a. Enter the **Encryption Passphrase**. The phrase is used to decrypt the backup file. Click to see the requirements for the Encryption Passphrase.

      NOTE: Ensure that the **Encryption Passphrase** has at least one of the following special characters **_ # ? ! @ $ % ^ & * -** to enable the **Apply** button . These can be used with a combination of other special characters, for example **#>**.

   b. Check that the **Storage** appears as available to proceed.
   c. **Running Taks**: Select to **Terminate running task then run export operation** (selected by default) or **Complete running task before running export operation**.
   d. Check that the **Plugins** appear as **All plugins enabled** to proceed and click **Apply**.
5. Log in to the target console and follow the instructions to begin the migration.

   NOTE:
   - The **Abort** migration button is available when the migration task is running.
   - On clicking **Abort** migration, the task is aborted, and the appliance is moved to **RUNNING state**.

Results

A migration task is initiated and a banner with the **MAINTENANCE_PENDING** state is displayed above the menu bar, click the link for details. The **Export task** details page shows the ongoing activity logs for the task.

Next steps

When the export task is complete, the source appliance is ready to stream the data to the target appliance. The banner will display that the appliance is in **MAINTENANCE** state.

Related concepts

Migrate an appliance
Back up, restore, or migrate

Migrate in an appliance

Migrate in is an operation to stream the backup data, configure it from the source appliance and restore it on a target. Currently, this feature is only supported on OpenManage Enterprise 3.10.x, migrating to OpenManage Enterprise 4.0 or 4.0.1.

Prerequisites

- Ensure that you have followed the Migrate out an appliance process on the source appliance.
- Ensure that the appliance has connectivity to an OpenManage Enterprise update repository before starting the **Migrate In** operation otherwise the Update Readiness report may stop responding.
  - If using an Online update repository, ensure that the proxy is configured (if required) as outlined in the Configure network settings section.
  - If using an offline share, be sure to download the required plugins and configure the console's update path as outlined under the Configuring a local network share for offline update section.
- Ensure to take the target appliance snapshot before you begin the migration operation .
- Ensure you are logged in as the local admin account. See User roles for more information.
- Ensure that no plugins are installed on the target appliance. If any plugins are installed, manually uninstall them before proceeding with the migration.
- Ensure that the appliance is running on TLSv2. See Set the login security properties for more information.
- Ensure that all services are running with a stable network connection.
- Ensure the **Trust Certificate** from the source console (3.10.x appliance) is accepted to avoid validation failure.
- Ensure the certificate that is used for migration meets the following requirements:
  - For migration, a certificate chain must be used.
  - The certificate chain must include all certificates from the root to the host certificate.
  - The installed certificate must be signed by the same Certificate Authority on both the source and destination consoles.
  - The uploaded certificate must have both client and server authentication, and key encipherment enabled for Public Key Usage (Key Usage Extensions).
  - If any of the requirements are not met, an upload error is displayed (CGEN1008).

Steps

1. On the **Initial onboarding** wizard, select **Migrating from 3.10.x appliance into this appliance**. See Initial onboarding to make this selection.

   Alternatively, you can click **Backup / Restore** > **Migrate** > **Migrate In** after OpenManage Enterprise 4.0 or 4.0.1 is installed.
2. In **Sign Certificate**, you may choose to **Proceed with the self-signed certificate** that was shipped with the appliance or continue with a Certificate Authority (CA) signed **Upload certificate** option. If the CA signed certificate does not include the certificate chain, an error is displayed. Proceed with the Upload certificate option to upload the certificate that includes the chain.
   - **Proceed with self-signed certificate**
   - **Upload certificate**

     For migration, use a certificate chain. Select **Upload certificate** > **Generate certificate signing request** to generate a CSR for creating a new CA signed certificate. Under **SSL Certificates**, click **Upload** > **Certificate Chain** > **Select File** to upload the CA signed certificate.

     NOTE:
     - To generate a Certificate Signing Request (CSR), see Generate and download a certificate signing request and to download a chain certificate, see Assign a web server certificate to an appliance.
3. In **Setup Source Appliance Details**:
   a. **Enter Source Appliance Details**:

- **IP address**: Enter the IP address of the source appliance. The source IP address cannot be the same as the target OpenManage Enterprise console.
- **User**: Enter the username used to authenticate to the source OpenManage Enterprise console.
- **Password**: Enter the password used to authenticate to the source OpenManage Enterprise console.

b. If you used a self-signed certificate in **Step 1: Sign Certificate**,**Trust Source Appliance Certificate** option is displayed. Click it to accept the certificate. On trusting the certificate, the system undergoes an Apache web server restart, causing the user to be logged out. Relog in to continue the migration operation.

NOTE: Due to the Apache web server restart, you may see an *unable to connect* error message temporarily. After a short period, the regular login screen will appear.

However, if a user signed certificate is used in the Sign Certificate step, the **Trust Source Appliance Certificate** option does not appear. The system validates that the certificate uploaded is signed by the same CA that signed the source certificate.

c. **Validate Connection to Source**

Click **Validate Connection**.

4. **Check For Migration Readiness (Import)**. The readiness report is automatically retrieved from the source appliance and is autorefreshed every 30 seconds. You can also click to manually rerun the report. The readiness report must be completed without warning errors to begin the import .

This report provides the following information:

Component report	• Appliance version of the source and target appliance and status indicator that migration is supported. • List of installed plugins and status on whether or not the migrate-in appliance has access to a compatible version. • If any plugins are installed on the migrate-in appliance the report will indicate that they need to be uninstalled before the migration can continue.
Appliance report	• Whether the source appliance is ready for migration (in Maintenance mode). If there are any errors, ensure that the migration export task is complete, and the source appliance is in maintenance mode. • Whether the target appliance is registered on the source. • Whether the catalog is configured on target for plugins to auto install. If there are any errors, ensure the **Update Settings** in **Console and Plugins** is properly configured for online or offline update. See Updating the console and plugins. • The Storage, RAM, and CPU required vs availability information between source and target appliance based on default appliance deployment resource requirements and plugin resource requirements. If there are any errors, ensure that the target appliance meets the necessary hardware requirement. The migration readiness report includes resource allocation details for default plugins, which must be allocated even if you plan to decline them. For more information about hardware requirements, see *OpenManage Enterprise hardware requirements in the user's guide*. If you see any error in the appliance report, ensure all the steps are completed for migrate out on the source appliance to proceed. See Migrate out an appliance.

a. Enter the same **Encryption Passphrase** used in the Migrate out process at the source appliance.

b. Click **Import**.
The **Import Operation** wizard is displayed.

c. To proceed with default plugin (CloudIQ and Service Plugins) installation, select both the **End User License Agreement** and the **Infrastructure Telemetry Notice** and click **Accept** to proceed.

NOTE:
- All license agreements marked * must be accepted to proceed with the operation.
- If CIQP and OMES plugins are already registered and activated in OpenManage Enterprise 3.10.x, upon migration to 4.0 or 4.0.1, these plugins will be automatically registered and activated in the target appliance.

d. Click **Yes**.

When the import operation starts, the system displays the ongoing migration logs screen.

Results

- If migration is successful, the migrate-in appliance returns to the **Running state**.
- If the migration fails, the target system is in a nonfunctional state .

- In success or failure of the migration task, a banner is displayed below the menu bar stating the status of the import task . The user can **view logs** from this banner.

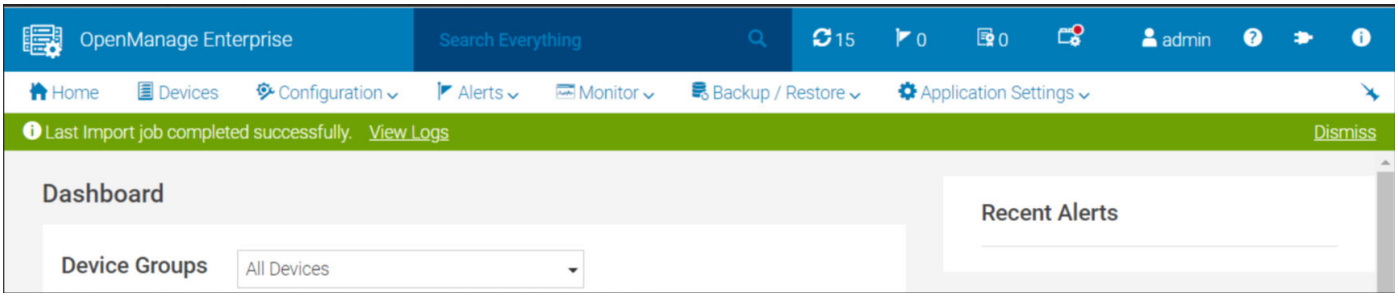


Figure 2. View logs

Next steps

- If the migration is successful, the source appliance moves to the **Decommission Ready** state. Once the target appliance is validated, shut down the source appliance and delete it .

  NOTE:

  - In case of a migration failure:
    1. A yellow banner is displayed saying the last import job failed.
    2. Click **View logs** to check for migration activity logs for the cause of the failure. Resolve the issue identified.
    3. Revert the appliance to a previous snapshot and retry the migration.
  - To go back to the source appliance:
    1. Shut down the target appliance.
    2. Start the source appliance and log in using backup administrator credentials.
    3. On logging in, a wizard is displayed and it confirms whether you want to move the appliance from **Decommission Ready** to **Running**.
    4. Click **Yes** to bring up the source appliance.
- If the migration fails and the source appliance is stuck in the **STREAMING_COMPLETED** state, browse to **Backup / Restore** > **Migrate** and under **Step 4** click the **Abort Migration** link to return the appliance to the **READY** state.
- After migration, manually remove the source OpenManage Enterprise IP as a trap destination from iDRACs to prevent alerts sent to both the source appliance (version 3.10.x) and the target appliance (version 4.0 or 4.0.1).
- If trap destination slots in any iDRAC are occupied during migration, the target appliance IP cannot be configured as trap destination. In this case, administrator should free-up a slot and re-onboard the device to configure the trap destination correctly. After decommissioning the source appliance, consider releasing its trap destination in iDRACs for efficient trap forwarding management. For more information on iDRAC trap destination, see iDRAC user's guide.

Related concepts

Migrate an appliance
Back up, restore, or migrate

19

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.

NOTE:

- 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 4.0 or 4.0.1, perform a migration from version 3.10.x.
- If your appliance is already running version 4.0, you can upgrade to version 4.0.1.

See the Migrate an appliance section for more information.

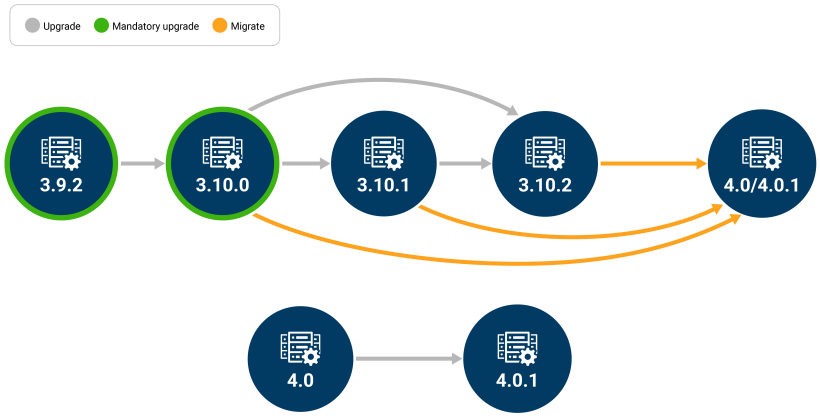


Figure 3. Potential upgrade paths to 4.0.x

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:

- 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 4.0 or 4.0.1.
- OpenManage Enterprise **Automatic** > **Online** method supports N-2 where N is the currently released version. For example, if the current released version is 4.0, you can update from 3.9 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
      - Heath 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 46. MIME types

fileExtension	mimeType
.xml	`application/xml`
.zip	`application/zip`
.tar.gz	`application/octet-stream`
.json	`application/json`
.xml.asc	`text/plain`
.zip.asc	`text/plain`
.json.asc	`text/plain`

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

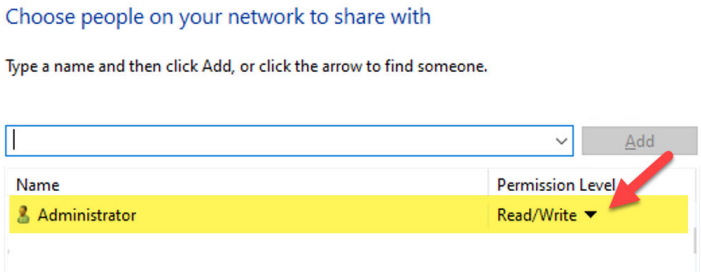
To backup and restore appliances, you will need to enable both read and write access to a Common Internet File System (CIFS) or a Network File System (NFS) network share on a Windows server.

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.



Results

You can Back up, restore, or migrate 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/openamange_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.
   - If the upgrade download has a problem connecting through proxy, clear the proxy settings, and then download.

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.

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.

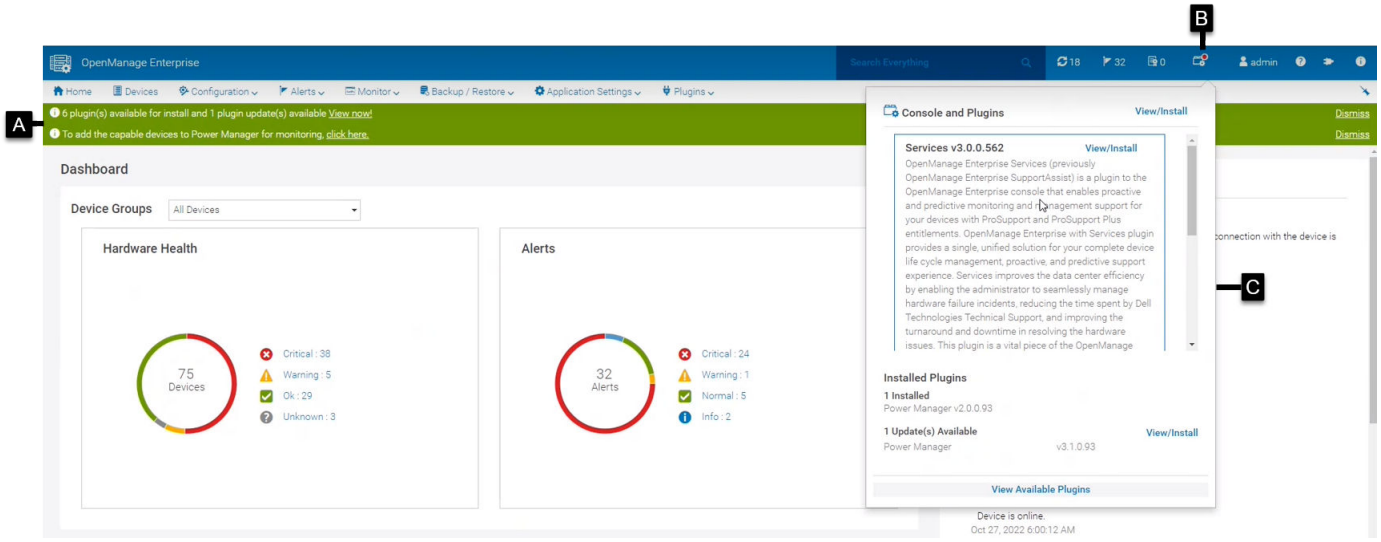
You can log in immediately after the appliance is updated and do not have to wait until the entire inventory is discovered. Post upgrade all discovery configurations are performed as part of the **Post upgrade Task**. You may log in to the appliance during this time, but do not restart the appliance or services until the **Post upgrade Task** is completed.

20

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 theOpenManage 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 Download update files to local network share 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 CloudIQ 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.

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.

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**.

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.

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.

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.

A

Troubleshooting

Definitions about some of the commonly displayed fields in OpenManage Enterprise are listed and defined here as well as other useful information.

Topics:

- Troubleshooting connectivity
- Firmware and DSU requirements for HTTPS
- Firmware schedule reference
- Firmware baseline field definitions
- Supported and unsupported actions on proxied sleds
- Schedule job field definitions
- Alert categories after EEMI relocation
- Token substitution in remote scripts and alert policy
- Catalog Management field definitions
- Devices with unknown compliance status
- Device rediscovery running for a long time after deleting iDRAC service account
- Dell Connectivity Service : Failed with exception: Unable to get access token from DCS

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 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. From the **Additional Settings** > **Protocol** list, select one of the following: SNMP, WSMAN, REDFISH, IPMI, SSH, VMWARE, REST_STORAGE

   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.

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. Click on **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 File	Download the .dat file.
Upload Signed .dat 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.

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 47. HTTPS Operations and minimum firmware and DELL EMC System Update (DSU) version requirements

Use Case or Operation.	13G servers	14G servers and above
Firmware Update	Firmware v2.70.70.70	Firmware v3.00.00.00
Driver Update	DSU v1.9.1	DSU v2.0.2
Server Configuration Profile (SCP) for template capture, deployment, configuration inventory, and remediation)	Firmware v2.70.70.70	Firmware v3.00.00.00
Technical Support Report (TSR)	N/A	Firmware v3.21.21.21
Remote Diagnostics	N/A	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.

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 48. Supported and unsupported actions on proxied sleds

ID	Action	Description	RedFish
1	POWER_CONTROL_ON	Power up	YES

Table 48. Supported and unsupported actions on proxied sleds (continued)

ID	Action	Description	RedFish
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**
31	REMOTE_IPMI	14G specific features	**No**
32	REMOTE_SSH	14G specific features	**No**

Schedule job field definitions

Defines fields 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:

- 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 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.

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 49. 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

Table 49. Alert categories (continued)

Previous Category	Previous Subcategory	New Category	New Subcategory
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
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	Devices	Configuration	Devices
Miscellaneous	Devices	Configuration	Devices
Audit	Security	Configuration	Security
Audit	Security	Configuration	Security
Audit	Security	Configuration	Security

Token substitution in remote scripts and alert policy

OpenManage Enterprise supports the use of tokens to enhance remote scripting and creation of the alert policies.

Table 50. Tokens supported in OpenManage Enterprise

Tokens	Description
$IP	Device IP Address
$MSG	Message
$DATE	Date
$TIME	Time
$SEVERITY	Severity
$SERVICETAG	Service tag
$RESOLUTION	Recommended Resolution
$CATEGORY	Alert Category Name
$ASSETTAG	Asset tag
$MODEL	Model Name
$HOSTNAME	FQDN or Hostname (if FQDN is not present).

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. 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, indicates 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.

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 51. False compliant devices

Device Category	Device List
Storage	• SC Series • MD Series • ME Series
Network devices in the FX2 and VRTX chassis	• F10 switch • Input or Output Aggregators (IOAs) • Input or Output Modules (IOMs)
Hyperconverged Appliances (HCI)	• VxRail • XC Series

Table 51. False compliant devices (continued)

Device Category	Device List
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.

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.

Dell Connectivity Service : Failed with exception: Unable to get access token from DCS

During a backup or migration operation, you may encounter a failure on the source appliance. The backup or export task will display the following error: `Dell Connectivity Service : Failed with exception: Unable to get access token from DCS.` This issue occurs when:

- A backup operation is aborted and then initiated again within a few minutes of aborting operation.
- A migrate out (export task) is aborted, and a new migrate out is initiated within a few minutes of aborting the operation.

To resolve this issue, wait for at least 5 minutes after aborting the task before retrying the backup or migrate out operation.