Dell EMC OpenManage Enterprise Version 3.6.1 User's Guide

June 2021
Rev. A00

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.

Contents

Tables

1

About Dell EMC OpenManage Enterprise

OpenManage Enterprise is a systems management and monitoring web application delivered as a virtual appliance. It provides a comprehensive view of the Dell EMC servers, chassis, storage, and network switches on the enterprise network. With OpenManage Enterprise, a web-based one-to-many systems management application, users can:

- Discover devices in a data center environment.
- View hardware inventory and monitor health of devices.
- View and manage alerts received by the appliance and configure alert policies.
- Monitor firmware / driver versions and 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 remediate 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.

NOTE:

- 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* available on the support site.

Some of the security features of OpenManage Enterprise are:

- Role-based access that limits access to console settings and device actions.
- Scope based access control allows administrators to restrict the device groups that device managers can access and manage.
- 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).
- Create and enforce firmware and configuration-related policies.
- Provision for configuring and updating the bare-metal servers.

OpenManage Enterprise has a domain-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 relevant device group, and enables you to manage the device. The typical sequence of tasks performed by OpenManage Enterprise users:

- Install OpenManage Enterprise on page 19
- Configure OpenManage Enterprise by using Text User Interface on page 26
- Discovering devices for monitoring or management on page 39
- Manage devices and device groups on page 52
- Monitor devices by using the OpenManage Enterprise dashboard on page 36
- Organize devices into groups on page 52
- Manage the device firmware and drivers on page 72
- View and configure individual devices on page 64
- Monitor and Manage device alerts on page 111
- View and renew device warranty on page 130
- Manage device deployment templates on page 81
- Managing the device configuration compliance on page 104
- Manage compliance templates on page 105
- Monitor audit logs on page 120
- Managing OpenManage Enterprise appliance settings on page 140
- Run an inventory job now on page 70

- Manage the device warranty on page 130
- Reports on page 132
- Managing MIB files on page 137
- Role and scope based access control in OpenManage Enterprise on page 15
- Directory services integration in OpenManage Enterprise on page 148

Topics:

New in this release

- Scope-based access control (SBAC) now allows a more efficient and secure management of the discovered devices. Administrators can now determine the device groups that the device managers are expected to manage.
- Seamless firmware updation on Multichassis Management (MCM) chassis with support for up to 20 chassis and their sleds.
- Ability to scan and expand appliance disk size on the Text User Interface (TUI) page.
- Supported product range expanded to the following 3rd Generation Intel® Xeon® powered YX5X (15G) PowerEdge servers: R650, R750, R750xa, MX750c, C6520.

Enhancements

- Redfish protocol is supported for discovery, inventory, monitoring, and for limited management (Power Control, Blink, diagnostics, and Technical Support Reports) on devices with iDRAC9 4.40.10.10 and later.
- Added a new Resource Utilization widget on the home page to graphically display the CPU and memory utilization by the appliance.
- An additional donut chart on All Devices page to display the installed plugin data.
- Test email functionality added to SMTP configuration.
- SNMPv3 support added for alert forwarding.
- Warranty Filtering added to Warranty Settings to customize the warranty page and reports.

Other information you may need

In addition to this guide, you can access the following documents that provide more information about OpenManage Enterprise and other related products.

Table 1. Other information you may need

Document	Description	Availability
Dell EMC OpenManage Enterprise Support Matrix	Lists the devices that are supported by OpenManage Enterprise.	1. Go to Dell.com/OpenManageManuals. 2. Click **Dell OpenManage Enterprise** and select the required version of OpenManage Enterprise. 3. Click **Documentation** to access these documents.
Dell EMC OpenManage Enterprise Release Notes	Provides information about known issues and workarounds in OpenManage Enterprise.	
Dell EMC OpenManage Mobile User's Guide	Provides information about installing and using the OpenManage Mobile application.	
Dell EMC Repository Manager User's Guide	Provides information about using the Repository Manager to manage system updates.	
Dell EMC OpenManage Enterprise and OpenManage Enterprise - Modular Edition RESTful API Guide	Provides information about integrating OpenManage Enterprise by using Representational State Transfer (REST) APIs and also includes examples of using REST APIs to perform common tasks.	

Table 1. Other information you may need (continued)

Document	Description	Availability
Dell EMC SupportAssist Enterprise User's Guide	Provides information about installing, configuring, using, and troubleshooting SupportAssist Enterprise.	Dell.com/ServiceabilityTools

Contacting Dell EMC

NOTE: If you do not have an active internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell EMC product catalog.

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical support, or customer service issues:

1. Go to Dell.com/support.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

OpenManage Enterprise Advanced license

NOTE: Installing and using OpenManage Enterprise does not require the *OpenManage Enterprise Advanced* license. Only the server configuration management feature—deploying device configurations and verifying configuration compliance on servers, requires that the *OpenManage Enterprise Advanced* license is installed on target servers. This license is not required for creating deployment templates from a server.

The *OpenManage Enterprise Advanced* license is a perpetual license that is valid for the life of a server, and can be bound to the Service Tag of only one server at a time. OpenManage Enterprise provides a built-in report to view the list of devices and their licenses. Select **OpenManage Enterprise** > **Monitor** > **Reports** > **License Report**, and then click **Run**. See Run reports on page 133.

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

OpenManage Enterprise Advanced license—Supported servers

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

- YX3X servers having the iDRAC8 2.50.50.50 or later firmware versions. The YX3X firmware versions are backward compatible and are installable on YX2X hardware. See Generic naming convention for Dell EMC PowerEdge servers on page 177.
- YX4X servers having the iDRAC9 3.10.10.10 or later firmware versions. See Generic naming convention for Dell EMC PowerEdge servers on page 177

Purchase OpenManage Enterprise Advanced license

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

Verify license information

OpenManage Enterprise provides a built-in report to view the list of devices monitored by OpenManage Enterprise, and their licenses. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **License Report**. Click **Run**. See Run reports on page 133.

You can verify if the *OpenManage Enterprise Advanced* license is installed on a server by:

- On all pages 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.

License-based features in OpenManage Enterprise

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

- Server configuration deployment.
- Server configuration compliance baseline creation and remediation.
- Boot to ISO.
- Activate the available plugins, such as the Power Manager, to extend the capability of the appliance.

NOTE: To access features of the OpenManage Enterprise such as the Virtual Console Support function, which depends on the iDRAC, you would need the iDRAC enterprise license. For more details, see the *iDRAC documentation* available on the support site.

2

Security features in OpenManage Enterprise

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.
- 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).
- Only browsers with 256-bit encryption are supported. for more information refer, Minimum system requirements for deploying OpenManage Enterprise on page 20

WARNING: Unauthorized users can obtain OS-level access to the OpenManage Enterprise appliance bypassing Dell EMC's security restrictions. One possibility is to attach the VMDK in another Linux VM as a secondary drive, and thus getting OS partition access, whereby OS-level login credentials can possibly be altered. Dell EMC recommends that customers encrypt the drive (image file) to make unauthorized access difficult. Customers must also ensure that for any encryption mechanism used, they can decrypt files later. Else, the device would not be bootable.

NOTE:

- Any change to the user role takes effect immediately and the impacted user(s) will be logged out of their active session.
- AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Admin, DeviceManager, or Viewer).
- Executing device management actions requires an account with appropriate privileges on the device.

Related information

Install OpenManage Enterprise on page 19

Topics:

OpenManage Enterprise user role types

NOTE:

- AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Admin, DeviceManager, or Viewer).
- Actions run on the devices require a privileged account on the device.

Table 2. OpenManage Enterprise User role types

User with this role...	Has the following user privileges
Administrator	Has full access to all the tasks that can be performed on the console. ● Full access (by using GUI and REST) to read, view, create, edit, delete, export, and remove information related to devices and groups monitored by OpenManage Enterprise.

Table 2. OpenManage Enterprise User role types (continued)

User with this role...	Has the following user privileges
	• Can create local, Microsoft Active Directory (AD), and LDAP users and assign suitable roles • Enable and disable users • Modify the roles of existing users • Delete the users • Change the user password
Device Manager (DM)	• Run tasks, policies, and other actions on the devices (scope) assigned by the Administrator.
Viewer	• Can only view information displayed on OpenManage Enterprise and run reports. • By default, has read-only access to the console and all groups. • Cannot run tasks or create and manage policies.

NOTE:

- If a Viewer or DM is changed to an Administrator, they get the full Administrator privileges. If a Viewer is changed to a DM, the Viewer gets the privileges of a DM.
- Any change to the user role takes effect immediately and the impacted user(s) will be logged out of their active session.
- An audit log is recorded when:
  - A group is assigned or access permission is changed.
  - User role is modified.

Related tasks

Install OpenManage Enterprise on page 19

Related information

Role and scope based access control in OpenManage Enterprise on page 15

Role and scope based access control in OpenManage Enterprise

OpenManage Enterprise has Role Based Access Control (RBAC) that clearly defines the user privileges for the three built-in roles — Administrator, Device Manager, and Viewer. Additionally, using the Scope-Based Access Control (SBAC) an administrator can limit the device groups that a device manager has access to. The following topics further explain the RBAC and SBAC features.

Role-Based Access Control (RBAC) privileges in OpenManage Enterprise

Users are assigned roles which 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 required for a certain action before allowing the action. For more information about managing users on OpenManage Enterprise, see Manage OpenManage Enterprise users on page 141.

This table lists the various privileges that are enabled for each role.

Table 3. Role-based user privileges in OpenManage Enterprise

OpenManage Enterprise features	Privilege Description	User levels for accessing OpenManage Enterprise		
		Admin	Device Manager	Viewer
Appliance setup	Global appliance settings involving setting up of the appliance.	**Y**	N	N
Security setup	Appliance security settings	**Y**	N	N
Alert management	Alerts actions / management	**Y**	N	N
Fabric management	Fabric actions / management	**Y**	N	N
Network management	Network actions / management	**Y**	N	N
Group management	Create, read, update and delete (CRUD) for static and dynamic groups	**Y**	N	N
Discovery management	CRUD for discovery tasks, run discovery tasks	**Y**	N	N
Inventory management	CRUD for inventory tasks, run inventory tasks	**Y**	N	N
Trap management	Import MIB, Edit trap	**Y**	N	N
Auto-deploy management	Manage auto-deploy configuration operations	**Y**	N	N
Monitoring setup	Alerting policies, forwarding, SupportAssist etc.	**Y**	**Y**	N
Power control	Reboot / cycle device power	**Y**	**Y**	N
Device configuration	Device configuration, application of templates, manage/migrate IO identity, storage mapping (for storage devices), etc	**Y**	**Y**	N
Operating system deployment	Deploy operating system, map to LUN, etc.	**Y**	**Y**	N
Device update	Device firmware update, application of updated baselines, etc.	**Y**	**Y**	N
Template management	Create / manage templates	**Y**	**Y**	N
Baseline management	Create / manage firmware / configuration baseline policies	**Y**	**Y**	N
Power management	Set power budgets	**Y**	**Y**	N
Job management	Job execution / management	**Y**	**Y**	N
Report management	CRUD operations on reports	**Y**	**Y**	N
Report run	Run reports	**Y**	**Y**	**Y**
View	View all data, report execution / management etc.	**Y**	**Y**	**Y**

Scope-Based Access Control (SBAC) in OpenManage Enterprise

With the use of Role-Based Access Control (RBAC) feature, 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 (DM) user, administrators can assign scope to restrict operational access of DM to one or more system groups, custom groups, and / or plugin 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.

Scope can be implemented as follows:

1. Create or Edit User
2. Assign DM role
3. Assign scope to restrict operational access

For more information about managing users, see Manage OpenManage Enterprise users on page 141.

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

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

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

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

In OpenManage Enterprise, scope can be assigned while creating a local or importing AD/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 DM role, admin can select one or more device groups that defines the scope for the DM.

For example, you (as an administrator) create a DM user named dm1 and assign group *g1* present under custom groups. Then dm1 will have operational access to all devices in *g1* only. The user dm1 will not be able to access any other groups or entities related to any other devices.

Furthermore, with SBAC, dm1 will also not be able to see the entities created by other DMs (let's say dm2) on the same group *g1*. That means a DM user will only be able to see the entities owned by the user.

For example, you (as an administrator) create another DM user named 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 will not have access to those entities and vice versa.

A DM with scope to All Devices has operational access as specified by RBAC privileges to all devices and group entities owned by the DM.

SBAC for AD/LDAP users:

While importing or editing AD/LDAP groups, administrators can assign scopes to user groups with DM role. If a user is a member of multiple AD groups, each with a DM 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 DM 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 DM 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 DM 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, DM, Viewer).

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

NOTE: Post upgrade of OpenManage Enterprise to version 3.6.x, the AD/LDAP and OIDC (PingFederate or KeyCloak) device managers would need to recreate all the previous-version entities as these entities are only available to the administrators post upgrade. For more information, see the Release Notes at https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

SBAC for OIDC users:

Scope assignment for OIDC users does not happen within the OME 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 will be available to OME. For more information about configuring user roles and scopes, see Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 153.

NOTE: If PingFederate is being used as the OIDC provider, then only administrator roles can be used. For more information, see Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 153 and the Release Notes at https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Transfer ownership : 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/or configuration baselines, configuration templates, alert policies, and profiles is 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 on page 148.

Related references

OpenManage Enterprise user role types on page 14

Related tasks

Install OpenManage Enterprise on page 19

3

Install OpenManage Enterprise

Dell EMC OpenManage Enterprise is provided as an appliance that you can install on a hypervisor and manage resources to minimize downtime. The virtual appliance can be configured from the application web console after initial network provisioning in the Text User Interface (TUI). For steps to view and update the console version, see Check and update the version of the OpenManage Enterprise and the available plugins on page 160. This chapter describes the installation prerequisites and minimum requirements.

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

Related references

OpenManage Enterprise user role types on page 14
OpenManage Enterprise Graphical User Interface overview on page 34
Security features in OpenManage Enterprise on page 14

Related information

Role and scope based access control in OpenManage Enterprise on page 15

Topics:

Installation prerequisites and minimum requirements

For a list of supported platforms, operating systems, and browsers, see the *Dell EMC OpenManage Enterprise Support Matrix* on the support site and Dell TechCenter.

To install OpenManage Enterprise, you require local system administrator rights and the system you are using must meet the criteria mentioned in the Minimum recommended hardware and Minimum system requirements for installing OpenManange Enterprise.

Minimum recommended hardware

This table describes the minimum recommended hardware for OpenManage Enterprise.

Table 4. Minimum recommended hardware

Minimum recommended hardware	Large deployments	Small deployments
Number of devices that can be managed by the appliance	Up to 8000	1000
RAM	32 GB	16 GB
Processors	8 cores total	4 cores total
Hard drive	400 GB	400 GB

Minimum system requirements for deploying OpenManage Enterprise

Table 5. Minimum requirements

Particulars	Minimum requirements

Supported hypervisors	• VMware vSphere versions:
	  ○ vSphere ESXi 5.5 onwards
	• Microsoft Hyper-V supported on:
	  ○ Windows Server 2012 R2 onwards
	• KVM supported on:
	  ○ Red Hat Enterprise Linux 6.5 onwards

Network	Available virtual NIC which has access to the management networks of all the devices which is managed from OpenManage Enterprise.
Supported browsers	• Internet Explorer (64-bit) 11 and later • Mozilla Firefox 52 and later • Google Chrome 58 and later • Microsoft Edge version 41.16299 and later
User interface	HTML 5, JS based

NOTE: For the latest update about the minimum requirements for OpenManage Enterprise, see the *Dell EMC OpenManage Enterprise Support Matrix* on the support site.

Deploy OpenManage Enterprise on VMware vSphere

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

NOTE: If a secondary adapter is added before powering on the appliance for the first time, the adapter will be 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.

1. Download the `openmanage_enterprise_ovf_format.zip` file from the 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. In vSphere Client, select **File** > **Deploy OVF Template**.
   The **Deploy OVF Template** wizard is displayed.
3. On the **Source** page, click **Browse**, and then select the OVF package. Click **Next**.
4. On the **OVF Template Details** page, review the information that is displayed. Click **Next**.
5. On the **End User License Agreement** page, read the license agreement and click **Accept**. To continue, click **Next**.
6. On the **Name and Location** page, enter a name with up to 80 characters, and then select an inventory location where the template will be stored. Click **Next**.
7. Depending on the vCenter configuration, one of the following options is displayed:
   - **If resource pools are configured** — On the **Resource Pool** page, select the pool of virtual servers to deploy the appliance VM.
   - **If resource pools are NOT configured** — On the **Hosts/Clusters** page, select the host or cluster on which you want to deploy the appliance VM.
8. If there are more than one datastores available on the host, the **Datastore** page displays such datastores. Select the location to store virtual machine (VM) files, and then click **Next**.
9. On the **Disk Format** page, click **Thick provision** to pre-allocate physical storage space to VMs at the time a drive is created.

10. On the **Ready to Complete** page, review the options you selected on previous pages and click **Finish** to run the deployment job.
    A completion status window displays where you can track job progress.

Deploy OpenManage Enterprise on Hyper-V 2012 R2 and earlier host

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be 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.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

1. Download the **`openmanage_enterprise_vhd_format.zip`** file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager** in the Windows Server 2012 R2 or an earlier version. 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** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.
5. On the **Specify Name and Location page**
   - provide the **Virtual machine name.**
   - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

   NOTE: If the check box is not selected, the VM is stored in the default folder.
6. Click **Next**
7. On the **Specify Generation** page, select **Generation 1** and click **Next**.

   NOTE: OpenManage Enterprise does not support Generation 2.
8. On the **Assign Memory** page, enter the startup memory in the **Startup memory** field and click **Next**.

   NOTE: Ensure that a minimum of 16,000 MB (16 GB) is assigned.
9. On the **Configure Networking** page, select the network adapter in the **Connection** drop-down list. Ensure that the **virtual switch** is connected to the network. Click **Next**.

   NOTE: If set to '**Not Connected**', OME will not function properly during the first reboot, and requires redeployment if this situation recurs.
10. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual disk drive**, and then browse to the location where the VHD file is copied as mentioned in **step 1**. Click **Next**.
11. Complete the on-screen instructions.

    NOTE: Make sure to have a minimum storage size of 20 GB
12. Open the **Settings** of the newly created VM and power on the VM.
13. On the TUI screen, accept the EULA and when prompted, change the password of the appliance and set network parameters to the IP of the appliance.

Deploy OpenManage Enterprise on Hyper-V 2016 host

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15

- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be 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.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

1. Download the **openmanage_enterprise_vhd_format.zip** file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager** in the Windows server 2016. 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** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.
5. On the **Specify Name and Location page**
   - provide the **Virtual machine name.**
   - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

   NOTE: If the check box is not selected, the VM is stored in the default folder.
6. Click **Next**
7. On the **Specify Generation** page, select **Generation 1** and click **Next**.

   NOTE: OpenManage Enterprise does not support Generation 2.
8. On the **Assign Memory** page, enter the startup memory in the **Startup memory** field and click **Next**.

   NOTE: Ensure that a minimum of 16,000 MB (16 GB) is assigned.
9. On the **Configure Networking** page, select the network adapter in the **Connection** drop-down list. Ensure that the **virtual switch** is connected to the network. Click **Next**.

   NOTE: If set to '**Not Connected**', OME will not function properly during the first reboot, and requires redeployment if this situation recurs.
10. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual disk drive**, and then browse to the location where the VHD file is copied as mentioned in **step 1**. Click **Next**.
11. Complete the on-screen instructions.

    NOTE: Make sure to have a minimum storage size of 20 GB
12. Open the **Settings** of the newly created VM and power on the VM.
13. On the TUI screen, accept the EULA and when prompted, change the password of the appliance and set network parameters to the IP of the appliance.

Deploy OpenManage Enterprise on Hyper-V 2019 host

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be 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.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

1. Download the **openmanage_enterprise_vhd_format.zip** file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager** in the Windows Server 2019. 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** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.

5. On the **Specify Name and Location page**
   - provide the **Virtual machine name.**
   - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

   NOTE: If the check box is not selected, the VM is stored in the default folder.
6. Click **Next**
7. On the **Specify Generation** page, select **Generation 1** and click **Next**.

   NOTE: OpenManage Enterprise does not support Generation 2.
8. On the **Assign Memory** page, enter the startup memory in the **Startup memory** field and click **Next**.

   NOTE: Ensure that a minimum of 16,000 MB (16 GB) is assigned.
9. On the **Configure Networking** page, select the network adapter in the **Connection** drop-down list. Ensure that the **virtual switch** is connected to the network. Click **Next**.

   NOTE: If set to '**Not Connected**', OME will not function properly during the first reboot, and requires redeployment if this situation recurs.
10. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual disk drive**, and then browse to the location where the VHD file is copied as mentioned in **step 1**. Click **Next**.
11. Complete the on-screen instructions.

    NOTE: Make sure to have a minimum storage size of 20 GB
12. Open the **Settings** of the newly created VM and power on the VM.
13. On the TUI screen, accept the EULA and when prompted, change the password of the appliance and set network parameters to the IP of the appliance.

Deploy OpenManage Enterprise by using Kernel-based Virtual Machine

NOTE:
- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be 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.

1. Install the required virtualization packages while installing the operating system.
2. Download the `openmanage_enterprise_kvm_format.zip` file from the support site. Extract the file to an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
3. Start the virtual manager and select **File** > **Properties**.
4. On the **Network Interfaces** page, 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**.
   A virtual interface is now created, and you can configure the firewall settings by using the terminal.
8. On the Virtual Machine Manager, click **File** > **New**.
9. Enter a name for the VM and select the **Import existing disk image** option, and then click **Forward**.
10. Navigate the file system and select the QCOW2 file that is downloaded in step 1, and then click **Forward**.
11. Assign 16 GB as the memory and select two processor cores, and then click **Forward**.
12. Assign the required disk space for the VM and click **Forward**.
13. Under **Advanced options**, ensure that the bridged host device network is selected and KVM is selected as the Virt Type.
14. Click **Finish**.
    OpenManage Enterprise appliance is now deployed by using the KVM. To get started with OpenManage Enterprise, see Log in to OpenManage Enterprise on page 26.

Deploy OpenManage Enterprise programmatically

OpenManage Enterprise can be deployed programmatically (using a script) on VMWare ESXi version 6.5 or later.

NOTE: Programmatic/scripted deployment is only supported using the primary interface.

NOTE: If a secondary adapter is added before powering on the appliance for the first time, the adapter will be 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.

NOTE: You must use the latest versions of OVF Tool and Python 3.0 or later for the programmatic deployment.

To programmatically deploy OpenManage Enterprise, do the following:

1. Download and extract the `openmanage_enterprise_ovf_format.zip` file or download the following OVF files individually from the support site:
   - `openmanage_enterprise.x86_64-0.0.1-disk1.vmdk`
   - `openmanage_enterprise.x86_64-0.0.1.mf`
   - `openmanage_enterprise.x86_64-0.0.1.ovf`
   - `openmanage_enterprise.x86_64-0.0.1.vmx`
   - `ovf_properties.config`
   - `update_ovf_property.py`
2. Open the `ovf_properties.config` and set the following parameters:

Table 6. Parameters used 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	Must contain at least one character in: uppercase, lowercase, digit, and special character. For example, Dell123$	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	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. Run the `update_ovf_property.py` script.

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

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

4. Run the modified ovftool command from the previous step.

NOTE: The ovftool command must be run with the --X:injectOvfEnv and --powerOn flags because they are required for programmatic deployment.

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

4

Get started with OpenManage Enterprise

Topics:

Log in to OpenManage Enterprise

When you boot the system for the first time from the Text User Interface (TUI), you are prompted to accept the EULA, and then change the administrator password. If you are logging in to OpenManage Enterprise for the first time, you must set the user credentials through the TUI. See Configure OpenManage Enterprise by using Text User Interface on page 26.

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

1. Start the supported browser.
2. In the **Address** box, enter the OpenManage Enterprise appliance IP address.
3. On the login page, type the login credentials, and then click **Log in**.

   NOTE: The default user name is `admin`.

If you are logging in to OpenManage Enterprise for the first time, the **Welcome to OpenManage Enterprise** page is displayed. Click **Initial Settings**, and complete the basic configuration setup. See Configure OpenManage Enterprise on page 29. 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 seconds by default. To change this duration, see Set the login security properties on page 156.

Configure OpenManage Enterprise by using Text User Interface

The Text User Interface (TUI) tool provides a text interface to change the Administrator password, view appliance status and network configuration, configure networking parameters, enable field service debug request, select the primary network, and to configure the appliance for automatic discovery of the servers in your network.

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.

On the TUI interface, use the arrow keys or press **Tab** to go to the next option on the TUI, and press **Shift + Tab** to go back to the previous options. Press **Enter** to select an option. The **Space** bar switch the status of a check box.

NOTE:

- To configure IPv6, ensure that it is already configured by a vCenter server.
- 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.

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

Table 7. Text User Interface options

Options	Descriptions
Change the Admin Password	Select **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.
Display Current Network Configuration	Select **Display Current Network Configuration** to view the IP configuration details. **Choose Network Adapter** menu lists all the available network adapters. Clicking on a network adapter will display its current settings.
Set Appliance Hostname	Select **Set Appliance Hostname** to configure the appliance hostname on the DNS. This field supports the following valid characters for host names: alphanumeric (a-z, A-Z, 0-9), periods (.), and dashes (-). **NOTE:** Using periods will designate domain name information. If the appliance DNS information is configured statically rather than getting domain details from DHCP, you must configure the hostname using the fully qualified domain name (FQDN) so that the domain search information can be populated.
Set Networking Parameters	Select **Set Networking Parameters** to reconfigure the network adapters. **Choose Network Adapter** menu lists all the available networks adapters. Select a network adapter, reconfigure its network parameters, and select **Apply** to save the changes to the appropriate interface. By default, only IPv4 is enabled on 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 OpenManage Enterprise appliance fails to acquire a IPv6 address, check if the environment is configured for router advertisements to have the managed bit (M) turned on. Network Manager from current Linux distributions causes a link failure when this bit is on, but DHCPv6 is not available. Ensure that DHCPv6 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 configured on the primary interface.
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 will have the routing priority if there is any

Table 7. Text User Interface options (continued)

Options	Descriptions
	ambiguity. The primary interface is also expected to be the 'public facing' interface which allows for corporate network/ internet connectivity. Different firewall rules are applied to the primary interface, which allow for tighter access control such as access restriction by IP range. **NOTE:** If multihoming is enabled, the appliance can be accessed from two networks. In this case, the primary interface is used by the appliance for all external communication and when proxy settings are used. For more information about multihoming on OpenManage, see*Remote script execution with Dell EMC OpenManage Enterprise* technical white paper on the 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 Dynamic DNS registration is enabled on the DNS server. Also, for 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 availability of disk space or new disk(s) and then allocate the additional disk space or disk(s) for the appliance if required. **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 remove a newly added disk or to reverse the increase in size of an existing disk you must revert to 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. • Scanning and allocation of disk space is limited to a maximum of four disks.
Enable Field Service Debug (FSD) Mode	Select **Enable Field Service Debug (FSD) Mode** for console debugging. For more information, see Field service debug workflow on page 174.

Table 7. Text User Interface options (continued)

Options	Descriptions
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 Debug Logs**—to collect the Debug logs of the application monitoring tasks, events, and the task execution history. • **Disable Debug Logs**—to disable the Debug logs. • **Enable SCP Retention**—to collect the template .XML files. • **Disable SCP Retention**—to disable the SCP retention. You can download the debug logs by clicking **Monitor** > **Audit Logs** > **Export** > **Export Console Logs** in OpenManage Enterprise.
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 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.

Configure OpenManage Enterprise

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

1. To configure the time manually do the following in the **Time Configuration** section:
   - Use the **Timezone** drop down menu to select an appropriate Timezone.
   - In the **Date** box, enter or select a date.
   - In the **Time** box, fill the time.
   - Click **Apply** to save the settings.
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 currently logged in users are automatically logged out from their OpenManage Enterprise sessions.

   - Select the **Use NTP** check box.
   - Enter the IP address or hostname in **Primary NTP Server Address** and **Secondary NTP Server Address** (optional) for time synchronization
3. If you want to set proxy server for external communication, In the Proxy Configuration section do the following:
   - Select the **Enable HTTP Proxy Settings** check box.
   - Enter the **Proxy Address**.
   - Enter the **Port number** for the proxy server.

- If the proxy server requires credentials to log in, select the **Enable Proxy Authentication** check box and enter the user name and password.
- Select the **Ignore Certificate Validation** check box if the configured proxy intercepts SSL traffic and does not use a trusted third-party certificate. Using this option will ignore the built-in certificate checks used for the warranty and catalog synchronization.

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

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

Recommended scalability and performance settings for optimal usage of OpenManage Enterprise

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

Table 8. Scalability and performance considerations of OpenManage Enterprise

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

Supported protocols and ports in OpenManage Enterprise

Supported protocols and ports on management stations

Table 9. OpenManage Enterprise Supported protocols and ports on management stations

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
22	SSH	TCP	256-bit	Management station	In	OpenManage Enterprise appliance	• Required for incoming only if FSD is used. OpenManage Enterprise

Table 9. OpenManage Enterprise Supported protocols and ports on management stations (continued)

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
							administrator must enable only if interacting with the Dell EMC support staff.
25	SMTP	TCP	None	OpenManage Enterprise appliance	Out	Management station	• To receive email alerts from OpenManage Enterprise.
53	DNS	UDP/TCP	None	OpenManage Enterprise appliance	Out	Management station	• For DNS queries.
68 / 546 (IPv6)	DHCP	UDP/TCP	None	OpenManage Enterprise appliance	Out	Management station	• Network configuration.
80*	HTTP	TCP	None	Management station	In	OpenManage Enterprise appliance	• The Web GUI landing page. This will redirect a user to HTTPS (Port 443).
123	NTP	TCP	None	OpenManage Enterprise appliance	Out	NTP Server	• Time synchronization (if enabled).
137, 138, 139, 445	CIFS	UDP/TCP	None	iDRAC/ CMC	In	OpenManage Enterprise appliance	• To upload or download deployment templates. • To upload TSR and diagnostic logs. • To download firmware/driver DUPs, and FSD process. • Boot to network ISO.
				OpenManage Enterprise appliance	Out	CIFS share	• To import firmware/driver catalogs from CIFS share.
111, 2049 (default)	NFS	UDP/TCP	None	OpenManage Enterprise appliance	Out	External NFS share	• To download catalog and DUPs from the NFS share for firmware updates. • For manual console upgrade from network share.
162*	SNMP	UDP	None	Management station	In/Out	OpenManage Enterprise appliance	• Event reception through SNMP. The direction is 'outgoing' only if

Table 9. OpenManage Enterprise Supported protocols and ports on management stations (continued)

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
							using the Trap forward policy.
443 (default)	HTTPS	TCP	128-bit SSL	Management station	In/Out	OpenManage Enterprise appliance	• Web GUI. • To download updates and warranty information from Dell.com. 256-bit encryption is allowed when communicating with the OpenManage Enterprise by using HTTPS for the web GUI. • Server-initiated discovery.
514	Syslog	TCP	None	OpenManage Enterprise appliance	Out	Syslog server	• To send alert and audit log information to Syslog server.
3269	LDAPS	TCP	None	OpenManage Enterprise appliance	Out	Management station	• AD/ LDAP login for Global Catalog.
636	LDAPS	TCP	None	OpenManage Enterprise appliance	Out	Management station	• AD/ LDAP login for Domain Controller.

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

Supported protocols and ports on managed nodes

Table 10. OpenManage Enterprise supported protocols and ports on the managed nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
22	SSH	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed node	• For the Linux OS, Windows, and Hyper-V discovery.
161	SNMP	UDP	None	OpenManage Enterprise appliance	Out	Managed node	• For SNMP queries.
162*	SNMP	UDP	None	OpenManage Enterprise appliance	In/ Out	Managed node	• Send and receive SNMP traps.
443	Proprietary/ WS-Man/ Redfish	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed node	• Discovery and inventory of iDRAC7 and later versions. • For the CMC management.

Table 10. OpenManage Enterprise supported protocols and ports on the managed nodes (continued)

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
623	IPMI/ RMCP	UDP	None	OpenManage Enterprise appliance	Out	Managed node	• IPMI access through LAN.
69	TFTP	UDP	None	CMC	In	Management station	• For updating CMC firmware.

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

NOTE: In an IPv6 environment, you must enable IPv6 and disable IPv4 in the OpenManage Enterprise appliance to ensure all the features work as expected.

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

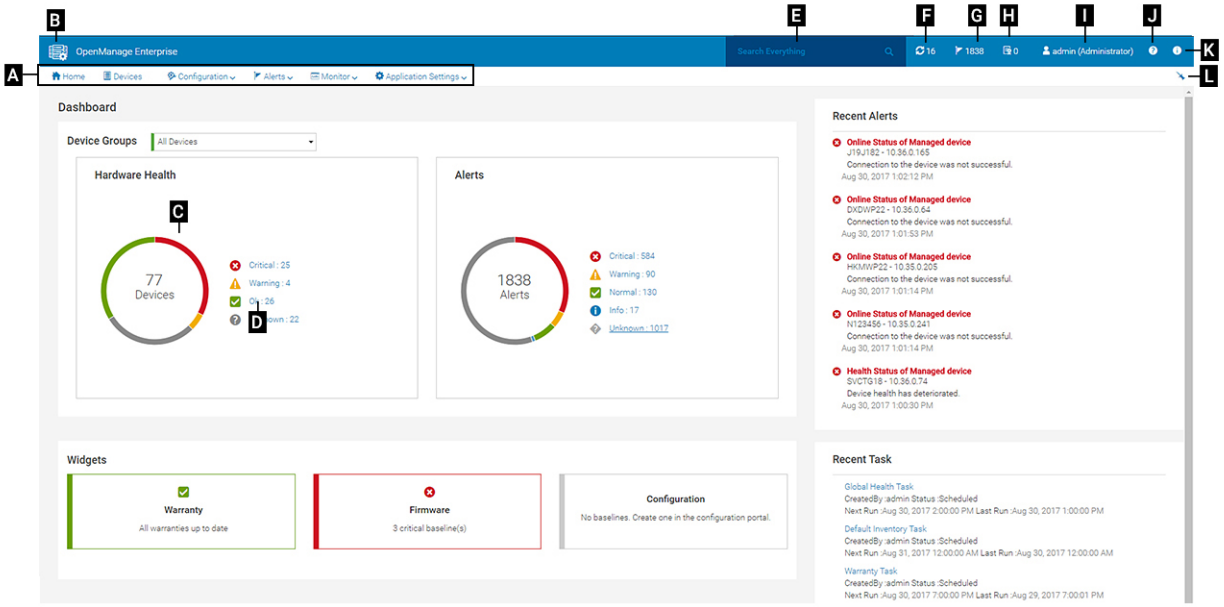
Table 11. Use case links for the supported protocols and ports in OpenManage Enterprise

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

5

OpenManage Enterprise Graphical User Interface overview

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



- A—The **OpenManage Enterprise** menu, on all the pages of OpenManage Enterprise, provides links to features that enable administrators view the dashboard (**Home**), manage devices (**Devices**), manage firmware/driver baselines, templates, and configuration compliance baselines (**Configuration**), create and store alerts (**Alerts**), and then run jobs, discover, collect inventory data, and generate reports (**Monitor**). You can also customize different properties of your OpenManage Enterprise (**Application Settings**). Click the pin symbol in the upper-right corner to pin the menu items so they appear on all the OpenManage Enterprise pages. To unpin, click the pin symbol again.
- B—The Dashboard symbol. Click to open the dashboard page from any page of OpenManage Enterprise. Alternately, click **Home**. See Dashboard.
- C—The Donut chart gives a snapshot of health status of all the devices monitored by OpenManage Enterprise. Enables you to quickly act upon the devices that are in critical state. Each color in the chart represents a group of devices having a particular health state. Click respective color bands to view respective devices in the devices list. Click the device name or IP address to view the device properties page. See View and configure individual devices on page 64.
- D—The symbols used to indicate the device health state. See Device health statuses on page 38.
- E—In the **Search Everything** box, enter about anything that is monitored and displayed by OpenManage Enterprise to view the results such as device IP, job name, group name, firmware/driver baseline, and warranty data on all the devices in your scope as defined by the Scope Based Access Control (SBAC). You cannot sort or export data that is retrieved by using the Search Everything feature. On individual pages or dialog boxes, enter or select from the **Advance Filters** section to refine your search results.
    - **The following operators are not supported: +, -, and ".**
- F—Number of OpenManage Enterprise jobs currently in the queue. Jobs that are related to discovery, inventory, warranty, firmware and/or drivers update, and so on. Click to view the status of jobs run under Health, Inventory, and the Report category on the Job Details page. To view all the events, click **All Jobs**. See Using jobs for device control on page 122. Click to refresh.

- G—The number of events generated in the alerts log. Also, based on your settings to whether or not view the unacknowledged alerts, the number of alerts in this section varies. By default, only the unacknowledged alerts are displayed. To hide or unhide the acknowledged alerts, see Customize the alert display on page 158. Deleting the alerts reduces the count. For information about symbols that are used to indicate severity statuses, see Device health statuses on page 38. Click a severity symbol to view all events in that severity category on the Alerts page. To view all the events, click **All events**. See Managing device alerts.
- H—Total number of device warranties in Critical (expired) and in Warning (expiring soon) statuses. See Managing device warranty.
- I—Username of the user who is currently logged in. Pause the pointer over the username to view the roles that are assigned to the user. For more information about the role-based users, see Role and scope based access control in OpenManage Enterprise on page 15. Click to log out, and then log in as a different user.
- J—Currently, the context-sensitive help file is displayed only for the page you are on, and not the Home portal pages. Click to view task-based instructions to effectively use links, buttons, dialog boxes, wizards, and pages in OpenManage Enterprise.
- K—Click to view the current version of OpenManage Enterprise installed on the system. Click **Licenses** to read through the message. Click appropriate links to view and download OpenManage Enterprise-related open-source files, or other open-source licenses.
- L—Click the symbol to pin or unpin the menu items. When unpinned, to pin the menu items, expand the **OpenManage Enterprise** menu and click the pin symbol.

Data about items that are listed in a table can be comprehensively viewed, exported in total, or based on selected items. See Export all or selected data on page 63. When displayed in blue text, in-depth information about items in a table can be viewed and updated, which either opens in the same window or on a separate page. Tabulated data can be filtered by using the **Advanced Filters** feature. The filters vary based on the content you view. Enter or select data from the fields. Incomplete text or numbers will not display the expected output. Data matching the filter criteria is displayed in the list. To remove filters, click **Clear All Filters**.

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

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

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

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

When logged in, all pages are automatically refreshed. After deploying the appliance, during subsequent login, if an updated version of OpenManage Enterprise is available, you are alerted to update the version immediately by clicking **Update**. Users with all the OpenManage Enterprise privileges (Administrator, Device Manager, and Viewer) can view the message, but only an Administrator can update the version. An Administrator can choose to get reminded later or dismiss the message. For more information about updating the OpenManage Enterprise version, see Check and update the version of the OpenManage Enterprise and the available plugins on page 160.

For all the job-based actions by OpenManage Enterprise, when a job is created or started to run, the lower-right corner displays an appropriate message. Details about the job can be viewed on the **Job Details** page. See View job lists on page 122.

Related information

Install OpenManage Enterprise on page 19

6

OpenManage Enterprise Home portal

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

- View the Dashboard to get a live snapshot about the health statuses of devices, and then take actions, where necessary. See Dashboard.
- View alerts under the critical and warning categories and resolve those. See Managing device alerts.
- The Widgets section lists the rollup warranty, firmware/driver compliance, and configuration compliance statuses of all devices. For more information about the features under Widgets, see Monitor devices by using the OpenManage Enterprise dashboard on page 36. The right pane lists the recent alerts and tasks generated by OpenManage Enterprise. To view more information about an alert or task, click the alert or task title. See Monitor and Manage device alerts on page 111 and Using jobs for device control on page 122.
- If an updated version of OpenManage Enterprise is available, you are immediately alerted when an update is available. To update, click **Update**. For more information about updating the OpenManage Enterprise version, see Check and update the version of the OpenManage Enterprise and the available plugins on page 160.
- The **Recent Alerts** section lists the most recent alerts generated by devices that are monitored by OpenManage Enterprise. Click the alert title to view in-depth information about the alert. See Managing device alerts.
- The **Recent Tasks** section lists the most recent tasks (jobs) created and run. Click the task title to view in-depth information about the job. See View job lists on page 122.

NOTE: If logged in as a device manager, the Home Portal displays information related to the device/device group the DM owns. Also, the Device Groups dropdown lists only the device groups that the device manager has operational access to. See Role and scope based access control in OpenManage Enterprise on page 15.

Topics:

Monitor devices by using the OpenManage Enterprise dashboard

NOTE: To perform any tasks on OpenManage Enterprise you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

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

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

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

By default, when you start the application the first time, the Dashboard page appears empty. Add devices to OpenManage Enterprise so that they can be monitored and displayed on the dashboard. To add devices, see Discovering devices for monitoring or management on page 39 and Organize devices into groups on page 52.

- Manage the device firmware and drivers on page 72
- Managing device alerts
- Discovering devices
- Creating reports
- Managing OpenManage Enterprise appliance settings on page 140

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

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

A Donut in the **Alerts** section lists the alerts received by devices in the selected device groups. See Monitor and Manage device alerts on page 111. The total number of alerts in the Donut chart varies based on the setting to whether or not view the unacknowledged alerts. By default, only the unacknowledged alerts are displayed. See Customize the alert display on page 158. To view alerts under each category, click the respective color bands. In the **Alerts** dialog box, the Critical section lists the alerts in critical status. To view all the generated alerts, click **All**. The **SOURCE NAME** column indicates the device that generated the alert. Click the name to view and configure device properties. See View and configure individual devices on page 64.

For more information about a Donut chart, see Donut chart on page 37 and Device health statuses on page 38. To view the summary of devices in a different device group monitored by OpenManage Enterprise, select from the **Device Groups** drop-down menu. To view the list of devices that belong to a health state, you can either click the color band associated with a health category, or click the respective health status symbol next to a Donut chart.

NOTE: In the Devices list, click the device name or IP address to view device configuration data, and then edit. See View and configure individual devices on page 64.

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

- **Warranty**: Displays the number of devices whose warranty is about to expire. This is based on the **Warranty Settings**. If the user opts for expire warranty notification, then the number of devices whose warranty is expired is shown. Otherwise, the number of expiring soon or the active warranty count is shown. Click to view more information in the **Warranty** dialog box. For information about managing device warranty, see Manage the device warranty on page 130. Pause the pointer over the **Warranty** section to read definitions about the symbols used in the section.
- **Firmware/Drivers**: Displays the status of firmware/driver compliance of the device baselines created on OpenManage Enterprise. If available, the Critical and Warning firmware/driver baselines are listed in this section.
  - For more information about Rollup Health status, see the *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* technical white paper on the Dell TechCenter.
  - Click to view more information in the **Firmware/Driver Compliance** page.
  - For information about updating a firmware, creating firmware catalog, creating firmware baseline, and generating baseline compliance report, see Manage the device firmware and drivers on page 72.
- **Configuration**: Displays the rolledup status of configuration compliance baselines created on OpenManage Enterprise. If available, the Critical and Warning configuration baselines are listed. See Manage compliance templates on page 105.
- **Resource Utilization**: Displays the CPU and the memory utilization by the appliance. The following color-coded checks are used to indicate the various stages of utilization:
  - Green — A less than 80% utilization of the resource
  - Yellow — A greater than 80% but less than 95% utilization of the resource
  - Red — A greater than 95% utilization of the resource

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

Donut chart

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

- The health status of devices: Displayed on the Dashboard page. Colors in the Donut chart split the ring proportionally to indicate the health of devices monitored by OpenManage Enterprise. Every device status is indicated by a color symbol. See Device health statuses on page 38. If the Donut chart indicates the health status of 279 devices in the group, in which 131=critical, 50=warning, and 95=ok, the circle is formed by using color bands proportionately representing these numbers.

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

- The alert statuses of devices: Indicates the total alerts generated for the devices monitored by OpenManage Enterprise. See Monitor and Manage device alerts on page 111.

NOTE: The total number of alerts in the Donut chart varies based on the setting to whether or not view the unacknowledged alerts. By default, only the unacknowledged alerts are displayed. See Customize the alert display on page 158.

- The firmware version compliance of a device against the version on the catalog: See Manage the device firmware and drivers on page 72.
- The configuration compliance baseline of devices and device groups: See Managing the device configuration compliance on page 104.

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

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

Device health statuses

Table 12. Device health statuses in OpenManage Enterprise

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

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

7

Discovering devices for monitoring or management

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

NOTE:

- To perform any tasks on OpenManage Enterprise you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- In order to support discovery with domain credentials, OpenManage Enterprise (version 3.2 and later) uses the OpenSSH protocol instead of the WSMAN protocol used in the previous versions. Hence, all the Windows and Hyper-V devices discovered prior to updating the appliance have to be deleted and re-discovered using their OpenSSH credentials. Refer the Microsoft documentation to enable OpenSSH on Windows and Hyper-V.
- On the **Discovery and Inventory Schedules** pages, the status of a scheduled job is indicated as **Queued** in the **STATUS** column. However, the same status is indicated as **Scheduled** on the **Jobs** page.
- By default, the last discovered IP of a device is used by OpenManage Enterprise for performing all operations. To make any IP change effective, you must rediscover the device.
- For third party devices, you might see duplicate entries if they are discovered using multiple protocols. This duplication can be corrected by deleting the entries and rediscovering the device(s) using only the IPMI protocol.

By using the Discovery feature, you can:

- View, add, and remove devices from the global exclusion list. See Global exclusion of ranges on page 46.
- Create, run, edit, delete, and stop the device discovery jobs.

Related tasks

Delete a device discovery job on page 51
View device discovery job details on page 45
Stop a device discovery job on page 46
Run a device discovery job on page 45
Specify discovery mode for creating a server discovery job on page 47
Create customized device discovery job protocol for servers –Additional settings for discovery protocols on page 47
Specify discovery mode for creating a Dell storage discovery job on page 49
Create customized device discovery job protocol for SNMP devices on page 50
Specify discovery mode for creating a MULTIPLE protocol discovery job on page 51
Edit a device discovery job on page 45

Topics:

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

Discover servers automatically by using the server-initiated discovery feature

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

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

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

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

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

1. Add the configuration information of OpenManage Enterprise on the DNS using one of following methods:
   - TUI—By using the TUI interface, enable the **Configure Server Initiated Discovery** option. For more information, see Configure OpenManage Enterprise by using Text User Interface on page 26.
   - 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 preferences on page 157.
3. Once the appliance is configured as mentioned in the previous steps, the servers can initiate contact with OpenManage Enterprise by querying the DNS. The appliance verifies the servers after ensuring that the client certificate of the servers is signed by the Dell CA.

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

     NOTE: The appliance triggers a Discovery job every 10 minutes to discover all the servers in the 'Ready to Discover' status. However, if the Discovery-Approval policy in the appliance is set as 'Manual,' then the user should manually trigger the Discovery job for each server. For more information, see Manage Console preferences on page 157
   - Job submitted for Discovery—This status indicates that the discovery job is initiated either automatically or manually for the server.
   - Discovered—The server is discovered and is listed on the All Devices page.

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

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

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

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

   NOTE: Entries corresponding to discovered servers are automatically be purged after 30 days.
4. **Export**—To export the server credentials in HTML, CSV, or PDF formats:
   a. Select one or more servers on the Sever-Initiated Discovery page.
   b. Click **Export**.

c. In the Export All wizard, select any of the following file formats: HTML, CSV, and PDF.
d. Click **Finish**. A job is created, and the data is exported to the selected location.

Create a device discovery job

The following steps describes how to initiate a device discovery job in OpenManage Enterprise to discover the devices in your data center using the Create Discovery Job wizard.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

1. To initiate the Create Discovery Job you can do one of the following steps:
   - Click **Monitor** > **Discovery** > **Create**.
   - Alternatively, from the All Devices page (**OpenManage Enterprise** > **Devices**), click the **Discovery** drop-down menu and click **Discover Devices**.
2. In the **Create Discovery Job** dialog box, a default job name is populated. To change it, enter the discovery job name. By default, the dialog box enables you to define properties of similar devices at a time.
   - To include more devices or ranges to the current discovery job, click **Add**. Another set of the following fields is displayed where you can specify the device properties: Type, IP/Hostname/Range, and Settings.

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

     NOTE: When discovering a large number of devices, avoid creating multiple discovery jobs using individual IP address and instead use IP range of the devices.
   - To discover devices by importing ranges from the .csv file. See Specify multiple devices by importing data from the .csv file on page 46.
   - To exclude certain devices, remove devices from being excluded, or to view the list of devices excluded from being discovered, see Globally excluding device(s) from discovery results.
3. From the **Device Type** drop-down menu, to discover:
   - A server, select **SERVER**. See Specifying discovery mode for creating a server discovery job.
   - A chassis, select **CHASSIS**. See Specifying discovery mode for creating a chassis discovery job.
   - A Dell EMC storage device, or network switch, select **DELL STORAGE**, or **NETWORKING SWITCH**. See Specifying discovery mode for creating a storage, Dell storage, and network switch discovery job.
   - To discover devices by using multiple protocols, select **MULTIPLE**. See Specify discovery mode for creating a MULTIPLE protocol discovery job on page 51.
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.
7. In the **Scheduling Discovery Job** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions on page 172.
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 need to 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 alerts on page 116. If you select this but do not configure SMTP, the **Finish** button is not displayed to continue the task.

11. Click **Finish**. The Finish button is not displayed if the fields are incorrectly or incompletely filled.
    A discovery job is created and run. The status is displayed on the **Job Details** page.

During device discovery, the user account that is specified for the discovery range is verified against all available privileges that are enabled on a remote device. If the user authentication passes, the device is automatically onboarded or the device can be onboarded later with different user credentials. See Onboarding devices on page 43.

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

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

Onboarding devices

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

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

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

NOTE:

- All devices that have been onboarded through this wizard remain onboarded through this user account and is not substituted by the discovery user account during future discoveries against these devices.
- For the already discovered devices, if the SNMP trap destination is 'manually' set in iDRAC as OpenManage Enterprise, the alerts are received and processed by the appliance. However, the device's Managed State displayed on the All Devices page remains the same as its initial discovered state of 'Monitored,' 'Managed' or 'Managed with Alerts.'
- The All Devices page displays the **Managed State** of all the onboarded chassis as "Managed" irrespective of which chassis user-role credentials were used at the time of onboarding. If the chassis was onboarded with credentials of a "read-only" user, then there may be a failure during update activities performed on chassis. Hence, It is recommended to onboard chassis with credentials of a chassis Administrator to perform all activities.
- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

1. From the **OpenManage Enterprise** menu, under **Devices**, click **All Devices**.
   A Donut chart indicates status of all devices in the working pane. See the Donut chart. The table lists the properties of devices selected along with their following onboarding status:
   - **Error**: Device cannot be onboarded. Try by logging in by using the recommended privileges. See Role and scope based access control in OpenManage Enterprise on page 15.
   - **Managed**: Device successfully onboarded, and can be managed by the OpenManage Enterprise console.
   - **Monitored**: Device does not have management option (such as the one discovered by using SNMP).
   - **Managed with alerts**: Device is successfully onboarded, and the OpenManage Enterprise console has successfully registered its IP address with the device as a trap destination during discovery.
2. In the working pane, select a check box corresponding to the device(s), click **More Actions** > **Onboarding**.
   Ensure that you select only the device types from the All Devices page that are supported for onboarding. You can search for suitable devices in the table by clicking **Advanced Filters**, and then select or enter onboarding status data in the filter box.

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

3. In the **Onboarding** dialog box, enter the WS-Man credentials—username and password.
4. In the **Connection Settings** section:
   a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
   b. In the **Timeout** box, enter the time after which a job must stop running.
      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 discovered** check box is effective only for servers discovered by using their iDRAC interface. Selection is ineffective for other servers—such as those devices discovered by using OS discovery.

Protocol support matrix for discovering devices

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

NOTE: The functionality of the supported protocols to discover, monitor, and manage the PowerEdge YX1X servers with iDRAC6 is limited. See Generic naming convention for Dell EMC PowerEdge servers on page 177 for more information.

Table 13. 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	Not supported
PowerEdge C*	**Supported**	Not Supported	Not supported	Not supported	Not supported	Not supported	Not supported
PowerEdge chassis (CMC)	**Supported**	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
PowerEdge MX7000 chassis	Not supported	**Supported**	Not supported	Not supported	Not supported	Not supported	Not supported
Storage devices	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported	Not supported
Ethernet switches	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported	Not supported
ESXi	Not supported	Not supported	Not supported	Not supported	Not supported	**Supported**	Not supported
Linux	Not supported	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported

Table 13. Protocol support matrix for discovery (continued)

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**
Windows	Not Supported	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported
Hyper-V	Not Supported	Not supported	Not supported	**Supported**	Not supported	Not supported	Not supported
Non-Dell servers	Not supported	Not supported	Not supported	Not supported	**Supported**	Not supported	Not supported
PowerVault ME	Not supported	Not supported	Not supported	Not supported	**Supported**	Not supported	**Supported**

View device discovery job details

1. Click **Monitor** > **Discovery**.
2. Select the row corresponding to the discovery job name, and then click **View Details** in the right pane.
   The **Job Details** page displays the respective discovery job information.
3. For more information about managing jobs, see Using jobs for device control on page 122.

Related information

Discovering devices for monitoring or management on page 39

Edit a device discovery job

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

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

Related information

Discovering devices for monitoring or management on page 39

Run a device discovery job

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

To run a device discovery job:

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

Related information

Discovering devices for monitoring or management on page 39

Stop a device discovery job

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

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

   NOTE: Multiple jobs cannot be stopped at a time.

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

Related information

Discovering devices for monitoring or management on page 39

Specify multiple devices by importing data from the .csv file

1. In the **Create Discovery Job** dialog box, by default, a discovery job name is populated in **Discovery Job Name**. To change it, type a discovery job name.
2. Click **Import**.

   NOTE: Download the sample .CSV file, if necessary.

3. In the **Import** dialog box, click **Import**, browse through to the .CSV file which contains a list of valid ranges, and then click **OK**.

   NOTE: An error message is displayed if the .CSV file contains invalid ranges, and duplicate ranges are excluded during the import operation.

Global exclusion of ranges

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

NOTE: Currently, you cannot exclude a device by using its hostname, but exclude only by using its IP address or FQDN.

1. To activate the Global Exclusion of Ranges wizard, you can do one of the following:
   - From the All Devices page (**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 on page 42.

   NOTE:
   - The range size is limited to 16,385 (0x4001).
   - The IPv6 and IPv6 CIDR formats too are supported.

3. Click **Add**.

4. When prompted, click **YES**.
   The IP address or the range is globally excluded, and then displayed in the list of excluded ranges. Such devices are globally excluded which implies that they do not take part in any activity performed by OpenManage Enterprise.

   NOTE: The device that is globally excluded is clearly identified as 'Globally excluded' on the **Job Details** page.

   To remove a device from the global exclusion list:
   a. Select the check box and click **Remove from Exclusion**.
   b. When prompted, click **YES**. The device is removed from the global exclusion list. However, a device removed from the global exclusion list is not automatically monitored by OpenManage Enterprise. You must discover the device so that OpenManage Enterprise starts monitoring.

NOTE:

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

.

Specify discovery mode for creating a server discovery job

1. From the **Device Type** drop-down menu, select **SERVER**.
2. When prompted, select:
   - **Dell iDRAC**: To discover by using iDRAC.
   - **Host OS**: To discover by using an VMware ESXi, Microsoft Windows Hyper-V, or Linux operating system.
   - **Non-Dell Servers (via OOB)**: To discover third party servers by using IPMI.
3. Click **OK**.
   Based on your selection, the fields change under **Settings**.
4. Enter the IP address, host name, or IP range associated with the protocol in **IP/Hostname/Range**.
5. Under **Settings**, enter the username and password of the server to be discovered.
6. To customize discovery protocols by clicking **Additional Settings**, see Creating customized device discovery job template for servers.
7. Schedule the discovery job. See Schedule job field definitions on page 172.
8. Click **Finish**.
   A discovery job is created and displayed in the list of discovery jobs.

Related information

Discovering devices for monitoring or management on page 39

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

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

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

1. To **Discover using WS-Man/Redfish (iDRAC, Server, and/or Chassis)**
   a. In the Credentials section, enter **User Name** and **Password**.
   b. In the **Connection Settings** section:
      - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
      - In the **Timeout** box, enter the time after which a job must stop running.
      - Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 30
      - Select the **Enable Common Name (CN)** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
      - Select the **Enable Certificate Authority (CA)** check box, if needed.
2. To **Discover using IPMI (non-Dell via OOB)**
   a. In the Credentials section, enter **User Name** and **Password**.
   b. In the **Connection Settings** section:
      - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
      - In the **Timeout** box, enter the time after which a job must stop running.
      - In the **KgKey** box, enter an appropriate value.
3. To **Discover using SSH (Linux, Windows, Hyper-V)**

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

   a. In the Credentials section, enter **User Name** and **Password**.
   b. In the **Connection Settings** section:
      - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
      - In the **Timeout** box, enter the time after which a job must stop running.
      - Enter in the **Port** box to edit the port number. By default, 22 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 30
      - Select the **Verify the known Host key** check box to validate host against known host keys.

        NOTE: Known host keys are added via the */DeviceService/HostKeys REST API* service. Please refer to the *OpenManage Enterprise RESTful API Guide* for more information on how to manage host keys.
      - Select the **Use SUDO Option** check box if sudo accounts are preferred.

        NOTE: For sudo accounts to work, the server(s) `/etc/sudoer` file must be configured to use NOPASSWD.
4. To **Discover using ESXi (VMware)**
   a. In the Credentials section, enter **User Name** and **Password**.
   b. In the **Connection Settings** section:
      - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
      - In the **Timeout** box, enter the time after which a job must stop running.
      - Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 30
      - Select the **Enable Common Name (CN)** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
      - Select the **Enable Certificate Authority (CA)** check box, if needed.

Related information

Discovering devices for monitoring or management on page 39

Specify discovery mode for creating a chassis discovery job

1. From the **Device Type** drop-down menu, select **CHASSIS**.
   Based on your selection, the fields change under **Settings**.
2. Enter the IP address, host name, 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 customized discovery template by clicking **Additional Settings**, see Create customized device discovery job protocol for Chassis – Additional settings for discovery protocols on page 49.

NOTE: Currently, for any M1000e chassis that is discovered, the date in the TIMESTAMP column under Hardware Logs is displayed as JAN 12, 2013 in the CMC 5.1x and earlier versions. However, for all versions of CMC VRTX and FX2 chassis, correct date is displayed.

NOTE: When a server in a chassis is separately discovered, slot information about the server is not displayed in the **Chassis Information** section. However, when discovered through a chassis, the slot information is displayed. For example, an MX740c server in an MX7000 chassis.

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

In the **Additional Settings** dialog box:

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

   NOTE: For chassis, the **Discover using WS-Man/Redfish** check box is selected by default. Implies that the chassis can be discovered by using either of these two protocols. The M1000e, CMC VRTX, and FX2 chassis support the WS-Man commands. The MX7000 chassis supports Redfish protocol.

2. Enter username and password of the chassis to be detected.
3. In the **Connection Settings** section:
   a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
   b. In the **Timeout** box, enter the time after which a job must stop running.
   c. Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 30.
   d. Select the **Enable Common Name (CN) check** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
   e. Select the **Enable Certificate Authority (CA) check** check box.
4. To discover IO modules, select the **Discover IO Modules with chassis** check box.

   NOTE: Applicable only for the CMC VRTX, M1000e, and FX2 chassis (models FN2210S, FN410T and FN410S). For the MX7000 chassis, the IO modules are automatically detected.

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

   a. Select **Use chassis credentials** if the M I/O Aggregator user credentials are the same as that of the chassis.
   b. Select **Use different credentials** if the M I/O Aggregator user credentials are different from the chassis credentials and do the following:
      - Enter the **User Name** and **Password**.
      - Change the default values for **Retries**, **Timeout**, and **Port** if required.
      - Select **Verify known Host key**, to validate host against known host keys.

        NOTE: Known host keys are added via */DeviceService/HostKeys REST API* service. Please refer to the *OpenManage Enterprise RESTful API Guide* for more information on how to manage host keys.
      - Select **Use SUDO Option** if needed.
5. Click **Finish**.
6. Complete the tasks in Create a device discovery job on page 42.

Specify discovery mode for creating a Dell storage discovery job

1. From the **Device Type** drop-down menu, select **DELL STORAGE**.
2. When prompted, select:

- PowerVault ME: To discover the storage devices using the HTTPS protocol like the PowerVault ME.
- Others: To discover storage devices which use SNMP protocol.

Based on your selection, the fields change under **Settings**.

3. Enter the IP address, host name, or IP range in **IP/Hostname/Range**.
4. Under **Settings**, depending on your initial selection — enter the **User Name** and **Password** for Storage HTTPS or enter the **SNMP version** and the **community type** of the device to be detected.
5. Click **Additional Settings** to customize the respective discover protocol. See Creating customized device discovery job template for SNMP devices or see Create customized device discovery job protocol HTTPS storage devices –Additional settings for discovery protocols on page 50.
6. Complete the tasks in Create a device discovery job on page 42.

Related information

Discovering devices for monitoring or management on page 39

Specify discovery mode for creating a network switch discovery job

1. From the **Device Type** drop-down menu, select **NETWORK SWITCH**.
2. Enter the IP address, host name, or IP range in **IP/Hostname/Range**.
3. Under **Settings** enter the **SNMP version** and the **community type** of the device to be detected.
4. Click **Additional Settings** to customize the respective discover protocol. See Creating customized device discovery job template for SNMP devices
5. Complete the tasks in Create a device discovery job on page 42.

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

In the **Additional Settings** dialog box:

1. Enter username and password of the PowerVault ME to be detected.
2. In the **Connection Settings** section:
   a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
   b. In the **Timeout** box, enter the time after which a job must stop running.
   c. Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 30.
   d. Select the **Enable Common Name (CN) check** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
   e. Select the **Enable Certificate Authority (CA) check** check box.
3. Click **Finish**.
4. Complete the tasks in Create a device discovery job on page 42.

Create customized device discovery job protocol for SNMP devices

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

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

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

   NOTE: Currently, the settings in the **Retries box** and the **Timeout box** do not have any functional impact on the discovery jobs for SNMP devices. Hence, these settings can be ignored.
3. Click **Finish**.
4. Complete the tasks in Create a device discovery job on page 42.

Related information

Discovering devices for monitoring or management on page 39

Specify discovery mode for creating a MULTIPLE protocol discovery job

1. From the **Type** drop-down menu, select **MULTIPLE** to discover devices using multiple protocols.
2. Enter the IP address, host name, or IP range in **IP/Hostname/Range**.
3. To create customized discovery template by clicking **Additional Settings**, see Create customized device discovery job protocol for servers –Additional settings for discovery protocols on page 47.

Related information

Discovering devices for monitoring or management on page 39

Delete a device discovery job

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

To delete a device discovery job:

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

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

NOTE: A device discovery job cannot be deleted from the **Jobs** page.

Related information

Discovering devices for monitoring or management on page 39

8

Manage devices and device groups

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

The left pane displays the device groups as follows:

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

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

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

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

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

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

NOTE:

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

Topics:

Organize devices into groups

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

- Group the devices. For example, you can group devices based on functions, OSs, user profiles, location, jobs run, and then run queries to manage devices.
- Filter the device-related data while managing devices, updating firmware, discovering devices, and managing alert policies and reports.
- You can manage the properties of a device in a group. See View and configure individual devices on page 64.

OpenManage Enterprise provides a built-in report to get an overview of the OpenManage Enterprise monitored devices. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Devices Overview Report**. Click **Run**. See Run reports on page 133.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

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

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

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

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

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

  - **MCM group**—Indicates the Multi-Chassis Management (MCM) group that has more than one chassis identified by the following syntax: `Group_<MCM group name>_<Lead_Chassis_Svctag>` where:
    - `<MCM group name>`: Name of the MCM group
    - `<Lead_Chassis_Svctag>`: The Service Tag of the lead chassis. The chassis, sleds, and network IOMs form this group.
  - **Stand-alone Chassis group**—Identified by using the `<Chassis_Svctag>` syntax. The chassis, sleds, and network IOMs form this group.
- **Network Devices**: Dell Force10 networking switches and Fibre Channel switches
- **Servers**: Dell iDRAC servers, Linux servers, Non-Dell servers, OEM servers, and Windows servers
- **Storage Devices**: Dell Compellent storage Arrays, PowerVault MD storage arrays, and PowerVault ME storage arrays
- **Discovery Groups**: Groups that map to the range of a discovery task. Cannot be edited or deleted because the group is controlled by the discovery job where the include/exclude condition is applied. See Discovering devices for monitoring or management on page 39.

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

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

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

NOTE: Static and Query groups:

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

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

On the **All Devices** page, in the left pane, you can create child groups under the parent Static and Query group. See Create a Static device group on page 54 and Create a Query device group on page 55.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

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

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

Related tasks

Delete devices from OpenManage Enterprise on page 60
Refresh device inventory of a single device on page 67
Refresh the device health of a device group on page 61

Create a custom group (Static or Query)

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

To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15

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

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

Create a Static device group

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

To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

1. To activate the Create Static Group wizard, do one of the following:
   - Under CUSTOM GROUPS, **Static Groups** either right click or click the three vertical dots menu, and then click **Create New Static Group**.
   - Click **Group Actions** > **Create Custom Group** > **Static Group** .
2. In the **Create Static Group Wizard** dialog box, enter a Name and Description (optional) for the group, and then select a parent group under which the new static group must be created.

   NOTE: The static or dynamic group names and server configuration related names in OpenManage Enterprise must be unique (not case-sensitive). For example, *name1* and *Name1* cannot be used at the same time.

3. Click **Next**.
4. From the Group Member Selection dialog box, select the devices that must be included in the static group.
5. Click **Finish**.

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

Create a Query device group

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

1. To activate the Create Query Group wizard, you can do one of the following:
   - Under Custom Groups, either right click on **Query Groups** or click the three dots vertical menu next to the Query Groups, and then click **Create New Query Group.**
   - Click **Group Actions** > **Create Custom Group** > **Query Group**.
2. In the **Create Query Group Wizard** dialog box, enter a **Name** and **Description**(optional) for the group.
3. Click **Next**.
4. In the **Query Criteria Selection** dialog box, from the **Select existing query to copy** drop-down menu, select a query, and then select the other filter criteria. See Select a query criteria on page 55.
5. Click **Finish**.
   The query group is created and listed under the Query group section in the left pane.

Select a query criteria

Define filters while creating query criteria for:

- Generating customized reports. See Creating reports on page 134.
- Creating Query-based device groups under the CUSTOM GROUPS. See Create a Query device group on page 55.

Define the query criteria by using two options:

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

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

NOTE: When selected, the filters of an existing query criteria is copied only virtually to build a new query criteria. The default filters associated with an existing query criteria is not changed. The definition (filters) of a built-in query criteria is used as a starting point for building a customized query criteria. For example:

1. *Query1* is a built-in query criteria that has the following predefined filter: `Task Enabled=Yes`.
2. Copy the filter properties of *Query1*, create *Query2*, and then customize the query criteria by adding another filter: `Task Enabled=Yes` AND `(Task Type=Discovery)`.
3. Later, open *Query1*. Its filter criteria still remains as `Task Enabled=Yes`.

1. In the **Query Criteria Selection** dialog box, select from the drop-down menu based on whether you want to create a query criteria for Query groups or for report generation.
2. Add or remove a filter by clicking the plus or dustbin symbol respectively.
3. Click **Finish**.
   A query criteria is generated and saved in the list of existing queries. An audit log entry is made and displayed in the Audit logs list. See Monitor audit logs on page 120.

Related information

Managing the device configuration compliance on page 104
Edit a configuration compliance baseline on page 108

Remove a configuration compliance baseline on page 110

Edit a static group

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

The changes made to the static group are implemented.

Edit a query group

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

To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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**.

The changes made to the query group are implemented.

Rename a static or query group

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

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

Delete a static or query device group

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

To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See, Role and scope based access control in OpenManage Enterprise on page 15.

NOTE: This procedure is applicable only for deleting a static or query group, however the devices in the group would not be deleted from the All Devices page. To remove devices from OpenManage Enterprise, see Delete devices from OpenManage Enterprise on page 60.

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

The group is deleted from the CUSTOM GROUPS.

Clone a static or query group

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15

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

Add devices to a new group

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

To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

Add devices to existing group

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

1. From the **OpenManage Enterprise** menu, click **Devices**.
   All Devices page is displayed.
2. In devices list, select the check box corresponding to the device(s), and then click **Group Actions** > **Add To Existing Group**.
3. In the **Add Selected Devices to Existing Group** dialog box, enter or select data. For more information about groups, see Device Groups.
4. Click **Finish**.
   The devices are added to the selected existing group.
   NOTE: For creating groups or adding devices to a group, you must follow the parent-child relationship of groups. See Device Groups.

Refresh health on group

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

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- For the in-band devices discovered using the ESXi and Linux operating systems, the Health State ( ) is displayed as Unknown ( ).

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

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

All Devices page - devices list

The list of devices displays the device properties such as IP address and Service Tag. You can select a maximum of 25 devices per page and navigate the pages to select more devices and perform tasks. For more information about the tasks you can perform on the All Devices page, see All Devices page — device list actions on page 59.

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

- **Health State** indicates the working state of the device. The health statuses—Normal, Critical, and Warning—are identified by respective color symbols. See Device health statuses on page 38
- **Power State** indicates if the device is turned on or off
- **Connection State** indicates whether or not the device is connected to OpenManage Enterprise
- **Name** indicates device name.
- **IP Address** indicates the IP address of the iDRAC installed on the device
- **Identifier** indicates the service tag of the device
- **Model** indicates the model number
- **Type** indicates the type of device—Server, Chassis, Dell Storage, and Networking switch
- **Chassis Name** indicates chassis name
- **Slot Name** indicates the slot name for the chassis devices
- **Managed State** column indicates if the device is monitored, managed, or is proxied. See Discovering devices for monitoring or management on page 39.

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

NOTE: In the Devices list, click the device name or IP address to view device configuration data, and then edit. See View and configure individual devices on page 64.

NOTE: The working pane displays the Donut chart of the selected device group. By using the Donut chart, you can view the list of devices that belongs to other health statuses in that group. To view devices of other health status, click the

corresponding color band on the Donut chart. The data in the table changes. For more information about using the Donut chart, see Donut chart.

All Devices page — device list actions

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

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

- From **Group Actions** drop-down, you can:
  - Create custom device groups. See Create a custom group (Static or Query) on page 54.
  - Create static groups. See Create a Static device group on page 54.
  - Create query groups. See Create a Query device group on page 55
  - Edit static or query groups. See Edit a static group on page 56 and Edit a query group on page 56.
  - Clone groups. See Clone a static or query group on page 57.
  - Rename group. See Rename a static or query group on page 56.
  - Delete groups. See Delete a static or query device group on page 56.
  - Add device(s) to a new group. See Add devices to a new group on page 57.
  - Add device(s) to an existing group. See Add devices to existing group on page 57.
- From **Discovery** drop-down, you can:
  - Discover and onboard devices. See Discovering devices for monitoring or management on page 39 and Onboarding devices on page 43.
  - Exclude devices. See Exclude devices from OpenManage Enterprise on page 60.
  - Edit Exclude ranges. See Global exclusion of ranges on page 46.
- From **Inventory** drop-down, you can:
  - Run inventory on a device group. See Create and run an inventory job.
  - Run inventory on devices. See Run inventory on devices on page 60.
- From **Refresh Health** drop-down, you can:
  - Refresh health on group. See Refresh health on group on page 58.
  - Refresh health on devices. See Refresh health on devices on page 62.
- From **More Actions** drop-down, you can:
  - Turn LED on. See Create a job to turn device LEDs on page 127.
  - Turn LED off. See Create a job to turn device LEDs on page 127.
  - Power on the device(s). See Create a job for managing power devices on page 127.
  - Power off the device(s). See Create a job for managing power devices on page 127.
  - Graceful shutdown of the device(s). See Create a job for managing power devices on page 127.
  - Power Cycle a system (Cold Boot). See Create a job for managing power devices on page 127.
  - System reset (Warm Boot). See Create a job for managing power devices on page 127.
  - Perform IPMI CLI remote command on a device. See Run remote–RACADM and IPMI–commands on individual devices on page 67.
  - Perform RACADM CLI remote command on a device. See Run remote–RACADM and IPMI–commands on individual devices on page 67.
  - Delete device(s) from OpenManage Enterprise. See Delete devices from OpenManage Enterprise on page 60.
  - Export data on all the devices. See Export all or selected data on page 63
  - Export data on the selected devices. See Export all or selected data on page 63

Delete devices from OpenManage Enterprise

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

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See, Role and scope based access control in OpenManage Enterprise on page 15.
- A device on which a profile is assigned cannot be deleted unless the profile is unassigned from it. For more information, see Unassign profiles on page 102.
- A device can be deleted even when tasks are running on it. Any tasks initiated on a device fails if the device is deleted before the completion of the tasks.

To delete the discovered devices:

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

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

Related information

Organize devices into groups on page 52

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.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

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.

To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15

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

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

Update the device firmware and drivers by using baselines

You can update the firmware and/or driver version of device(s) on the All Devices page or from the Firmware/Driver Compliance page (see Update firmware and/or drivers using the baseline compliance report on page 78). Updating using the All Devices page is recommended when updating firmware and/driver of a single device.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- Driver updates are applicable only for devices associated with 64-bit Windows versions.
- Driver updates on the devices cannot be rolled back.
- If the firmware update is done using the **'Stage for next server reboot'** option, then the inventory and baseline check must be executed manually after the package is installed in the remote device.
- If the device is not associated with any baseline, the **Baseline** drop-down menu is not populated. To associate a device to a baseline, see Creating the firmware baseline.
- If you select multiple devices, only the devices that are associated with the selected baseline are listed in the table.

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

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

2. In the **Device Update** dialog box:
   a. In the **Select Update Source** section select one of the following:
      - From the **Baseline** drop-down menu, select the baseline. A list of devices that are associated with the selected baseline is displayed. The compliance level of each device is displayed in the 'compliance' column. Based on the compliance level, you can update the firmware and/or driver version. For information about the field description on this page, see Viewing device firmware compliance report.
        i. Select the check boxes corresponding to the devices that must be updated.
        ii. Click **Next**.
      - You can update the firmware and/or drivers by using Individual Update package also. Click **Individual Package**, and then complete the on-screen instructions. Click **Next**.

   b. In the **Schedule** section:

   - Under **Schedule Update**, click **Additional Information** to view the important information and select one of the following:
     a. **Update Now**: To apply the firmware/driver updates immediately.
     b. **Schedule Later**: To specify a date and a time when the firmware and/or driver version must be updated. This mode is recommended if you do not want to disturb your current tasks.
   - Under **Server Options** select one of the following reboot options :
     a. To reboot the server immediately after the firmware/driver update, choose **Reboot server immediately** and from the dropdown menu select one of the following options:
        i. **Graceful Reboot without Forced Shutdown**
        ii. **Graceful Reboot with Forced Shutdown**
        iii. **PowerCycle** for a hard reset of the device.
     b. Select **Stage for next server reboot** to trigger the firmware/driver update when the next server reboot happens. If this option is selected, then the inventory and baseline check must be executed manually after the package is installed in the remote device.

3. Click **Finish**.

A firmware/driver update job is created and listed in the Jobs list. See Using jobs for device control on page 122.

Refresh the device health of a device group

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

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.

The latest working status of selected device(s) is collected and displayed on the Dashboard and other relevant sections of OpenManage Enterprise. To download a device inventory, see Export the single device inventory on page 63.

Related information

Organize devices into groups on page 52

Refresh health on devices

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

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- For the in-band devices discovered using the ESXi and Linux operating systems, the Health State ( ) is displayed as Unknown ( ).

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

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

Roll back an individual device's firmware version

You can roll back the firmware version of a device that is later than the firmware version of the baseline it is associated with. This feature is available only when you view and configure properties of an individual device. See View and configure individual devices on page 64. You can upgrade or roll back the firmware version of an individual device. You can roll back the firmware version of only one device at a time.

NOTE:

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

Any device firmware that is updated by using the iDRAC GUI is not listed here and cannot be updated. For information about creating baseline, see Create a firmware/driver baseline on page 76.

1. In the left pane, select the group, and then click the device name in the list.
2. On the **<device name>** page, click **Firmware/Drivers**.
3. From the **Baseline** drop-down menu, select the baseline to which the device belongs to.
   All the devices that are associated with the selected baseline are listed. For information about field description in the table, see View the baseline compliance report on page 78.
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

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

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

Performing more actions on chassis and servers

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

- **Turn LED On**: Turn on the LED of the device to identify the device among a group of devices in a data center.
- **Turn LED Off**: Turn off the LED of the device.
- **Power On**: Turn on the device(s).
- **Power Off**: Turn off the device (s).
- **Graceful Shutdown**: Click to shut down the target system.
- **Power Cycle System (Cold Boot)**: Click to power off and then restart the system.
- **System Reset (Warm Boot)**: Click to shut down and then reboot the operating system by forcefully turning off the target system.
- **Proxied**: Displayed only for the MX7000 chassis. Indicates that the device is discovered through an MX7000 lead chassis in case of Multi-Chassis Management (MCM).
- **IPMI CLI**: Click to run an IMPI command. See Create a Remote command job for managing devices on page 128.
- **RACADM CLI**: Click to run a RACADM command. See Create a Remote command job for managing devices on page 128.
- **Update Firmware**: See Update the device firmware and drivers by using baselines on page 61.
- **Onboarding**: See Onboarding devices on page 43.
- **Export All and Exported Selected**: See Export all or selected data on page 63.

Hardware information displayed for MX7000 chassis

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

Export all or selected data

You can export data:

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

NOTE:

- Avoid exporting 'wide' tables that have column(s) with long strings or with too many columns to PDF. Due to a limitation in the PDFMaker library, the right-most section of such exported data is truncated or cut off.
- A single device inventory can be exported only into a .csv format. See Export the single device inventory on page 63
- Only in case of reports, you can export only selected reports at a time and not all the reports. See Export selected reports on page 136.

.

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

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

View and configure individual devices

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

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

- View information about the health and power status, device IP, and Service Tag.
- View general information about the device and perform device control and troubleshooting tasks.
- View device information such as RAID, PSU, OS, NIC, memory, processor, and storage enclosure. OpenManage Enterprise provides a built-in report to get an overview about the NIC, BIOS, Physical Disk and Virtual Disk used on the devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise** > **Monitor** > **Reports**.
- Update or roll back firmware versions of components in a device that are associated with a firmware baseline. See Manage the device firmware and drivers on page 72.

  NOTE: Updating a device using the Individual Package workflow only supports executable (EXE) based Dell Update Packages. When updating an FX2 CMC, the executable DUP must be installed via one of the sleds in the chassis.
- Acknowledge, export, delete, or ignore the alerts pertaining to a device. See Managing device alerts.
- View and export hardware log data of a device. See Managing individual device hardware logs on page 66.
- View and manage the configuration inventory of the device for the purposes of configuration compliance. A compliance comparison is initiated when the configuration inventory is run against the devices.
- View the compliance level of a device against the configuration compliance baseline it is associated with. See Managing the device configuration compliance on page 104.

Device Overview

- On the **<device name>** page, under **Overview**, the health, power status, and Service Tag of the device is displayed. Click the IP address to open the iDRAC login page. See the *iDRAC User's Guide* available on the Dell support site.
  - **Information**: Device information such as Service Tag, DIMM slots, iDRAC DNS name, processors, chassis, operating system, and data center name. Multiple management IP addresses correlated to the device are listed and can be clicked to activate the respective interfaces.
  - **Recent Alerts**: The recent alerts generated for the device.
  - **Recent Activity**: A list of recent jobs run on the device. Click **View All** to view all the jobs. See Using jobs for device control on page 122.
  - **Remote Console**: Click **Launch iDRAC** to start the iDRAC application. Click **Launch Virtual Console** to start the virtual console. Click the **Refresh Preview** symbol to refresh the **Overview** page.
  - **Server Subsystem**: Displays health status of other components of the device such as PSU, fan, CPU, and battery.

    NOTE: The time taken to collect subsystem data of sensor components discovered using IPMI depends on network connectivity, target server, and target firmware. If you experience timeouts while collecting the sensor data, reboot the target server.
  - The **Last Updated** section indicates the last time when the device inventory status was updated. Click the **Refresh** button to update the status. An Inventory job is started and the status is updated on the page.
- By using **Power Control**, turn on, turn off, power cycle, and gracefully shut down a device.
- By using **Troubleshoot**:

- Run and download the Diagnostics report. See Run and download Diagnostic reports on page 65.
- Reset iDRAC.
- Extract and download the SupportAssist report. See Extract and download SupportAssist reports on page 66.

- Refresh the device status.
- Refresh the device inventory.
- Export the device inventory that is collected by clicking **Refresh Inventory**. See Export all or selected data on page 63.
- Run a remote RACADM, and IPMI command on the device. See Run remote–RACADM and IPMI–commands on individual devices on page 67.

OpenManage Enterprise provides a built-in report to get an overview of devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Devices Overview Report**. Click **Run**. See Run reports on page 133.

Device hardware information

OpenManage Enterprise provides a built-in report about the components and their compliance with the firmware compliance baseline. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Firmware Compliance per Component Report**. Click **Run**. See Run reports on page 133.

- **Device Card Information**—Information about cards used in the device.
- **Installed Software**—List of firmware and software installed on different components in the device.
- **Processor**—Processor information such as sockets, family, speed, cores, and model.
- **RAID Controller Information**—PERC and RAID controller used on the storage devices. The rollup status is equal to the status of the RAID that has high severity. For more information about Rollup Health status, see the *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* white paper on the Dell TechCenter.
- **NIC Information**—Information about NICs used in the device.
- **Memory Information**—Data about DIMMs used in the device.
- **Array Disk**: Information about the drives installed on the device. OpenManage Enterprise provides a built-in report about the HDDs or virtual drives available on the devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Physical Disk Report**. Click **Run**. See Run reports on page 133.
- **Storage Controller** : Storage controller installed on the device. Click the plus symbol to view individual controller data.
- **Power Supply Information**: Information about the PSUs installed on the device.
- **Operating System**—OS installed on the device.
- **Licenses**—Health status of different licenses installed on the device.
- **Storage Enclosure**—Storage enclosure status and EMM version.
- **Virtual Flash**—List of virtual flash drives and its technical specification.
- **FRU**—List of Field Replaceable Units (FRUs) that can be handled and repaired only by the field technicians. OpenManage Enterprise provides a built-in report about the Field Replacable Units (FRUs) installed on the devices monitored by OpenManage Enterprise. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **FRU Report**. Click **Run**. See Run reports on page 133.
- **Device Management Info**—IP address information of the iDRAC installed only in case of a server device.
- **Guest Information**—Displays the guest devices monitored by OpenManage Enterprise. UUID is the Universally Unique Identifier of the device. The **GUEST STATE** column indicates the working status of the guest device.

Run and download Diagnostic reports

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. SeeRole and scope based access control in OpenManage Enterprise on page 15

NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See Manage Console preferences on page 157 and Generic naming convention for Dell EMC PowerEdge servers on page 177for more information.

1. On the **<Device name>** page, from the **Troubleshoot** drop-down menu, select **Run Diagnostics**.
2. In the **RemoteDiagnostic Type** dialog box, from the **Remote Diagnostic Type** drop-down menu, select one of the following to generate a report.
   - **Express**: In the least possible time.

- **Extended**: At nominal speed.
- **Long Run**: At a slow pace.

NOTE: See the *Remotely Running Automated Diagnostics Using WS-Man and RACADM Commands* technical white paper at https://en.community.dell.com/techcenter/extras/m/white_papers/20438187.

3. To generate the Diagnostics report now, select **Run Now**.
4. Click **OK**. When prompted, click **YES**.

   WARNING: Running a Diagnostics report automatically restarts the server.

   A job is created and displayed on the **Jobs** page. To view information about the job, click **View Details** in the right pane. See View job lists on page 122. The job status is also displayed in the **Recent Activity** section. After the job is successfully run, the status of the job is indicated as **Diagnostic Completed**, and the **Download** link is displayed in the **Recent Activity** section.
5. To download the report, click the **Download** link, and then download the <*Servicetag-jobid*>.TXT Diagnostics report file.
   - Else, click **Troubleshoot** > **Download Diagnostics Report**, and then download the file.
6. In the **Download RemoteDiagnostics Files** dialog box, click the .TXT file link, and then download the report.
7. Click **OK**.

Extract and download SupportAssist 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 control in OpenManage Enterprise on page 15

NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See Manage Console preferences on page 157 and Generic naming convention for Dell EMC PowerEdge servers on page 177 for more information.

1. On the **<Device name>** page, from the **Troubleshoot** drop-down menu, select **Extract SupportAssist Report**.
2. In the **Extract SupportAssist Report** dialog box:
   a. Enter the file name where the SupportAssist report must be saved.
   b. Select the check boxes corresponding to the log types whose SupportAssist report must be extracted.
3. Click **OK**.
   A job is created and displayed on the **Jobs** page. To view information about the job, click **View Details** in the right pane. See View job lists on page 122. 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

NOTE: The hardware logs are available for YX4X servers, MX7000 chassis and sleds. See Generic naming convention for Dell EMC PowerEdge servers on page 177 for more information.

- On the **<Device name>** page, click **Hardware logs**. All the event and error messages generated for the device is listed. For field descriptions, see Monitor audit logs on page 120.
- For a chassis, the real-time data about the hardware logs are retrieved from the chassis.
- To add a comment, click **Add Comment**.
- In the dialog box, type the comment, and then click **Save**. The comment is saved and identified by a symbol in the **COMMENT** column.
- To export selected log data to a .CSV file, select the corresponding check boxes, and then click **Export** > **Export Selected**.

- To export all logs on a page, click **Export** > **Export Current Page**.

Run remote–RACADM and IPMI–commands on individual devices

RACADM and IPMI commands can be sent to a device's iDRAC from the 'Device name' page to remotely manage the respective device.

NOTE:
- The RACADM CLI only allows for one command at a time.
- The use of the following special characters as RACADM and IPMI CLI parameters is not supported: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, *, and **'**.

1. Select the check box corresponding to the device and click **View Details**.
2. On the **<device name>** page, click **Remote Command Line**, and then select **RACADM CLI** or **IPMI CLI**.

   NOTE: The RACADM CLI tab is not displayed for the following servers because the corresponding task is not available in the device pack — MX740c, MX840c, and MX5016S.

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 on page 122.
5. Click **Finish**.
   The **Recent Alerts** section displays the job completion status.

Start Management application iDRAC of a device

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 page is displayed. Log in by using the iDRAC credentials.

   For more information about using iDRAC, visit Dell.com/idracmanuals.

   NOTE: You can also start the management application by clicking the IP address in the Device list. See All Devices page - devices list on page 58.

Start the Virtual Console

The **Virtual Console** link works on the iDRAC Enterprise license of YX4X servers. On the YX2X and YX3X servers, the link works on the 2.52.52.52 and later versions of iDRAC Enterprise license. If the link is clicked when the current plugin type for virtual console is Active X, a message indicates prompting you to update the console to HTML 5 for better user experience. See Create a job to change the virtual console plugin type on page 128and Generic naming convention for Dell EMC PowerEdge servers on page 177for more information.

1. Select the check box corresponding to the device.
   The device working status, name, type, IP, and Service Tag are displayed.
2. In the right pane, click **Launch Virtual Console**.
   The remote console page on the server is displayed.

Refresh device inventory of a single device

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:

1. Select the check box corresponding to the device on the All Devices page (**OpenManage Enterprise** > **Devices**) and click **View Details** on the right pane. The device's Overview page is displayed.

2. Click **Refresh Inventory** to initiate an Inventory job.
   The status of the inventory job can be viewed on the Inventory page (**OpenManage Enterprise** > **Monitor** > **Inventory**) . Select the Inventory job and click on **View Details** to view the collected inventory of selected device. For more information about viewing the refreshed inventory data, see View and configure individual devices on page 64. To download a device inventory, see Export the single device inventory on page 63.

Related information

Organize devices into groups on page 52

9

Managing device inventory

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

By clicking **OpenManage Enterprise** > **Monitor** > **Inventory**, you can generate a device inventory report to better manage your data center, reduce maintenance, maintain minimum stock, and reduce operational costs. By using the Inventory Schedules feature in OpenManage Enterprise, you can schedule jobs to run at predefined time, and then generate reports. You can schedule inventory jobs on the 12th generation and later PowerEdge servers, networking devices, PowerEdge chassis, EqualLogic arrays, Compellent Arrays, and PowerVault devices.

On this page, you can create, edit, run, stop, or delete inventory schedules. A list of existing inventory schedule jobs is displayed.

- **NAME**: The inventory schedule name.
- **SCHEDULE**: Indicates if the job is scheduled to run now or later.
- **LAST RUN**: Indicates the time the job was last run.
- **STATUS**: Indicates if the job is running, completed, or failed.

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

To preview a job information, click the row corresponding to the job. The right pane displays the job data and the target groups associated with the inventory task. To view information about the job, click **View Details**. The **Job Details** page displays more information. See View an individual job information on page 127.

Related tasks

Run an inventory job now on page 70
Stop an inventory job on page 70
Delete an inventory job on page 71
Create an inventory job on page 69

Topics:

Create an inventory job

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

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- Inventory collection on chassis storage sleds is not supported in OpenManage Enterprise if they are managed via chassis device management.

1. To initiate the Inventory wizard, do one of the following:
   a. On the All Devices page (**OpenManage Enterprise** > **Devices**), select a group on the left pane and from **Inventory** drop-down menu click **Run Inventory on Group**.
   b. On the Inventory page (**OpenManage Enterprise** > **Monitor** > **Inventory**), click **Create**.

2. In the **Inventory** dialog box, a default inventory job name is populated in **Inventory Job Name**. To change, enter an inventory job name.
3. From the **Select Groups** drop-down menu, select the device groups on which the inventory must be run.

   If you have initiated the Inventory job from the All Devices page after selecting a group, then Select Groups will be prepopulated with the selected group name. For information about device groups, see Organize devices into groups on page 52.
4. In the **Scheduling** section, run the job immediately or schedule for a later point of time.

   See Schedule job field definitions on page 172.
5. The following **Additional Options** can be selected while running the inventory job:
   - Select the **Collect configuration inventory** check box to generate an inventory of the configuration compliance baseline.
   - Select the **Collect driver inventory** check box to collect driver inventory information from the Windows server. Also, to install the Inventory Collector and Dell System Update on the Windows server if these components are not available on the server.

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

   For information about configuration compliance baselines, see Managing the device configuration compliance on page 104.
6. Click **Finish**.
7. The job is created and listed in the queue.
   An inventory job is created displayed in the list of inventory jobs. The **SCHEDULE** column specifies whether the job is Scheduled or Not Scheduled. See Run an inventory job now on page 70.

Related information

Managing device inventory on page 69

Run an inventory job now

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

1. In the list of existing inventory schedule jobs, select the check box corresponding to the inventory job you want to run immediately.
2. Click **Run Now**.

   The job starts immediately and a message is displayed in the lower-right corner.

Related information

Managing device inventory on page 69

Stop an inventory job

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

1. In the list of existing inventory schedule jobs, select the check box corresponding to the inventory schedule job you want to stop.
2. Click **Stop**.
   The job is stopped and a message is displayed in the lower-right corner.

Related information

Managing device inventory on page 69

Delete an inventory job

NOTE: You cannot delete a job if it is running.

1. In the list of existing inventory schedule jobs, select the check box corresponding to the inventory job you want to delete.
2. Click **Delete**.
   The job is deleted and a message is displayed in the lower-right corner.

Related information

Managing device inventory on page 69

Edit an inventory schedule job

1. Click **Edit**.
2. In the **Inventory Schedule** dialog box, edit the inventory job name in **Inventory Job Name**. See Create an inventory job on page 69.
   The inventory schedule job is updated and displayed in the table.

10

Manage the device firmware and drivers

On the **OpenManage Enterprise** > **Configuration** > **Firmware/Driver Compliance** page, you can manage the firmware of all the 'managed' devices. You can also update the drivers of the 64-bit Windows-based devices.

NOTE:

- To perform any tasks on OpenManage Enterprise you must have the necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.
- The device firmware or driver version, if earlier than baseline version, is not automatically updated and the user must initiate the update.
- It is recommended that the firmware and driver updation is done during the maintenance windows to prevent the devices or environment going offline during business hours.
- To manage a device's firmware and/or driver, the Onboarding status of the system should be either 'Managed' or 'Managed with Alerts'. See Onboarding devices on page 43
- Currently, the catalog contains drivers for only the 64-bit Windows-based devices.

By using the Firmware/driver feature, you can:

- Use a firmware and driver catalog from Dell.com either directly or after saving it on a network path. See Add a catalog by using Dell.com on page 73 or Creating a firmware catalog by using local network.
- Create a firmware and driver baseline by using the available catalogs. These baselines serve as benchmarks to compare the firmware and driver version on the devices against the version in the catalog. See Creating the firmware baseline.
- Run a compliance report to check if the devices associated with the baseline comply to the baseline firmware and driver versions. See Checking firmware compliance. The **COMPLIANCE** column displays:
  - **OK** — if the target device's firmware and/or driver version is same as the baseline.
  - **Upgrade** — if the target device's has one or more versions earlier than the baseline's firmware or driver version. See Updating the device firmware version
  - **Critical** — if the device is not in compliance with the baseline, and indicates that it is a critical upgrade and the device's firmware and driver/s must be upgraded to ensure proper functionality.
  - **Warning** — if the device firmware and/or driver are not in compliance with the baseline, and the device firmware can be upgraded to enhance the functionality.
  - **Downgrade** — if the device firmware and/or driver is later than the baseline version.
  - Export the compliance report for statistical and analytical purposes.
  - Update device firmware and/or driver version by using the baseline. See Update the device firmware and drivers by using baselines on page 61 .

NOTE:

- When a firmware/driver baseline with many devices is checked for compliance, the warning alerts CDEV9000 on the Alerts page is logged for only one random non-compliant device from that baseline.
- The firmware or driver compliance status of network switches, modular IOAs, and Dell storage devices is displayed as **Unknown** as these are not updatable using the Dell catalog. It is recommended to perform individual firmware or driver updates for these devices using their respective individual Update package. To perform individual firmware or driver updates, select a device on the All Devices page, and click **View Details** > **Firmware/Drivers** and select the individual package option. For more information about the list of unsupported devices, refer Firmware/driver compliance baseline reports— devices with 'Unknown' compliance status on page 176 .

You can update firmware version of a device also on the:

- All Devices page. See Updating the device firmware version.
- Device Details page. In the Devices List, click the device name or IP address to view device configuration data, and then edit. See View and configure individual devices on page 64.

NOTE: Updating a device using the Individual Package workflow only supports executable (EXE) based Dell Update Packages. When updating an FX2 CMC, the executable DUP must be installed via one of the sleds in the chassis.

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

Topics:

Manage firmware and driver Catalogs

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 control in OpenManage Enterprise on page 15.

For field definitions on the Catalog Management page, see Catalog Management field definitions on page 176. The sources of catalog that you can currently access are:

NOTE:

- Firmware catalog management using Dell.com or a local network path is limited to only the Enterprise Server Catalog.
- Catalogs with base location pointing to 'Downloads.dell.com' can be used without the Dell Update Packages (DUPs) while importing catalog in OpenManage Enterprise version 3.5 from a network share. During the firmware upgrade process, the DUPs will be downloaded directly from https://downloads.dell.com.

- **Latest component versions on Dell.com**: Lists the latest firmware and driver (64-bit Windows) versions of devices. For example, iDRAC, BIOS, PSU, and HDDs that are rigorously tested and released and posted to Dell.com. See Creating a firmware catalog by using Dell.com.
- **Network Path**: Location where the firmware and driver catalogs are downloaded by the Dell Repository Manager (DRM) and saved on a network share. See Creating a firmware catalog by using local network.

Add a catalog by using Dell.com

NOTE: To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See Manage Console preferences on page 157 and Generic naming convention for Dell EMC PowerEdge servers on page 177 for more information.

1. On the **Catalog Management** page, click **Add**.
2. In the **Add Update Catalog** dialog box:
   a. In the **Name** box, enter a firmware catalog name.
   b. For the **Catalog Source**, select the option **Latest component versions on Dell.com**.
   c. In the **Update Catalog** box, select either **Manually** or **Automatically**.
   d. If **Automatically** is selected in the **Update Catalog** box, **Update Frequency** need to be selected as either **Daily** or **Weekly** followed by time in the 12-hour format with AM/PM.
   e. Click **Finish**.

The **Finish** button appears only after you have entered all the fields in the dialog box

A new firmware catalog is created and listed in the Catalog table on the **Catalog Management** page.

3. To go back to the **Firmware/Driver Compliance** page, click **Return to Firmware/Driver Compliance**.

Add a catalog to the local network

Catalog containing the firmware and drivers (64-bit Windows) can be downloaded using the Dell Repository Manager (DRM) and saved on a network share.

1. On the **Catalog Management** page, click **Add**.
2. In the **Add Update Catalog** dialog box:
   a. In the **Name** box, enter a catalog name.
   b. For the Catalog Source, select the option **Network Path**.
   The **Share Type** drop-down menu is displayed.
   c. Select one of the following:

   NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any firmware tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See Manage Console preferences on page 157 and Generic naming convention for Dell EMC PowerEdge servers on page 177 for more information.

   - NFS
     i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
     ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: *nfsshare\catalog.xml*
   - CIFS
     i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
     ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: *Firmware\m630sa\catalog.xml*
     iii. In the **Domain** box, enter the domain name of the device.
     iv. In the **User Name** box, enter the user name of the device where the catalog is stored.
     v. In the **Password** box, enter the password of the device to access the share. Type the username and password of the shared folder where the catalog.xml file is stored.
   - HTTP
     i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
     ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: *compute/catalog.xml*.
   - HTTPS
     i. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
     ii. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: *compute/catalog.xml*.
     iii. In the **User Name** box, enter the user name of the device where the catalog is stored.
     iv. In the **Password** box, enter the password of the device where the catalog is stored.
     v. Select the **Certificate Check** check box.

     The authenticity of the device where the catalog file is stored is validated and a Security Certificate is generated and displayed in the **Certificate Information** dialog box.

   d. After you have entered the **Share Address** and the **Catalog File Path**, the **Test now** link is displayed. To validate a connection to the catalog click **Test now**. If the connection to the catalog is established, a *Connection Successful* message is displayed. If connection to the share address or the catalog file path is not established, *Connection to path failed* error message is displayed. This is an optional step.
   e. In the **Update Catalog** box, select either **Manually** or **Automatically**.
   If the **Update Catalog** is selected as **Automatically**, select either **Daily** or **Weekly** as the update frequency and enter time in the 12-hour format.
3. Click **Finish**. The **Finish** button appears only after you have entered all the fields in the dialog box.

A new firmware catalog is created and listed in the Catalog table on the **Catalog Management** page.

4. To go back to the **Firmware/Driver Compliance** page, click **Return to Firmware/Driver Compliance**.

Related tasks

Delete a catalog on page 76

SSL Certificate Information

The catalog files for firmware and driver updates can be downloaded from the Dell support site, Dell EMC Repository Manager (Repository Manager), or a web site within your organization network.

If you choose to download the catalog file from the web site within your organization network, you can accept or decline the SSL certificate. You can view details of the SSL certificate in the **Certificate Information** window. The information comprises the validity period, issuing authority and the name of the entity to which the certificate is issued.

NOTE: The **Certificate Information** window is displayed only if you create the catalog from the **Create Baseline** wizard.

Actions

Accept	Accepts the SSL certificate and allows you to access the web site.
Cancel	Closes the **Certificate Information** window without accepting the SSL certificate.

Update a catalog

The existing firmware and driver catalogs can be updated from the Dell.com site (base location).

To update a catalog:

1. On the Catalog Management page, select a catalog.
2. Click the **Check for update** button that is located in the right pane of the **Catalog Management** page.
3. Click **YES.**
   If the selected catalog was an online catalog, it is replaced by the most up-to-date version that is maintained at the Dell.com site. For the local network catalogs, all the latest firmware and drivers available in the base location are considered for computing the baseline compliance.

Edit a catalog

1. On the **Catalog Management** page, select a catalog.
   The catalog details are displayed in the **<catalog name>** right pane.
2. Click **Edit** in the right pane.
3. In the **Edit Update Catalog** wizard, edit the properties.
   The properties that you cannot edit are grayed-out. For field definitions, see Add a catalog by using Dell.com on page 73 and Add a catalog to the local network on page 74.
4. Enter the **Share Address** and the **Catalog File Path**, the **Test now** link is displayed. To validate a connection to the catalog click **Test now**. If the connection to the catalog is established, a `Connection Successful` message is displayed. If connection to the share address or the catalog file path is not established, `Connection to path failed` error message is displayed. This is an optional step.
5. In the **Update Catalog** box, select either **Manually** or **Automatically**.
   If the **Update Catalog** is selected as **Automatically**, select either **Daily** or **Weekly** as the update frequency and enter time in the 12-hour format.
6. Click **Finish**.
   A job is created and run immediately. The job status is indicated in the **REPOSITORY LOCATION** column of the **Catalog Management** page.

Delete a catalog

1. On the **Catalog Management** page, select the catalogs, and then click **Delete**.
   The catalogs are deleted from the list.
2. To go back to the **Firmware/Driver Compliance** page, click **Return to Firmware/Driver Compliance**.

NOTE: Catalogs cannot be deleted if linked to a baseline.

Related information

Add a catalog to the local network on page 74

Create a firmware/driver baseline

A baseline is a set of devices or group of devices that are associated with a firmware/driver catalog. A baseline is created for compliance evaluation of the firmware and drivers for the devices in that baseline against the versions specified in the catalog. To create a baseline:

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- 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.
- Post upgrade to version 3.6.x, any firmware/driver baselines created by device managers from any of the prior OpenManage Enterprise releases are only assigned to the administrator. Hence, the device managers must recreate the firmware/driver baselines from previous versions post upgrade.
- 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.

1. Under **Firmware**, click **Create Baseline**.
2. In the **Create Update Baseline** dialog box:
   a. In the **Baseline Information** section:
      i. From the **Catalog** drop-down menu, select a catalog.
      ii. To add a catalog to this list, click **Add**. See Managing firmware Catalogs.
      iii. In the **Baseline Name** box, enter a name for the baseline, and then enter the baseline description.
      iv. Click **Next**.
   b. In the **Target** section:
      - To select the target device(s):
        i. Select **Select Devices**, and then click the **Select Devices** button.
        ii. In the **Select Devices** dialog box, all the devices monitored by OpenManage Enterprise, IOMs, and devices under static or query group are displayed in respective groups.
        iii. In the left pane, click the category name. Devices in that category are displayed in the working pane.
        iv. Select the check box corresponding to the device(s). The selected devices are listed under the **Selected Devices** tab.
      - To select the target device group(s):
        i. Select **Select Groups**, and then click the **Select Groups** button.
        ii. In the **Select Groups** dialog box, all the devices monitored by OpenManage Enterprise, IOMs, and devices under static or query group are displayed in respective categories.
        iii. In the left pane, click the category name. Devices in that category are displayed in the working pane.
        iv. Select the check box corresponding to the group(s). The selected groups are listed under the **Selected Groups** tab.
3. Click **Finish**.
   A message is displayed that a job is created for creating the baseline.

In the Baseline table, data about the device and baseline job is displayed. For field definitions, see Firmware baseline field definitions on page 172.

Delete configuration compliance baselines

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15

To delete the configuration compliance baselines:

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

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

Edit a baseline

The baselines on the **Configurations** > **Firmware/Driver Compliance** page can be edited as follows:

1. Select a baseline, and then click **Edit** in the right pane.
2. Modify data as described in Creating the firmware baseline.
   The updated information is displayed in the Baseline list.
3. To go back to the **Firmware/Driver Compliance** page, click **Return to Firmware/Driver Compliance**.

Check the compliance of a device firmware and driver

On the **Configuration** > **Firmware/Driver Compliance** page, you can check for the compliance of the firmware and drivers of baseline devices against the associated catalog, view the report, and update the firmware and drivers of non-compliant devices.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- The firmware and drivers (64-bit Windows) for the non-compliant devices in the baseline are not automatically updated and must be updated by the user. It is recommended to update device firmware and drivers during the maintenance windows to prevent the devices or environment going offline during business hours.
- To collect the inventory information, the Inventory Collector and Dell System Update must be available on the Windows server. If these components are not available on the server, then initiate an inventory job and select **Collect driver inventory**. The discovery job also collects driver inventory information, but only the inventory job installs the necessary components on the server. To collect the driver inventory information, create or edit an inventory job and select the **Collect driver inventory** check box. For more information, see Create an inventory job on page 69 and Edit an inventory schedule job on page 71.

1. Select the check box corresponding to the baseline(s), and click **Check Compliance**.
   The baseline compliance job is run.

   NOTE: If the devices are not associated to a catalog, the compliance is not verified. A job is created only for the devices that are associated and listed in the Compliance table. To associate a device to a catalog, see Creating the firmware baseline.

   In the Baseline table, data about the device and baseline job is displayed. For field definitions, see Firmware baseline field definitions on page 172.
2. To view the Compliance report and to upgrade the firmware and driver version of device(s), click **View Report** in the right pane.

   See Viewing device firmware compliance report.

   NOTE: Rollback is not supported for drivers.

View the baseline compliance report

On the **Configuration** > **Firmware/Driver Compliance** page, the compliance status of the baselines is indicated. A Donut chart provides a summary of baselines' compliance to their respective catalogs. When more than one device is associated with a baseline, the status of the least compliant device to the baseline is indicated as the compliance level of that baseline. For example, the compliance level of a baseline with only one device with compliance as 'critical, is indicated as 'critical' even if most of the devices are compliant.

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

- Select the check box corresponding to the baseline and click **View Report** in the right pane.

  On the **Compliance Report** page the list of devices associated with the baseline and their compliance level is displayed. By default, the devices in **Critical** and **Warning** statuses are displayed.

  NOTE: If each device has its own status, the highest severity status is considered as the status of the group. For more information about Rollup Health status, see the *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* white paper on the Dell TechCenter.
- **COMPLIANCE**: Indicates the compliance level of a device to the baseline. For more information about symbols used for device firmware/driver compliance levels, see Manage the device firmware and drivers on page 72.
- **TYPE**: Type of device for which the compliance report is generated.
- **DEVICE NAME/COMPONENTS**: By default, the Service Tag of the device is displayed.
  1. To view information about components in the device, click the **>** symbol.

     A list of components and their compliance to the catalog is displayed.

     NOTE: For all the devices (except the MX7000 chassis) which are fully in compliance with the associate firmware baseline, the **>** symbol is not displayed.
  2. Select one or more check boxes corresponding to the devices whose firmware compliance status is 'Critical' and requires an update.
  3. Click **Make Compliant**. See Update the device firmware version by using the baseline compliance report.
- **SERVICE TAG**: Click to view complete information about the device on the **<device name>** page. For more information about tasks you can complete on this page, see View and configure individual devices on page 64.
- **REBOOT REQ**: Indicates if the device must be restarted after updating the firmware.
- **Info** : Symbol corresponding to every device component is linked to the support site page from where the firmware/driver can be updated. Click to open the corresponding Driver Details page on the support site.
- **CURRENT VERSION**: Indicates the current firmware version of the device.
- **BASELINE VERSION**: Indicates the corresponding firmware and driver version of the device available in the associated catalog.
- To export the compliance report to an Excel file, select the check boxes corresponding to the device, and then select from **Export**.
- To go back to the **Firmware** page, click **Return to Firmware**.
- To sort data based on a column, click the column title.
- To search for a device in the table, click **Advanced Filters**, and select or enter data in the filter boxes. See Advanced Filters in OpenManage Enterprise Graphical User Interface overview on page 34.

Update firmware and/or drivers using the baseline compliance report

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

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

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

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

Prerequisites:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- You must create an inbound firewall rule to allow communication with port 22.
- If HTTP and HTTPS shares were configured using the proxy settings, ensure that these local URLs are included in the proxy-exception list before initiating any update tasks.
- Only one update task can be initiated on the target machine at a given time.

NOTE:

- The Reset iDRAC function is not supported for the devices under an MCM chassis that are in a 'Proxied' onboarding state and for updating only the drivers of the devices. For more information about onboarding states, see Onboarding devices on page 43.
- The firmware or driver compliance status of network switches, modular IOAs, and Dell storage devices is displayed as Unknown as these are not updatable using the Dell catalog. It is recommended to perform individual firmware or driver updates for these devices using their respective individual Update package. To perform individual firmware or driver updates, select a device on the All Devices page, and click **View Details** > **Firmware/Drivers** and select the individual package option. For more information about the list of unsupported devices, refer Firmware/driver compliance baseline reports— devices with 'Unknown' compliance status on page 176

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

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

The driver updates are available only on devices discovered as 64-bit Windows servers. Before updating the drivers, do the following:

- Be aware that the rollback of the driver updates is not supported.
- In-band driver updates are only supported on Windows with OpenSSH. Driver updates on third party SSH hosted on Windows, such as the CygwinSSH, are not supported.
- To collect the inventory information, the Inventory Collector and Dell System Update must be available on the Windows server. If these components are not available on the server, then initiate an inventory job and select **Collect driver inventory**. The discovery job also collects driver inventory information, but only the inventory job installs the necessary components on the server. To collect the driver inventory information, create or edit an inventory job and select the **Collect driver inventory** check box. For more information, see Create an inventory job on page 69 and Edit an inventory schedule job on page 71.

To update a device firmware and/or driver by using the baseline compliance report:

1. On the **Configuration** > **Firmware/Driver Compliance** page, select the check box corresponding to the baseline to which the device is attached, and then click **View Report** in the right pane.

   On the **Compliance Report** page, the list of devices associated with the baseline and their compliance level is displayed. For field descriptions, see View the baseline compliance report on page 78.
2. Select the check box corresponding to the device whose firmware or driver must be updated. You can select more than one device with similar properties.
3. Click **Make Compliant**.
4. In the **Make Devices Complaint** dialog box, you can do the following:
   - Under **Schedule Update**, click **Additional Information** to view the important information and select one of the following:
     a. **Update Now**: To apply the firmware/driver updates immediately.
     b. **Schedule Later**: Select to specify a date and time when the firmware and/or driver version must be updated. This mode is recommended if you do not want to disturb your current tasks.
   - Under **Server Options** select one of the following reboot options :

a. To reboot the server immediately after the firmware/driver update, choose **Reboot server immediately** and from the dropdown menu select one of the following options:
   i. **Graceful Reboot without Forced Shutdown**
   ii. **Graceful Reboot with Forced Shutdown**
   iii. **PowerCycle** for a hard reset of the device.
b. Select **Stage for next server reboot** to trigger the firmware/driver update when the next server reboot happens.

   NOTE: If the firmware/driver update jobs are created with the 'Stage for next server reboot' option, then the inventory and baseline check must be executed manually after the package is installed in the remote device.

- **Clear Job Queue:** Select to delete all jobs (scheduled, completed, and failed) on the target device, before the update job is initiated.

  NOTE: This function is not supported for updating the drivers.
- **Reset iDRAC:** Select to initiate a reboot of the iDRAC before the update job is initiated.

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

5. Click **Update**.

A firmware/driver update job is created to update the device's firmware and/or driver. You can view the status of the job on the **Monitor** > **Jobs** page.

11

Manage device deployment templates

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

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

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

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

To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. Role and scope based access control in OpenManage Enterprise on page 15.

A device manager can view and perform tasks on the default templates and only the custom templates that are owned by that device manager.

Topics:

Create a deployment template from a reference device

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See Manage Console preferences on page 157 and Generic naming convention for Dell EMC PowerEdge servers on page 177.

You can create or edit a deployment template by using a reference device or by importing from an existing deployment template. To create by using a reference device:

1. From the **OpenManage Enterprise** menu, click **Configuration** > **Templates** > **Create Template**, and then select **From Reference Device**.
2. In the **Create Template** dialog box:
   a. In the **Template Information** section, enter a name for the deployment template and description for the template.
   b. Select the Deployment template type:
      - **Clone Reference Server**: Enables you to clone the configuration of an existing server.
      - **Clone Reference Chassis**: Enables you to clone the configuration of an existing chassis.
      - **Clone Reference IOA**: Enables you to clone the configuration of an existing M I/O aggregator.

        NOTE: The attributes in the IOA template are uneditable. Only the **name** and **description** of an IOA template can be edited.
   c. Click **Next**.
   d. In the **Reference Device** section, click **Select Device** to select the device whose configuration properties must be used for creating the new deployment template. For more information about selecting devices, see Selecting target devices and device groups.

      NOTE: You can select only one device as a reference device.

      NOTE: Only the IOA templates that were extracted at the time of chassis discovery are available for cloning . See Create customized device discovery job protocol for servers –Additional settings for discovery protocols on page 47
   e. In the **Configuration Elements** section, select the check boxes corresponding to the device elements that must be cloned. For creating a deployment template by using server as the device, you can select to clone the server properties such as iDRAC, BIOS, Lifecycle Controller, and Event Filters. By default, all elements are selected.
   f. Click **Finish**.
   After successful creation, the job is displayed in the list. A deployment template creation job is started and the status is displayed in the **STATUS** column.

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

Create a deployment template by importing a template file

NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See Manage Console preferences on page 157 and Generic naming convention for Dell EMC PowerEdge servers on page 177for more information.

1. From the **OpenManage Enterprise** menu, click **Configuration** > **Templates** > **Create Template**, and then select **Import from File**.
2. In the **Import Template** dialog box:
   a. Enter a name for the new deployment template.
   b. Click **Select a File**, and then select a template file.
   c. Select either **Server**, **Chassis**, or **IOA**to indicate the template type.
3. Click **Finish**.
   The properties of an existing template file is imported and a new deployment template is created.

- To view information about a deployment template, select the check box, and then click **View Details** in the right pane. On the **Template Details** page, you can deploy or edit a deployment template. See Deploy device deployment templates on page 85 and Create a deployment template from a reference device on page 81.
- 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**.

1. In the list of deployment templates, select the check box corresponding to the required device template.
2. In the working pane, click **View Details**.
   On the **Template Details** page, the deployment template name, description, the reference device from which the deployment template was created, and the last updated date by the OpenManage Enterprise user information is displayed.
3. Right-click an element to expand all or collapse all the child elements in the **Configuration Details** section to display all the attributes that are used for creating the deployment template. You can also expand individual child elements specific to a parent element. For example, if you selected that iDRAC and BIOS elements must be used for cloning on the target device, attributes related only to such elements are displayed.

Edit a server deployment template

Built-in deployment templates cannot be edited. Only the user-created deployment templates that are identified as 'Custom' can be edited. You can edit the attributes of a deployment template irrespective of whether you created it by using a reference template file or a reference device.

1. On the **Configuration** > **Templates** page, select the required custom template check box, and then click **Edit**.
2. In the **Edit Template** dialog box:
   a. In the **Template Information** section, edit the deployment template name and description. The template type cannot be edited.
   b. Click **Next**.
   c. In the **Edit Components** section, the deployment template attributes are displayed in:
      - The **Guided view** — This view of attributes displays only common attributes, grouped together by function. Attributes from the following categories are shown:
        i. In the **BIOS Settings** section, select any one of the following:
           - **Manually**: Enables you to manually define the following BIOS properties:
             - **System profile**: From the drop-down menu, select to specify the type of performance optimization to be achieved in the system profile.
             - **User accessible USB ports**: From the drop-down menu, select to specify the ports that the user can access.
             - By default, the use of logical processor and in-band manageability are enabled.
           - **Optimize based on workload**: From the Select workload profile drop-down menu, select to specify the type of workload performance optimization you want achieve on the profile.
        ii. Click **Boot** and define the boot mode:
           - If you select BIOS as the boot mode, do the following:
             - To retry the boot sequence, select the **Enabled** check box.
             - Drag the items to set the boot sequence and hard drive sequence.
           - If you select UEFI as the boot mode, drag the items to set the UEFI boot sequence. If required, select the check box to enable the Secureboot feature.
        iii. Click **Networking**. All the networks associated with the deployment template are displayed under **Network Interfaces**.
           - To associate an optional identity pool to the deployment template, select from the **Identity pool** drop-down menu. The networks associated with the selected identity pool is displayed. If the deployment template is edited in the Advanced view, the Identity pool selection is disabled for this deployment template.
             - To view the network properties, expand the network.
             - To edit the properties, click the corresponding pen symbol.
               - Select the protocol to be used for booting. Select only if the protocol is supported by your network.
               - Select the Untagged and Tagged network to be associated to the network
               - The partition, max, and min bandwidth are displayed from the deployment template (profile) we created earlier.
             - Click **Finish**. The network settings of the deployment template is saved.
      - The **Advanced view** — This view lists all the deployment template attributes that can be changed (including those shown in the Guided view). This view allows you to specify not only attribute values (like the Guided view), but also whether or not each attribute gets included when the deployment template is deployed to a target device.

Attributes are grouped together functionally for display. Vendor-specific attributes are grouped under Other Attributes. Each individual attribute is displayed with a check box preceding its name. The check box indicates whether or not the attribute will be included when the deployment template is deployed to a target device. Because of attribute dependencies, if you change the setting for whether or not a particular attribute gets deployed, it could cause unexpected results on the target device, or cause deployment to fail. Each group also has a check box to the left of its name. The icon in group check boxes has one of three values:

i. Checked — Indicates that all of the attributes in the group are selected for deployment.
ii. Hyphen — Indicates some (but not all) of the attributes are selected for deployment.
iii. Clear — Indicates that none of the attributes in the group are selected for deployment

NOTE:

- Using this option requires care and a good knowledge of attributes and attribute dependencies as various attributes depend on the value in another attribute to determine their behavior.
- You can click on the group icons to toggle the deployment setting for all the attributes in the group.
- The attributes with secure information, such as passwords, are hidden and would appear as 'empty' when initially loaded and the changes to these secure attribute values are masked.
- A deployment template's associated Identity pool cannot be changed if a profile is already associated to it.

3. Click **Next**.
   In the **Summary** section, the attributes you edited by using the Guided and Advanced mode are displayed.
4. This section is read-only. Read through the settings and click **Finish**.
   The updated template attributes are saved to the deployment template.

Edit a chassis deployment template

Editing chassis deployment templates is possible with OpenManage Enterprise.

NOTE:

- To edit chassis deployment templates you must have the privileges of an Administrator or a Device Manager. For more details, see Role and scope based access control in OpenManage Enterprise on page 15.
- User passwords can't be set on the MX7000 chassis and the Chassis Management Controller (CMC) deployment templates.

To edit a chassis deployment template:

1. Select **OpenManage Enterprise** > **Configuration** > **Templates** to get the list of deployment templates.
2. Select the check box corresponding to the required chassis template, and click **Edit**. Ensure that the deployment template is identified as "Custom".
3. Edit the **Template Name** and **Description** in the **Template Information** section. You cannot edit the **Template Type**.
4. Click **Next**.
5. In the **Edit Components** section under **Advanced View**, you can select or unselect the attributes to include or exclude in the deployment template.
6. Click **Next** .
7. You can review the changes to the attributes under **Summary**. A circle appears next to the changed attributes.
8. Click **Finish** to save the changes to the chassis deployment template.

Edit IOA deployment template

The attributes in the IOA deployment template are uneditable. Only the **name** and **description** of an IOA deployment template can be edited.

NOTE:

IOA template attributes must not be edited outside of the appliance, as the template will be considered as a corrupt file during deployment.

Edit network properties of a deployment template

On the **Configuration** > **Templates** page, you can edit the network configuration for the deployment templates that contains applicable NIC attributes.

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.

1. Click **IO Pool Assignment** and from the **Identity Pool** list, select an identity pool for the deployment template. Click **Next**.
2. In the **Bandwidth** section, edit the **Minimum Bandwidth (%)** and the **Maximum Bandwidth (%)** of the associated NICs and click **Next**.

   NOTE: Bandwidth settings are only applicable to the partitioned NICs.

3. In the **VLANs** section (applicable only for the modular systems):
   a. Select an appropriate **NIC Teaming** option.
   b. Select the **Propagate VLAN settings immediately** check box, to propagate the changed VLAN settings on the associated modular-system servers immediately without the need for a server reboot. Click **View Details** to view the devices that would be affected.

      NOTE:
      - **Propagate VLAN settings immediately** is implemented only if the deployment template has been already deployed.
      - Before propagating the VLAN settings, ensure that the network profiles are already created for the modular system servers in the fabric.
      - If the **Propagate VLAN settings immediately** check box is selected, then a job named **VLAN Propagation** is created to apply the changes. Status of the job can be checked on the **Monitor** > **Jobs** page.

   c. Select the **Use strict checking** check box to match the VLANs with like characteristics. If unselected, only VLAN name and QoS are used for matching.

      NOTE: This option applies only to the modular-system sleds.

   d. Make changes to the **Untagged Network** and **Tagged Network** attributes of the associated NICs as required.
4. Click **Finish** to apply the changes.

Deploy device deployment templates

You can deploy a deployment template that includes a set of configuration attributes to specific devices. Deploying a device deployment template on the devices ensures that the devices are uniformly configured.

NOTE:
- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- If a device manager is deploying templates, then only the target group(s) and devices that are in that device manager's scope and which are capable of deployment are displayed.

Before you begin deploying a device deployment template, ensure that:
- You have either created a device deployment template or cloned a sample deployment template. See Create a deployment template from a reference device on page 81.
- The target devices meet the requirements that are specified in Minimum system requirements for deploying OpenManage Enterprise on page 20.
- The OpenManage Enterprise Advanced license is installed on the target devices.

CAUTION: Ensure that only the appropriate devices are selected for deployment. After deploying a deployment template on a repurpose and bare-metal device, it might not be possible to revert the device to its original configuration.

NOTE: During deployment of an MX7000 chassis template:

- The target device can only be the lead MX7000 chassis.
- If an MX7000 chassis is removed from group, it has to be rediscovered in OpenManage Enterprise.
- Users on the MX7000 chassis are replaced by the users who are configured in the template.
- Imported Active Directory settings are replaced with the values in chassis profile.

1. From the list of deployment templates on the **Configuration** > **Templates** page, select the check box corresponding to the deployment template you want to deploy, and then click **Deploy Template**.
2. In the **Deploy Template: <template_name>** dialog box, under **Target**:
   a. Click **Select**, and then select device(s) in the **Job Target** dialog box. See Selecting target devices and device groups.
   b. During deployment of the device deployment template, the configuration changes might require a forceful reboot of the server. If you do not wish to reboot the server, select the **Do not forcefully reboot the host OS** option.
   A graceful reboot of the server is attempted when the **Do not forcefully reboot the host OS** option is selected. If the reboot fails, you must rerun the template deployment task.
   c. Select the **Use strict checking** check box to match the VLANs with like characteristics. If unselected, only VLAN name and QoS are used for matching

      NOTE: This option is displayed only if the selected target devices are modular system sleds.

   d. Click **Next**.
3. If the target device is a server, in the **Boot to Network ISO** section:
   a. Select the **Boot to Network ISO** check box.
   b. Select either **CIFS** or **NFS** as the share type, and then enter information in the fields such as ISO image file path and share location where the ISO image file is stored. Use the tool tips to enter the correct syntax.
   c. Select the **Time to Attach ISO** dropdown menu options to set the number of hours the network ISO file will remain mapped to the target device(s). By default, this value is set as four hours.
   d. Click **Next**.
4. In the **iDRAC Management IP** section, change the target device IP settings if required, and then click **Next**.

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

5. In the **Target Attributes** section, the non-virtual identity attributes specific to each of the selected target devices, such as the location attributes and IP address, can be changed before deploying the deployment template. When the template is deployed, these changed target attributes are implemented on only the specific devices. To change the device-specific, non-virtual identity attributes:
   a. Select a target device from the list displaying the previously-selected target devices.
   b. Expand the attribute categories and then select or clear the attributes that must be included or excluded during template deployment on the target device.
   c. Click **Next**.
6. In the **Virtual Identities** section, click **Reserve identities**.
   The assigned virtual identities of the NIC cards of the selected target device are displayed. To view all the assigned identities of the identity pool of the selected target device, click **View all NIC details**.

   NOTE: If identities are already assigned outside of the appliance, then a new deployment will not use those identities unless they are cleared. For more information, see Identity pools on page 90
7. In the **Schedule** section, run the job immediately or schedule for a later time. See Schedule job field definitions on page 172.
8. Click **Finish**. Review the warning message and click **YES**.
   A Device Configuration job is created. See Using jobs for device control on page 122.

Deploy IOA deployment 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 control in OpenManage Enterprise on page 15.

Before you begin deploying an IOA deployment template, ensure that:

- You have created an IOA deployment template for deployment. See Create a deployment template from a reference device on page 81.
- The target devices meet the requirements that are specified in Minimum system requirements for deploying OpenManage Enterprise on page 20.
- Firmware version of the target device is the same as the IOA deployment template.
- Only the following cross template deployments are supported:

Table 14. Supported cross template deployments

IOA Deployment template mode	Supported IOA template modes of target
Standalone	Standalone, PMUX
PMUX (Programmable MUX)	PMUX, Standalone
VLT	VLT

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.

1. From the list of deployment templates on the **Configuration** > **Templates** page, select the check box corresponding to the IOA template you want to deploy, and click **Deploy Template**.
2. In the **Deploy Template: <template_name>** dialog box, under **Target**:
   a. Click **Select**, and then select device(s) in the **Job Target** dialog box. See Selecting target devices and device groups.
   b. 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 encountered. Click **Next**.
5. In the **Schedule** section, run the job immediately or schedule for a later time. See Schedule job field definitions on page 172.
6. Click **Finish**. Review the warning message and click **YES**.
   A Device Configuration job is created under Jobs. See Using jobs for device control on page 122.

Clone deployment templates

1. From the **OpenManage Enterprise** menu, 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 deployment of configuration on yet-to-be-discovered servers or chassis

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** page, click **OpenManage Enterprise** > **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 page 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 page is automatically deleted and moved to the All Device page. Also, a profile is created on the Profiles page which contains the configuration settings of the device.

The following actions can be performed on the Auto Deploy page:

- **Create** templates for auto deployment. See Create auto deployment targets on page 88
- **Delete** templates that are not needed. SeeDelete auto deployment targets on page 89
- **Export** the auto deployment templates to different formats. See Export auto deployment target details to different formats on page 89

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 control in OpenManage Enterprise on page 15.

Create auto deployment targets

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15

To create auto deployment targets :

1. Click **OpenManage Enterprise** > **Configuration** > **Auto Deploy** > **Create**
   The Auto Deploy Template wizard is displayed.
2. On the **Template Information** page, 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** page is displayed.
5. On the **Target Information** page, 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** page, specify a subgroup under the **Static group** if available. For more information about grouping of devices, see Organize devices into groups on page 52. 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** page :
   - 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** page, 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** page.

Delete auto deployment targets

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15

NOTE: If a template that is associated with auto deployment targets is deleted from the **OpenManage Enterprise** > **Configuration** > **Templates** page, the associated auto deploy entries would also get deleted irrespective of their current state.

To remove the auto deployment targets from the **Auto Deploy** list.

1. Go to the Auto Deploy page by clicking **OpenManage Enterprise** > **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 page.

Export auto deployment target details to different formats

1. Go to the Auto Deploy page by clicking **OpenManage Enterprise** > **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.**
A job is created and the auto deploy target data is exported in the selected format.

Overview of stateless deployment

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.

Manage identity pools—Stateless deployment

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 **OpenManage Enteprise** > **Configuration** > **Identity Pools**page 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 on page 15
- 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.

Create Identity Pool - Pool Information

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.

Identity pools

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.

To create a pool of virtual identity types:

1. On the **Configuration** page, 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.

   NOTE: 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.

   NOTE: The WWPN and WWNN addresses are generated by prefixing the provided postfix with 0x2001 and 0x2000 respectively.

The identity pool is created and is listed under the **Identity Pools** tab.

Create Identity Pool - Fibre Channel

You can add Fibre Channel (FC) addresses to the identity pool. The FC comprises 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** page.

Cancel — Closes the **Create Identity Pool** wizard without saving the changes.

Create Identity Pool - iSCSI

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.

Actions

Previous	Displays the **Ethernet** tab.
Next	Displays the **FCoE** tab.
Finish	Saves the changes and displays the **Configuration** page.
Cancel	Closes the **Create Identity Pool** wizard without saving the changes.

Create Identity Pool - Fibre channel over Ethernet

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.

Actions

Previous	Displays the **iSCSI** tab.
Next	Displays the **Fibre Channel** tab.
Finish	Saves the changes and displays the **Identity Pools** page.
Cancel	Closes the **Create Identity Pool** wizard without saving the changes.

Create Identity Pool - Ethernet

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.

Actions

Previous	Displays the **Pool Information** tab.
Next	Displays the **iSCSI** tab.
Finish	Saves the changes and displays the **Identity Pools** page.
Cancel	Closes the **Create Identity Pool** wizard without saving the changes.

View definitions of identity pools

To view the definitions of an identity pool:

1. On the **Configuration** page, 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.

To edit the definitions of an identity pool:

1. On the **Configuration** page, 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**.

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.

To delete an identity pool:

1. On the **Configuration** page, click **Identity Pools**.
2. Select the identity pool, and then click **Delete**.
3. Click **Yes**.

The identity pool is deleted and the reserved identities associated with one or more deployment templates are removed.

Define networks

On the VLANs page, you can enter information of the networks that are currently configured in your environment which the devices can access.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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 MX7000 chassis. For more information about the network types, see Network types on page 95.
4. Click **Finish**.

The network currently configured in your environment is now defined and resources can access the network.

NOTE: Scope-based restrictions don't apply to VLANs as these are common resource pools. Once a VLAN is defined by the administrator, it is available to all the device managers for use.

Network types

NOTE: You can select a network type for MX7000 chassis only.

Table 15. Network types

Network types	Description
General Purpose (Bronze)	Used for low priority data traffic.
General Purpose (Silver)	Used for standard or default priority data traffic
General Purpose (Gold)	Used for high priority data traffic
General Purpose (Platinum)	Used for extremely high priority data traffic
Cluster Interconnect	Used for cluster heartbeat VLANs
Hypervisor Management	Used for hypervisor management connections such as the ESXi management VLAN
Storage - iSCSI	Used for iSCSI VLANs
Storage - FCoE	Used for FCoE VLANs
Storage - Data Replication	Used for VLANs supporting storage data replication such as for VMware Virtual Storage Area Network (VSAN)
VM Migration	Used for VLANs supporting vMotion and similar technologies
VMWare FT Logging	Used for VLANs supporting VMware Fault Tolerance

Edit or delete a configured network

1. Go to the VLANs page 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: VLAN configuration on M1000e and FX2 chassis is not supported in an IPv6 infra, as the IPv6 addressing is not supported by M I/O Aggregator (IOA) and FN I/O modules.

NOTE: The changed VLAN name and IDs are not updated on the target MX7000 chassis after a stateless deployment task is run.

3. To delete the network, select the network and click **Delete**.
4. Click **Yes**.

Export VLAN definitions

The network definitions available in OpenManage Enterprise can downloaded either as a CSV or as a JASON file.

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:

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. Navigate to the file location and select an existing .json or .csv file containing the VLAN definitions, and click **Open**.

   NOTE:
   - Invalid entries or content type in the files are flagged and are not imported.
   - VLAN definitions in the .csv and .json file(s) must be entered in the following formats:

   Table 16. 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

   and

   Table 17. VLAN definition format for JSON files

```
[{"Name":"VLAN1","Description":"VLAN with single ID
","VlanMinimum":1,"VlanMaximum":1,"Type":1},

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

   d. Click **Finish**. A job 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 need to be imported and click **OK**. A job with name **ImportVLANDefinitionsTask** is created to import the networks from the selected chassis.

Upon completion of the job, refresh the **Configuration** > **VLANs** page to view the successfully imported VLAN definitions.

To view the execution details of the job and for status of each network that was imported from the chassis, go to the **Jobs** page by clicking **Monitor** > **Jobs**, select the job, and click **View Details**.

12

Manage 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** page 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 18. Manage Profiles - Field definitions

Field Name	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.

On the right side — Description, Last deployed Time, Last Modified Time, Created On, and Created By are displayed for the selected profile. 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** page as mentioned below:

NOTE: Create and Delete operations are not listed as part of the table.

Table 19. Profile states and possible operations

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

Table 19. Profile states and possible operations (continued)

Profile State	Edit	Assign Target	Unassign Target	Re-Deploy	Migrate
Deployed	Yes	No	Yes	Yes	Yes

- Create profiles and pre-reserve virtual identities. See, Create profiles on page 99
- View profile details. See, View Profile details on page 100
- Edit profile attributes and settings. See, Edit a profile on page 100
- Assign a profile to a device or service tag (through auto-deploy). See, Assign a Profile on page 101
- Unassign a profile from a device or service tag. See, Unassign profiles on page 102
- Redeploy profile changes to the associated target device. See, Redeploy profiles on page 102
- Migrate profile from one target (device or service tag) to another.
- Delete profiles. See, Delete Profiles on page 103
- Export and then download profile(s) data to HTML, CSV or PDF. See, Export Profile(s) data as HTML, CSV, or PDF on page 103

Topics:

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.

NOTE:

- Only users with OpenManage Enterprise Administrator or Device Manager privileges are allowed to perform the Profile Management tasks. See Role and scope based access control in OpenManage Enterprise on page 15.
- Post upgrade to version 3.6.x, any profiles created by the AD/LDAP and OIDC (PingFederate or KeyCloak) device managers from any of the prior OpenManage Enterprise releases are only assigned to the administrator. Hence, the device managers must recreate the profiles post upgrade.

To create a profile from an existing deployment template:

1. Go to the Profiles page 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** page, 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** page, 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**.

Profiles are created based on the deployment template name and the count provided. These profiles are listed on the Profiles page.

View Profile details

To just view the details of an existing profile without editing:

1. Select a profile from the list of profiles on the **Configurations** > **Profiles** page.
2. Click **View** to activate the View Profile Wizard.
3. On the **Details** page of the wizard, Source Template, Name, Description, and Target information are displayed.
4. Click **Next**. On the **Boot to Network ISO** page, the ISO image file path, the share location of the ISO image file, and the Time to Attach ISO value are displayed if the profile was initially set with that preference.

Profiles — view network

To view the network bandwidth and VLAN allocations for the NIC ports associated to a profile:

1. Select a profile on the **Configuration** > **Profiles** page.
2. Click **View** > **View Network** to activate 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**
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** to close the View Network wizard.

Edit a profile

An existing profile can be edited on the **Configurations** > **Profiles** page. 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.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15

To rename, edit network, or edit the attributes of an existing profile, select the profile on the Profiles page and click **Edit**. The following edit options can be selected:

1. Select **Rename** and in the Rename Profile wizard edit the profile name in the **Name** box.
2. Select **Edit Profile** to activate the Edit Profile wizard and edit the following:
   a. On the **Details** page, you can edit the **Name** and **Description**. Click **Next**.
   b. On the Boot to Network ISO page, select the **Boot to Network ISO** check box to specify the full ISO path and the share location 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** page, 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** page, you can select and edit the BIOS, System, NIC, iDRAC, and virtual identity attributes of the profile.
   e. Click **Finish** to save the changes.

Assign a Profile

From the **Configuration** > **Profiles** page, an unassigned profile can be either deployed on an existing server or can be reserved for auto deployment on a yet-to-be discovered server.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- 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.

1. To **Deploy a profile**:
   a. Select an unassigned profile on the **Configuration** > **Profiles** page, click **Assign** > **Deploy** to activate the Deploy Profile wizard.
   b. The **Details** page displays the source template, profile name and description. Click **Next**.
   c. On the **Target** page:
      - Click **Select** and from the list of devices, select a target device.
        NOTE: Devices that are already assigned a profile will be greyed out and not selectable in the target list.
      - If a reboot is required after the deployment, select the **Do not forcefully reboot the host OS if the graceful reboot fails** check box.
      - Click **Next**.
   d. (Optional) On the **Boot to Network ISO** page, select the **Boot to Network ISO** check box and provide the relevant ISO path, share location details, and the Time to Attach ISO value. Click **Next**.
   e. On the **iDRAC Management IP** page, select from one of the following options and provide further relevant details.
      - Don't change IP settings
      - Set as DHCP
      - Set static IP
   f. On the **Target Attributes** page, the attributes are displayed under the BIOS, System, NIC, and iDRAC sections. You can select, unselect, or edit the attributes before deployment.
   g. On the **Virtual Identities** page, 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** page, you can choose **Run Now** to immediately deploy the profile, or choose **Enable Schedule** and select an appropriate Date and Time for the profile deployment.
   i. Click **Finish**.

   NOTE: If identities are already assigned outside of the appliance, then a new deployment will not use those identities unless they are cleared. For more information, see Identity pools on page 90

2. To **Autodeploy a profile**:

   NOTE: For modular devices, the strict checking of the VLAN definitions is enabled by default.

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

Unassign profiles

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

To unassign profiles:

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

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

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

Redeploy profiles

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

To redeploy profile(s):

1. On the **Configuration** > **Profiles** page, select the profile(s) that are 'Deployed' and/or 'Modified' ( ) and click **Re-deploy** .
2. On the Re-deploy wizard's Attribute Deploy Options page choose one of the following attribute deploy options and click **Next**:
   - **Modified attributes only**: To redeploy only the modified attributes on the target device.
   - **All Attributes**: To redeploy all the attributes, along with any modified attributes, on the target device.
3. On the Schedule page, choose from one of the following options:
   - **Run Now** to implement the changes immediately.
   - **Enable Schedule** and select a date and time to schedule the redeployment.
4. Click **Finish** to proceed.

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

Migrate a Profile

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

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

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.
- Migrate profile will move settings defined by the profile (including deployed virtual identities) from source to the target.
- You can force the migration of a profile even if the source device cannot be contacted. In this case, the user must ensure that there are no virtual identity conflicts.
- True target specific attributes are not reclaimed from the 'source' server as part of migration. Due to this, same inventory details can be present on two servers post migration.

To Migrate a profile:

1. On the **Configuration** > **Profiles page**, select a profile and click **Migrate** to activate the Migrate Profile wizard.
2. On the Selection page:
   a. From the **Select source profile** drop down, select the profile that you want to migrate
   b. Click **Select Target** and from the Job target dialog box, select a target device and click **Ok**.

c. If needed, select the 'Force the migration even if the source device cannot be contacted' check box.

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

d. Click **Next**.

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

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

Delete Profiles

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

NOTE:

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

To delete the unassigned profiles:

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

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

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

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

13

Managing the device configuration compliance

By selecting **OpenManage Enterprise** > **Configuration** > **Configuration Compliance**, you can create configuration-compliance baselines by using the built-in or user-created compliance templates. You can create a compliance template from an existing deployment template, reference device, or by importing from a file. To use this feature, you must have the Enterprise level license of OpenManage Enterprise and iDRAC for servers. For Chassis Management Controller, no license is required. User's only with certain privileges are permitted to use this feature. See Role and scope based access control in OpenManage Enterprise on page 15.

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

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

The Overall Compliance Summary report displays the following fields:

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

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

Use the query builder feature to generate device level compliance to the selected baseline. See Select a query criteria on page 55.

OpenManage Enterprise provides a built-in report to view the list of monitored devices and their compliance to the configuration compliance baseline. Select **OpenManage Enterprise** > **Monitor** > **Reports** > **Devices per Template Compliance Baseline**, and then click **Run**. See Run reports on page 133.

Related tasks

Create a configuration compliance baseline on page 107
Edit a configuration compliance baseline on page 108
Remove a configuration compliance baseline on page 110
Manage compliance templates on page 105
Select a query criteria on page 55

Topics:

Manage compliance templates

Use compliance template to create compliance baselines and then periodically check the configuration compliance status of devices that are associated with the baseline. See Managing the device configuration compliance on page 104.

You can create compliance templates by using deployment template, reference device, importing from a file. See Manage compliance templates on page 105.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

- You can create compliance template by:
  - Using a deployment template. See Create a compliance template from deployment template on page 105.
  - Using a reference device. See Create a compliance template from reference device on page 106.
  - Importing from a template file. See Create a compliance template by importing from a file on page 106.
- Edit a compliance template. See Edit a compliance template on page 106.
- Clone a compliance template. See Clone a compliance template on page 106.
- Export report about a compliance template. On the **Compliance Templates** page, select the corresponding check box, and then click **Export**. See Export all or selected data on page 63.
- Delete a compliance template. On the **Compliance Templates** page, select the corresponding check box, and then click **Delete**.

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

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

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

Related information

Managing the device configuration compliance on page 104
Edit a configuration compliance baseline on page 108
Remove a configuration compliance baseline on page 110
Create a compliance template from deployment template on page 105
Edit a compliance template on page 106

Create a compliance template from deployment template

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

Related tasks

Manage compliance templates on page 105
Clone a compliance template on page 106

Create a compliance template from reference device

To use the configuration properties of a device as a template for creating configuration baseline, the device must be already onboarded. See Onboarding devices on page 43.

1. Click **Configuration** > **Configuration Compliance** > **Template Management** > **Create** > **From Reference Device**.
2. In the **Create Compliance Template** dialog box, enter a name and description for the compliance template.
3. Select the options to create the compliance template by cloning properties of either a server or chassis.
4. Click **Next**.
5. In the **Reference Device** section, select the device that must be used as the 'reference' for creating the compliance template. See Select target devices and device groups on page 129.
   a. If you select a server as the reference, select the server configuration properties that must be cloned.
6. Click **Finish**.
   A template creation job is created and run. The newly-created compliance template is listed on the **Compliance Templates** page.

Create a compliance template by importing from a file

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

Clone a compliance template

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

Related information

Create a compliance template from deployment template on page 105
Edit a compliance template on page 106

Edit a compliance template

The compliance templates can be edited on the **Configuration Compliance** > **Compliance Templates** page.

NOTE:

- Editing a compliance template that is already associated with other baseline(s), will automatically trigger a configuration compliance for all devices across all the baselines that use the template.
- Editing a compliance template that is linked to multiple baselines having large number of devices may result in a session timeout as the configuration compliance check for all the associated devices may take several minutes. A session timeout does not indicate that the changes made to the compliance template had any issue.
- When editing a compliance template on large-scale systems consisting of 1,000 or configuration inventory of a maximum of 6,000 managed devices, ensure that there are no other configuration inventory or compliance operations running at

the same time. Additionally, **disable** the default system generated Configuration Inventory job on the **Monitor** > **Jobs** page (set source to System generated).

- It is recommended that you associate a maximum of 1500 devices per baseline for optimal performance.
- If there is a use case of frequent template edits, it is recommended that you associate a maximum of 100 devices per baseline for optimal performance.

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

Related tasks

Manage compliance templates on page 105
Clone a compliance template on page 106

Create a configuration compliance baseline

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

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

The list of compliance baselines available to you depends on your role and scope based access privileges in OpenManage Enteprise. For example, an administrator can view and manage all the compliance baselines, however, a device manager can only view and manage the compliance baselines created and owned by that device manager. Also, the target devices available to the device managers are restricted by the devices / device groups that are in their respective scope.

You can create a configuration compliance baseline by:

- Using an existing deployment template. See Managing the device configuration compliance on page 104.
- Using a template captured from a support device. See Create a compliance template from reference device on page 106.
- Using a template imported from a file. See Create a compliance template by importing from a file on page 106.

When you select a template for creating a baseline, the attributes associated with the templates are also selected. However, you can edit the baseline properties. See Edit a configuration compliance baseline on page 108.

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

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

1. Select **Configuration** > **Configuration Compliance** > **Create Baseline**.
2. In the **Create Compliance Baseline** dialog box:
   - In the **Baseline Information** section:
   a. From the **Template** drop-down menu, select a compliance template. For more information about templates, see Managing the device configuration compliance on page 104.
   b. Enter a compliance baseline name and description.
   c. Click **Next**.
   - In the **Target** section:
   a. Select devices or device groups. Only compatible devices are displayed. See Select target devices and device groups on page 129.

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

3. Click **Finish**.
   A compliance baseline is created and listed. A compliance comparison is initiated when the baseline is created or updated. The overall compliance level of the baseline is indicated in the **COMPLIANCE** column. For information about the fields in the list, see Managing the device configuration compliance on page 104.

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

Related information

Managing the device configuration compliance on page 104
Remove a configuration compliance baseline on page 110

Edit a configuration compliance baseline

You can edit the devices, name, and other properties associated with a configuration baseline. For field descriptions displayed in the list, see Managing the device configuration compliance on page 104.

CAUTION: If a compliance template used for a baseline is already associated with another baseline, editing the template properties changes the baseline compliance levels of devices already associated. See Edit a compliance template on page 106. 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.

1. Select **Configuration** > **Configuration Compliance**.
2. From the list of configuration compliance baselines, select the corresponding check box, and then click **Edit**.
3. In the **Edit Compliance Baseline** dialog box, update the information. See Create a configuration compliance baseline on page 107.

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

Related tasks

Manage compliance templates on page 105
Select a query criteria on page 55

Related information

Managing the device configuration compliance on page 104
Remove a configuration compliance baseline on page 110

Delete configuration compliance baselines

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15

To delete the configuration compliance baselines:

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

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

Refresh compliance of the configuration compliance baselines

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

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

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

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

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

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

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

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

Remediate noncompliant devices

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

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

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

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

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

To remediate one or more noncompliant devices:

1. Select **Configuration** > **Configuration Compliance**.
2. From the list of configuration compliance baselines, select the corresponding check box, and then click **View Report**.
3. From the list of noncompliant devices, select one or more devices, and then click **Make Compliant**.
4. Schedule the configuration changes to run immediately or later, and then click **Finish**.

   To apply the configuration changes after the next server reboot, you can select the **Stage configuration changes to device(s) on next reboot** option.

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

Export the Compliance Baseline report

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

On Compliance Report page of a configuration baseline

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

Remove a configuration compliance baseline

You can remove the configuration compliance level of devices associated with a configuration baseline. For field descriptions displayed in the list, see Managing the device configuration compliance on page 104.

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.

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

Related tasks

Create a configuration compliance baseline on page 107
Select a query criteria on page 55
Manage compliance templates on page 105
Edit a configuration compliance baseline on page 108

Related information

Managing the device configuration compliance on page 104

14

Monitor and Manage device alerts

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

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

NOTE:

- To manage and monitor device alerts on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- Alert policies and alert logs are governed by the scope based access that you have in OpenManage Enterprise. For example, an administrator can view and manage all the alert policies, however, device managers can only view and manage the default alert policies and the policies that they create and own. Also, the device managers can only view the alerts for the devices that are in their scope.
- Currently, only the SNMPv1 and SNMPv2 alerts are received by OpenManage Enterprise from the following PowerEdge servers— MX840c and MX5016s.
- OpenManage Enterprise provides a built-in report to view the list of devices monitored by OpenManage Enterprise and the alerts generated for each device. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Alert Counts per Device Report**. Click **Run**. See Run reports on page 133

Related concepts

View alert logs on page 111

Topics:

View alert logs

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

By default, only the unacknowledged alerts are displayed. You can customize the list of the alerts using either the **Advanced Filters**, located on the top left hand side of the alert list, or by changing the **Alert Display Settings** in the **Application Settings** page. See Customize the alert display on page 158. You can view the alerts details as follows:

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

  NOTE: Alerts cannot be filtered based on the IP address (source name) if the alert is generated from an undiscovered device or in case of an internal alert.
- **Category**: The category indicates the type of alert. For example, system health and audit.
- **Message ID**: The ID of the generated alert.
- **Message**: The generated alert.

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

NOTE: OpenManage Enterprise version 3.2 and above tracks the **Last Updated By** data point, however, in the previous versions this was not tracked. Therefore, be aware that if the Alert log is refined using the **User** advanced filter field, the acknowledged alerts from the previous versions will not be displayed.

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

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

Related information

Monitor and Manage device alerts on page 111

Manage alert logs

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

Acknowledge alerts

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

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

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

Unacknowledge alerts

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

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

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

Ignore alerts

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

Export alerts

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

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

Delete alerts

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

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

View archived alerts

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

Table 20. Alert purging

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

Download archived alerts

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

1. Click **Archived Alerts**.

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

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

NOTE: To download archived alerts, you must have necessary privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

Alert policies

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

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

Use alert policies to perform the following functions:

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

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

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

Related tasks

Configure and manage alert policies on page 114

Configure and manage alert policies

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

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

Related information

Alert policies on page 113
Forward audit logs to remote Syslog servers on page 115

Create an alert policy

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

NOTE: Post upgrade to version 3.6.x, any alert policy created by device managers from any of the prior OpenManage Enterprise releases are assigned only to the administrator. Hence, the device managers must recreate the alert policies post upgrade to continue receiving alerts.

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

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

   You can expand each category to view and select the sub categories. To know more about categories and subcategories, see Alert definitions on page 118.
3. Select the devices or groups for which an alert is required and click **Next**. An alert can be applied for:
   - A device or devices.
   - A group or groups of devices.
   - A specified undiscovered device by entering its IP address or hostname.
   - Any undiscovered device.

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

     NOTE: Alerts of SNMPv1, SNMPv2, and SNMPv3 protocols sent by such undiscovered (foreign) devices are recognized by OpenManage Enterprise.
4. (Optional) Specify the duration for when the alert policy is applicable by selecting the required values for **Date Range**, **Time Interval** and **Days**, and then click **Next**.
5. Select the severity of the alert and click **Next**.

   To select all the severity categories, select the **All** check box.
6. Select one or more alert actions and click **Next**. The available options are:
   - Email—Select Email to send an email to a designated recipient by specifying information for each field and use tokens if required for the subject and message. See Token substitution in remote scripts and alert policy on page 174

NOTE: Emails for multiple alerts of the same category, message ID and content are triggered only once every 2 minutes to avoid repeated or redundant alert messages in the inbox.

- SNMP Trap Forwarding (Enable)—Click Enable to view the SNMP Configuration window where you can configure the SNMP settings for the alert. See Configure SMTP, SNMP, and Syslog alerts on page 116.
- Syslog (Enable)—Click Enable to view the Syslog Configuration window where you can configure the system log settings for the alert. See Configure SMTP, SNMP, and Syslog alerts on page 116.
- Select the Ignore check box to ignore the alert message and not activate the alert policy.
- Send an SMS to specified phone number.
- Power Control—Select Power Control check box to view the actions where you can turn on, turn off, power cycle, or gracefully shutdown a device. To shut down an operating system before performing power control actions, select the **Shut down OS First** check box.
- Remote Script Execution (Enable)—Click Enable to view the Remote Command Setting window where you can add and run remote commands on remote nodes. For more information about adding remote commands, see Execute remote commands and scripts on page 117.

  From the drop-down menu, select the script that you want to run when this alert policy is run. You can set up running the remote command also as described in Managing OpenManage Enterprise appliance settings on page 140.

- Send a notification to the mobile phone registered with OpenManage Enterprise. See OpenManage Mobile settings on page 167.

7. Review the details of the created alert policy in the Summary tab and click **Finish**.
   The alert policy is successfully created and listed in the **Alert Policies** section.

Manage alert policies

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

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

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

- **Edit an alert policy**: Select an alert policy and click **Edit** to edit the required information in the Configure and manage alert policies on page 114 dialog box.

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

  NOTE: The Time Interval check box is disabled by default for alert policies on OpenManage Enterprise versions before version 3.3.1. After upgrading, enable the Time Interval and update the fields to reactivate the policies.
- **Enable alert policies**: Select the alert policy and click **Enable**. A check mark appears under the **Enabled** column when an alert policy is enabled. The **Enable** button of an alert policy that is already enabled appears grayed-out.
- **Disable alert policies**: Select the alert policy and click **Disable**. The alert policy is disabled and the tick mark in the **ENABLED** column is removed.

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

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

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

Forward audit logs to remote Syslog servers

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

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

1. Select **Alerts** > **Alert Policies** > **Create**.
2. In the **Create Alert Policy** dialog box, in the **Name and Description** section, enter a name and description of the alert policy.

a. The **Enable Policy** check box is selected by default to indicate that the alert policy will be enabled once it is created. To disable the alert policy, clear the check box. For more information about enabling alert policies at a later time, see Configure and manage alert policies on page 114.
b. Click **Next**.

3. In the **Category** section, expand **Application** and select the categories and subcategories of the appliance logs. Click **Next**.
4. In the **Target** section, the **Select Devices** option is selected by default. Click **Select Devices** and select devices from the left pane. Click **Next**.

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

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

   If Syslog servers are not configured in OpenManage Enterprise, click **Enable** and enter the destination IP address or the hostname of Syslog servers. For more information about configuring Syslog servers, see Configure SMTP, SNMP, and Syslog alerts on page 116.
8. Click **Next**.
9. In the **Summary** section, details of the alert policy you defined are displayed. Carefully read through the information.
10. Click **Finish**.

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

Related tasks

Configure and manage alert policies on page 114
Monitor audit logs on page 120

Configure SMTP, SNMP, and Syslog alerts

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

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

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

To configure the SNMP alert forwarding configuration:

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

   NOTE: Entering of the console IP is disallowed to avoid duplication of alerts.
4. From the **SNMP VERSION** menu select the SNMP version type as SNMPv1, SNMPv2, or SNMPv3 and fill the following fields:
   a. In the COMMUNITY STRING box, enter the SNMP community string of the device that must receive the alert.
   b. Edit the PORT NUMBER if needed. Default port number for SNMP traps=162. See Supported protocols and ports in OpenManage Enterprise on page 30.

c. If SNMPv3 is selected, provide the following additional details:
   i. USERNAME: Provide a username.
   ii. AUTHENTICATION TYPE : From the drop down list select SHA, MD_5, or None.
   iii. AUTHENTICATION PASSPHRASE: Provide an authentication passphrase having a minimum of eight characters.
   iv. PRIVACY TYPE: From the drop down list select DES, AES_128, or None.
   v. PRIVACY PASSPHRASE: Provide a privacy passphrase containing a minimum of eight characters.
5. To test an SNMP message, click the **Send** button of the corresponding trap.
6. Click **Apply**. To reset the settings to default attributes, click **Discard**.

To update the Syslog forwarding configuration:
1. Expand **Syslog Forwarding Configuration**.
2. Select the check box to enable the Syslog feature on the respective server in the **SERVER** column.
3. In the **DESTINATION ADDRESS/HOST NAME** box, enter the IP address of the device that receives the Syslog messages.
4. Default port number by using UDP=514. Edit if necessary by entering or selecting from the box. See Supported protocols and ports in OpenManage Enterprise on page 30.
5. Click **Apply**.
6. To reset the settings to default attributes, click **Discard**.

Execute remote commands and scripts

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 **'**.

1. Click **Application Settings** > **Script Execution**.
2. In the **Remote Command Setting** section, do the following:
   a. To add a remote command, click **Create**.
   b. In the **Command Name** box, enter the command name.
   c. Select any one of the following command type:
      i. Script
      ii. RACADM
      iii. IPMI Tool
   d. If you select **Script**, do the following:
      i. In the **IP Address** box, enter the IP address.
      ii. Select the authentication method: **Password** or **SSH Key**.
      iii. Enter the **user name** and **password** or the **SSH Key**.
      iv. In the **Command** box, type the commands.
         - Up to 100 commands can be typed with each command required to be on a new line.
         - Token substitution in scripts is possible. See Token substitution in remote scripts and alert policy on page 174
      v. Click **Finish**.
   e. If you select **RACADM**, do the following:
      i. In the **Command Name** box, enter the command name.
      ii. In the **Command** box, type the commands. Up to 100 commands can be typed with each command required to be on a new line.
      iii. Click **Finish**
   f. If you select **IPMI Tool**, do the following:
      i. In the **Command Name** box, enter the command name.
      ii. In the **Command** box, type the commands. Up to 100 commands can be typed with each command required to be on a new line.
      iii. Click **Finish**
3. To edit a remote command setting, select the command, and then click **Edit**.
4. To delete a remote command setting, select the command, and then click **Delete**.

Automatic refresh of MX7000 chassis on insertion and removal sleds

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

When a standalone or a lead MX7000 chassis is discovered or onboarded by using OpenManage Enterprise (versions 3.4 and later), an alert policy is created simultaneously on the the MX7000 chassis. For more information on discovering and onboarding devices in OpenManage Enterprise, see Create a device discovery job on page 42 and Onboarding devices on page 43.

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

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

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

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

NOTE:

- The alert policy on MX7000 is only specific to the sleds and are not applicable to the other components of the chassis, such as the IOMs.
- MX7000 alert preferences can be set in OpenManage Enterprise to either receive all the alerts or only the chassis-category alerts from the MX7000 chassis. For more information, see Manage Console preferences on page 157.
- Some delay is to be expected between the actual action on the sleds and the triggering of the chassis inventory refreshing on OpenManage Enterprise.
- The automatically created alert policy is deleted if the MX7000 chassis is deleted from the device inventory of OpenManage Enterprise.
- The All Devices page will list the **Managed State** for a successfully onboarded MX7000 chassis with automatic alert forwarding policy as 'Managed with Alerts'. For more information on onboarding, refer Onboarding devices on page 43

Alert definitions

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

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

An Error and Event message has:

- **MESSAGE ID**: Messages are classified based on components such as BIOS, power source (PSU), storage (STR), log data (LOG), and Chassis Management Controller (CMC).
- **MESSAGE**: The actual cause of an event. Events are triggered for information purpose only, or when there is an error in performing tasks.
- **CATEGORY**: Class to which the error message belongs to. For information about categories, see the *Event and Error Message Reference Guide for Dell EMC PowerEdge Servers* available on the support site.
- **Recommended Action**: Resolution to the error by using GUI, RACADM, or WS-Man commands. Where necessary, you are recommended to refer to documents on the support site or TechCenter for more information.
- **Detailed Description**: More information about an issue for easy and fast resolution.

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

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

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

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

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

15

Monitor audit logs

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

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

The audit log files can be exported to the CSV file format. See Export all or selected data on page 63.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.
- Scope-based restrictions are not applicable to the Audit logs.

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** respectively. For more information about exporting the audit logs, see Export all or selected data on page 63.
7. To export the console logs as a .ZIP file, click **Export** > **Export Console Logs**.

NOTE:

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

Related information

Forward audit logs to remote Syslog servers on page 115

Topics:

- Forward audit logs to remote Syslog servers

Forward audit logs to remote Syslog servers

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

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

1. Select **Alerts** > **Alert Policies** > **Create**.
2. In the **Create Alert Policy** dialog box, in the **Name and Description** section, enter a name and description of the alert policy.
   a. The **Enable Policy** check box is selected by default to indicate that the alert policy will be enabled once it is created. To disable the alert policy, clear the check box. For more information about enabling alert policies at a later time, see Configure and manage alert policies on page 114.
   b. Click **Next**.
3. In the **Category** section, expand **Application** and select the categories and subcategories of the appliance logs. Click **Next**.
4. In the **Target** section, the **Select Devices** option is selected by default. Click **Select Devices** and select devices from the left pane. Click **Next**.

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

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

   If Syslog servers are not configured in OpenManage Enterprise, click **Enable** and enter the destination IP address or the hostname of Syslog servers. For more information about configuring Syslog servers, see Configure SMTP, SNMP, and Syslog alerts on page 116.
8. Click **Next**.
9. In the **Summary** section, details of the alert policy you defined are displayed. Carefully read through the information.
10. Click **Finish**.

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

Related tasks

Configure and manage alert policies on page 114
Monitor audit logs on page 120

16

Using jobs for device control

A job is a set of instructions for performing a task on one or more devices. The jobs include discovery, firmware update, inventory refresh for devices, warranty, and so on. You can view the status and details of jobs that are initiated in the devices and its components, on the **Jobs** page. OpenManage Enterprise has many internal maintenance jobs which are triggered on a set schedule automatically by the appliance. For more information on the 'default' jobs and their schedule, see OpenManage Enterprise default jobs and schedule on page 124.

Prerequisites:

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

- You must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15
- Each job type is limited to devices that you must have:
  - permissions to access.
  - ability to complete the required action.

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

- View list of jobs currently running, failed, and successfully completed.
- Create jobs to blink device LEDs, control the device power, and run remote command on devices. See Create a Remote command job for managing devices on page 128, Creating jobs for managing power devices, and Creating job to blink device LEDs. You can perform similar actions on a server on the device details page. See View and configure individual devices on page 64.
- Manage jobs such as run, stop, enable, disable or delete jobs.

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

Topics:

View job lists

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

- **Job Status**: Provides the execution status of a job.

  See Jobs status and Jobs type description on page 123.

- **State**: Provides the state of a job. The available options are Enabled or Disabled.
- **Job Name**: Name of a job.
- **Job Type**: Provides the type of a job.

  See Jobs status and Jobs type description on page 123.

- **Description**: Detail description of a job.
- **Last Run**: Last run period of a job.

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

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

To view more information about a job, select a job and click **View Details** in the right pane. See View an individual job information on page 127.

OpenManage Enterprise provides a built-in report to view the list of scheduled jobs. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Scheduled Jobs Report**. Click **Run**. See Run reports on page 133.

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

Jobs status and Jobs type description

Table 21. Job status and description

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

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

Table 22. Job Types and description

Job Type	Description
Health	Checks the health status of the devices. See Device health statuses on page 38.
Inventory	Creates inventory report of the devices. See Managing device inventory on page 69.
Device Config	Creates device configuration compliance baseline. See Managing the device configuration compliance on page 104.
Report_Task	Creates reports about devices by using built-in or customized data fields. See Reports on page 132.
Warranty	Generate data about devices' warranty status. See Manage the device warranty on page 130.
Onboarding_Task	Onboards the discovered devices. See Onboarding devices on page 43.
Discovery	Discovers devices. See Discovering devices for monitoring or management on page 39.
Console Update Execution Task	Console Upgrade Job is being tracked using this task, This task helps to identify if the upgrade is completed or failed

Table 22. Job Types and description (continued)

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

OpenManage Enterprise default jobs and schedule

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

Table 23. The following table lists the OpenManage Enterprise Default job names and their schedule.

Job Name	Cron Expression	Cron Expression Description	Example
Configuration Inventory	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• 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	0 0 5 * * ? *	At 05:00:00am every day	• Tue May 18 05:00:00 UTC 2021

Table 23. The following table lists the OpenManage Enterprise Default job names and their schedule. (continued)

Job Name	Cron Expression	Cron Expression Description	Example
			• 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 1st, 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 1st, 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	0 0 0/1 1/1 * ? *	At second :00, at minute :00, every hour starting at 00am, every day starting on the 1st, every month	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021
Internal Sync Task	0 0/5 * 1/1 * ? *	At second :00, every 5 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 18:45:00 UTC 2021 • Mon May 17 18:50:00 UTC 2021
Metrics Purge Task	0 0 * ? * *	At second :00 of minute :00 of every hour	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 21:00:00 UTC 2021
Metrics Task	0 0/15 * 1/1 * ? *	At second :00, every 15 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 18:45:00 UTC 2021 • Mon May 17 19:00:00 UTC 2021
Mobile Subscription Task	0 0/2 * 1/1 * ? *	At second :00, every 2 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 18:54:00 UTC 2021 • Mon May 17 18:56:00 UTC 2021
Node Initiated Discovery Task	0 0/10 * 1/1 * ? *	At second :00, every 10 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 19:10:00 UTC 2021
Password Rotation Task	0 0 0/6 1/1 * ? *	At second :00, at minute :00, every 6 hours starting at 00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 06:00:00 UTC 2021 • Tue May 18 12:00:00 UTC 2021

Table 23. The following table lists the OpenManage Enterprise Default job names and their schedule. (continued)

Job Name	Cron Expression	Cron Expression Description	Example
Periodic Metrics Registration	0 0 3 * * ?	At 03:00:00am every day	• Tue May 18 03:00:00 UTC 2021 • Wed May 19 03:00:00 UTC 2021
Purge On Demand Health Task for Table: Task	0 0 0/5 1/1 * ? *	At second :00, at minute :00, every 5 hours starting at 00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 05:00:00 UTC 2021 • Tue May 18 10:00:00 UTC 2021
Purge Task Table :Event_Archive	0 0 18/12 ? * * *	At second :00, at minute :00, every 12 hours starting at 18pm, of every day	• Tue May 18 18:00:00 UTC 2021 • Wed May 19 18:00:00 UTC 2021 • Thu May 20 18:00:00 UTC 2021
Purge Task Table :Group_Audit	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
Purge Task Table :Task	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
Purge Task Table :announced_target	0 0 0 1/1 * ? *	At 00:00:00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
Purge Task for Table: Core Application Log	0 0 0/5 1/1 * ? *	At second :00, at minute :00, every 5 hours starting at 00am, every day starting on the 1st, every month	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 05:00:00 UTC 2021
Purge Task for Table: Event	0 0/30 * 1/1 * ? *	At second :00, every 30 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 19:30:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 20:30:00 UTC 2021
Purge Task for Table: Infrastructure Device	0 0/30 * 1/1 * ? *	At second :00, every 30 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 19:30:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 20:30:00 UTC 2021

Table 23. The following table lists the OpenManage Enterprise Default job names and their schedule. (continued)

Job Name	Cron Expression	Cron Expression Description	Example
Subscription poller task	0 0/30 * 1/1 * ? *	At second :00, every 30 minutes starting at minute :00, every hour, every day starting on the 1st, every month	• Mon May 17 19:30:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 20:30:00 UTC 2021

View an individual job information

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

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

   NOTE: If a configuration remediation task is stopped, the overall task status is indicated as 'Stopped', but the task continues to run. However, the status is indicating as Running in the **Execution History** section.
4. To export data to an Excel file, select the corresponding or all check boxes, and then click **Export**. See Export all or selected data on page 63.

Create a job to turn device LEDs

The following steps describe how you can blink the LEDs of the specified devices using the Blink Devices Wizard.

To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15

1. The Blink Devices wizard can be activate in the following ways:
   a. From the Jobs page (**OpenManage Enterprise** > **Monitor** > **Jobs**) click **Create**, and then select **Blink Devices**.
   b. From the All Devices page (**OpenManage Enterprise** > **Devices**), select the devices and click the **More Actions** drop down and then either click **Turn LED On** or **Turn LED Off**.
2. In the **Blink Devices Wizard** dialog box:
   a. In the **Options** section:
      i. In the **Job Name** box, enter a job name.
      ii. From the **Blink LED Duration** drop-down menu, select options to blink the LED for a set duration, turn on, or to turn off.
      iii. Click **Next**.
   b. In the **Target** section, select the target devices or target groups and click **Next**. See Select target devices and device groups on page 129.
   c. In the **Schedule** drop down select **Run Now**, or **Run Later**, or **Run on Schedule**. See Schedule job field definitions on page 172.
3. Click **Finish**.
   A Blink LED job is created and listed in the Jobs page (**OpenManage Enterprise** > **Monitor** > **Jobs**) **JOB STATUS** column.

Create a job for managing power devices

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

1. Click **Create**, and then select **Power Control Devices**.
2. In the **Power Control Devices Wizard** dialog box:
   a. In the **Options** section:
      i. Enter the job name in **Job Name**.
      ii. From the **Power Options** drop-down menu, select any one of the tasks: **Power on**, **Power off**, or **Power cycle**.
      iii. Click **Next**.
   b. In the **Target** section, select the target devices and click **Next**. See Select target devices and device groups on page 129.
   c. In the **Schedule** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions on page 172.
3. Click **Finish**.
   The job is created and listed in the Jobs list and identified by an appropriate status in the **JOB STATUS** column.
4. If the job is scheduled for a later point of time, but you want to run the job immediately:
   - On the Jobs page, select the check box corresponding to the Scheduled job.
   - Click **Run Now**. The job is run and the status is updated.
   - To view the job data, click **View Details** in the right pane. See View an individual job information on page 127.

Create a Remote command job for managing devices

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

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

      NOTE: The commands in the Arguments box are run one at a time.

   d. Click **Next**.
      A green tick mark next to **Options** indicates that the necessary data is provided.
3. In the **Target** section, select the target devices and click **Next**. See Select target devices and device groups on page 129.
4. In the **Schedule** section, run the job immediately or schedule for a later time. See Schedule job field definitions on page 172.
5. Click **Finish**.
   The job is created and listed in the Jobs list and identified by an appropriate status in the **JOB STATUS** column.
6. If the job is scheduled for a later point, but you want to run the job immediately:
   - On the Jobs page, select the check box corresponding to the Scheduled job.
   - Click **Run Now**. The job is run and the status is updated.
   - To view the job data, click **View Details** in the right pane. See View an individual job information on page 127.

Create a job to change the virtual console plugin type

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

1. Click **OpenManage Enterprise** > **Monitor** > **Jobs**
2. Click **Create**, and then select **Change Virtual Console Plugin on Devices**.
3. In the **Change Virtual Console Plugin Wizard** dialog box, in the **Options** section:
   a. Enter the job name in **Job Name**. By default, the plugin type is displayed as HTML5.
   b. Click **Next**.

4. In the **Job Target** section, select the target devices and click **Next**. See Select target devices and device groups on page 129.
   a. Click **Next**.
5. In the **Schedule** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions on page 172.
6. Click **Finish**.
   The job is created and listed in the Jobs list and identified by an appropriate status in the **JOB STATUS** column.
7. If the job is scheduled for a later point of time, but you want to run the job immediately:
   - On the Jobs page, select the check box corresponding to the Scheduled job.
   - Click **Run Now**. The job is run and the status is updated.
   - To view the job data, click **View Details** in the right pane. See View an individual job information on page 127.

Select target devices and device groups

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

NOTE: The device groups and devices displayed are governed by the scope-based operational access that the user has to the devices. For more information, see Role and scope based access control in OpenManage Enterprise on page 15.

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 page - devices list on page 58. For information about device groups, see Organize devices into groups on page 52.
2. Select the check box corresponding to a device and click **OK**.
   The selected devices are displayed in the **All Selected Devices** section of the selected group.

Manage jobs

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

- **Run jobs**: Select the check box corresponding to a job, and then click **Run Now** to execute the task on the targeted devices. You can run a job when it is in enabled status.
- **Enable jobs**: Select the check box corresponding to a job, and then click **Enable**.
- **Disable jobs**: Select the check box corresponding to a job, and then click **Disable**.
  NOTE: Only the 'Scheduled' jobs can be disabled from running. Jobs which are active and in their 'Running' state cannot be disabled midway.
- **Stop jobs**: Select the check box corresponding to a job, and then click **Stop**. You can stop a job when it is in running status.
- **Delete**: Select the check box corresponding to a job, and then click **Delete**.

17

Manage the device warranty

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

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

- **STATUS** of the warranty
  NOTE: Warranty status is determined by the settings that the Administrator selects. See Manage warranty settings on page 160
  -  means **critical**, indicating the warranty has expired.
  -  means **warning**, indicating the warranty is approaching expiration.
  -  means **normal**, indicating the warranty is active.
- **SERVICE TAG**
- **DEVICE MODEL**
- **DEVICE TYPE**
- **WARRANTY TYPE**:
  - Initial: The warranty provided with the purchase of OpenManage Enterprise.
  - Extended: The warranty is extended because the initial warranty duration is expired.
- **SERVICE LEVEL DESCRIPTION**: Indicates the Service Level Agreement (SLA) associated with the device warranty.
- **DAYS REMAINING**: Number of days left for the warranty to expire. You can set the days before which you get an alert. See Manage warranty settings on page 160.

OpenManage Enterprise provides a built-in report about the warranties that expire in the next 30 days. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **Warranties Expiring in Next 30 days**. Click **Run**. See Run reports on page 133.

To filter data displayed in the table, click **Advanced Filters**. See about advanced filters section in OpenManage Enterprise Graphical User Interface overview on page 34.

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

To export all or selected warranty data, click **Export**. See Export all or selected data on page 63.

Related tasks

View and renew device warranty on page 130

Topics:

View and renew device warranty

Click **OpenManage Enterprise** > **Monitor** > **Warranty** to get a list of warranty statuses of all the devices monitored by OpenManage Enterprise, along with their Service Tag, model name, device type, associated warranty, and service level information. For field descriptions, see Manage the device warranty on page 130.

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

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

Related information

Manage the device warranty on page 130

18

Reports

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

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

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

Advantages of the Reports feature:

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

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

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

Related tasks

Run reports on page 133
Run and email reports on page 133
Edit reports on page 134
Delete reports on page 134

Topics:

Run reports

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

When you run a report, the first 20 rows are displayed and paginated results can be paged through. To view all the rows at one time, download the report. To edit this value, see Export all or selected data on page 63. Data displayed in the output cannot be sorted because it is defined in the query used to build a report. To sort data, edit the report query or export it to an Excel sheet. It is recommended to not run more than five (5) reports at a time because reporting consumes system resources. However, this value of five reports depends on the devices discovered, fields used, and number of tables joined to generate report. A Reports job is created and run when a report generation is requested. For role-based privileges to generate reports, see Creating reports on page 134.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.
- Reports generated by device managers will only have data pertaining to the devices that are in their scope.
- It is not recommended to frequently run a report because it consumes processing and data resources.
- For a report whose category is 'Device', the first columns by default are Device name, Device model, and Device Service Tag. You may exclude columns while customizing your report.

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

To download a report:

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

To email a report:

1. Click **Email**.
2. In the **Email Report** dialog box, select the file format, type the receiver's email address, and then click **Finish**. The report is emailed. You can email reports to 20-30 recipients at a time.
3. If the email address is not configured, click **Go to SMTP Settings**. For more information about setting SMTP properties, see Set SNMP Credentials on page 160.

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

Related information

Reports on page 132

Run and email reports

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

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

1. Select the report and click **Run and Email**.
2. In the **Email Report** dialog box:
   a. From the **Format** drop-down menu, select one of the file format in which the report must be generated — HTML, CSV, PDF, or MS-Excel.
   b. In the **To** box, enter the email address of the recipient. If the email address is not configured, click **Go to SMTP Settings**. For more information about setting SMTP properties, see Set SNMP Credentials on page 160.
   c. Click **Finish**.
   The report is emailed and recorded in the Audit logs.

Related information

Reports on page 132

Edit reports

Only user-created reports can be edited.

1. Select the report and click **Edit**.
2. In the **Report Definition** dialog box, edit the settings. See Creating reports.
3. Click **Save**.
   The updated information is saved. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

   NOTE: While editing a customized-report, if the category is changed, the associated fields are also removed.

Related information

Reports on page 132

Copy reports

Only user-created reports can be copied.

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

Delete reports

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.

1. From the **OpenManage Enterprise** menu, under **Monitor**, select **Reports**.
   A list of devices available reports is displayed.
2. Select the report, click **More Actions**, and then click **Delete**.

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

3. In the **Delete Report Definition** dialog box, when prompted whether or not the report must be deleted, click **Yes**.
   The report is deleted from the list of reports and the table is updated. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Related information

Reports on page 132

Creating 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 control in OpenManage Enterprise on page 15.
- The reports generated by device managers will only have data pertaining to the device groups which are in their scope.
- Some tables contain device-type-specific data which will effectively lock the report to that device type. Mixing columns from multiple device specific tables of different types (for example servers and chassis) will result in an invalid report with no results.

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

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

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

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

Table 25. The role-based access privileges for generating reports on OpenManage Enterprise

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

1. Click **Reports** > **Create**.
2. In the **Report Definition** dialog box:
   a. Type the name and description of the new report to be defined.
   b. Click **Next**.
3. In the **Report Builder** section:
   a. From the **Category** drop-down menu, select the report category.
      - If you select Device as the category, select the device group also.
      - If necessary, edit the filter criteria. See Select a query criteria on page 55.
   b. Under the **Select Columns** section, select the check boxes of the fields that must appear as the report columns. Selected field names are displayed in the **Column Order** section.
   c. You can customize the report by
      - Using the **Sort by** and **Direction** boxes.
      - Dragging the fields either up or down in the **Column Order** section.
4. Click **Finish**.
   The report is generated and listed in the list of reports. You can export report for analytical purposes. See Export all or selected data on page 63. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Select query criteria when creating reports

Define filters while creating query criteria for:

- Generating customized reports. See Creating reports on page 134.
- Creating Query-based device groups under the CUSTOM GROUPS. See Create a Query device group on page 55.

Define the query criteria by using two options:

- **Select existing query to copy**: By default, OpenManage Enterprise provides a list of built-in query templates that you can copy and build your own query criteria. A maximum of 20 criteria (filters) can be used while defining a query. To add filters, you must select from the **Select Type** drop-down menu.
- **Select type**: Build query criteria from scratch using attributes listed in this drop-down menu. Items in the menu depend on the devices monitored by OpenManage Enterprise. When a query type is selected, only appropriate operators such as =, >, <, and null are displayed based on the query type. This method is recommended for defining query criteria in building customized reports.

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

NOTE: When selected, the filters of an existing query criteria is copied only virtually to build a new query criteria. The default filters associated with an existing query criteria is not changed. The definition (filters) of a built-in query criteria is used as a starting point for building a customized query criteria. For example:

1. *Query1* is a built-in query criteria that has the following predefined filter: `Task Enabled=Yes`.
2. Copy the filter properties of *Query1*, create *Query2*, and then customize the query criteria by adding another filter: `Task Enabled=Yes` AND `(Task Type=Discovery)`.
3. Later, open *Query1*. Its filter criteria still remains as `Task Enabled=Yes`.

1. In the **Query Criteria Selection** dialog box, select from the drop-down menu based on whether you want to create a query criteria for Query groups or for report generation.
2. Add or remove a filter by clicking the plus or dustbin symbol respectively.
3. Click **Finish**.
   A query criteria is generated and saved in the list of existing queries. An audit log entry is made and displayed in the Audit logs list. See Monitor audit logs on page 120.

Export selected reports

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

19

Managing MIB files

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15.

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

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

You manage MIBs by:

- Import MIB files on page 137
- Remove MIB files on page 139
- Resolve MIB types on page 139

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

Table 26. Role-based access for MIB files in OpenManage Enterprise

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

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

Topics:

Import MIB files

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.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope based access control in OpenManage Enterprise on page 15

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

1. Click **MIB** > **Import MIB**.
2. In the **Import MIB** dialog box, in the **Upload MIB Files** section, click **Choose File** to select a MIB file.

   If the MIB has import statements that are resolved by external MIBs, a message is displayed.

   a. Click **Resolve Types**. Resolve the MIB types. See Remove MIB files on page 139.
   b. Click **Finish**. If the MIB file is Dell EMC owned, a message indicates that the MIB is shipped with the product and cannot be modified.
3. Click **Next**.
4. In the **View Traps** section, a list of MIB files is displayed with the following information:
   - Alert category of the trap. You can edit the category to align with the OpenManage Enterprise category definitions. See Edit MIB traps on page 138.
   - Trap name is read-only. Defined by the third-party device.
   - Severity levels of an alert: Critical, Warning, Information, and Normal.
   - Alert message associated with an alert.
   - Trap OID is read-only and unique.
   - 'New' indicates that the trap is imported for the first time by OpenManage Enterprise. Already imported traps are indicated as 'Imported'. 'Overwrite' indicates the traps whose definition is rewritten because of an import operation.

   To edit the default alert categories or severity level of a MIB file, see Edit MIB traps on page 138. 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.

NOTE: If you import a MIB, and then import it again, the MIB status is shown as **IMPORTED**. However, if you re-import a MIB file that is deleted, the trap status is indicated as **NEW**.

NOTE: Traps that are already imported to OpenManage Enterprise cannot be imported.

NOTE: MIB files shipped by default with OpenManage Enterprise cannot be imported.

NOTE: Events that are generated after the trap is imported will be formatted and displayed according to the new definition.

Edit MIB traps

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

Remove MIB files

NOTE: You cannot remove a MIB file that has trap definitions used by any of the alert policies. See Alert policies on page 113.

NOTE: 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.

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**.
   The MIB files are removed and the MIB table is updated.

Resolve MIB types

1. Import the MIB files. See Import MIB files on page 137.
   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 on page 137.

Download an OpenManage Enterprise MIB file

1. On the **Monitor** page, click **MIB**.
2. Expand and select an OpenManage Enterprise MIB file, and then click **Download MIB**.

   NOTE: You can download only the OpenManage Enterprise-related MIB files.

20

Managing OpenManage Enterprise appliance settings

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

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

By clicking **OpenManage Enterprise** > **Application Settings**, you can:

- Configure and manage the OpenManage Enterprise network settings such as IPv4, IPv6, time, and proxy settings. See Configuring network settings.
- Add, enable, edit, and delete users. See Managing users.
- Set the device health and dashboard monitoring properties. See Managing Console preferences.
- Manage user login and lockout policies. See Setting login security properties.
- View current SSL certificate, and then generate a CSR request. See Generate and download the certificate signing request on page 155.
- Configure emails, SNMP, and Syslog properties for alert management. See Configure SMTP, SNMP, and Syslog alerts on page 116.
- Set the SNMP listener and Trap Forward settings. See Managing incoming alerts.
- Set the credentials and time to receive notification about warranty expiry. See Managing warranty settings.
- Set the properties to check for availability of updated version and then update the OpenManage Enterprise version. See Check and update the version of the OpenManage Enterprise and the available plugins on page 160.
- Set the user credentials to run remote command by using RACADM, and IPMI. See Executing remote commands & scripts.
- Set and receive alert notifications on your mobile phone. See OpenManage Mobile settings on page 167.

Related tasks

Delete Directory services on page 151

Topics:

Configure OpenManage Enterprise network settings

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

1. To only view the current network settings of all the active network connections of OpenManage Enterprise such as DNS domain name, FQDN, and 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 (1-1440)** value. Inactivity timeout value can be set between 1 minute to 1440 minutes (24 hours). By default the Universal timeout is grayed out. 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.
3. The current system time and the source—local time zone or NTP server IP are displayed. To configure the system time zone, date, time, and NTP server synchronization, expand **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 the **Use NTP** option is selected.

   e. Click **Apply**.
   f. To reset the settings to default attributes, click **Discard**.
4. To configure the OpenManage Enterprise proxy settings, expand **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 synchronization.
   d. Click **Apply**.
   e. To reset the settings to default attributes, click **Discard**.

To understand all the tasks that you can perform by using the Application Settings feature, see Managing OpenManage Enterprise appliance settings on page 140.

Manage OpenManage Enterprise users

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.
- Any change to the user role will not affect the active session of the impacted user(s) and will take effect from subsequent login.
- If a Device Manager user is demoted to a Viewer, that DM will lose access to all the owned entities such as jobs, firmware or configuration templates and baselines, alert policies, and profiles. These entities can be managed only by the administrator and can't be restored even when the same user is 'promoted' from a Viewer to DM.

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

- View, add, enable, edit, disable, or delete the OpenManage Enterprise local users. For more information, see Add and edit OpenManage Enterprise local users
- Assign OpenManage Enterprise roles to Active Directory users by importing the directory groups. AD and LDAP directory users can assigned an Admin, or a Device Manager, or a Viewer role in OpenManage Enterprise. For more information, see Import AD and LDAP groups on page 147
- View details about the logged-in users, and then end (terminate) a user session.
- Manage Directory Services. For more information, see Add or edit Active Directory groups to be used with Directory Services on page 149
- View, add, enable, edit, disable, or delete OpenID connect providers (PingFederate and/or Key Cloak). For more information, see OpenManage Enterprise login using OpenID Connect providers on page 151

By default, the list of users is displayed under **Users**. The right pane displays the properties of a user name 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**. See Enable OpenManage Enterprise users on page 146. The recommended characters for user names are as follows:
  - 0–9
  - A–Z
  - a–z
  - - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >
  - The recommended characters for passwords are as follows:
    - 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. See Enable OpenManage Enterprise users on page 146 and Disable OpenManage Enterprise users on page 146.
- **ROLE**: Indicates the user role in using OpenManage Enterprise. For example, OpenManage Enterprise administrator and Device Manager. See OpenManage Enterprise user role types on page 14.

Related references

Disable OpenManage Enterprise users on page 146
Enable OpenManage Enterprise users on page 146

Related tasks

Delete Directory services on page 151
Delete OpenManage Enterprise users on page 146
Ending user sessions on page 148

Role and scope based access control in OpenManage Enterprise

OpenManage Enterprise has Role Based Access Control (RBAC) that clearly defines the user privileges for the three built-in roles — Administrator, Device Manager, and Viewer. Additionally, using the Scope-Based Access Control (SBAC) an administrator can limit the device groups that a device manager has access to. The following topics further explain the RBAC and SBAC features.

Role-Based Access Control (RBAC) privileges in OpenManage Enterprise

Users are assigned roles which 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 required for a certain action before allowing the action. For more information about managing users on OpenManage Enterprise, see Manage OpenManage Enterprise users on page 141.

This table lists the various privileges that are enabled for each role.

Table 27. Role-based user privileges in OpenManage Enterprise

OpenManage Enterprise features	Privilege Description	User levels for accessing OpenManage Enterprise		
		Admin	Device Manager	Viewer
Appliance setup	Global appliance settings involving setting up of the appliance.	**Y**	N	N
Security setup	Appliance security settings	**Y**	N	N
Alert management	Alerts actions / management	**Y**	N	N
Fabric management	Fabric actions / management	**Y**	N	N
Network management	Network actions / management	**Y**	N	N
Group management	Create, read, update and delete (CRUD) for static and dynamic groups	**Y**	N	N
Discovery management	CRUD for discovery tasks, run discovery tasks	**Y**	N	N
Inventory management	CRUD for inventory tasks, run inventory tasks	**Y**	N	N
Trap management	Import MIB, Edit trap	**Y**	N	N
Auto-deploy management	Manage auto-deploy configuration operations	**Y**	N	N
Monitoring setup	Alerting policies, forwarding, SupportAssist etc.	**Y**	**Y**	N
Power control	Reboot / cycle device power	**Y**	**Y**	N
Device configuration	Device configuration, application of templates, manage/migrate IO identity, storage mapping (for storage devices), etc	**Y**	**Y**	N
Operating system deployment	Deploy operating system, map to LUN, etc.	**Y**	**Y**	N
Device update	Device firmware update, application of updated baselines, etc.	**Y**	**Y**	N
Template management	Create / manage templates	**Y**	**Y**	N
Baseline management	Create / manage firmware / configuration baseline policies	**Y**	**Y**	N
Power management	Set power budgets	**Y**	**Y**	N
Job management	Job execution / management	**Y**	**Y**	N
Report management	CRUD operations on reports	**Y**	**Y**	N
Report run	Run reports	**Y**	**Y**	**Y**
View	View all data, report execution / management etc.	**Y**	**Y**	**Y**

Scope-Based Access Control (SBAC) in OpenManage Enterprise

With the use of Role-Based Access Control (RBAC) feature, 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 (DM) user, administrators can assign scope to restrict operational access of DM to one or more system groups, custom groups, and / or plugin 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.

Scope can be implemented as follows:

1. Create or Edit User
2. Assign DM role
3. Assign scope to restrict operational access

For more information about managing users, see Manage OpenManage Enterprise users on page 141.

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

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

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

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

In OpenManage Enterprise, scope can be assigned while creating a local or importing AD/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 DM role, admin can select one or more device groups that defines the scope for the DM.

For example, you (as an administrator) create a DM user named dm1 and assign group *g1* present under custom groups. Then dm1 will have operational access to all devices in *g1* only. The user dm1 will not be able to access any other groups or entities related to any other devices.

Furthermore, with SBAC, dm1 will also not be able to see the entities created by other DMs (let's say dm2) on the same group *g1*. That means a DM user will only be able to see the entities owned by the user.

For example, you (as an administrator) create another DM user named 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 will not have access to those entities and vice versa.

A DM with scope to All Devices has operational access as specified by RBAC privileges to all devices and group entities owned by the DM.

SBAC for AD/LDAP users:

While importing or editing AD/LDAP groups, administrators can assign scopes to user groups with DM role. If a user is a member of multiple AD groups, each with a DM 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 DM 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 DM 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 DM 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, DM, Viewer).

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

NOTE: Post upgrade of OpenManage Enterprise to version 3.6.x, the AD/LDAP and OIDC (PingFederate or KeyCloak) device managers would need to recreate all the previous-version entities as these entities are only available to the administrators post upgrade. For more information, see the Release Notes at https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

SBAC for OIDC users:

Scope assignment for OIDC users does not happen within the OME 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 will be available to OME. For more information about configuring user roles and scopes, see Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 153.

NOTE: If PingFederate is being used as the OIDC provider, then only administrator roles can be used. For more information, see Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 153 and the Release Notes at https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Transfer ownership : 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/or configuration baselines, configuration templates, alert policies, and profiles is 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 on page 148.

Related references

OpenManage Enterprise user role types on page 14

Related tasks

Install OpenManage Enterprise on page 19

Add and edit OpenManage Enterprise local users

This procedure is specific to only adding and editing the local users. While editing local users, you can edit all the user properties. However, for Directory Users, only the role and device groups (in the case of a Device Manager) can be edited. To integrate Directory Services in OpenManage Enterprise and to import the Directory users, see Directory services integration in OpenManage Enterprise on page 148 and Import AD and LDAP groups on page 147.

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.
- You cannot enable, disable, or delete the admin/system/root users. You can only change the password by clicking **Edit** in the right pane.

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 control in OpenManage Enterprise on page 15.
      By default, the **Enabled** check box is selected to indicate that the user privileges currently being 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.

NOTE: 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.

3. Click **Finish**.
   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

1. On the **Application Settings** page, under **Users**, select the check box corresponding to the user.
2. Complete the tasks in Add and edit OpenManage Enterprise local users on page 145.
   The updated data is saved.

   NOTE: When you change the role of a user, the privileges available for the new role automatically get applied. For example, if you change a device manager to an administrator, the access rights and privileges provided for an administrator will be automatically enabled for the device manager.

Enable OpenManage Enterprise users

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 on page 151
Delete OpenManage Enterprise users on page 146
Ending user sessions on page 148

Related information

Manage OpenManage Enterprise users on page 141

Disable OpenManage Enterprise users

Select the check box corresponding to the user name 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 on page 151
Delete OpenManage Enterprise users on page 146
Ending user sessions on page 148

Related information

Manage OpenManage Enterprise users on page 141

Delete OpenManage Enterprise users

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

Related references

Disable OpenManage Enterprise users on page 146
Enable OpenManage Enterprise users on page 146

Related information

Manage OpenManage Enterprise users on page 141

Import AD and LDAP groups

NOTE:

- The users without Administrator rights cannot enable or disable the Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) users.
- Before importing AD groups in OpenManage Enterprise, you must include the user groups in a UNIVERSAL GROUP while configuring the AD.
- AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Admin, 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.
- Post upgrade of OpenManage Enterprise to version 3.6.x, the AD/LDAP and OIDC (PingFederate or KeyCloak) device managers would need to recreate all the previous-version entities as these entities are only available to the administrators post upgrade. For more information, see the Release Notes at https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

1. Click **Import Directory Group**.
2. In the **Import Active Directory** dialog box:
   a. From the **Directory Source** drop-down menu, select an AD or LDAP source that must be imported for adding groups. For adding directories, see Add or edit Active Directory groups to be used with Directory Services on page 149.
   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 control in OpenManage Enterprise on page 15.
   b. Click **Assign Role**.
   The users in the group under the selected directory service are assigned with 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.

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 the user is a member of.

- 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 or configuration templates and baselines, alert policies, and profiles that are created by one device manager to another device manager. Administrator can initiate a 'transfer of ownership' when a device manager leaves the organization.

NOTE:

- To perform this task on OpenManage Enterprise you must have the administrator user privileges. Role and scope based access control in OpenManage Enterprise on page 15.
- 'Transfer of ownership' transfers only the entities and not the device groups (scope) owned by a device manager to another.
- Before a transfer of ownership of entities is initiated, the administrator must first reassign the device groups owned by the former device manager to the device manager who will be taking over.
- If the ownership of the entities is transferred to an Active Directory user group, then the ownership is transferred to all the members of that AD group.

To transfer the ownership of entities such as jobs, firmware or configuration templates and baselines, alert policies, and profiles from one device manager to another do the following:

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

   NOTE: The Source User will only list the local, active directory, OIDC, or deleted device managers who have entities such as jobs, FW or configuration templates, alerts policies and profiles associated with them.
3. From the **Target User** drop-down list, select the device manager to whom the entities will be transferred.
4. Click **Finish** and then click **Yes** at the prompt message.

All the owned entities such as jobs, firmware or configuration templates, alert policies, and profiles are transferred from the 'source' device manager to the 'target' device manager.

Ending user sessions

1. Select the check box corresponding to the username, and then click **Terminate**.
2. When prompted to confirm, click **YES**.
   The selected user session is ended and the user is logged out.

Related references

Disable OpenManage Enterprise users on page 146
Enable OpenManage Enterprise users on page 146

Related information

Manage OpenManage Enterprise users on page 141

Directory services integration in OpenManage Enterprise

Directory Services enables you to import directory groups from AD or LDAP for use on the console. OpenManage Enterprise supports integration of the following directory services:

1. Windows Active Directory
2. Windows AD/LDS
3. OpenLDAP
4. PHP LDAP

Pre-requisites/supported attributes for LDAP Integration

Table 28. OpenManage Enterprise Pre-requisites/supported attributes for LDAP Integration

	Attribute of User Login	Attribute of Group Membership	Certificate Requirement
AD/LDAP	Cn, sAMAccountName	Member	• Subject to Domain Controller Certificate needs to have FQDN. SAN field can have IPv4 and/or IPv6 or FQDN. • Only Base64 certificate format is supported
OpenLDAP	uid, sn	Uniquemember	Only PEM certificate format is supported
PHP LDAP	uid	MemberUid	

User pre-requisites for directory service integration

You must ensure that the following user pre-requisites are met before you begin with the directory service integration:

1. BindDN user and user used for 'Test connection' should be the same.
2. If Attribute of User Login is provided, only the corresponding username value assigned to the attribute is allowed for appliance login.
3. User used for Test connection should be part of any non-default group in LDAP
4. Attribute of Group Membership should have either the 'userDN' or the short name (used for logging in) of the user.
5. When MemberUid is used as 'Attribute of Group Membership,' the username used in appliance login will be considered case sensitive in some LDAP configurations.
6. When search filter is used in LDAP configuration, user login is not allowed for those users who is not part of the search criteria mentioned.
7. Group search will work only if the groups have users assigned under the provided Attribute of Group Membership .

NOTE: If the OpenManage Enterprise is hosted on an IPv6 network, the SSL authentication against domain controller using FQDN would fail if IPv4 is set as preferred address in DNS. To avoid this failure, do one of the following:

- DNS should be set to return IPv6 as preferred address when queried with FQDN.
- DC certificate needs to have IPv6 in SAN field.

To use the Directory Services:

- Add a directory connection. See Add or edit Active Directory groups to be used with Directory Services on page 149.
- Import directory groups and map all users in the group to a specific role. See Import AD and LDAP groups on page 147.
- For DM users, edit the directory group to add the groups the DM can manage. See Add and edit OpenManage Enterprise local users on page 145.

Add or edit Active Directory groups to be used with Directory Services

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 directory type is Active Directory (AD):

   NOTE: To create an LDAP user group by using Directory Services, see Add or edit Lightweight Directory Access Protocol groups to be used with Directory Services on page 150.

   a. Enter a desired 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 controllers.
- **Manual**: In the **Method** box, enter the FQDN or the IP address of the domain controller. For multiple servers, a maximum of three servers are supported, use a comma-separated list.

c. In the **Group Domain** box, enter the group domain as suggested in the tool tip syntax.

3. In the **Advanced Options** section:
   a. By default, Global Catalog Address port number 3269 is populated. For the Domain Controller Access, enter 636 as the port number.

      NOTE: Only LDAPS ports are supported.

   b. Enter the network timeout and search timeout duration in seconds. The maximum timeout duration supported is 300 seconds.
   c. To upload an SSL certificate, select **Certificate Validation** and click **Select a file**. The certificate should be a Root CA Certificate encoded in Base64 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.

   NOTE: 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 successful connection.
7. Click **Ok**.
8. Click **Finish**.
   A job is created and run to add the requested directory in the Directory Services list.

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 Lightweight Directory Access Protocol groups to be used with Directory Services

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

   NOTE: To create an AD user group by using Directory Services, see Add or edit Active Directory groups to be used with Directory Services on page 149.

   a. Enter a desired 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 controllers.
      - **Manual**: In the **Method** box, enter the FQDN or the IP address of the domain controller. For multiple servers, a maximum of three servers are supported, use a comma-separated list.

   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, LDAP port number of 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. Enter the **User attributes** already configured in the LDAP system. It is recommended that this is unique within the selected Base DN. Else, configure a search filter to ensure that it is unique. If the user DN cannot be uniquely identified by the search combination of attribute and search filter, the login operation fails.

NOTE: The user attributes should be configured in the LDAP system used to query before integrating on the directory services.

NOTE: You need to enter the user attributes as **cn** or **sAMAccountName** for AD LDS configuration and **UID** for LDAP configuration

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 supported is 300 seconds.
f. To upload an SSL certificate, select **Certificate Validation** and click **Select a file**. The certificate should be a Root CA Certificate encoded in Base64 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 successful connection.
6. Click **Ok**.
7. Click **Finish**.
   A job is created and run to add the requested directory in the Directory Services list.

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

Select the check box corresponding to the Directory Services to be deleted, and then click **Delete**.

Related references

Disable OpenManage Enterprise users on page 146
Enable OpenManage Enterprise users on page 146

Related information

Managing OpenManage Enterprise appliance settings on page 140
Manage OpenManage Enterprise users on page 141

OpenManage Enterprise login using OpenID Connect 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. Currently, OpenManage Enterprise provides support for PingFederate and Keycloak.

WARNING: User roles and scopes are reset to 'default' on client re-registration with OIDC provider PingFederate (PingIdentity). This issue might lead to resetting of the privileges and scope of non-admin roles (DM and Viewer) to that of the Administrator. Re-registration of the appliance console with OIDC provider is triggered in the event of 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 control in OpenManage Enterprise on page 15.
- Only a maximum of four OpenID Connect provider IDs can be added in the appliance.
- Post upgrade of OpenManage Enterprise to version 3.6.x, the AD/LDAP and OIDC (PingFederate or KeyCloak) device managers would need to recreate all the previous-version entities as these entities are only available to the administrators post upgrade. For more information, see the Release Notes at https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

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 OpenID Connect provider to OpenManage Enterprise on page 152.
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 called **dxcua** (Dell extended claim for user authentication). For more information, see:
   - Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 153
   - Configure an OpenID Connect provider policy in Keycloak for role-based access to OpenManage Enterprise on page 154

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

- Name - The OpenID Connect provider's name when it was added in the appliance
- Enabled - A 'check' on this field indicates that the OpenID Connect provider is enabled in the appliance
- Discovery URI - The URI (Uniform Resource Identifier) 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 will not be allowed even when they are enabled.
  - In Progress - This status is displayed when the appliance tries to register with OpenID Connect provider.

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

On the **Application Settings** > **Users** > **OpenID Connect Providers** page you can do the following:

- Add an OpenID Connect provider to OpenManage Enterprise on page 152
- Edit an OpenID Connect provider details in OpenManage Enterprise on page 154
- Test the registration status of OpenManage Enterprise with the OpenID Connect provider on page 154
- Enable OpenID Connect providers on page 155
- Disable OpenID Connect providers on page 155
- Delete OpenID Connect providers on page 155

Add an OpenID Connect provider to OpenManage Enterprise

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

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

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

1. Click **Add** to activate the Add New OpenID Connect Provider page.
2. Fill the following information in the respective fields:
   a. Name - Name for the OIDC client.
   b. Discovery URI - Uniform Resource Identifier of the OIDC provider
   c. Authentication type - Choose from one of the following methods the access token must use to access the appliance:
      i. Initial Access Token - Provide the Initial access token
      ii. Username and Password - Provide the username and password

d. (Optional) Certificate Validation check box - You can select the check box and upload the OIDC provider's certificate by clicking **Browse** and locating the certificate or by dragging and dropping the certificate in the 'broken line' box.
e. (Optional) Test connection - 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, as 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 login to the appliance.

3. Click **Finish**.

The newly added OpenID Connect provider is listed on the Application Settings > Users > OpenID Connect providers page and the Client ID can be located on the right pane.

Next steps:

Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 153

Configure an OpenID Connect provider policy in Keycloak for role-based access to OpenManage Enterprise on page 154

Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise

To enable OpenManage Enterprise OpenID Connect login using PingFederate, you must add and map a scope **dxcua** (Dell extended claim for user authentication) to the Client ID and define the user privileges as follows:

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

1. Add an 'exclusive' or 'default' scope called **dxcua** under Scope Management in OAuth Settings.
2. Map the scope created in **OpenID Connect Policy Managment** > **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 unselected in OpenID Connect provider client settings, the registration will work with Username and password. If the option is enabled, then the registration will work only with the Initial Access token.

Configure an OpenID Connect provider policy in Keycloak for role-based access to OpenManage Enterprise

To enable OpenManage Enterprise OpenID Connect login using Keycloak, you must first add and map a scope **dxcua** to the Client ID and define the user privileges as follows:

NOTE: The Discovery URI specified in the OpenID Connect provider configuration wizard should have a valid endpoint of the provider listed.

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, in OpenManage Enterprise 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 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

Test the registration status of OpenManage Enterprise with the OpenID Connect provider

On the **Application Settings** > **Users** > **OpenID Connect Providers** page do the following:

1. Select an OpenID Connect provider.
2. On the right pane, click **Test Registration Status**.

   NOTE: Test connection does not depend on the username and password or the initial access token details, as it only checks for the validity of the Discovery URI.

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

Edit an OpenID Connect provider details in OpenManage Enterprise

On the **Application Settings** > **Users** > **OpenID Connect Providers** page do the following:

1. Select an OpenID Connect provider.
2. Click **Edit** on the right pane.
3. 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.
4. Click **Finish** to implement, or click **Cancel** to discard the changes.

Enable OpenID Connect providers

If an OpenID Connect provider's login was not enabled at the time when it was added to the appliance, then to activate the login you must 'enable' it in the appliance.

On the **Application Settings** > **Users** > **OpenID Connect providers** page do the following:

1. Select the OpenID Connect provider(s).
2. Click **Enable**.

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

Delete OpenID Connect providers

On the **Application Settings** > **Users** > **OpenID Connect Providers** page do the following:

1. Select the OpenID Connect provider(s).
2. Click **Delete**.

Disable OpenID Connect providers

On the **Application Settings** > **Users** > **OpenID Connect providers** page do the following:

1. Select the OpenID Connect provider(s).
2. Click **Disable**.

The client access token from the 'disabled' OIDC providers will be rejected by the appliance.

Security Certificates

By clicking **Application Settings** > **Security** > **Certifciates**, you can view information about the currently available SSL certificate for the device.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

To generate a Certificate Signing Request (CSR), see Generate and download the certificate signing request on page 155.

Generate and download the certificate signing request

To generate a Certificate Signing Request (CSR) for your device, and then apply for an SSL:

NOTE: You must generate the CSR from within the OpenManage Enterprise appliance only.

1. Click **Generate Certificate Signing Request**.
2. In the **Generate Certificate Signing Request** dialog box, enter information in the fields.
3. 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.
4. 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**.

Assigning a webserver certificate to OpenManage Enterprise using the Microsoft Certificate Services

1. Generate and download the Certificate Signing Request (CSR) in OpenManage Enterprise. See Generate and download the certificate signing request on page 155
2. Open a web session to the certification server (https://x.x.x.x/certsrv) and click on the **Request a certificate** link .
3. On the Request a Certificate page, click on the **submit an advanced certificate request** link.
4. On the Advanced Certificate Request page, click on 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** link.
5. On the Submit a Certificate Request or Renewal Request page do the following:
   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.
6. On the Certificate Issued page, select the option **Base 64 encoded** and then click the **Download Certificate** link to download the certificate.
7. Upload the certificate in OpenManage by navigating to the **Application Settings** > **Security** > **Certificates**page and then clicking **Upload**.

Set the login security properties

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

NOTE: AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Admin, DeviceManager, or Viewer).

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

- Expand **Restrict Allowed IP Range**:
  NOTE: When "Restrict Allowed IP Range", is configured in appliance, any inbound connection to 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 will work on all devices.
  1. To specify the IP address range that must be allowed to access OpenManage Enterprise, select the **Enable IP Range** check box.
  2. In the **IP Range Address (CIDR)** box, enter the IP address range.
     NOTE: Only one IP range is allowed.
  3. 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**.
- Expand **Login Lockout Policy** :
  1. Select the **By User Name** check box to prevent a specific user name from logging in to OpenManage Enterprise.
  2. Select the **By IP address** check box to prevent a specific IP address from logging in to OpenManage Enterprise.
  3. 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.
  4. In the **Lockout Fail Window** box, enter the duration for which OpenManage Enterprise must display information about a failed attempt.
  5. In the **Lockout Penalty Time** box, enter the duration for which the user is prevented from making any login attempt after multiple unsuccessful attempts.
  6. Click **Apply**. To reset the settings to default attributes, click **Discard**.

Manage Console preferences

NOTE: To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

By clicking **OpenManage Enterprise** > **Application Settings** > **Console Preferences**, you can set the default properties of the OpenManage Enterprise GUI. For example, default time after which a device health is automatically checked and updated on the dashboard, and preferred settings used for discovering a device. The following options are available:

1. **Report Settings**: To set the maximum number of rows that you can view on OpenManage Enterprise reports:
   a. Expand **Report Settings**.
   b. Enter a number in the **Reports row limit** box. The default limit is set at 1,000 rows, however, the maximum rows permitted is 2,000,000,000.
   c. Click **Apply**. A job is run and the setting is applied.
2. **Device Health**: To set the time after which the health of the devices must be automatically monitored and updated on the OpenManage Enterprise Dashboard:
   a. Expand **Device Health**.
   b. Enter the frequency at which the device health must be recorded and data stored.
   c. 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 the device is not anymore monitored by OpenManage Enterprise.
   d. Click **Apply** to save the changes to the settings or click **Discard** to reset the settings to default attributes.
3. **Discovery Setting**: 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.
   a. **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 page.
   b. **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.
   c. To specify the invalid device hostnames and the common MAC addresses expand the **Advance Settings**
      i. Enter one or more invalid hostnames separated by a comma in **Invalid Device Hostname**. By default, a list of invalid device hostname is populated.
      ii. Enter the common MAC addresses separated by a comma in **Common MAC Addresses**. By default, a list of common MAC addresses is populated.
   d. Click **Apply** to save the changes to the settings or click **Discard** to reset the settings to the default attributes.
4. **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.

5. **MX7000 Onboarding Preferences**: Specify one of the following alert-forwarding behavior on MX7000 chassis when they are onboarded:
   - Receive All Alerts
   - Receive 'Chassis' category alerts only
6. **SMB Setting**: To select one of the following Server Message Block (SMB) version that must be used for network communication:
   - **Disable V1**: SMBv1 is disabled. This is the default selection in the appliance.
   - **Enable V1**: To enable SMBv1.

   NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. See Manage Console preferences on page 157 and Generic naming convention for Dell EMC PowerEdge servers on page 177 for more information.
7. **Email Sender Settings**: To set the address of the user who is sending an email message:
   a. Enter an email address in the **Sender Email ID** box.
   b. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.
8. **Trap Forwarding Format**: To set the trap forwarding format —
   a. 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.

   b. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.
9. **Metrics Collection Settings**: To set the frequency of the PowerManager extension data maintenance and purging do the following:
   a. In the **Data purge interval** box, enter the frequency to delete the PowerManager data. You can enter values within 30 to 365 days.
   b. Click **Apply** to save changes or click **Discard** to reset the settings to the default attributes.

Customize the alert display

1. Click **OpenManage Enterprise** > **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 pages:
   - The upper-right corner of all the OpenManage Enterprise pages. See OpenManage Enterprise Graphical User Interface overview on page 34.
   - The Dashboard page. See Monitor devices by using the OpenManage Enterprise dashboard on page 36.
   - The Devices page. See Donut chart on page 37.
   - The **Alert Log** table under the Alerts page. See View alert logs on page 111.

Configure SMTP, SNMP, and Syslog alerts

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

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

1. Expand **Email Configuration**.
2. Enter the SMTP server network address that sends email messages.

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

To configure the SNMP alert forwarding configuration:

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

   NOTE: Entering of the console IP is disallowed to avoid duplication of alerts.
4. From the **SNMP VERSION** menu select the SNMP version type as SNMPv1, SNMPv2, or SNMPv3 and fill the following fields:
   a. In the COMMUNITY STRING box, enter the SNMP community string of the device that must receive the alert.
   b. Edit the PORT NUMBER if needed. Default port number for SNMP traps=162. See Supported protocols and ports in OpenManage Enterprise on page 30.
   c. If SNMPv3 is selected, provide the following additional details:
      i. USERNAME: Provide a username.
      ii. AUTHENTICATION TYPE : From the drop down list select SHA, MD_5, or None.
      iii. AUTHENTICATION PASSPHRASE: Provide an authentication passphrase having a minimum of eight characters.
      iv. PRIVACY TYPE: From the drop down list select DES, AES_128, or None.
      v. PRIVACY PASSPHRASE: Provide a privacy passphrase containing a minimum of eight characters.
5. To test an SNMP message, click the **Send** button of the corresponding trap.
6. Click **Apply**. To reset the settings to default attributes, click **Discard**.

To update the Syslog forwarding configuration:

1. Expand **Syslog Forwarding Configuration**.
2. Select the check box to enable the Syslog feature on the respective server in the **SERVER** column.
3. In the **DESTINATION ADDRESS/HOST NAME** box, enter the IP address of the device that receives the Syslog messages.
4. Default port number by using UDP=514. Edit if necessary by entering or selecting from the box. See Supported protocols and ports in OpenManage Enterprise on page 30.
5. Click **Apply**.
6. To reset the settings to default attributes, click **Discard**.

Manage incoming alerts

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 15.

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

- To set the SNMP credentials for incoming alerts:

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

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 on the home page Alert widget, scoreboard across all pages, the Warranty page, and the reports.

To change the warranty settings:

1. Click **OpenManage Enterprise** > **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' as well as '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.
5. Click **Apply** or **Discard** to either save the warranty settings or to discard the changes and retain the old settings.

Check and update the version of the OpenManage Enterprise and the available plugins

To go to the Console and plugins page, click **Application Settings** > **Console and Plugins**. On the Console and plugins page you can do the following:

1. View the current version of your OpenManage Enterprise, check if updates are available, and then upgrade to a newer version. You can click the **Update Settings** button to:
   a. Check for the updates Automatically or Manually.
   b. Choose from the Online or Offline modes of updating the appliance.

   For more information see Update settings in OpenManage Enterprise on page 161
2. Download and install more plugins (extensions) such as the Power Manager plugin to enhance the functionality of the appliance. For more information about the installation of plugins, see plugin

   NOTE: The OpenManage Enterprise Advanced license is required for the plugins to be fully functional after installation. For more in-depth information about the plugins, refer the respective documentation available on the Dell Support site.

   NOTE: Installing a plugin on OpenManage Enterprise restarts the appliance services.
3. With the already-installed plugins you can do the following:

- Click **More Actions** drop-down menu to learn more about the plugin, disable, uninstall, enable, or to change the settings of the plugin. For more information, see plugin, plugin, plugin
- You can click on **Update Available** as and when new versions of the plugins are available.

Related information

Update from Dell.com on page 162
Update from an internal network share on page 163

Update settings in OpenManage Enterprise

By clicking the **Update Settings** on the Console and Extensions page (**Application Settings** > **Console and Extension**) the following update settings can be selected:

1. **How to check for updates** — Select from the following methods:
   a. **Automatic**: The appliance checks for the availability of the updates automatically every Monday from the source specified in the **Where to check for updates**.
   b. **Manual**: When configured to Manual, the user has to manually check for the availability of the update from the source specified in the **Where to check for updates**.
2. **Where to check for updates** — The location from where the appliance checks for updates can be specified. The following options are available:
   a. **Dell.com** (online)— When this option is selected, the appliance checks for the availability of update directly from https://downloads.dell.com/openmanage_enterprise.
   b. **Network Share** (offline)— Specify an NFS, HTTP, or HTTPS path that contains the update package. Click on **Test Now** to validate connection to the specified network share.

   NOTE: For the offline updates (Network Share), the Administrator should create appropriate folder structures before downloading the update package depending on whether a minimal or a full upgrade is needed. For more information about updating OpenManage Enterprise to the latest version and permissible folder structure for updates, see the Upgrade the Dell EMC OpenManage Enterprise appliance version (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) technical white paper on the support site.

3. 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.

   NOTE: 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 Extensions** page. The OpenManage Enterprise section of the Console and Extensions page displays all the new features and enhancements of the available update. Click **Update** to initiate the update.

Update OpenManage Enterprise

Based on the update settings (**Application Settings** > **Console and Extensions** > **Update Settings)**, your existing OpenManage Enterprise can be updated automatically or manually from the Dell.com site directly or from an already downloaded update package in the network share.

When a new and upgradable version of OpenManage Enterprise is identified, additional details such as the version, size, and new features of the update are displayed on the Console and Extension page and an active **Update** button is available. Also, a banner with details of the new version is displayed. All users can view the banner, however, only users with Administrator privilege can opt for the remind later or dismiss the message option.

NOTE:

- Only OpenManage Enterprise versions starting 3.4 and later can be directly updated to version 3.6.1 by the **Automatic** > **Online** method.
- OpenManage Enterprise versions earlier than version 3.4, such as, version 3.3x and version 3.2, must first be updated to version 3.4 before considering an upgrade to 3.6.1.

- A direct update from the OpenManage Enterprise—Tech Release version is not supported. TechRelease version should be first upgraded to OpenManage Enterprise either version 3.0 or 3.1.
- After you upgrade to version 3.6.x, the existing device managers will have all devices in their scope by default. However, if required, the administrator can edit the device manager(s) scope using the SBAC feature. For more information, see Role and scope based access control in OpenManage Enterprise on page 15 and Manage OpenManage Enterprise users on page 141.

Before updating to the latest version, the Administrator should:

- Take a VM snapshot of the console as a backup in case something unexpected occurs. Allocate more downtime for this if necessary.
- Allocate at least an hour for the update process. Allocate more time if the update must be downloaded by using a slower network connection.
- Ensure that no device configuration, deployment, or extension (plugin) 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.
- Notify other console users of the impending scheduled update.
- If the upgrade fails, the appliance would restart. It is recommended to revert the VM snapshot and upgrade again.

For upgrades from OpenManage Enterprise version 3.5, the outcome of the upgrade process is indicated by a banner on the console pages. By default, the banner is displayed for 24 hours after the upgrade, however, you could make it disappear by clicking 'Dismiss' on the far-right of the banner. When the upgrade from OpenManage Enterprise version 3.5 is successful, the banner is in green and has a 'upgrade success' message indicating the new version number of the appliance. However, if the upgrade fails, the appliance is automatically restored to its previous version and the banner is shown in orange and with a 'failure' message. You can click 'View Details' on the banner to view the execution history of the Upgrade job on the Job Details page.

NOTE:

- When you update OpenManage Enterprise with more than 8,000 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.
- Adding a second network interface should be done only after the completion of the post-console upgrade tasks. Attempt to add a second NIC while the post-upgrade task is in progress would be ineffective.
- You can login immediately after the appliance is updated and don't have to wait till the entire inventory is discovered. Post update, the discovery task will run in the background and you can see the progress occasionally.
- Clicking **Update** would initiate an Upgrade Bundle Download job. This job finishes by itself after all the update files are downloaded and cannot be terminated by the user.

1. To update online from Dell.com, refer Update from Dell.com on page 162.
2. To update offline from an already downloaded update package in the NFS or HTTPS network share, refer Update from an internal network share on page 163.

   NOTE: Depending on whether a minimal or a full upgrade is needed, the Administrator should create appropriate folder structures before downloading the update package. For more information about permissible folder structures and updating of OpenManage Enterprise to the latest version, see the *Upgrade the Dell EMC OpenManage Enterprise appliance version* technical white paper on the support site.

Update from Dell.com

Your existing OpenManage Enterprise can be updated online, either automatically or manually, from Dell.com (https://downloads.dell.com/openmanage_enterprise).

Online update pre-requisites:

- Update settings **Where to check for updates** should be specified as Dell.com. For more information, refer Update settings in OpenManage Enterprise on page 161.
- You must ensure that the OpenManage Enterprise appliance can access Dell.com and the expected update.
- Before you begin the update, ensure to take a VM snapshot of the console as a backup in case something unexpected occurs. Allocate more downtime for this if necessary.

When a new and upgradable version of OpenManage Enterprise is identified, additional details such as the version, size, and new features of the update are displayed on the Console and Extension page and an active **Update** button is available. Also, a banner

with details of the new version is displayed. All users can view the banner, however, only users with Administrator privilege can opt for the remind later or dismiss the message option.

1. Click **Update** and perform an update.

   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 would restart. It is recommended to revert the VM snapshot and upgrade again

2. 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 any errors, export the audit log and save for tech support.

After the appliance is updated:

- Clear the browser cache. Not clearing the browser cache, may cause failing of new tasks post update.
- Adding a second network interface should be done only after the completion of the post-console upgrade tasks. Attempt to add a second NIC while the post-upgrade task is in progress would be ineffective.
- You can login immediately after the appliance is updated and don't have to wait till the entire inventory is discovered. Post update, the discovery task will run in the background and you can see the progress occasionally.

Related tasks

Check and update the version of the OpenManage Enterprise and the available plugins on page 160

Update from an internal network share

You must set up a local network share and manually download the update package when you are not automatically connected to Dell.com. An audit log is created after every manual attempt to find an update.

NOTE:
- OpenManage Enterprise versions earlier than versions 3.4, for example, version 3.3x and version 3.2, must first be updated to version 3.4 before considering an upgrade to 3.6.x through a shared Network File Share (NFS).
- A direct update from the OpenManage Enterprise—Tech Release version is not supported. TechRelease version should be first upgraded to OpenManage Enterprise either version 3.0 or 3.1.
- For the offline updates (Network Share), the Administrator should create appropriate folder structures before downloading the update package depending on whether a minimal or a full upgrade is needed. For more information about updating OpenManage Enterprise to the latest version and permissible folder structure for updates, see the Upgrade the Dell EMC OpenManage Enterprise appliance version (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) technical white paper on the support site.
- When updating local shares for a manual upgrade of versions without any installed extensions/plugins (such as 3.1 and 3.2), the audit log displays warning entries such as "Unable to retrieve the source file of type Extension Catalog because the file does not exist" and "The status of downloading the Extension Catalog is Failed". These error messages do not have any functional impact on the upgrade process and can be ignored.

Before you begin the update:

- Ensure to take a VM snapshot of the console as a backup in case something unexpected occurs. (Allocate more downtime for this, if necessary).
- If the upgrade fails, the appliance would restart. It is recommended to revert the VM snapshot and upgrade again.
- Adding a second network interface should be done only after the completion of the post-console upgrade tasks. Attempt to add a second NIC while the post-upgrade task is in progress would be ineffective.
- You must ensure that the security certificates are signed by a trusted third-party certificate authority when using the HTTPS method of update.

To update the OpenManage Enterprise:

1. Download the applicable files from https://downloads.dell.com and save on a network share preserving the same folder structure that can be accessed by the console.
2. Select **Manual** and **Offline**.
3. Enter the local path information where the downloaded files are saved, and then click **Check Now**. Example paths: *nfs://<IP Address>/<Folder_Name>*, *http://<IP Address>/<Folder_Name>*, *https://<IP Address>/<Folder_Name>*.

The available update version with a brief description of the new features are displayed.

4. 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 step is an optional.
5. Click **Update**, and perform an update (applicable for future upgrades).

   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 by the user
   - If the upgrade download has a problem connecting through proxy, uncheck the proxy settings and then download.

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 any errors, export the audit log and save for tech support.

After the appliance is updated:

- Clear the browser cache. Not clearing the browser cache, may cause failing of new tasks post update.
- If upgrading from OpenManage Enterprise version 3.1, it is recommended that you re-configure or import the Active Directory groups for enhanced performance.
- You can login immediately after the appliance is updated and don't have to wait till the entire inventory is discovered. Post update, the discovery task will run in the background and you can see the progress occasionally.

Related tasks

Check and update the version of the OpenManage Enterprise and the available plugins on page 160

Install a plugin

You can install the Power Manager, SupportAssist-Enterprise, and Update Manager plugins based on your requirements to enhance the functionality of OpenManage Enterprise.

- 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, you must manually download the package to your network share and update the location on the Update Settings page in OpenManage Enterprise.

For more information about Update Settings configuration, see Update settings in OpenManage Enterprise on page 161.

NOTE: Installing a plugin on OpenManage Enterprise restarts the appliance services.

To install a plugin, perform the following steps:

1. In OpenManage Enterprise, click **Application Settings** > **Console and plugins**
   The **Console and Plugins** page is displayed.
2. In the **Plugins** section, click **Install** for the plugin you want to install.
   The **Install Plugin** wizard is displayed.
3. From the **Available Version(s)** list, select the version that you want to install.
4. Review and ensure that you meet the list of prerequisites that are mentioned under the **Prerequisite** section, and then click **Download Plugin**.

   NOTE: The lists of prerequisites change as you select the version of plugin that you want to install.

   The install operation validates the prerequisites to install the plugin. If installation prerequisites are not fulfilled, an appropriate error message is displayed.

   After the plugin is downloaded successfully, the status that appears on the top of the plugin changes from **Available** to **Downloaded**.
5. To install the OpenManage Enterprise plugin, in the **Install Plugin** wizard, click **Install Plugin**.
6. A consent form is displayed to inform you about the End User License Agreement (EULA). Click **Accept** to continue to install the plugin.
   The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirmation** dialog box.
7. To confirm the installation, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action** option, and then click **Confirm Install**.

The status of installation operation is displayed. After the successful installation of the plugin, the status that appears on the top of the plugin section changes from **Available** or **Downloaded** to **Installed**.

Disable a plugin

Disables all the functionality of the plugin on OpenManage Enterprise.

NOTE: Disabling a plugin on OpenManage Enterprise restarts the appliance services.

1. In OpenManage Enterprise, click **Application Settings** > **Console and Plugins**.
   The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Disable** for the plugin you want to disable.
   The **Disable Plugin** wizard is displayed.
3. To disable the plugin, click **Disable Plugin**.
   The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirmation** dialog box.
4. To confirm, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action.** option, and then click **Confirm Disable**.

NOTE: After disabling the plugin, you cannot see any information or pages related to the plugin on OpenManage Enterprise.

Uninstall a plugin

Uninstalls and deletes all the data that is collected by the plugin.

1. In OpenManage Enterprise, click **Application Settings** > **Console and Plugins**.
   The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Uninstall** for the plugin you want to uninstall.
   The **Uninstall Plugin** wizard is displayed.
3. To uninstall the plugin from the OpenManage Enterprise, click **Uninstall Plugin**.
   The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirmation** dialog box.
4. To confirm the uninstall, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action.** option, and then click **Confirm Uninstall**.

All functionality and data associated with the plugin will be uninstalled.

Enable plugin

All plugin pages are displayed on OpenManage Enterprise and plugin functionality is enabled on OpenManage Enterprise.

NOTE: Enabling a plugin on OpenManage Enterprise restarts the appliance services.

1. In OpenManage Enterprise, click **Application Settings** > **Console and Plugins**.
   The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Enable** for the plugin you want to enable.
   The **Enable Plugin** wizard is displayed.
3. To enable the plugin, click **Enable Plugin**.
   The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirmation** dialog box.
4. To confirm, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action.** option, and then click **Confirm Enable**.

Update a plugin

Based on the update settings, the appliance checks for the availability of an update of the installed plugins. 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** page. The Plugin section of the Console and Plugins page displays all the new features and enhancements of the available plugin update.

Before you update a plugin, ensure that the update settings is configured as mentioned in Update settings in OpenManage Enterprise on page 161.

To update a plugin, do the following:

1. In the Plugin section, click **Update Available** for the plugin you want to update.
   The **Update Plugin** page is displayed.
2. Select the plugin version, and then click **Download Plugin**.
   The plug-in is downloaded, and the status of the download is displayed on a green color band.
3. To update the plugin, click **Update Plugin**.
   In the **Confirmation** window, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action** option, and then click **Update**.

After update operation is complete, the version is displayed in the plugin section.

Execute remote commands and scripts

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 **'**.

1. Click **Application Settings** > **Script Execution**.
2. In the **Remote Command Setting** section, do the following:
   a. To add a remote command, click **Create**.
   b. In the **Command Name** box, enter the command name.
   c. Select any one of the following command type:
      i. Script
      ii. RACADM
      iii. IPMI Tool
   d. If you select **Script**, do the following:
      i. In the **IP Address** box, enter the IP address.
      ii. Select the authentication method: **Password** or **SSH Key**.
      iii. Enter the **user name** and **password** or the **SSH Key**.
      iv. In the **Command** box, type the commands.
         - Up to 100 commands can be typed with each command required to be on a new line.
         - Token substitution in scripts is possible. See Token substitution in remote scripts and alert policy on page 174
      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

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:

- 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 tasks

Enable or disable alert notifications for OpenManage Mobile on page 167
Enable or disable OpenManage Mobile subscribers on page 167
Delete an OpenManage Mobile subscriber on page 168
View the alert notification service status on page 168
Troubleshooting OpenManage Mobile on page 170

Related information

Enable or disable alert notifications for OpenManage Mobile on page 167
Enable or disable OpenManage Mobile subscribers on page 167
Troubleshooting OpenManage Mobile on page 170

Enable or disable alert notifications for OpenManage Mobile

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.

NOTE: The administrator rights are required for enabling or disabling alert notifications for OpenManage Mobile.

NOTE: For OpenManage Enterprise to send alert notifications to OpenManage Mobile, ensure that the OpenManage Enterprise server has outbound (HTTPS) Internet access.

To enable or disable alert notifications from OpenManage Enterprise to OpenManage Mobile:

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

Related tasks

OpenManage Mobile settings on page 167

Related information

OpenManage Mobile settings on page 167
Delete an OpenManage Mobile subscriber on page 168

Enable or disable OpenManage Mobile subscribers

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.

To enable or disable alert notifications to the OpenManage Mobile subscribers:

1. Click **OpenManage Enterprise** > **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 tasks

OpenManage Mobile settings on page 167

Related information

OpenManage Mobile settings on page 167
Delete an OpenManage Mobile subscriber on page 168

Delete an OpenManage Mobile subscriber

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.

NOTE: The administrator rights are required for deleting an OpenManage Mobile subscriber.

To delete an OpenManage Mobile subscriber:

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

Related tasks

Enable or disable alert notifications for OpenManage Mobile on page 167
Enable or disable OpenManage Mobile subscribers on page 167
Delete an OpenManage Mobile subscriber on page 168
View the alert notification service status on page 168

Related information

OpenManage Mobile settings on page 167
Delete an OpenManage Mobile subscriber on page 168

View the alert notification service status

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 tasks

View the alert notification service status on page 168

Related information

OpenManage Mobile settings on page 167
Delete an OpenManage Mobile subscriber on page 168

View the alert notification service status on page 168

Notification service status

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

Table 29. Notification service status

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

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, in OpenManage Enterprise, 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

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

Table 30. 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.

Table 30. OpenManage Mobile subscriber information (continued)

Field	Description
LAST PUSH	The date and time the last alert notification was sent successfully from OpenManage Enterprise to the Alert Forwarding Service.
LAST CONNECTION	The date and time the user last accessed OpenManage Enterprise through OpenManage Mobile.
REGISTRATION	The date and time the user added OpenManage Enterprise in OpenManage Mobile.

Troubleshooting OpenManage Mobile

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

Table 31. 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 tasks

OpenManage Mobile settings on page 167

Related information

OpenManage Mobile settings on page 167

21

Other references and field descriptions

Definitions about some of the commonly displayed fields on the OpenManage Enterprise Graphical User Interface (GUI) are listed and defined in this chapter. Also, other information that is useful for further reference is described here.

Topics:

Schedule Reference

- **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

- **COMPLIANCE**: The health status of the firmware baseline. Even if one device associated with a firmware baseline is in critical health status, the baseline health itself is declared as critical. This is called the rollup health status, which is equal to the status of the baseline that has high severity. For more information about Rollup Health status, see the *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* white paper on the Dell TechCenter.
- **NAME**: The firmware baseline name. Click to view the baseline compliance report on the **Compliance Report** page. For more information about creating a firmware baseline, see Create a firmware/driver baseline on page 76.
- **CATALOG**: The firmware catalog to which the firmware baseline belongs to. See Manage firmware and driver Catalogs on page 73.
- **LAST RUN TIME**: The time when the baseline compliance report is last run. See Check the compliance of a device firmware and driver on page 77.

Schedule job field definitions

- **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.

Alert categories after EEMI relocation

Table of EEMI relocations

Table 32. Alert categories in OpenManage Enterprise

Previous Category	Previous Subcategory	New Category	New Subcategory
Audit	Devices	System Health	Devices
Audit	Devices	Configuration	Devices
Audit	Devices	Configuration	Devices
Audit	Devices	Configuration	Devices
Audit	Devices	Configuration	Devices
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Devices	Audit	Users
Audit	Templates	Configuration	Templates
Audit	Templates	Configuration	Templates
Audit	Templates	Configuration	Templates
Audit	Templates	Configuration	Templates
Audit	Templates	Configuration	Templates
Configuration	Inventory	Configuration	Job
Configuration	Inventory	Configuration	Job
Configuration	Inventory	Configuration	Job
Configuration	Inventory	Configuration	Devices
Configuration	Inventory	Configuration	Devices
Configuration	Inventory	Configuration	Devices
Configuration	Firmware	Configuration	Jobs
Configuration	Firmware	Configuration	Jobs
Miscellaneous	Jobs	Configuration	Jobs
Miscellaneous	Jobs	Configuration	Jobs
Miscellaneous	Jobs	Configuration	Jobs
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic
Miscellaneous	Generic	Configuration	Generic

Table 32. Alert categories in OpenManage Enterprise (continued)

Previous Category	Previous Subcategory	New Category	New Subcategory
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 use of tokens to enhance remote scripting and creation of the alert policies.

Table 33. 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

Field service debug workflow

In OpenManage Enterprise, you can authorize console debugging by using the Field Service Debug (FSD) option.

By using FSD, you can perform the following tasks:

- Allow enabling and copying of debug logs
- Allow copying of real-time logs
- Allow backing up or restoring of database to VM.

The topics referenced in each task provide detailed instructions. To enable FSD, perform the following tasks:

1. Unblock FSD capability. See Unblock the FSD capability on page 175.
2. Install or grant signed FSD DAT.ini file. See Install or grant a signed FSD DAT.ini file on page 175.
3. Invoke FSD. See Invoke FSD on page 175.
4. Disable FSD. See Disable FSD on page 176.

Unblock the FSD capability

You can unblock the FSD capability through the TUI screen.

1. Navigate to the TUI main menu.
2. On the TUI screen, to use the FSD option, select **Enable Field Service Debug (FSD) Mode**.
3. To generate a new FSD unblock request, on the **FSD Functions** screen, select **Unblock FSD Capabilities**
4. To determine the duration of the debug capabilities being requested, select a start and end date.
5. On the **Choose Requested Debug Capabilities** screen, select a debug capability from a list of debug capabilities unique to the console. In the lower-right corner, select **Generate**.

   NOTE: The debug capability that is current supported is, `RootShell`.

6. On the **Download DAT file** screen, view the signing instructions and the URL address of the share where the DAT.ini file exists.
7. Use an external client to extract the DAT.ini file from the URL address of the share mentioned in step 6.

   NOTE: The download share directory has read-only privileges and supports only one DAT.ini file at a time.

8. Perform either of the following tasks depending on whether you are an external user or an internal Dell EMC user:
   - Send the DAT.ini file to a Dell EMC contact for signing if you are an external user.
   - Upload the DAT.ini file to appropriate Dell Field Service Debug Authentication Facility (FSDAF) and submit.
9. Wait for a Dell EMC signed and approved DAT.ini file to be returned.

Install or grant a signed FSD DAT.ini file

Ensure that you have received the DAT.ini file, which is signed and approved by Dell EMC.

NOTE: After Dell EMC approves the DAT.ini file, you must upload the file to the console appliance that generated the original unblock command.

1. To upload a signed DAT.ini file, on the **FSD Functions** screen, select **Install/Grant Signed FSD DAT File**.

   NOTE: The upload share directory has write-only privileges and supports only one DAT.ini file at a time. The DAT.ini file size limit is 4 KB.

2. On the **Upload signed DAT file** screen, follow the instructions about uploading the DAT.ini file to a given file share URL.
3. Use an external client to upload the DAT.ini file to a share location.
4. On the **Upload signed DAT file** screen, select **I have uploaded the FSD DAT file**.

If there are no errors during DAT.ini file upload, a message confirming the successful installation of the certificate is displayed. To continue, click **OK**.

The DAT.ini file upload can fail because of any of the following reasons:

- The upload share directory has insufficient disk space.
- The uploaded DAT.ini file does not correspond to the previous debug capability request.
- The signature provided by Dell EMC for the DAT.ini file is not valid.

Invoke FSD

Ensure that the DAT.ini file is signed, returned by Dell EMC, and uploaded to OpenManage Enterprise.

1. To invoke a debug capability, on the **FSD Functions** screen, select **Invoke FSD Capabilities**.
2. On the **Invoke Requested Debug Capabilities** screen, select a debug capability from a list of debug capabilities that is approved in the Dell EMC signed DAT.ini file. In the lower-right corner, click **Invoke**.

   NOTE: The debug capability that is currently supported is, `RootShell`.

While the `invoke` command is run, OpenManage Enterprise can start an SSH daemon. The external SSH client can attach with OpenManage Enterprise for debugging purposes.

Disable FSD

After you invoke a debug capability on a console, it continues to operate until the console is restarted, or the debug capability is stopped. Else, the duration determined from the start and end date exceeds.

1. To stop the debug capabilities, on the **FSD Functions** screen, select **Disable Debug Capabilities**.
2. On the **Disable Invoked Debug Capabilities** screen, select a debug capability or capabilities from a list of currently invoked debug capabilities. From the lower right corner of the screen, select **Disable**.

Ensure that you stop any SSH daemon or SSH sessions that are currently using the debug capability.

Catalog Management field definitions

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.

Firmware/driver compliance baseline reports—devices with 'Unknown' compliance status

The firmware or driver compliance status of the following storage, networking, and hyperconverged infrastructure (HCI) devices in the firmware/driver baseline compliance reports is displayed as Unknown as the Dell firmware/driver catalog does not support the firmware or software updates for these devices.

Table 34. Firmware/driver compliance baseline reports—'false' compliant devices

Device Category	Device List
Storage	• SC Series • MD Series • ME Series
Network devices in the FX2, VRTX, and M1000e chassis	• F10 switches • IOAs (Input/Output Aggregators) • IOMs (Input/Output Modules)
Hyperconverged Appliances (HCI)	• VXRail • XC Series
Devices updatable using individual device's Dell Update Package (DUP) but not directly supported on Dell catalog	• MX9116n Fabric Engine • MX5108n 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, please refer the respective device's Installation Guide.	• MX7116n Fabric Expander Module • PowerEdge MX 25GbE PTM

NOTE: For the complete list of devices in the SC, MD, ME, and XC series, refer https://topics-cdn.dell.com/pdf/dell-openmanage-enterprise_compatibility-matrix2_en-us.pdf

Generic naming convention for Dell EMC PowerEdge servers

To cover a range of server models, the PowerEdge servers are now be referred to using the generic naming convention and not their generation.

This topic explains how to identify the generation of a PowerEdge server that are referred to using the generic naming convention.

Example:

The R740 server model is a rack, two processor system from the 14th generation of servers with Intel processors. In the documentation, to refer to R740, generic naming convention **YX4X** server is used, where:

- The letter **Y** (alphabet) is used to denote the following server form factors:
  - **C** = Cloud - Modular server nodes for hyper-scale environments
  - **F** = Flexible - Hybrid rack-based sleds for rack-based FX2/FX2s enclosure
  - **M** or **MX*** = Modular - Blade servers for the modular enclosure MX7000, M1000e and/or VRTX
  - **R** = Rack-mountable servers
  - **T** = Tower Servers
- The letter **X** (digit) denotes the class (number of processors) of the server.
- The digit **4** denotes the generation of the server.
- The letter **X** (digit) denotes the make of the processor.

Table 35. PowerEdge servers naming convention and examples

YX3X servers	YX4X systems
PowerEdge M630	PowerEdge M640
PowerEdge M830	PowerEdge R440
PowerEdge T130	PowerEdge R540