Dell EMC OpenManage Enterprise Version 3.0

User's Guide

DELL EMC

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.

2018 - 09

Rev. A01

1

About Dell EMC OpenManage Enterprise

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

- Discover and manage devices in a data center environment.
- Create and manage OpenManage Enterprise users.
- Group and manage devices.
- Monitor the health of your devices.
- Manage device firmware versions and perform system updates and remote tasks.
- Create and deploy device configuration templates.
- Create and assign identity pools, and perform stateless deployment on target devices.
- Create configuration compliance baselines and remediate devices
- View and manage system alerts and alert policies.
- View hardware inventory and compliance reports.
- Monitor and report about warranty and licenses.

NOTE: 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.
- 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:

- Deploying and managing OpenManage Enterprise
- Configure OpenManage Enterprise by using Text User Interface
- Discovering devices for monitoring or management
- Managing All Devices
- Monitoring devices by using the OpenManage Enterprise dashboard
- Organize devices into groups
- Manage the device firmware
- Viewing and configuring devices
- Monitoring device alerts
- View archived alerts
- View device warranty information
- Manage device configuration templates
- Manage the device configuration compliance baseline
- Monitor device compliance with compliance templates
- Manage audit logs
- Managing OpenManage Enterprise appliance settings
- Run an inventory job now
- Manage the device warranty
- Reports
- Managing MIB files
- Role-based OpenManage Enterprise user privileges

- Directory services integration in OpenManage Enterprise

Topics:

- New in this release
- OpenManage Enterprise—Server Configuration Management License

New in this release

- You can now edit the deployment template attributes by using:
  - Guided view
  - Advanced view
- Support for discovery and inventory of MX7000 chassis—as a standalone chassis and as a lead chassis in a Multi-Chassis Management (MCM) group.
- Support for configuration compliance and remediation of MX7000 chassis.
- Ability to assign virtual identities to servers and perform stateless deployment, and support for VLAN management.
- Ability to monitor devices and remediate tasks in Dell EMC OpenManage Mobile by integrating with OpenManage Enterprise.
- Dell EMC Repository Manager can generate firmware catalogs from the OpenManage Enterprise inventory.
- Support for the following devices:
  - Latest 14th generation PowerEdge servers including the new blade servers of MX7000 chassis
  - PowerEdge FD332 storage module
  - Dell Compellent FS8600 storage device
- Support of alert policies for devices not discovered in OpenManage Enterprise.
- Support of additional remote tokens for remote script execution.
- REST API services for network configuration, identity pool creation, device template configuration, and profile management.

OpenManage Enterprise—Server Configuration Management License

NOTE: Installing and using OpenManage Enterprise does not require the *OpenManage Enterprise — Server Configuration Management* license. Only the server configuration management feature requires that the *OpenManage Enterprise — Server Configuration Management* license is installed on target servers. This license is not required for creating device configuration template from a server. The *OpenManage Enterprise — Server Configuration Management* and *OpenManage Essentials* licenses are required only for deploying device configurations and verifying configuration compliance on servers.

The *OpenManage Enterprise — Server Configuration Management* license enables you to deploy a device configuration and verify device configuration compliance on licensed servers. The 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. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **License Report**. Click **Run**. See Run reports.

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

Licensable Servers

You can deploy the *OpenManage Enterprise — Server Configuration Management* license on the following PowerEdge servers:

- 13th generation (13G) servers having the iDRAC8 2.50.50.50 or later firmware versions. 13G iDRAC versions are backward compatible to support the iDRAC7 versions (12G) also.
- 14th generation (14G) servers having the iDRAC9 3.10.10.10 or later firmware versions.

Purchasing License

You can purchase the *OpenManage Enterprise — Server Configuration Management* 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.

Verifying License Information

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

You can verify if the *OpenManage Enterprise — Server Configuration Management* 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

To view the latest version of the installed OpenManage Enterprise appliance:

- Click the **i** symbol in the upper-right corner commonly displayed on all the OpenManage Enterprise pages.
- Click **Application Settings** > **Console Update**.

NOTE: To view if any newer version of OpenManage Enterprise is available, see Check and update the OpenManage Enterprise version. Also, see the *OpenManage Enterprise Release Notes* available on the support site.

2

Security features in OpenManage Enterprise

Some of the security features of OpenManage Enterprise are:

- Role-based access that limits access to console settings and device actions.
- 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).

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: 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 can be used only till logging in to the console. Actions run on the devices require a privileged account on the device.

Related information

Deploying and managing OpenManage Enterprise

Topics:

Role-based OpenManage Enterprise user privileges

Users are assigned roles which determine their level of access to the console settings and device management features. This is termed as Role-Based Access Control (RBAC). This is a common list of RBAC for users based on their roles and OpenManage Enterprise features. However, where required, an individual task-level user RBAC list is provided in respective sections for quick reference. Therefore, the console enforces one role per account. For more information about managing users on OpenManage Enterprise, see Manage OpenManage Enterprise users.

Table 1. Role-based user privileges in OpenManage Enterprise

OpenManage Enterprise features	User levels for accessing OpenManage Enterprise		
	Admin	Device Manager	Viewer
Run reports	Y	Y	Y
View	Y	Y	Y
Manage Baseline	Y	Y	N
Configure device	Y	Y	N
Update device	Y	Y	N
Manage jobs	Y	Y	N
Create monitoring policies	Y	Y	N
Deploy OS	Y	Y	N
Power control	Y	Y	N

OpenManage Enterprise features	User levels for accessing OpenManage Enterprise		
	Admin	Device Manager	Viewer
Manage reports	Y	Y	N
Manage templates	Y	Y	N
Set up the OpenManage Enterprise appliance	Y	N	N
Manage discovery	Y	N	N
Manage groups	Y	N	N
Refresh inventory	Y	N	N
Set up security	Y	N	N
Manage traps	Y	N	N

Related tasks

Deploying and managing OpenManage Enterprise

Related reference

OpenManage Enterprise user role types

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). The Single-Sign-On (SSO) feature can be used only till logging in to the console. 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. • 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) **NOTE: DMs can share permissions to the tasks and policies created by each other. This sharing occurs by having complete overlap with the device groups contained in the task or policy, and those assigned to the DM. If the DM loses complete overlap with the groups contained in the task or policy, the DM will no longer be able to run or edit it unless this overlap is restored.**	• Get only device permissions from the admin. All other permissions are fixed. • Run tasks, policies, and other actions on the devices assigned by the administrator. • Cannot delete or modify any groups. **NOTE: Users with Device Manager (DM) privileges cannot be assigned groups.**
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.

User with this role...	Has the following user privileges
	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 DM has the same privileges as a viewer. **NOTE: A change in the user role will not affect a logged-in user. The changes become effective only after the next user login.**

NOTE: An audit log is recorded when:

- **A group is assigned or access permission is changed.**
- **User role is modified.**

Related tasks

Deploying and managing OpenManage Enterprise

Related information

Role-based OpenManage Enterprise user privileges

3

Deploying and managing OpenManage Enterprise

Dell EMC OpenManage Enterprise is provided as an appliance that you can deploy 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 OpenManage Enterprise version. 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 reference

OpenManage Enterprise user role types
Process map for checking and updating the OpenManage Enterprise version
OpenManage Enterprise Graphical User Interface overview
Security features in OpenManage Enterprise

Related information

Role-based OpenManage Enterprise user privileges

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

Table 3. 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	16 GB	16 GB
Processors	8 cores total	4 cores total
Hard drive	200 GB	20 GB

Minimum system requirements for deploying OpenManange Enterprise

Table 4. Minimum requirements

Particulars	Minimum requirements

Supported hypervisors	• VMware vSphere versions:
	  • vSphere ESXi 6.5
	  • vSphere ESXi 6.0
	  • vSphere ESXi 5.5
	• Microsoft Hyper-V supported on:
	  • Windows Server 2016
	  • Windows Server 2012 R2
	• KVM supported on:
	  • Red Hat Enterprise Linux 7.2
	  • Red Hat Enterprise Linux 7.0
	  • Red Hat Enterprise Linux 6.5

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
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-based OpenManage Enterprise user privileges.

1. Extract the .zip 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, select one of the following options:

- To allocate storage space to VMs, as required, click **Thin Provision**.
- To pre-allocate physical storage space to VMs at the time a drive is created, click **Thick provision**.

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

1. Extract the `openmanage_enterprise_vhd_format.zip` file, and then move or copy the enclosed VHD file into the appropriate location on your system where you want to store the OpenManage Enterprise (OME) virtual drive.
2. Start Hyper-V Manager in the Windows Server 2012 R2 and earlier versions. The Windows Hyper-V should be displayed under Hyper-V Manager. If not, right-click **Hyper-V Manager**, and then select **Connect to Server**.
3. Click **Action** > **New** > **Virtual Machine**.
4. On the **Specify Name and Location** page, select the VM name and a storage location appropriately for your environment.
5. Navigate to the **Specify Generation** page and select **Generation 1**. OpenManage Enterprise does not support Generation 2.

   NOTE: Ensure that 8192 MB is assigned as the memory. Dynamic memory can be turned on, but for best performance, it is recommended to leave the option 'disabled'.
6. On the **Networking Configuration** page, ensure that the network adapter is connected to the network. If set to 'Not Connected', OME will not function properly during the first reboot, and requires redeployment if this situation recurs.
7. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual disk drive**, and then go to the VHD file you copied in step 1.
8. Complete the on-screen instructions.
9. Open the settings of the newly created VM.

Deploy OpenManage Enterprise on Hyper-V 2016 host

1. Extract the `openmanage_enterprise_vhd_format.zip` file, and then move or copy the enclosed VHD file into the appropriate location on your system where you want to store the OpenManage Enterprise (OME) virtual drive.
2. Start Hyper-V Manager.
3. Select the host and select **Action** > **Import Virtual Machine**.
4. Select the folder that contains the OpenManage Enterprise virtual appliance including snapshots, virtual drives, VMs, and import files. Click **Next**.
5. On the **Select Virtual Machine** page, select the virtual machine to import (there is only one option available), and then click **Next**.
6. On the **Choose Import Type** page, select **Copy the virtual machine**, and then click **Next**.
7. On the **Choose Destination** page, retain the default values, or select the location of the VM, snapshot, and smart paging.
8. Click **Next**.
9. On the **Choose Storage Folders** page, retain the default values or click **Browse** and select the location of virtual drives, and then click **Next**.
10. On the **Summary** page, review the options you selected on earlier pages, and then click **Finish** to deploy OpenManage Enterprise virtual appliance on the Hyper-V host.
11. After OpenManage Enterprise virtual appliance is deployed, select the OpenManage Enterprise virtual appliance, and then click **Start** under **Actions**.

    NOTE: The OpenManage Enterprise appliance file can also be deployed by using a compatible KVM environment.

Deploy OpenManage Enterprise by using Kernel-based Virtual Machine

1. Download the `openmanage_enterprise.qcow2` file into the appropriate location on your system where you want to store the OpenManage Enterprise (OME) virtual drive.

2. Install Kernel-based Virtual Machine (KVM) by running the following command on any Linux system:

```
yum install qemu-kvm python-virtinst virt-manager \
```

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 8192 MB 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.

4

Getting 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.

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. To discover the devices, click **Discover Devices**.

NOTE: If incorrect OpenManage Enterprise login credentials are entered, your OpenManage Enterprise account is locked and you will not be able to log in until completing the lockdown period. By default, the lockdown duration is 900 seconds. To change this duration, see Set the login security properties.

Configure OpenManage Enterprise by using Text User Interface

The Text User Interface (TUI) tool provides you a text interface to change the admin password, view appliance status and network configuration, configure networking parameters, and enable field service debug request.

NOTE: To navigate on the TUI interface, use the arrow keys or press Tab to step forward, and press Shift + Tab to step back through the options. Press Enter to select an option. The Space bar toggles the status of a check box.

1. Before logging in to the TUI, accept EULA when prompted.
   a) On the **Change admin password** screen, enter the new password and confirm the password.

      NOTE: For the first time, you must change the password by using the TUI screen.

   b) Use the arrow keys or press **Tab** to select **Apply**.
   c) On the confirmation screen, select **Yes**, and then press **Enter**.

   Now you can configure OpenManage Enterprise through the TUI. On the TUI screen, you can view the following options:

   - **Change the Admin Password**
   - **Display Current Appliance Status**
   - **Display Current Network Configuration**
   - **Set Networking Parameters**
   - **Enable Field Service Debug (FSD) Mode**
   - **Reboot the Appliance**

NOTE: Possibly after running a command to restart the services, it may be observed that the TUI displays the following message: `NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439]`. This soft lockup issue likely occurs as a result of the hypervisor being overloaded. In such environments, 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.

- **Setup Debug Logging**
  - **Enable Debug Logs**
  - **Disable Debug Logs**
  - **Enable SCP Retention**
  - **Disable SCP Retention**
- **Restart Services**

2. To confirm the current appliance administrator password, select **Change the Admin Password**, and then enter the password. Press **Tab** and select **Continue**.
3. On the TUI screen:
   a) To view appliance status and the IPv4 and IPv6 statuses and addresses, select **Current Appliance Status**.
   b) To configure network interface, select **Set Networking Parameters**.
   On the **Configure Network Interface** screen, to enable IPv4, or IPv6, or both, press **Enter**. Select **Apply**.

   NOTE: If the OpenManage Enterprise appliance fails to acquire a V6 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: To perform any write operations on TUI, ensure that you type the admin password, and then configure IPv4 or IPv6.

   NOTE: To configure IPv6, ensure that it is already configured by vCenter server.

   NOTE: In an IPv6 environment, when a Router Advertisement is configured for stateless configuration of multiple IPv6 IPs on a port, iDRAC supports a maximum of 16 IPs addresses. In such a case, OpenManage Enterprise displays only the last discovered IP and uses that IP as the out-of-band interface to iDRAC.

   NOTE: 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.

   c) To enable console debug, select **Enable Field Service Debug (FSD) Mode**. See Field service debug workflow.
   d) To collect the debug logs of the application, monitoring tasks, events, and task execution history, select **Setup Debug Logging** . In addition, to collect the template .XML files, select the **Enable SCP retention** option under **Setup Debug Logging** . You can download the debug logs by clicking **Monitor** > **Audit Logs** > **Export** > **Export Console Logs** in OpenManage Enterprise.
   e) To restart OpenManage Enterprise, select **Reboot the Appliance**.

Configure OpenManage Enterprise

If you are logging in to OpenManage Enterprise for the first time, the **Welcome to OpenManage Enterprise** page is displayed. To configure the basic settings, click **Initial Settings**, and type or select the following data in the dialog box:

1. From the **Time Zone** drop-down menu, select a time zone. Click **Apply** to save the selected time zone. To set the time zone to a default value, click **Discard**. After updating the time zone, all active users are logged out of OpenManage Enterprise.
2. If you want to use the NTP Server for time synchronization, select the **Use NTP Server** check box.

   NOTE: When the NTP Server settings are updated, the currently logged in users are automatically logged out from their OpenManage Enterprise sessions.
3. Type the IP address or hostname in **Primary NTP Server Address** and **Secondary NTP Server Address** (optional) for time synchronization.
4. If you want to set proxy server for external communication, select the **Use HTTP Proxy Settings** check box.
5. In the **Server IP Address** box, enter the IP address or host name for the proxy server.
6. In the **Port** box, enter the port number for the proxy server.
7. If the proxy server requires credentials to log in, select the **Use Proxy Credentials** check box, enter the username and password.

8. Click **FINISH**.

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 5. Scalability and performance considerations of OpenManage Enterprise

Tasks	Recommended frequency of running the tasks	Tasks whether pre-canned?	Maximum devices that are recommended per task
Discovery	Once a day for environment with frequent network changes.	No	4000/task
Inventory	OpenManage Enterprise provides a pre-canned task that automatically refreshes inventory once a day.	Yes. You can disable this feature.	Device monitored by OpenManage Enterprise
Warranty	OpenManage Enterprise provides a pre-canned 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 update	Need-basis		100/task
Configuration inventory	Need-basis		50/baseline

Supported protocols and ports in OpenManage Enterprise

Supported protocols and ports on management stations

Table 6. OpenManage Enterprise supported protocols and ports on the management stations

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
21	FTP	TCP	256-bit	In/Out	To download updates from **Dell.com**.
22	SSH	TCP	256-bit	In/Out	Required for incoming only if FSD is used. OpenManage Enterprise administrator must enable only if interacting with the Dell EMC support staff.
25	SMTP	TCP	None	Out	To receive email alerts from OpenManage Enterprise.
53	DNS	UDP/TCP	None	Out	For DNS queries.
68 / 546 (IPv6)	DHCP	UDP/TCP	None	Out	Network configuration.

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
80	HTTP	TCP	None	In/Out	The Web GUI landing page. Will redirect a user to HTTPS.
111	NFS	TCP	None	In/Out	For read-only NFS share used for iDRAC firmware update.
123	NTP	TCP	None	Out	Time synchronization (if enabled).
137, 138	CIFS	UDP/TCP	None	In/Out	To upload or download device configuration templates.
139, 445	CIFS	TCP	None	In/Out	Miscellaneous Management functions.
162*	SNMP	UDP	None	In/Out	Event reception through SNMP. The direction is 'outgoing' only if using the Trap forward policy.
443 (default)	HTTPS	TCP	128-bit SSL	In/Out	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.
514	Syslog	TCP	None	Out	To receive alerts from Syslog server.
892	MOUNTD	UDP/TCP	None	In/Out	For read-only NFS share used for iDRAC firmware update.
2049	MOUNTD	UDP/TCP	None	In/Out	For read-only NFS share used for iDRAC firmware update.
3268	AD/LDAP	TCP	None	Out	LDAP login for Global Catalog.

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

Supported protocols and ports on managed nodes

Table 7. OpenManage Enterprise supported protocols and ports on the managed nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
22	SSH	TCP	256-bit	In/Out	For the Linux OS discovery only.
80	HTTP	TCP	None	In/Out	Contextual application launch — Networking console.
161	SNMP	UDP	None	In/Out	For SNMP queries.
162*	SNMP	UDP	None	In/Out	Traps to a management station.
443	Proprietary/ WS-Man/ Redfish	TCP	256-bit	In/Out	Discovery and inventory of iDRAC7 and later versions, and for the CMC management.
623	RMCP	UDP	None	In/Out	IPMI access through LAN.

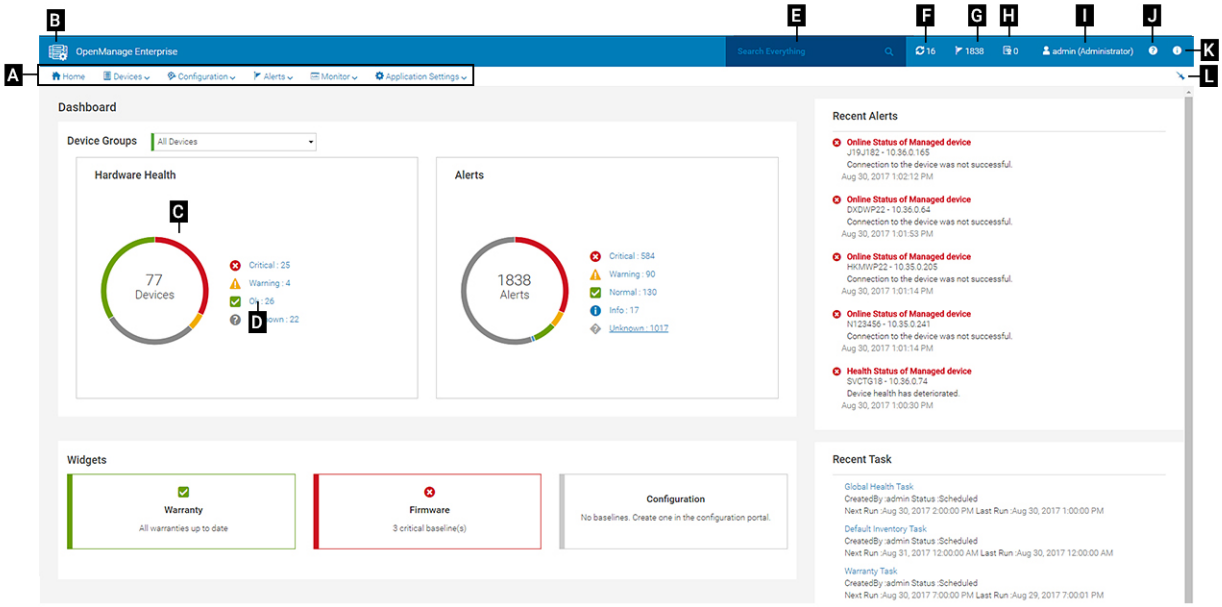
* Port can be configured up to 499 excluding the port numbers that are already allocated.

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.

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 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 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 Viewing and configuring devices.
- D—The symbols used to indicate the device health state. See Device health statuses.
- E—In the **Search Everything** box, type about anything that is monitored and displayed by OpenManage Enterprise to view the results such as device IP, job name, group name, firmware baseline, and warranty data. You cannot sort or export data retrieved by using the Search Everything feature. On individual pages or dialog boxes, type or select from the **Advance Filters** section to refine your search results.
  - The following operators are not supported: +, -, and ".
  - Text typed as search criterion is case-sensitive.
  - The following wildcard characters are not supported: `#`, `@`, `%`, `-`, `:`, `=`, `&`, `$`, `+`, `|`, `/`, `.`, `_`, `(`, and `)`.
- F—Number of OpenManage Enterprise jobs currently in the queue. Jobs related to discovery, inventory, warranty, firmware 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. Click to refresh.

- G—The number of events generated in the alerts log. Deleting the alerts reduces the count. For information about symbols used to indicate severity statuses, see Device health statuses. 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—Number of devices whose warranty status is critical and requires immediate attention. Click to view the system alerts under each category. To activate this feature, enable the warranty settings. See Managing device warranty.
- I—Username of the user who is currently logged in. Pause the pointer over the username to view the roles assigned to the user. For more information about the role-based users, see Role-based OpenManage Enterprise user privileges. 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 listed in a table can be comprehensively viewed, exported in total or based on selected items. See Export all or selected data. 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. Type 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 retrieved by using the Search Everything feature.

Symbols are used to identify major main items, dashboard, status of device health, alert category, firmware compliance status, connection state, power status, and others. Click the forward and backward button 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 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 Now**. Users with all the OpenManage Enterprise privileges (Administrator, Device Manager, and Viewer) can view the message. Only an Administrator and Device Manager 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 OpenManage Enterprise version.

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 the jobs list.

Related information

Deploying and managing OpenManage Enterprise

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 compliance, and configuration compliance statuses of all devices.

  For more information about the features under Widgets, see Monitoring devices by using the OpenManage Enterprise dashboard. The right pane lists the recent alerts and tasks generated by OpenManage Enterprise. To view more information about an alert or task, click the alert or task title. See Monitoring device alerts and Using jobs for device control.
- If an updated version of OpenManage Enterprise is available, you are immediately alerted when an update is available. To update, click **Update Now**. For more information about updating the OpenManage Enterprise version, see Check and update the OpenManage Enterprise version.
- 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 the jobs list.

Topics:

Monitoring devices by using the OpenManage Enterprise dashboard

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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 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 they can be monitored and displayed on the dashboard. To add devices, see Organize devices into groups and Discovering devices for monitoring or management.

- Manage the device firmware
- Managing device alerts
- Discovering devices
- Creating reports
- Managing OpenManage Enterprise appliance settings

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 Monitoring device alerts. 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 Viewing and configuring devices.

To filter data, click **Advanced Filters**. Export data into Excel, CSV, HTML, or PDF format. See Export all or selected data.

For more information about a Donut chart, see Donut chart and Device health statuses. To view the summary of devices in a different device group monitored by OpenManage Enterprise, select from the **Device Groups** drop-down menu. To view the 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 Viewing and configuring devices.

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. Click to view more information in the **Warranty** dialog box. See Manage device warranty by using the OpenManage Enterprise dashboard. For information about managing device warranty, see Manage the device warranty. Pause the pointer over the **Warranty** section to read definitions about the symbols used in the section.
- **Firmware**: Displays the rolledup status of firmware compliance baselines created on OpenManage Enterprise. If available, the Critical and Warning firmware 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** dialog box.
  - See Manage firmware baseline by using the OpenManage Enterprise dashboard.
  - For information about updating a firmware, creating firmware catalog, creating firmware baseline, and generating baseline compliance report, see Manage the device firmware.
- **Configuration**: Displays the rolledup status of configuration compliance baselines created on OpenManage Enterprise. If available, the Critical and Warning configuration baselines are listed. See Monitor device compliance with compliance templates.

Manage firmware baseline by using the OpenManage Enterprise dashboard

On the OpenManage Enterprise dashboard page, in the **Widgets** section, the **Firmware** section displays the number of firmware baselines that have one or more devices in critical health status. See Device health statuses. For more information about firmware management, see Manage the device firmware.

To view a list of baselines, click **Firmware**. For definitions about fields in the **Firmware** dialog box, see Firmware baseline field definitions.

Manage device warranty by using the OpenManage Enterprise dashboard

On the OpenManage Enterprise dashboard page, in the **Widgets** section, the **Warranty** section displays the number of devices whose warranty is about to expire or has already expired. For more information about managing device warranty, see Manage the device warranty.

To view a list of warranties that are about to expire, click **Warranty**. In the **Warranty** dialog box, along with the Service Tag, the following information is displayed:

- The Service Tag, model name, and model type of a device.
- **WARRANTY TYPE**:
  - Initial: The warranty is still valid by using the Warranty provided when OpenManage Enterprise was first purchased.
  - Extended: The warranty is extended because the Warranty duration provided when OpenManage Enterprise was first purchased 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.

Manage the device compliance baseline by using the OpenManage Enterprise dashboard

On the OpenManage Enterprise dashboard page, in the **Widgets** section, the **Configuration** section displays the number of configuration compliance baselines that do not comply with the properties of the template it is compared against.

To view a list of configuration compliance baselines that drift from the template properties, click **Configuration**. In the **Configuration** dialog box:

- **COMPLIANCE** indicates the level to which the configuration compliance baseline drifts.
- **TEMPLATE NAME** indicates the compliance baseline template against which the baseline is compared.

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

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 Viewing and configuring devices.

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.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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 EMC Compellent 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.

  NOTE: The Discovery Group feature is not supported in OpenManage Enterprise 3.0 and later versions. If you have created Discovery Groups in OpenManage Enterprise-Tech Release and upgraded to OpenManage Enterprise 3.0, all the associated data is removed after the update, and the associated jobs and tasks are not run.

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

Custom Groups: Created by the user 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 be mixed.**
- **Cannot have more than one parent group. Meaning, a group cannot be added as a sub-group under its parent group.**

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 or edit a Static device group and Create a Query device group.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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.

Related tasks

Delete devices from OpenManage Enterprise
Refresh the device inventory
Refresh the device status

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. 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 Monitoring device alerts.
- The firmware version compliance of a device against the version on the catalog: See Manage the device firmware.
- The configuration compliance baseline of devices and device groups: See Manage the device configuration compliance baseline.

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 8. 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

Managing All Devices

By clicking **OpenManage Enterprise** > **Devices** > **All Devices** you can view the devices and device groups managed by OpenManage Enterprise. The System groups are default groups created by OpenManage Enterprise when shipped, and Custom groups are created by users such as administrators and device managers. You can create child groups under these two parent groups. For information about the parent-child rules, see Device Groups. In the working pane, a Donut chart graphically displays the health and number of devices in the group selected in the left pane. For more information about Donut chart, see Donut chart.

The table after the Donut chart lists the properties of device(s) selected in the left pane. To view properties of a device and edit the configuration, click the device name or IP address in the list. For more information about the device list, see Device list.

NOTE: After you upgrade OpenManage Enterprise to the latest version, the devices list will be updated after the discovery jobs are rerun.

NOTE: In the Devices list, click the device name to view device configuration data, and then edit. To log in to the management application installed on the device (say, iDRAC), click the IP address. See Viewing and configuring devices.

NOTE: 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 the Devices <device name> page.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

You can select a maximum of 25 devices per page and navigate the pages to select more devices and perform tasks. You can perform the following device-related tasks:

- Create new group and add devices. See Adding devices to new group and Adding devices to existing group.
- Delete a device from OpenManage Enterprise. See Delete devices from OpenManage Enterprise.
- Exclude a device from OpenManage Enterprise monitoring. See Exclude devices from OpenManage Enterprise.
- Update the firmware version of a device. See Updating the device firmware version.
- Update the hardware and software inventory of selected devices. See Refreshing device inventory.
- Collect the latest working status of selected device(s).
- Onboard devices. See Onboarding devices.
- Export the items in a device group list to PDF, HTML, or CSV format. See Exporting device group inventory.
- Export data about selected or all devices from the More Actions tab. See Exporting data.
- View complete information and manage a device. See Viewing and configuring devices.
- Start the iDRAC with Lifecycle Controller management application. See Starting Management application (iDRAC) of a device.
- Start the virtual console. See Start the Virtual Console.

For device group-related tasks, see Organize devices into groups.

In the upper-right corner, in the **QUICK LINKS** section, use the quick links to the following features of OpenManage Enterprise:

- Discovering devices
- Running inventory schedule job now
- Globally excluding device(s) from discovery results

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. To clear selections, click **Clear Selection**.

NOTE: For more information about specific events and errors that are displayed on the GUI or stored in the log for information purposes, see the latest *Event and Error Message Reference Guide for Dell EMC PowerEdge Servers* available on the support site.

Topics:

- Organize devices into groups
- Viewing and configuring devices
- Start Management application iDRAC of a device

- Start the Virtual Console

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 Viewing and configuring devices.

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.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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 EMC Compellent 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.

  NOTE: The Discovery Group feature is not supported in OpenManage Enterprise 3.0 and later versions. If you have created Discovery Groups in OpenManage Enterprise-Tech Release and upgraded to OpenManage Enterprise 3.0, all the associated data is removed after the update, and the associated jobs and tasks are not run.

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

Custom Groups: Created by the user 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 be mixed.**
- **Cannot have more than one parent group. Meaning, a group cannot be added as a sub-group under its parent group.**

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 or edit a Static device group and Create a Query device group.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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.

Related tasks

Delete devices from OpenManage Enterprise
Refresh the device inventory
Refresh the device status

Create or edit a Static device group

On the All Devices page, you can create or edit child groups under the parent Static group. To perform these tasks, you must have appropriate user privileges. See Role-based OpenManage Enterprise user privileges.

1. Right-click **Static Groups**, and then click **Create New Static Group**.
2. In the **Create Static Group Wizard** dialog box, enter the group name, 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 **Finish**.
   The group is created and listed under the parent group in the left pane. The child groups are indented from its parent group.

   NOTE: You cannot add devices directly under Static Groups. You must create child Static groups, and then add devices under the child groups.

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 group is updated.

Create a Query device group

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

1. Right-click **Query Groups**, and then click **Create New Query Group**.
   For definitions about Static or Query (Dynamic) groups, see Organize devices into groups.
2. In the **Create Query Group Wizard** dialog box, enter the group name.

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.
5. Click **Finish**.
   The query group is created and listed in line with the parent group in the left pane.

   NOTE: You cannot add devices directly under Query Groups. You must create child Query groups, and then add devices under the child groups.

   To edit a Query group:

   a. In the left pane, right-click the child Query group and click **Edit**.
   b. Alternately, click the child Query group in the left pane. The list of devices in the group is listed in the working pane. Click the **Edit** link in the gray band that appears on top of the Devices list. The **Create Query Group Wizard** dialog box is displayed.
   c. In the **Create Query Group Wizard** dialog box, type or select data as described earlier in this section.

Select a query criteria

Define filters while creating query criteria for:

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

Define the query criteria by using two options:

- **Select existing query to copy**: By default, OpenManage Enterprise provides a list of built-in query templates that you can copy and build your own query criteria. The number of filters predefined for every existing query varies based on the query type. For example, the query for **Hypervisor Systems** has 6 predefined filters, while the query for **Networking Switches** has only three. A maximum of 20 criteria (filters) can be defined 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 Manage audit logs.

Related information

Manage the device configuration compliance baseline
Edit a configuration compliance baseline
Remove a configuration compliance baseline

Adding or editing devices in a Static child group

By using the Static child groups, you can classify your servers based on their use, configuration, department of use, customers, and so on. You can add or remove devices to the child groups, and then edit, remove, delete, and clone such groups.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

1. Right-click the Static child group, and then click **Add Devices**. For definitions about Static groups, see Organize devices into groups.
2. In the **Add Devices to Group <name>** dialog box, select the check boxes of devices that must be added to the group. The selected devices are displayed under the **All Selected Devices** tab.
3. Click **Finish**.
   The devices are added to the selected Static child group and displayed in the right pane.

To edit the properties of the Static child group, or remove devices from the Static child group:

1. Right-click the Static group, and then click **Edit**.
2. In the **Edit Devices to Group <name>** dialog box, edit the group properties, and then click **Next**.
3. In the **Group Member Selection** dialog box, select or clear the check boxes of devices that must be added or removed from the group. The selected devices are displayed under the **All Selected Devices** tab.
4. Click **Finish**. The devices are added to or removed from the selected Static child group.

NOTE: This procedure is applicable only for modifying the device properties in a group. To remove a device from OpenManage Enterprise or globally exclude a device, see Delete devices from OpenManage Enterprise and Globally excluding devices.

Rename child groups of Static or Query Dynamic groups

1. Right-click the Static or Query group, and then click **Rename**.
   For definitions about Static or Query (Dynamic) groups, see Organize devices into groups.
2. In the **Rename Group** dialog box, enter the group name, and then click **Finish**.
   The updated name is listed in the left pane.

Clone a Static or Query Group

By using the Static or Query groups, you can classify your servers based on their use, configuration, department of use, customers, and so on. You can add devices to Static and Query groups, and then edit, remove, delete, and clone such groups. To clone a Static or Query group:

1. Right-click the Static or Query group, and then click **Clone**.
2. In the **Clone Group** dialog box, enter the group name, and then select a parent group under which the cloned Static or Query group must be created.
3. Click **Finish**.
   The cloned group is created and listed under the parent group in the left pane.

   NOTE: You can clone only the Custom groups. Must have the 'edit' and 'view' permissions. See Role-based OpenManage Enterprise user privileges.

   NOTE: You can add devices directly under the cloned Static or Query groups.

Add devices to a new group

1. In the working pane, select the check box corresponding to the device(s), click **Add to Group** , and then click **Add to New Group**.
   a. In the **Add Devices to New Group Wizard** dialog box, type or select data. For more information about groups, see Device Groups.
   b. To add more devices to the group, click **Next**. Else, go to step 5.
2. 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**. See Device list.
3. 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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

1. From the **OpenManage Enterprise** menu, under **Devices**, click **All Devices**.
2. In the Devices list, click the device name or IP address to view device configuration data, and then edit. See Viewing and configuring devices.
3. In the working pane, select the check box corresponding to the device(s), click **Add to Group**, and then click **Add to Existing Group**.
   a. In the **Add Devices to Existing Group** dialog box, enter or select data. For more information about groups, see Device Groups.
   b. To add more devices to the group, click **Next**. Else, go to step 5.
4. 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**. See Device list.
5. 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.

Delete devices from OpenManage Enterprise

1. In the left pane, select the device(s).
2. In the devices list, select the check box corresponding to the device(s), and then click **Delete**.
3. When prompted indicating that the device(s) will be globally excluded, click **YES**.
   The device is deleted and not anymore monitored by 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 a remote device that has been deleted, you can remove OpenManage Enterprise from the remote device.

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.

Related information

Organize devices into groups

Exclude devices from OpenManage Enterprise

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

Devices are grouped for efficient handling of repeated tasks such as firmware update, discovery, and inventory generation. However, you can exclude a device so that the excluded device does not participate in any of these activities because it is not monitored by OpenManage Enterprise. This task is similar to the global exclusion. See Globally excluding device(s) from discovery results.

1. In the left pane, select the System group or Custom group whose device must be excluded.
2. In the devices list, select the check box corresponding to the device(s), and then click **Exclude**.
3. When prompted whether or not to exclude the selected device(s), click **YES**.
   The devices are excluded, added to the global exclusion list, and not anymore monitored by OpenManage Enterprise.
4. To remove the global exclusion and make OpenManage Enterprise monitor the device again, delete it from the global exclusion range, and then rediscover.

Upgrade or downgrade device firmware by using the firmware baseline

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

You can upgrade or downgrade the firmware version of device(s) on the:

- All Devices page: Recommended for updating firmware of multiple devices. From the **Devices** menu, select **Devices**. Select the devices, click **More Actions** > **Update Firmware**.
- All Devices page: Recommended for updating firmware of a single device. From the **Devices** menu, select **Devices**. Select the device, click **View Details** > **Firmware**.
- Configuration-Firmware page: From the **Configuration** menu, select **Firmware**. Select the devices, click **Check Compliance** > **View Report**.

NOTE: When a device is connected, the firmware version, if earlier than baseline 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. In the left pane, select the group to which the device(s) belongs to. Devices associated with the group are listed. See Device list.

   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 devices list, select the check box corresponding to the device(s).
3. Click **More Actions** > **Update Firmware**.
4. In the **Update Firmware** dialog box:
   a. In the **Select Source** section:
      - From the **Baseline** drop-down menu, select the baseline that must be used for comparing and upgrading or rolling back the device firmware. A list of devices that are associated with the selected firmware baseline is displayed. The compliance level of each device is displayed in the COMPLIANCE column. Based on the compliance level, you can upgrade or downgrade the firmware version. For information about the field description on this page, see Viewing device firmware compliance report. However, when you are checking the compliance of an individual device on the View Details page, you can upgrade or roll back the firmware version. See Roll back an individual device firmware version.
        1. Select the check boxes corresponding to the devices that must be updated.
        2. Click **Next**.
      - You can upgrade or downgrade by using individual update package also. Click **Individual Package**, and then complete the on-screen instructions. Click **Next**.

   b. In the **Prerequisites** section, prerequisites if any, for the device are displayed. Click **Next**.
   c. In the **Schedule** section, select:
      - **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. You can run the job at a later time.
5. Click **Finish**. A firmware update job is created and listed in the Jobs list. See Using jobs for device control.

   NOTE: 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.

   NOTE: If you select multiple devices, only the devices that are associated with the selected baseline are listed in the table.

Select Firmware Source

In the **Select Firmware Source** tab, you can select the required baseline or individual update package to update the firmware.

Baseline	Select this option to update the baseline version of the firmware which you want to update. Select the required baseline version from the drop-down.
COMPLIANCE	Indicates the significance of the firmware update, based on the compliance status of the individual component. The possible options are:

	• OK—The current firmware version of the device or component matches the baseline defined in the catalog file. • Critical—The current firmware version of the component or device is older than the baseline defined in the catalog file. The update is essential for the proper functioning of the device or component. • Downgrade—The current firmware version of the component or device is newer than the baseline defined in the catalog file. • Warning—The current firmware version of the component or device is older than the baseline defined in the catalog file. The update is an enhancement of the device or component.
MODEL	Displays the model of the device.
SERVICE TAG	Displays the service tag of the device for which the firmware is updated.
DEVICE NAME / COMPONENTS	Displays the name of the device or component.
REBOOT REQUIRED	Indicates if the system must be restarted after the firmware is installed.
PREREQUISITES	Displays the prerequisites for the firmware update.
IMPACT ASSESSMENT	Displays a message about the impact of the firmware update.
CURRENT VERSION	Displays the version of the firmware installed.
BASELINE VERSION	Displays the baseline of the firmware stored in the baseline.
Individual package	Select this option to update the firmware from a catalog. Click **Browse** to navigate to the location where the catalog file is located.

Actions

Next	Displays the **Schedule** tab.
Cancel	Closes the wizard without saving the changes.

Roll back an individual device 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 Viewing and configuring devices. You can upgrade or roll back the firmware version of an individual device. You can roll back the firmware version of only one device at a time.

NOTE: Only the firmware that is upgraded by using the individual device update feature can be rolled back.

NOTE: 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 updated by using the iDRAC GUI is not listed here and cannot be updated. For information about creating baseline, see Create a firmware baseline.

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**.
3. From the **Baseline** drop-down menu, select the baseline to which the device belongs to.
   All the devices associated with the selected baseline are listed. For information about field description in the table, see View the device firmware compliance report.
4. Select the check box corresponding to the device whose firmware version must be rolled back which is identified by .
5. Click **Rollback Firmware**.
6. In the **Rollback Firmware** dialog box, the following information is displayed:
   - **COMPONENT NAME**: Component on the device whose firmware version is later than the baseline version.
   - **CURRENT VERSION**: Current version of the component.

- **ROLLBACK VERSION**: Suggested firmware version to which the component can be downgraded.
- **ROLLBACK SOURCE**: Click **Browse** to select a source from where the firmware version can be downloaded.

7. Click **Finish**. The firmware version is rolled back.

NOTE: Currently, the Rollback feature tracks only the version number from which the firmware is rolled back. Rollback does not consider the firmware version that is installed by using the Rollback feature (by rolling back the version).

Refresh the device inventory

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 device or group at any moment:

1. In the left pane, select the group to which the device belongs to. Devices associated to the group are listed in the Devices list.
2. Select the check box corresponding to the device, and then click **Refresh Inventory**. The job is created and listed in the Jobs list and identified as **New** in the JOB STATUS column.
   The inventory of selected device(s) is collected and stored for future retrieval and analysis. For more information about viewing the refreshed inventory data, see Viewing and configuring devices. To download a device inventory, see Export the single device inventory.

Related information

Organize devices into groups

Refresh the device status

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, and then click **Refresh Status**.
   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.

Related information

Organize devices into groups

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.

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 Managing All Devices .

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—OK, critical, and warning—are identified by respective color symbols. See Device health statuses.
- **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.
- **TYPE** indicates the type of device—Server, Chassis, Dell Storage, and Networking switch.
- **IP address** indicates the IP address of the iDRAC installed on the device.
- **ONBOARDING STATE** column indicates whether or not the device is onboarded. See Onboarding devices.

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 Viewing and configuring devices.

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.

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.
- **RACADM CLI**: Click to run a RACADM command. See Create a Remote command job for managing devices.
- **Update Firmware**: See Upgrade or downgrade device firmware by using the firmware baseline.
- **Onboarding**: See Onboarding devices.
- **Export All and Exported Selected**: See Export all or selected data.

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.
- **Stacked Members**

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, PDF, and MS-Excel.

NOTE: However, a single device inventory can be exported only into a .csv format. See Export the single device inventory.

NOTE: Only in case of reports, you can export only selected reports at a time and not all the reports. See Export selected reports.

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.

Viewing and configuring 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** > **All 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.
- 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.
- 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 Manage the device configuration compliance baseline.

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. Click the Management IP address to open the iDRAC login page.
  - **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.
  - **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 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.
  - Reset iDRAC.
  - Extract and download the SupportAssist report. See Extract and download SupportAssist reports.
- 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.
- Run a remote RACADM, and IPMI command on the device. See Run remote–RACADM and IPMI–commands on individual devices.

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.

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.

- **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.
- **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.
- **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

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

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 the jobs list. 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 14G servers, MX7000 chassis and sleds.

- On the **<Device name>** page, click **Hardware logs**. All the event and error messages generated for the device is listed. For field descriptions, see Manage audit logs.
- For a chassis, the real-time data about the hardware logs are retrieved from the chassis.
- To add a comment, click **Add Comment**.
- In the dialog box, type the comment, and then click **Save**. 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

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. 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 -U root -P calvin <command>`
4. Click **Send**.
   A job is created and displayed in the dialog box. The job is also listed on the Job Details. See View the jobs list.
5. Click **Finish**.
   The **Recent Alerts** section displays the job completion status.
   NOTE: Do not run the following RACADM commands:
   - `chassislog view -n all`
   - `chassislog view -n`
   - `getraclog`

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 Devices list.

Start the Virtual Console

The **Virtual Console** link works on the iDRAC Enterprise license of 14G servers. On the 12G and 13G servers, the link works on the 2.52.52.52 and later versions of OME Enterprise license. If the link is clicked when the current plugin version for virtual console is Active X, a message indicates prompting you to update the console to HTML 5 for better user experience. See Change the virtual console plugin type.

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.

8

Manage the device firmware

By clicking **OpenManage Enterprise** > **Configuration**, and selecting:

- **Firmware**: Manage the firmware of devices by using firmware baselines.
- **Deploy**: Create templates to define configuration compliance baseline and manage such templates.
- **Compliance**: Create device or device group configuration compliance baseline and manage device configuration. To get a quick overview of baselines that drift from the templates it is associated with, see Manage the device compliance baseline by using the OpenManage Enterprise dashboard.

NOTE: When a device is connected, the firmware version, if earlier than baseline 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.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges. To manage these settings, you must have the OpenManage Enterprise administrator level credentials.

- By using the Firmware feature, you can:
  - Create a firmware catalog by using catalogs available on Dell.com, or on the network path. See Create a firmware catalog by using Dell.com or Creating a firmware catalog by using local network. The customized firmware catalog is used for creating firmware baselines that act as a local benchmark to quickly compare the firmware version on the devices against the version in the catalog,
  - Create a firmware baseline by using the available firmware catalogs. See Creating the firmware baseline. You can view the firmware baseline report on the Dashboard also. See Manage firmware baseline by using the OpenManage Enterprise dashboard.
  - Run a compliance report to check if the devices associated with the firmware baseline comply to the baseline versions. See Checking firmware compliance. The **COMPLIANCE** column displays:
    - **OK** — A green box  with a white tick, if the target device(s) version is same as the firmware baseline.
    - **Upgrade** — A red color circle with a white multiplication symbol inside  , if the target device(s) has one or more versions earlier than the firmware baseline. See Updating the device firmware version.
    - **Downgrade** — A blue color downward arrow  , if the device firmware is later than the baseline version.
  - Export the compliance report for statistical and analytical purposes.
  - Update device firmware version by using the firmware baseline. See Upgrade or downgrade device firmware by using the firmware baseline.

NOTE: The compliance level of devices in all the available baselines is indicated by a Donut chart. When more than one device is associated with a baseline, the status of a device with the least compliance level to the baseline is indicated as the compliance level of that baseline. For example, if many devices are associated to a firmware baseline, and the compliance level of many devices is OK and Downgrade, but if the compliance of one device in the group is Upgrade, the compliance level of the baseline is indicated as Upgrade.

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 Viewing and configuring devices.

  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.

Related tasks

Delete a firmware baseline

Topics:

Manage firmware Catalogs

Catalogs are bundles of firmware based on device types. All the available catalogs (update packages) are validated and posted to Dell.com. You can create firmware baselines which downloads these catalogs and act as a local repository for your devices. This reduces the extra effort of administrators and device managers to frequently access Dell.com, and also reduces the overall updating and maintenance time. For field definitions on the Catalog Management page, see Catalog Management field definitions. The sources of catalog that you can currently access are:

- **Latest component firmware versions on Dell.com**: Lists the latest firmware 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 a catalog and optionally associated updates are saved after unpacking (locally downloading) from Dell.com or Dell Repository Manager (DRM). See Creating a firmware catalog by using local network.

  NOTE: As a part of local network catalog, you can use a single device update package stored on the local system.

Create a firmware catalog by using Dell.com

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

1. On the **Catalog Management** page, click **Add**.
2. In the **Add Firmware Catalog** dialog box:
   a) Enter the name for firmware catalog, and then select **Latest component firmware versions on Dell.com**.
   b) Click **Finish**.

   A new firmware catalog is created and listed in the Catalog table on the **Catalog Management** page.
3. To go back to the **Firmware** page, click **Back to Firmware**.

Create a firmware catalog by using local network

1. On the **Catalog Management** page, click **Add**.
2. In the **Add Firmware Catalog** dialog box:
   a) Enter a name for the firmware catalog, and then select **Network Path**.
   The **Share Type** drop-down menu is displayed.
   b) Select one of the following:

   NOTE: On the PowerEdge 12G and 13G servers that have iDRAC version 2.52.52.52 and earlier (only up to 2.50.50.50), you must enable SMBv1 for the server configuration and deployment feature to work.

   - NFS
     1. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
     2. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `nfsshare\catalog.xml`
     3. Click **Finish**.
   - CIFS
     1. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
     2. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `\Firmware\m630sa\catalog.xml`
     3. In the **Domain** box, enter the domain name of the device.
     4. In the **User Name** box, enter the user name of the device where the catalog is stored.
     5. 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

  1. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
  2. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `\M830Bharath \catalog.xml`

- HTTPS

  1. In the **Share Address** box, enter the IP address of the system where the firmware catalog is stored on the network.
  2. In the **Catalog File Path** box, enter the full file path of the catalog file location. Example path: `\M830Bharath \catalog.xml`
  3. In the **User Name** box, enter the user name of the device where the catalog is stored.
  4. In the **Password** box, enter the password of the device where the catalog is stored.
  5. 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.

3. Click **Add**.
   A new firmware catalog is created and listed in the Catalog table on the **Catalog Management** page.
4. To go back to the **Firmware** page, click **Return to Firmware**.

Related tasks

Delete a firmware catalog

SSL Certificate Information

The catalog files for firmware 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.

Edit a firmware catalog

1. On the **Catalog Management** page, select the check box corresponding to the catalog.
   The firmware catalog details are displayed in the **<catalog name>** right pane.
2. Click **Edit** in the right pane.
3. In the **Edit Firmware Catalog** dialog box, edit the properties.

   The properties that you cannot edit are grayed-out. For field definitions, see Create a firmware catalog by using Dell.com and Create a firmware catalog by using local network.
4. 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 firmware catalog

1. On the **Catalog Management** page, select the check box corresponding to the catalog, and then click **Delete**.
   The catalog file is deleted from the list.
2. To go back to the **Firmware** page, click **Back to Firmware**.

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

Related information

Create a firmware catalog by using local network

Create a firmware baseline

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

NOTE: When a device is connected, the firmware version, if earlier than baseline 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.

Baseline is a customized and locally-stored set of firmware versions that are easy to access and apply. A baseline can be applied on the basis of one baseline-to-many device, many baselines-to-one device, and many baselines-to-many devices. For example, the baseline you create for a BIOS version can be applied to many servers running the same BIOS. Similarly, you can apply two baselines to one device—say, one for the firmware version and the other for BIOS. To create a firmware baseline:

1. Under **Firmware**, click **Create Baseline**.
2. In the **Create Firmware Baseline** dialog box:
   a) In the **Baseline Information** section:
      1. From the **Catalog** drop-down menu, select a catalog.
      2. To add a catalog to this list, click **Add**. See Managing firmware Catalogs.
      3. In the **Baseline Name** box, enter a name for the baseline, and then enter the baseline description.
      4. Click **Next**.
   b) In the **Select Devices** section:
      - To select the target device(s):
        1. Select **Select Devices**, and then click the **Select Devices** button.
        2. 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.
        3. In the left pane, click the category name. Devices in that category are displayed in the working pane.
        4. 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):
        1. Select **Select Groups**, and then click the **Select Groups** button.
        2. 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.
        3. In the left pane, click the category name. Devices in that category are displayed in the working pane.
        4. 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.

Delete a firmware baseline

Under **Firmware**, a list of available firmware baselines is displayed. Select the check box corresponding to the baseline and click **Delete**. The firmware baseline is deleted and removed from the baseline list.

Check the compliance of a device firmware against its baseline

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

NOTE: When a device is connected, the firmware version, if earlier than baseline 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.

NOTE: You can view the firmware baseline report on the Dashboard also. See Manage firmware baseline by using the OpenManage Enterprise dashboard.

After you create firmware baseline, you can periodically check the compliance of firmware version of components of a device against the baseline version defined by using a catalog. To check the firmware version compliance of a device:

1. Select the check box corresponding to the baseline, and click **Check Compliance**.
   The firmware baseline compliance job is rerun.

   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.

   NOTE: When checking the firmware baseline compliance level of Dell EMC M1000e and VRTX chassis, the compliance level is indicated as 'Downgrade' even when the firmware versions are same. This is because of difference in naming convention in firmware versions between OpenManage Enterprise and FTP. It is recommended to ignore such status and not downgrade the firmware version.
2. To view the compliance report and upgrade or downgrade the firmware version of device(s), click **View Report** in the right pane.

   See Viewing device firmware compliance report.

View the device firmware compliance report

The compliance level of devices in all the available baselines is indicated by a Donut chart on the Firmware page. 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 many devices is OK and Downgrade, but if the compliance of one device in the group is Critical, the compliance level of the baseline is indicated as Critical.

However, you can view the firmware compliance of individual devices associated with a firmware baseline to either upgrade or downgrade the firmware version on that device. To view the device firmware 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.

  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 compliance levels, see Manage the device firmware.

  NOTE: When checking the firmware baseline compliance level of Dell EMC M1000e and VRTX chassis, the compliance level is indicated as 'Downgrade' even when the firmware versions are same. This is because of difference in naming convention in firmware versions between OpenManage Enterprise and FTP. It is recommended to ignore such status and not downgrade the firmware version.
- **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 firmware baseline is displayed.
  2. Select the check box(es) corresponding to the devices whose firmware compliance status is Critical and requires an update.
  3. Click **Update Firmware**. See Updating the device firmware version.
- **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 Viewing and configuring devices.
- **REBOOT REQ**: Indicates if the device must be restarted after updating the firmware.

- **Info** : Symbol corresponding to every device component is linked to the support site page from where the firmware 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 version of the device available in the firmware baseline.
- 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.

Update the device firmware version by using the baseline compliance report

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

NOTE: When a device is connected, the firmware version, if earlier than baseline 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.

After you run a firmware compliance report, if the firmware version on the device is earlier than the version on the catalog, the Compliance Report page indicates the device firmware status as Upgrade . To update a device firmware by using the baseline compliance report:

1. 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 Viewing device firmware compliance report.
2. Select the check box corresponding to the device whose firmware must be updated. You can select more than one device with similar properties.
3. Click **Update Firmware**.
4. In the **Update Firmware** dialog box, select:
   - **Update Now**: The firmware version is updated and matched to the version available on the associated catalog. To make the update 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. This mode is recommended if you do not want to disturb your current tasks.
5. Click **Update**.

   NOTE: To update a device, you must associate the device and catalog to each other.

Edit a firmware baseline

1. Select the check box corresponding to the 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** page, click **Back to Firmware**.

Delete a firmware baseline

Select the check box corresponding to the baseline, and then click **Delete**. The firmware baseline is deleted and the updated information is displayed in the Baseline list.

Related information

Manage the device firmware

9

Manage device configuration templates

By clicking **OpenManage Enterprise** > **Configuration** > **Deploy**, and selecting **Deploy**, you can set the configuration properties such as network properties, and BIOS versions of servers, and chassis by using predefined templates. Templates enable you to optimize your data center resources, Subject Matter Expert (SME) bandwidth, and reduce the cycle time in creating clones and deployments. Templates enhance your business-critical operations in converged infrastructure that uses software-defined infrastructures.

NOTE: Standard users are allowed only to view and use templates for which administrator has granted the permissions. To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role-based OpenManage Enterprise user privileges.

Topics:

View a template information

From the **OpenManage Enterprise** menu, click **Configuration** > **Deploy**. A list of available templates is displayed.

1. In the list of templates, select the check box corresponding to the device.
2. In the working pane, click **View Details**.
   On the **Template Details** page, the **Configuration Details** section displays the attributes used for creating the template. 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. Right-click an element to expand or collapse all child elements.
3. Expand the elements to view the child components:
   - To deploy the template, see Deploy device templates.
   - To edit the template, see Create a template.
   - To export template data, select the corresponding check box, and then click **Export**. See Export all or selected data.
   - To filter data in the list, click **Advanced Filters**.

Create a template

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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

1. Click **Create**, and then select **From Reference Device**.
2. In the **Create Template** dialog box:
   a) In the **Template Information** section, enter the template name and description.
   b) Select the template type:

- **Clone Reference Server**: Enables you to clone the configuration of an existing server.

  NOTE: On the PowerEdge 12G and 13G servers that have iDRAC version 2.52.52.52 and earlier (only up to 2.50.50.50), you must enable SMBv1 for the server configuration and deployment feature to work.
- **Clone Reference Chassis**: Enables you to clone the configuration of an existing chassis.

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 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.

e) In the **Configuration Elements** section, select the check boxes corresponding to the device elements that must be cloned. For creating template by using server as the device, you can select to clone the server properties such as iDRAC, BIOS, Lifecycle Controller, and Event Filters. For example, iDRAC and RAID. By default, all elements are selected.

f) Click **Finish**.

A template creation job is started and the status is displayed in the **STATUS** column. After successful creation, the job is displayed in the list. The job information is displayed on the Jobs page also.

To create by importing from an existing template file, see Create template by importing a template file. To view information about a template, select the check box, and then click **View Details** in the right pane.

Edit a template

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

- The Guided view enables you to edit the attributes such as BIOS, boot sequence, and networking. If the configuration elements are not set while creating the template, they will not be displayed during the edit mode.
- The Advanced mode enables you to edit all the available server configuration settings.

1. Select the corresponding check box, and then click **Edit**.
2. In the **Edit Template** dialog box:
   a) In the **Template Information** section, edit the template name and description. A template type cannot be edited.
   b) Click **Next**.
   c) In the **Edit Components** section, the template attributes are displayed in:
      - Guided view—Lists the BIOS, boot, and network settings of the selected template.
      - Advanced view—Lists all the properties of the selected template.

      1. 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 drown-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.
      2. 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. If permitted, select the check box to enable the Secureboot feature.
           - 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.
      3. Click **Networking**. All the networks associated with the template are displayed under **Network Interfaces**.
         - To associate an optional identity pool to the template, select from the **Identity pool** drop-down menu. The networks associated with the selected identity pool is displayed. If the template is edited in the Advanced view, the Identity pool selection is disabled for this 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 template (profile) we created earlier.
- Click **Finish**. The network settings of the template is saved.

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 template.

Create template by importing a template file

1. Click **Create** and then select **Import from File**.
2. In the **Import Template** dialog box:
   a) Enter a name for the new template.
   b) Click **Select a File**, and then select a template file.
   c) Select **Server** or **Chassis** to indicate the template type.
3. Click **Finish**. The properties of an existing template file is imported and a new template is created.

- To view information about a 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 template. See Deploy device templates and Create a template.
- To edit a template:

  1. Select the corresponding check box, and then click **Edit**.
  2. In the **Edit Template** dialog box, edit the template name, and then click **Finish**. Updated information is displayed in the list of templates.

Edit network properties

You can edit the network configuration of any template that contains applicable NIC attributes. The NIC serial number, NIC identifier, port number, and partition fields are read-only.

1. Edit the following as appropriate:
   - **Untagged Network** and **Tagged Network**: For the templates created by using modular servers, select the tagged and untagged networks.
   - **Minimum Bandwidth (%)**: The minimum bandwidth of the partition.
   - **Maximum Bandwidth (%)**: The maximum bandwidth of the partition.
2. Click **Finish**.

The updated network properties are saved.

Deploy device templates

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

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

Before you begin deploying a device deployment template, ensure that:

- You have either created a device deployment template or cloned a sample template. See Create a template.
- The target devices meet the requirements specified in Minimum system requirements for deploying OpenManange Enterprise.
- The OpenManage Enterprise license is installed on all the target devices.

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

NOTE: During deployment of a MX7000 chassis template:

- **The target device can only be the lead MX7000 chassis.**
- **If a MX7000 chassis is removed from group, it has to be rediscovered in OpenManage Enterprise.**
- **Users on the MX7000 chassis is replaced by the users configured in the template.**

- **Imported Active Directory settings will be replaced with the values in chassis profile.**

1. From the list of templates, select the check box corresponding to the template you want to deploy.
2. On the **Template Details** page, click **Deploy Template**.
3. 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.
   NOTE: OpenManage Enterprise displays a list of templates only that are recommended for the selected device.
   b) Click **Next**.
4. In the **Boot to Network ISO** section:
   a) Select the **Boot to Network ISO** check box. This check box is displayed only if the target device is a server.
   b) Select either **CIFS** or **NFS**, and then enter information in the fields such as ISO image file path and share location where the ISO image file is stored.
   c) Click **Next**.
5. In the **Schedule** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions.
6. Click **Finish**. Review the Warning message and click **YES**.
   A Device Configuration job is created under Jobs. See Using jobs for device control.

Clone templates

1. From the **OpenManage Enterprise** menu, under **Configuration**, click **Deploy**.
   A list of available 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 template, and then click **Finish**.
   The cloned template is created and displayed in the list of templates.

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 configuration 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 **Identity Pools** tab allows you to create, edit, delete, or export virtual I/O pools.

Overview of stateless deployment

To deploy a device configuration 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 device 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 device template from the **Templates** pane, and click **Edit Network** to assign an identity pool to the device template. You can also select the Tagged and Untagged network, and assign the minimum and maximum bandwidth to the ports.
4. **Deploy the device template on target devices**—Use the **Deploy Template** task under the **Deploy** tab to deploy the device template and virtual identities on the target devices.

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.

Pool Name	Enter a name of the identity pool. The pool name can have a maximum length of 255 characters.
Description	Enter a description for the identity pool. The maximum length of the description is 255 characters.

Actions

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

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 identity which is defined by the Media Access Control (MAC) address. MAC addresses are required for Ethernet (LAN) communications.
- Fibre Channel (FC) identity which is 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.
- iSCSI identity which is defined by the iSCSI Qualified Name (IQN). IQN identities are required to support boot-from-SAN by using the iSCSI protocol.

OpenManage Enterprise uses the identity pools to automatically assign virtual identities to the device template that is used for deploying a server.

Create identity pools

You can create an identity pool that contains one or more virtual identity types.

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 iSCSI MAC Addresses	Select the check box to add the iSCSI MAC addresses to the identity pool.
Starting 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.

Starting 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 MAC Address	Enter the starting 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 1-50. 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.

Define networks

1. On the **Configuration** page, click **Networks**.
2. Click **Define**.
3. In the **Define Network** dialog box, enter a name and an appropriate description.
4. Enter the VLAN ID, and then select the network type.
5. Click **Finish**.

The network currently configured in your environment is now defined and resources can access the network. You can also export the list of networks as a .csv file by clicking the **Export** button.

Edit or delete a configured network

1. On the **Configuration** page, click **Networks**.
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: As IPv6 addressing is not supported by M I/O Aggregator (IOA) and FN I/O modules, VLAN configuration on M1000e and FX2 chassis is not supported in an IPv6 infra.

   NOTE: In OpenManage Enterprise 3.0, 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**.

Stateless deployment

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

Before you perform a stateless deployment, ensure that:

- You have either created a device deployment template or cloned a sample template. See Create a template.
- You have created and configured an identity pool. See Create identity pools.
- The target devices meet the requirements specified in Minimum system requirements for deploying OpenManange Enterprise.
- The OpenManage Enterprise license is installed on all the target devices.

NOTE: Identity pools cannot be associated to templates created in earlier versions of OpenManage Enterprise.

1. From the list of templates, select the check box corresponding to the device whose template must be deployed.
2. Click **Edit Network**.
3. In the **Edit Network** dialog box, select the identity pool, and the Tagged and Untagged network.
4. Enter the maximum and minimum bandwidth and click **Finish.**
5. On the **Template Details** page, click **Deploy Template**.
6. In the **Deploy Template: <template name>** dialog box, under **Target**:

a) Click **Select**, and then select device(s) in the **Job Target** dialog box and click **Ok**. See Selecting target devices and device groups.
b) Click **Next**.

7. In the **Boot to Network ISO** section:
   a) Select the **Boot to Network ISO** check box. This check box is displayed only if the target device is a server.
   b) Select either **CIFS** or **NFS**, and then enter information in the fields such as an .ISO image file path and share location where the .ISO image file is stored.
   c) Click **Next**.
8. In the **iDRAC Management IP** section, change the target device IP settings, if required, and then click **Next**.

   NOTE: 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.
9. In the **NIC Configurations** section, click **Assign Identities**.
10. The assigned virtual identities of the NIC cards are displayed. To view all the assigned identities of the identity pool, click **View all NIC details**, and then click **Next**.
11. In the **Schedule** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions.
12. Click **Finish**. Review the message and click **YES**.
    A Device Configuration job is created under Jobs. See Using jobs for device control.

Delete identity pools

You cannot delete an identity pool if the identities are reserved or assigned to a configuration 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 templates are removed.

Reclaim assigned virtual identities

You can reclaim the assigned virtual identities from a device based on your preference.

To reclaim the assigned virtual identities:

1. On the **device name** page, under **Overview**, click **Configuration Profile** > **Reclaim identities**.
   The Reclaim Identites page is displayed.
2. If you want to continue reclaiming the assigned virtual identities of the device, click **Yes**.

   NOTE: During the reclaim process, the identities which are not deployed from OpenManage Enterprise are not reclaimed and the System Configuration job fails. To reclaim these identities, you must use the 'Force reclaim identities if removal fails' option.

After the identities are reclaimed, they can be associated to a different configuration template for stateless deployment tasks.

Migrate device profile

You can migrate the attributes of a device configuration template and the virtual identities of the source device to target devices. The target devices must have identical Lifecycle Controller system, iDRAC, BIOS, RAID, NIC for servers, and CMC for chassis configuration settings as that of the source device.

To migrate the profile:

1. On the **device name** page, under **Overview**, click **Configuration Profile** > **Migrate Profile**.
2. Select the target device with identical hardware configuration as the source device.

   NOTE: During the migration process, the identities which are not deployed from OpenManage Enterprise are not migrated and the System Configuration job fails. To migrate these identities, you must use the 'Force migration if the profile removal fails' option.

   CAUTION: When using the 'Force migration if the profile removal fails' option, there is a possibility of identities being duplicated if the source device is turned on.

3. Click **Migrate Profile**.
   The virtual identities are now reclaimed from the source device and assigned to the target device.

10

Manage the device configuration compliance baseline

By clicking **OpenManage Enterprise** > **Configuration** > **Compliance**, and selecting **Compliance**, you can create configuration baselines by using the built-in or user-created templates. You can create a configuration compliance baseline template from an existing deploy 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-based OpenManage Enterprise user privileges. Also see Manage the device compliance baseline by using the OpenManage Enterprise dashboard.

NOTE: After a configuration baseline is created by using a template, the summary of compliance level of each baseline is listed in a table. Each device has its own status, 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 Dell TechCenter.

NOTE: You can create configuration baseline of only the lead MX7000 chassis.

By using this feature, you can:

- Create configuration compliance baseline. See Create a configuration compliance baseline.
- Check compliance of devices or device groups against configuration compliance baseline.
- Manage compliance templates. See Monitor device compliance with compliance templates.

Use configuration compliance baseline data to set alert policies that alert you if a baseline policy is deviated. The alert is generated based on a compliance baseline that can be viewed on the dashboard page of OpenManage Enterprise. For more information about setting the alert policies, see Monitoring device alerts.

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 last time a configuration inventory report is run to check the compliance level of this baseline.

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.

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

Related tasks

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

Topics:

Create a configuration compliance baseline

OpenManage Enterprise can assign 10 baselines to a single device and check the compliance level of maximum 500 devices at a time. To view the list of baselines, click **OpenManage Enterprise** > **Configuration** > **Compliance**.

You can create a configuration compliance baseline by:

- Using an existing deployment template. See Manage the device configuration compliance baseline.
- Using a template captured from a support device. See Create a compliance baseline template from reference device.
- Using a template imported from a file. See Create a compliance baseline by importing from a file.

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.

CAUTION: If a 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. Click **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 Manage the device configuration compliance baseline.
   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.
   NOTE: Only compatible devices are listed. If you select a group, the devices that are not compatible with the baseline 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 Manage the device configuration compliance baseline.

Related information

Manage the device configuration compliance baseline
Remove a configuration compliance baseline

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 Manage the device configuration compliance baseline.

CAUTION: If a 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 baseline compliance template. Read through the Error and Event message displayed and act accordingly. For more information about error and event messages, see the *Error and Event Message Reference Guide* available on the support site.

1. Click **OpenManage Enterprise** > **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.

Related tasks

Manage compliance baseline templates
Select a query criteria

Related information

Manage the device configuration compliance baseline
Remove a configuration compliance baseline

Remediate noncompliant devices

You can remediate the devices which are not conforming to the associated baseline by changing the attribute values to match with the associated baseline attributes. To view the drifted attributes, from the device compliance report, click **View Report**. The Compliance Details table lists the attribute names with the expected and current values of the attributes.

To remediate one or more noncompliant devices:

1. Click **OpenManage Enterprise** > **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.

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 Manage the device configuration compliance baseline.

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 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 **OpenManage Enterprise** > **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
Select a query criteria
Manage compliance baseline templates
Edit a configuration compliance baseline

Related information

Manage the device configuration compliance baseline

11

Monitor device compliance with compliance templates

Use compliance template to create compliance baselines and then periodically check the configuration compliance status of devices associated with the baseline. See Manage the device configuration compliance baseline. You can create baseline templates by using deployment template, reference device, importing from a file. See Manage compliance baseline templates.

By clicking **OpenManage Enterprise** > **Configuration** > **Compliance**, you can view the **Overall Compliance Summary** page, where the **Template Management** tab enables you to manage the templates used to create configuration compliance baselines.

Related tasks

Manage compliance baseline templates
Clone a compliance baseline template

Topics:

- Manage compliance baseline templates

Manage compliance baseline templates

You can create baseline templates by using deployment template, reference device, or by importing from a file.

By clicking **OpenManage Enterprise** > **Configuration** > **Compliance** > **Template Management**, you can view the list of compliance templates. On this page:

- You can create compliance template by:
  - Using a deployment template. See Create a compliance baseline template from deployment template.
  - Using a reference device. See Create a compliance baseline template from reference device.
  - Importing from a template file. See Create a compliance baseline by importing from a file.
- Edit a compliance template. See Edit a baseline compliance template.
- Clone a compliance template. See Clone a compliance baseline template.
- 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.
- Delete a compliance template. On the **Compliance Templates** page, select the corresponding check box, and then click **Delete**.

Related information

Manage the device configuration compliance baseline
Edit a configuration compliance baseline
Remove a configuration compliance baseline
Monitor device compliance with compliance templates
Create a compliance baseline template from deployment template
Edit a baseline compliance template

Create a compliance baseline template from deployment template

1. Click **Configuration** > **Compliance** > **Template Management** > **Create** > **From Deploy Template**.
2. In the **Clone Deployment Template** dialog box, from the **Template** drop-down menu, select a template that must be used as the baseline for the new template.

3. Enter a name for the baseline compliance template.
4. Click **Finish**.
   A compliance template is created and listed in the list of configuration compliance baselines.

Related tasks

Manage compliance baseline templates
Clone a compliance baseline template

Create a compliance baseline template from reference device

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

1. Click **Configuration** > **Compliance** > **Template Management** > **Create** > **From Reference Device**.
2. In the **Create Compliance Template** dialog box, enter a name for the baseline compliance template.
3. Select the options to create the 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 master for creating the template. See Select target devices and device groups.
   a) If you select 'server' as the master, also select the server configuration properties that must be cloned.
6. Click **Finish**.
   A template creation job is created and run. The newly created compliance baseline template is listed on the **Compliance Templates** page.

Create a compliance baseline by importing from a file

1. Click **Configuration** > **Compliance** > **Template Management** > **Create** > **Import from File**.
2. In the **Import Compliance Template** dialog box, enter a name for the baseline 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 configuration compliance baseline is created and listed.

Clone a compliance baseline template

1. Click **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 template.
4. Click **Finish**.
   The new template is created and listed under **Compliance Templates**.

Related information

Monitor device compliance with compliance templates
Create a compliance baseline template from deployment template
Edit a baseline compliance template

Edit a baseline compliance template

When you want to edit the configuration baseline properties, you can edit the properties of the template linked to it.

CAUTION: If a 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.

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 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 **Finish**.
   The template is edited and the updated information is saved.

Related tasks

Manage compliance baseline templates

Clone a compliance baseline template

12

Monitoring device alerts

By clicking the **OpenManage Enterprise** menu, and selecting items under **Alerts**, you can:

- Manage alerts by:
  - Acknowledge alerts
  - Ignore alerts
  - View archived alerts and Download archived alerts
- Create and manage alert policies. See Alert policies.
- View alert definitions. See Alert definitions.
- Export all or selected alert data. See Exporting data.

  NOTE: Currently, only the SNMPv1 and SNMPv2 alerts are received by the OME from the following PowerEdge servers—MX740c, MX840c, and MX5016s.

NOTE: To manage these settings, you must have the OpenManage Enterprise administrator level credentials. See Role-based OpenManage Enterprise user privileges.

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.

Related concepts

View the alert logs

Related tasks

Delete alerts

Topics:

View the alert logs

Click **OpenManage Enterprise** > **Configuration** > **Alerts** > **Alert Log**. A list of alerts is displayed. The severity of alerts, time when generated, source device that generated the alert, alert category, and alert message are displayed.

- SEVERITY indicates the severity of an alert.
- ACKNOWLEDGE displays a tick mark when an alert is viewed and acknowledged. The total number of alerts generated is also displayed in the header of OpenManage Enterprise. See OpenManage Enterprise Graphical User Interface overview.
- Click the hyper-linked device name under **SOURCE NAME** to view and configure device properties that generated the alert. See Viewing and configuring devices.

  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 indicates the alert category. For example, system health and audit.

  The **ACKNOWLEDGE** column corresponding to an alert displays a tick mark when the alert is viewed and acknowledged.

On this page, you can acknowledge, unacknowledge, ignore, export, delete, and archive alert data. For more information about archiving alerts, see View archived alerts.

Related tasks

Delete alerts

Related information

Monitoring device alerts

Acknowledge alerts

After you view an alert and understand its contents, you can acknowledge that you have read through the alert message. To acknowledge, select the check box corresponding to the alert, and then click **Acknowledge**. A tick mark is displayed in the **ACKNOWLEDGE** column.

Unacknowledge alerts

You can unacknowledge an alert if incorrect or repeated. Select the check box corresponding to the alert, and then click **Unacknowledge**. The tick mark is removed corresponding to the alert in the **ACKNOWLEDGE** column. Else, you can click the tick mark to unacknowledge an already acknowledged alert message.

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.

Delete alerts

You can delete an alert to permanently remove that occurrence of the alert from the console. To prevent future occurrences of the alert from being displayed on OpenManage Enterprise, ignore the alert. See Ignore alerts.

1. Select the check box corresponding to the alert, and then click **Delete**.
   A message is displayed prompting you to confirm the deletion process.
2. Click **YES**.
   The alert is deleted.

The total number of alerts displayed in the header row of OpenManage Enterprise is decremented.

Related concepts

View the alert logs

Related information

Monitoring device alerts

View archived alerts

At a time, a maximum of 50,000 alerts can be generated and viewed by using 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 9. 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. See Download archived 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: Note: To download archived alerts, you must have necessary privileges. See Role-based OpenManage Enterprise user privileges.

Alert policies

By clicking **OpenManage Enterprise** > **Alerts** > **Alert Policies**, you can:

- Automatically trigger actions based on the input from an alert.
- Send your alerts to email address, phone, SNMP traps, and perform device power control actions such as turning on or turning off a device when an alert of a predefined category is generated.
- Create, edit, enable, disable, and delete the alert policies.

A tick mark corresponding to an alert policy indicates that the alert policy is enabled. When an alert is received that meets the policy criteria, you can configure the policy to perform actions such as sending email message and enabling SNMP trap forwarding. After prior setting, you can do the following:

- Send an email message:
  1. Click the **EMAIL** cell corresponding to the alert policy.
  2. In the **Alert Actions: Email** dialog box, type information about the message to be sent. Use the sample message pattern indicated in the text boxes.
  3. Click **Finish**. A tick mark is displayed in the cell. Email message is sent when an alert is received that meets the set policy criteria.
- Forward an SNMP trap:
  1. Click the **SNMP TRAP** cell corresponding to the alert policy.
  2. When prompted, click **YES**.
  3. Under Alerts, expand **SNMP Configuration**.
  4. Complete the tasks in Configure SMTP, SNMP, and Syslog alerts. A tick mark is displayed in the cell. An SNMP trap is activated when an alert is received that meets the set policy criteria.
- Ignore the alert policy:
  1. Click the **IGNORE** cell corresponding to the alert policy.
  2. When prompted that all actions associated with the policy will be removed, click YES**.** A tick mark is displayed in the cell. Any alert received that meets the policy criteria will be ignored.
- Send notification to a mobile device. You must set up OpenManage Enterprise and mobile phone for sending push notifications. See OpenManage Mobile settings.

1. Click the **MOBILE** cell corresponding to the alert policy. If enabled, the policy is disabled and the tick mark disappears. Vice-versa if disabled.

- Send an SMS message:
  1. Click the **SMS** cell corresponding to the alert policy.
  2. In the **Alert Actions: SMS** dialog box, type phone number.
  3. Click **Finish**. A tick mark is displayed in the cell. SMS message is sent when an alert is received that meets the set policy criteria.

     NOTE: An SMS is sent to only the US-based cell phones.
- Perform a power control action on the device:
  1. Click the **Power Control** cell corresponding to the alert policy.
  2. In the **Alert Actions: Power Control** dialog box, select to indicate if you want power cycle, turn off, or turn on a device.
  3. Click **Finish**. A tick mark is displayed in the cell. SMS message is sent when an alert is received that meets the set policy criteria.
- Run a remote script:
  1. Click the **Remote Script Execution** cell corresponding to the alert policy.

     NOTE: Because the remote script feature is supported only on the Linux servers, the SSH commands can be run only on the Linux servers but not on the Windows servers.
  2. When prompted, click **YES**.
  3. On the **Script Execution** tab, under **Remote Command Setting**, complete the tasks in Create a Remote command job for managing devices. A tick mark is displayed in the cell. The specified command is run when an alert is received that meets the set policy criteria.

Related tasks

Delete alert policies
Disable alert policies
Enable alert policies
Edit alert policies
Create alert policies

Create alert policies

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

1. Click **Alert Policies** > **Create**.
2. In the **Create Alert Policy** dialog box, in the **Name and Description** section, enter the name and description of the alert policy.
   a) To enable an alert policy by default, select the **Enable Policy** check box.
   b) Click **Next**.
3. In the **Category** section, select the **All** check box to apply the alert policy to all the available categories. By default, the following categories are displayed, but not applied. To view sub-categories under each category, expand the category:
   a) Click **Next**.
4. In the **Target** section, add devices or groups. See Select target devices and device groups.
   - To specify an undiscovered device (third-party device), select **Specific Undiscovered Devices**, and then type the IP address or host name.
   - To specify any undiscovered device, select **Any Undiscovered Devices**.

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

     NOTE: Alerts from such foreign and undiscovered devices can be ignored.

     NOTE: Alerts of SNMPv1, SNMPv2, and SNMPv3 protocols sent by such undiscovered (foreign) devices are recognized by OME.
   - Click **Next**.
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 dates on which the alert policies must be run.

b) Click **Next**.

6. In the **Severity** section, select the severity level of the alert 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 one or more check boxes to initiate the following actions when the policy is run:
   - Send email to a designated recipient by selecting the **Email** check box, and specifying data in the fields.
   - Configure SNMP alerts by clicking **Enable** next to the **SNMP Trap Forwarding** check box. In the **SNMP Configuration** dialog box, enter or select data. See Configure SMTP, SNMP, and Syslog alerts.
   - Configuring Syslog properties.
   - Select the **Ignore** check box to ignore the alert message and not activate the alert policy.
   - Send SMS to a telephone number by entering a phone number in **To**.
   - Control the power of the device by power cycling, turning on, or turn off the device. To shut down an OS before performing power control actions, select the **Shut down OS First** check box.
   - Run a remote command by clicking **Enable** next to **Remote Script Execution**:
     - In the **Remote Command Setting** dialog box, type or select information to set up the remote commands you want to run. See Execute remote commands and scripts.
     - From the drop-down menu, select the script 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.
   - **Mobile**: Send notifications to the mobile phone(s) registered with this OpenManage Enterprise version. See OpenManage Mobile settings.
8. Click **Next**.
9. In the **Summary** section, details of the alert policy you defined is displayed. Carefully read through the information.
10. Click **Finish**.
    The alert policy is successfully created and listed in the **Alert Policies** section.

Related information

Alert policies

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 destinations, and Syslog 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 then 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. Click **Apply**.
7. To reset the settings to default attributes, click **Discard**.

To configure the SNMP trap forwarding:

1. Expand **SNMP 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.
4. Select the SNMP version type from the **SNMP VERSION** drop-down menu. Currently, only SNMP1 and SNMP2 versions are supported.
5. In the **COMMUNITY STRING** box, enter the SNMP community string of the device that must receive the alert.
6. Default port number for SNMP traps=162. Edit if necessary. See Supported protocols and ports in OpenManage Enterprise.
7. To test an SNMP message, click the **Send** button of the corresponding trap.
8. Click **Apply**. To reset the settings to default attributes, click **Discard**.

To configure the Syslog messages:

1. Expand **Syslog 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.
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 to set up a policy that opens a ticket on your third party ticketing system for alert management. You can create and store only four remote commands for running immediately or at a later time.

1. Enter the following in the **Remote Command Setting** dialog box:
   a) Script name which helps you in selecting and running a correct script at a later time.
   b) IP address of the OpenManage Enterprise server that runs the command.
   c) Credentials to log in to the OpenManage Enterprise server.
   d) Command that must be run on the OpenManage Enterprise server to open a ticket. For example, `./RCE.sh $IP $MODEL $DATE $ASSETTAG $SERVICETAG`
2. Click **Save**.

   The command is saved. You can set and run these commands also while setting your alert policies. See Creating alert policies.

   NOTE:

   - **You can run only one executable or script at a time.**
   - **The executable or script can be saved on a server that is not necessarily discovered or managed by OpenManage Enterprise—not necessarily discovered by OpenManage Enterprise.**
   - **Script can have a maximum of 1024 characters.**
   - **OpenManage Enterprise supports token substitution that may be helpful to the script or ticketing system. Supported tokens: `$IP`, `$MSG`, `$HOSTNAME`, `$SEVERITY`, `$SERVICETAG`, `$RESOLUTION`, `$CATEGORY`, `$ASSETTAG`, `$DATE`, `$TIME`, and `$MODEL`.**
   - **If an invalid token type is entered, the output appears blank.**
   - **Example command: `./RCE.sh $IP $MODEL $DATE $ASSETTAG $SERVICETAG`**

Enable alert policies

You can enable an alert policy, only if disabled. Enable an alert policy while creating an alert policy by selecting the **Enable Policy** check box in the **Name and Description** section. See Create alert policies.

To enable an alert policy, select the check box corresponding to the alert policy and click **Enable**. The alert policy is enabled and the tick mark indicating that the alert policy is enabled (the **ENABLED** column) is displayed.

NOTE: You can enable 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.

NOTE: The Enable button of an alert policy that is already enabled appears grayed-out.

Related information

Alert policies

Edit alert policies

1. Select the check box corresponding to the alert policy and click **Edit**.
2. In the **Create Alert Policy** dialog box, edit the properties of the alert policy.
   For navigating through different sections in the dialog box, see Create alert policies.

Related information

Alert policies

Disable alert policies

You can disable an alert policy, only if enabled. You disable an alert policy while creating an alert policy by clearing the **Enable Policy** check box in the **Name and Description** section. See Create alert policies.

To disable an alert policy, select the check box corresponding to the alert policy and click **Disable**. The alert policy is disabled and the tick mark indicating that the alert policy is enabled (the **ENABLED** column) is removed.

NOTE: You can disable 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. However, an alert policy must have at least one action associated to it.

NOTE: The Disable button of an alert policy that is already disabled appears grayed-out.

Related information

Alert policies

Delete alert policies

To delete an alert policy, select the check box corresponding to the alert policy and click **Delete**. The alert policy is deleted and removed from the **Alert Policies** table.

NOTE: 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.

Related information

Alert policies

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.

13

Manage audit logs

Audit logs lists the actions that were performed on the devices monitored by OpenManage Enterprise. Log data help you or Dell EMC Support teams in troubleshooting and analysis. The audit log files can be exported to the CSV file format. See Export all or selected data.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

By clicking **OpenManage Enterprise** and selecting the items under **Monitor**, you can:

- Create jobs to control status of device power and device LEDs. See Using jobs for device control.
- Discover and manage devices. See Discovering devices.
- Schedule jobs to generate device inventory. See Managing device inventory.
- Create and receive alerts about device warranty. See Managing device warranty.
- Create reports about device components. See Reporting device performance.
- Manage MIBs. See Managing MIBs.

NOTE: An audit log is recorded when:

- **A group is assigned or access permission is changed.**
- **User role is modified.**

By clicking **OpenManage Enterprise** > **Monitor** > **Audit Logs**, you can manage the audit logs that OpenManage Enterprise stores and displays about the tasks performed by using the OpenManage Enterprise. For example, user login attempts, creation of alert policies, and running different jobs.

1. From the **OpenManage Enterprise** menu, under **Monitor**, select **Audit Logs**.
   a) To sort data in any of the columns, click the column title.

   On the **Monitor** page, under **Audit Logs**, a list of different activities performed is displayed with information about severity, time, user name, message ID, system IP, category, and activity description.
2. 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.
3. Enter or select data in the following fields:
   - **Severity**: Select the severity level of a log data.
   - **Start Time** and **End Time**: Select the approximate start and end time when the task was performed.
   - **User**: Enter the username of the system that performed the task.
   - **Source Address**: Enter the IP address of the system that performed the task.
   - **Category**: Select a category to which the task belongs. All messages in that category are displayed.
   - **Description Contains**: Enter the text or phrase contained in the log data your 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, all items in the list are removed and only the message ID you search for is displayed.
4. To remove the filter, click **Advanced Filters**.
5. To export the console logs as a .zip file, click **Export** > **Export Console Logs**.

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, the correct date is displayed.

To export the audit log data, see Export all or selected data.

14

Using jobs for device control

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

NOTE: Each job type is limited to devices that:

- **The user has permissions to access.**
- **Have the ability to complete the required action.**

This rule is applicable to all tasks such as blink, power control, managing firmware baselines, and managing configuration compliance baseline, where the device selection task is involved.

By clicking **OpenManage Enterprise** > **Monitor** > **Jobs**, you can:

- 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, 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 Viewing and configuring devices.
- Run job by selecting the check box corresponding to a job and clicking **Run Now**.
- Stop job by selecting the check box corresponding to a job and clicking **Stop**.
- Enable job by selecting the check box corresponding to a job and clicking **Enable**.
- Disable job by selecting the check box corresponding to a job and clicking **Disable**.
- Delete job by selecting the check box corresponding to a job and clicking **Delete**.

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 the jobs list

Click **OpenManage Enterprise** > **Monitor** > **Jobs**, to view the list of existing jobs. Information such as job status, job type, and date-time are displayed. To view more information about a job, select a job and click **View Details** in the right pane. See View an individual job information. The statuses of a job are:

- New: The job is created but not yet run. To run a job, select the corresponding check box and click **Run Now**. The job is started and the **JOB STATUS** column indicates the status as **Running**.
- Running
- Scheduled
- Completed
- Completed with errors
- Failed
- Stopped

A job belongs to any one of the following types:

- **Health**: Get the health status of a device. See Device health statuses.
- **Inventory**: Create inventory report of a device. See Managing device inventory.
- **Device Config**: Create device configuration compliance baseline. See Manage the device configuration compliance baseline.

- **Report_Task**: Create reports about devices by using inbuilt or customized data fields. See Reports.
- **Warranty**: Generate data about devices' warranty status. See Manage the device warranty.
- **Onboarding_Task**: See Onboarding devices.
- **Discovery**: Discover devices to be managed by OpenManage Enterprise. See Discovering devices for monitoring or management.

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.

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.

NOTE: By default, only the Create tab is enabled to create new jobs. However, if you select a job from the list, the tabs to run, delete, enable, stop, and disable a job are enabled.

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.

Create a job to blink device LEDs

1. Click **Create**, and then select **Blink Devices**.
2. In the **Blink Devices Wizard** dialog box:
   a) In the **Options** section:
      1. In the **Job Name** box, enter a job name.
      2. From the **Blink LED Duration** drop-down menu, select options to blink the LED for a set duration, turn on, or to turn off.
      3. Click **Next**.
   b) In the **Target** section, select the target devices and click **Next**. See Select target devices and device groups.
   c) In the **Schedule** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions.
3. Click **Finish**.
   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 job data, click **View Details** in the right pane. See View an individual job information.

Create a job for managing power devices

1. Click **Create**, and then select **Power Control Devices**.
2. In the **Power Control Devices Wizard** dialog box:
   a) In the **Options** section:
      1. Enter the job name in **Job Name**.
      2. From the **Power Options** drop-down menu, select any one of the tasks: **Power on**, **Power off**, or **Power cycle**.
      3. Click **Next**.
   b) In the **Target** section, select the target devices and click **Next**. See Select target devices and device groups.
   c) In the **Schedule** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions.

3. Click **Finish**.
   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.

Create a Remote command job for managing devices

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) In the **Arguments** box, enter the command, and then click **Next**.
   A green tick mark next to **Options** indicates that the necessary data is provided.
   NOTE: Do not run the `raclog` RACADM command in the Command Line Job Wizard dialog box. View the device hardware log data under the Hardware Logs tab.
3. In the **Target** section, select the target devices and click **Next**. See Select target devices and device groups.
4. In the **Schedule** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions.
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 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.

Change the virtual console plugin type

When the plugin used on your server is of version earlier that HTML5, a message is displayed prompting you to update the plugin type. To update, click **CHANGE TO HTML5**, and then do the following:

1. Click **Create**, and then select **Change Virtual Console Plugin on Devices**.
2. 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**.
3. In the **Job Target** section, select the target devices and click **Next**. See Select target devices and device groups.
   a) Click **Next**.
4. In the **Schedule** section, run the job immediately or schedule for a later point of time. See Schedule job field definitions.
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 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.

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**.

1. Click **Select Devices**.

In the **Job Target** dialog box, the left pane lists the devices monitored by OpenManage Enterprise. In the working pane, list of devices associated with each group, and device details are displayed. For field descriptions, see Devices list. For information about device groups, see Organize devices into groups.

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.

15

Discovering devices for monitoring or management

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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: MX7000 chassis is not discovered when you try to discover by using the OpenManage Enterprise—TechRelease version. After you upgrade to OpenManage Enterprise version 3.0, the same MX7000 chassis is discovered. However, the features available are limited. It is recommended to create a discovery task for MX7000 chassis in OpenManage Enterprise version 3.0 after the upgrade is complete.

NOTE: 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.

NOTE: 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.

By using the Discovery feature, you can:

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

Related tasks

Delete a device discovery job
View device discovery job details
Stop a device discovery job
Run a device discovery job
Specify 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 Dell storage and network switch discovery job
Create customized device discovery job protocol for SNMP devices
Specify discovery mode for creating a MULTIPLE protocol discovery job
Edit a device discovery job

Topics:

- Specify discovery mode for creating a chassis discovery job
- Specify discovery mode for creating a Dell storage and network switch discovery job
- Create customized device discovery job protocol for SNMP devices
- Specify discovery mode for creating a MULTIPLE protocol discovery job
- Delete a device discovery job
- Enable WS-Man in HTTPS mode for discovering Windows or Hyper-V servers

Create a device discovery job

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

To discover a device:

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

     WARNING: 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: If you are discovering more than 8,000 devices at a time, it is recommended that you discover them in less number of discovery jobs by entering an IP range. and thus avoid creating multiple jobs. Entering individual IP address is not recommended for discovering large number of devices.
   - To discover devices by importing ranges from the .csv file. See Specify multiple devices by importing data from the .csv file.
   - 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.
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.
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.
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.
9. 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. If you select this but do not configure SMTP, the **Finish** button is not displayed to continue the task.
10. 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.

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.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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-based OpenManage Enterprise user privileges.
   - 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 sucessfully onboarded, and the OpenManage Enterprise console is registered with the device as an alert receiver.
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.

Table 10. 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)
iDRAC6 and later	Supported	Supported	Not supported	Not supported	Not supported	Not supported
PowerEdge C*	Supported	Supported	Not supported	Not supported	Not supported	Not supported
PowerEdge chassis (CMC)	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
Storage devices	Not supported	Not supported	Supported	Not supported	Not supported	Not supported
Ethernet switches	Not supported	Not supported	Supported	Not supported	Not supported	Not supported
ESXi	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
Linux	Not supported	Not supported	Not supported	Supported	Not supported	Not supported
Windows (Hyper-V)	Supported	Not supported	Not supported	Not supported	Not supported	Not supported
Non-Dell servers	Not supported	Not supported	Not supported	Not supported	Supported	Not 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.

Related information

Discovering devices for monitoring or management

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

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

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

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.

Globally excluding devices

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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

When discovering device(s) from all the available devices, you can exclude certain device(s) from getting monitored by OpenManage Enterprise by doing the following:

1. 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.
2. Click **Add**.
3. 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.

   You can view the list of globally excluded devices by clicking:

   - **Devices** > **All Devices** > **Global Exclude**. The **Global Exclusion of Ranges** dialog box displays the list of excluded devices.
   - **Monitor** > **Discovery** > **Create** > **Global Exclude**. The **Global Exclusion of Ranges** dialog box displays the list of excluded devices.
   - **Monitor** > **Discovery** > **Global Exclusion List**. The **Global Exclusion of Ranges** dialog box displays the list of excluded devices.

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.

NOTE: 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 and chassis.
7. Schedule the discovery job. See Schedule job field definitions.
8. Click **Finish**.
   A discovery job is created and displayed in the list of discovery jobs.

Related information

Discovering devices for monitoring or management

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

In the **Additional Settings** dialog box:

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

   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 server 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.

- **Generate Trusted key**: Disabled by default. Select to generate a trusted device key for communicating with devices.

  NOTE: First time, a user must generate the trust key by using the REST API, only after which this option can be used. This key is generated per device and enables a trust relationship with the managed device.

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. Applicable only for the CMC VRTX, M1000e, and FX2 chassis. For the MX7000 chassis, the IO modules are automatically detected.
5. Select one of the following check boxes to enable discovering by using these protocols. Enter the corresponding device credentials:

   - **Enable SNMP**: For discovering SNMP-compatible devices.
   - **Enable RedFish**: For discovering servers.
   - **Enable IPMI**: For discovering servers.
   - **Enable SSH**: For discovering Linux servers.
   - **Enable VMware**: For discovering the ESXi hosts.
6. Click **Finish**.
7. Complete the tasks in Create a device discovery job.

Related information

Discovering devices for monitoring or management

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 Creating customized device discovery job template for servers and chassis.

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.

Specify discovery mode for creating a Dell storage and network switch discovery job

1. From the **Device Type** drop-down menu, select **DELL STORAGE** or **NETWORK SWTICH**.
   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 SNMP version of the device to be detected.
4. Enter the community type.
5. To create customized discovery template (for SNMP devices such as storage and networking) by clicking **Additional Settings**, see Creating customized device discovery job template for SNMP devices.
6. Complete the tasks in Create a device discovery job.

Related information

Discovering devices for monitoring or management

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.

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.
3. Click **Finish**.
4. Complete the tasks in Create a device discovery job.

Related information

Discovering devices for monitoring or management

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.

Related information

Discovering devices for monitoring or management

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

Enable WS-Man in HTTPS mode for discovering Windows or Hyper-V servers

By default, the WS-Man service is not enabled on the Windows servers. You must enable the WS-Man service on target servers in HTTPS mode.

Pre-requisites:

- IIS with HTTPS enabled
- WS-Man service with HTTPS enabled
- PowerShell 4.0 to configure the WS-Man service with certificate

Creating a Self-Sign Certificate

NOTE: If you have a publicly-signed certificate, things are easier and you can use Set-WSManQuickConfig -UseSSL. Run the following command on PowerShell by logging in as an administrator:

```
$Cert = New-SelfSignedCertificate -CertstoreLocation Cert:\LocalMachine\My -DnsName "myHost"
```

It is important to enter the name of the server that you want to manage remotely to the -DnsName parameter. If the server has a DNS name, you must use the fully qualified domain name (FQDN).

NOTE: The $Cert variable is important because it stores thumbprint for future command use.

Creating PowerShell Remoting on the host system

The Enable-PSRemoting command also starts a WS-Man listener, but only for HTTP.

```
Enable-PSRemoting -SkipNetworkProfileCheck -Force
```

1. If you do not want anyone to use HTTP to connect to the server, you can remove the HTTP listener by running the command:

   ```
   Get-ChildItem WSMan:\Localhost\listener | Where -Property Keys -eq "Transport=HTTP" |
   Remove-Item -Recurse
   ```

2. Remove all the WS-Man listeners to add the new HTTPS listener:

   ```
   Remove-Item -Path WSMan:\Localhost\listener\listener* -Recurse
   ```

3. Add your WS-Man HTTPS listener:

   ```
   New-Item -Path WSMan:\LocalHost\Listener -Transport HTTPS -Address * -
   CertificateThumbPrint $Cert.Thumbprint -Force
   ```

   NOTE: Use the $Cert variable that you defined earlier to read the Thumbprint. This variable allows the New-Item cmdlet to locate the certificate in your certificates store.

4. Add the firewall rule:

   ```
   New-NetFirewallRule -DisplayName "Windows Remote Management (HTTPS-In)" -Name "Windows
   Remote Management (HTTPS-In)" -Profile Any -LocalPort 5986 -Protocol TCP
   ```

5. Verify settings by running the following:

   ```
   C:\Windows\system32>winrm g winrm/config
   Config
       MaxEnvelopeSizekb = 500
       MaxTimeoutms = 60000
       MaxBatchItems = 32000
       MaxProviderRequests = 4294967295
       Client
           NetworkDelayms = 5000
           URLPrefix = wsman
           AllowUnencrypted = false
           Auth
               Basic = true
               Digest = true
   ```

```
            Kerberos = true
            Negotiate = true
            Certificate = true
            CredSSP = false
        DefaultPorts
            HTTP = 5985
            HTTPS = 5986
        TrustedHosts
    Service
        RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
        MaxConcurrentOperations = 4294967295
        MaxConcurrentOperationsPerUser = 1500
        EnumerationTimeoutms = 240000
        MaxConnections = 300
        MaxPacketRetrievalTimeSeconds = 120
        AllowUnencrypted = false
        Auth
            Basic = true
            Kerberos = true
            Negotiate = true
            Certificate = false
            CredSSP = false
            CbtHardeningLevel = Relaxed
        DefaultPorts
            HTTP = 5985
            HTTPS = 5986
        IPv4Filter = *
        IPv6Filter = *
        EnableCompatibilityHttpListener = false
        EnableCompatibilityHttpsListener = true
        CertificateThumbprint = 02554D694FD06BB3C765E5868EFB59B7D786ED67
        AllowRemoteAccess = true
    Winrs
        AllowRemoteShellAccess = true
        IdleTimeout = 7200000
        MaxConcurrentUsers = 2147483647
        MaxShellRunTime = 2147483647
        MaxProcessesPerShell = 2147483647
        MaxMemoryPerShellMB = 2147483647
        MaxShellsPerUser = 2147483647
```

NOTE: If `service-basic-authentication` is false, run the following command:

```
winrm set winrm/config/service/auth @{Basic="true"}
```

NOTE: In the WinRM configuration, enable HTTPS by running the command:

```
winrm set winrm/config/service @{EnableCompatibilityHttpsListener="true"}
```

6. **Enabling IIS to accept HTTPS on 443**–Run the following command on the Hyper-V server from a remote system to make sure the settings are working:

```
winrm e wmi/root/virtualization/v2/Msvm_SummaryInformation  -r:https://<hyper-v server
ip>:443/wsman -u:UserName -p:password -skipCNcheck -skipCAcheck -skipRevocationcheck -
a:Basic
```

7. Start IIS Manager.
8. In the **Site bindings over Default Website** dialog box, enter `443` as the HTTPS port number.
9. Select the SSL certificate which is created on PowerShell by logging in as an administrator.

16

Managing device inventory

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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.

Related tasks

Run an inventory job now
Stop an inventory job
Delete an inventory job
Create an inventory job

Topics:

Create an inventory job

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

1. 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.
   For information about device groups, see Organize devices into groups.
4. In the **Scheduling** section, run the job immediately or schedule for a later point of time.
   See Schedule job field definitions.
5. To generate an inventory of the configuration compliance baseline, select the **Additionally run configuration inventory** check box.
   For information about configuration compliance baselines, see Manage the device configuration compliance baseline.

6. Click **Finish**.
7. The job is created and listed in the queue.
   An inventory job is created displayed in the list of inventory jobs. The **SCHEDULE** column specifies whether the job is Scheduled or Not Scheduled. See Run an inventory job now.

Related information

Managing device inventory

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

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

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

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.
   The inventory schedule job is updated and displayed in the table.

17

Manage the device warranty

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

By clicking **OpenManage Enterprise** > **Monitor** > **Warranty**, you can view the warranty statuses of devices monitored by OpenManage Enterprise. You can export selected or all data to Excel sheet for statistical and analytical purposes. In the right pane, by clicking **Dell Warranty Renewal for Device**, you are redirected to the Dell EMC support site to enable you to manage your device warranty. On the Warranty page, along with the warranty state and Service Tag, the following information is displayed.

- The Service Tag, model name, and model type of the device.
- **WARRANTY TYPE**:
  - Initial: The warranty is still valid by using the warranty provided when OpenManage Enterprise was first purchased.
  - Extended: The warranty is extended because the warranty duration provided when OpenManage Enterprise was first purchased 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.

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.

To filter data displayed in the table, click **Advanced Filters**. See about advanced filters section in OpenManage Enterprise Graphical User Interface overview. To update data in the table, click **Refresh Warranty** in the upper-right corner. To export all or selected warranty data, click **Export**. See Export all or selected data.

Related tasks

View device warranty information

Topics:

- View device warranty information

View device warranty information

Click **OpenManage Enterprise** > **Monitor** > **Warranty**. A list of devices and their Service Tag, model, type, associated warranty, and service level information is displayed. To view a quick gist of devices whose warranty status is about to expire, see Manage device warranty by using the OpenManage Enterprise dashboard.

- For field descriptions, see Managing device warranty.
- To view warranty information of a device, select the check box corresponding to the device. The warranty information of the device is displayed in the right pane. Along with other information, service level code, service provider, and warranty start and end date are displayed.
- By clicking **Dell Warranty Renewal for Device**, you are redirected to the Dell EMC support site to enable you to manage your device warranty.
- To sort data in the table based on a column, click the column title.
- In the upper-right corner, click **Refresh Warranty** button to refresh data displayed in the warranty table.
- To search for a device, use the **Advanced Filters** option.

Related information

Manage the device warranty

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.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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

NOTE: The data displayed to you in a report depends on the privileges you have on OpenManage Enterprise. For example, when you generate a report, if you do not have permission to view a certain device group, the data about that group is not displayed to you.

Table 11. 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

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

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

Related tasks

Run reports
Run and email reports
Edit reports
Delete reports

Topics:

Run reports

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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. 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.

NOTE: It is not recommended to frequently run a report because it consumes processing and data resources.

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.

NOTE: 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 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.

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

Run and email reports

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. You can email reports to 20-30 recipients at a time. If the email address is not configured, click **Go to SMTP Settings**. For more information about setting SMTP properties, see Set SNMP Credentials.
   c) Click **Finish**.
   The report is emailed and recorded in the Audit logs.

Related information

Reports

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

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

Creating reports

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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 12. 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.
   b) Expand the **Columns** menu, and select the check boxes of the fields that must appear as the report columns. The data in these columns is populated by using the filter criteria you have defined.
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. An audit log entry is made whenever you generate, edit, delete, or copy a report definition.

Select a query criteria

Define filters while creating query criteria for:

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

Define the query criteria by using two options:

- **Select existing query to copy**: By default, OpenManage Enterprise provides a list of built-in query templates that you can copy and build your own query criteria. The number of filters predefined for every existing query varies based on the query type. For example, the query for **Hypervisor Systems** has 6 predefined filters, while the query for **Networking Switches** has only three. A maximum of 20 criteria (filters) can be defined 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 Manage audit logs.

Related information

Manage the device configuration compliance baseline
Edit a configuration compliance baseline

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 user privileges. See Role-based OpenManage Enterprise user privileges.

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
- Remove MIB files
- Resolve MIB types

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 13. Role-based access for MIB files in OpenManage Enterprise

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

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

Topics:

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

Import MIB files

Ideal process flow of MIB import: **User uploads the MIBs to OpenManage Enterprise** > **OpenManage Enterprise parses the MIBs** > **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 user privileges. See Role-based OpenManage Enterprise user privileges.

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.
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.
- 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. 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.

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.
   If the MIB type is unresolved, the **Unresolved Types** dialog box lists MIB type(s) indicating that the MIB type(s) will be imported only if resolved.
2. Click **Resolve Types**.
3. In the **Resolve Types** dialog box, click **Select Files**, and then select the missing file(s).
4. In the **Import MIB** dialog box, click **Next**. If there are still missing MIB types, the **Unresolved Types** dialog box again lists the missing MIB types. Repeat steps 1-3.
5. After all the unresolved MIB types are resolved, click **Finish**. Complete the importing process. See Import MIB files.

Download an OME MIB file

1. On the **Monitor** page, click **MIB**.
2. Expand and select an OME MIB file, and then click **Download MIB**.

   NOTE: You can download only the OME-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-based OpenManage Enterprise user privileges.

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

By clicking **OpenManage Enterprise**, 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.
- Configure emails, SNMP, and Syslog properties for alert management. See Configure SMTP, SNMP, and Syslog alerts.
- 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 OpenManage Enterprise version.
- 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.

Related tasks

Delete Directory services

Topics:

Configure OpenManage Enterprise network settings

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

NOTE: If you have more than one IP for OpenManage Enterprise by using vNIC, you must use only the IPv4 address that is indicated in the Current IP Address field (click Application Settings > Current Settings) for accessing the REST API.

Expand the **Current Settings**, **Time Configuration**, and **Proxy Configuration** links to view or edit the OpenManage Enterprise network properties.

- To only view the current network settings of OpenManage Enterprise such as DNS domain name, FQDN, and IPv4 and IPv6 settings, expand **Current Settings**.
- To configure the time zone, date, and NTP properties of OpenManage Enterprise, expand **Time Configuration**:
  a. Select or type data in the fields.
  b. Click **Apply**.
  c. To reset the settings to default attributes, click **Discard**.
- To configure the OpenManage Enterprise proxy settings, expand **Proxy Configuration**:
  a. Select the **Enable Proxy Authentication** check box to enable proxy credentials, and then enter the username and password.

     By default, the **Enable HTTP Proxy Settings** check box is cleared and fields appear grayed-out. Select to edit the data. Default proxy address=10.116.2.243. Port number=80.
  b. Click **Apply**.
  c. 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.

Manage OpenManage Enterprise users

NOTE: To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role-based OpenManage Enterprise user privileges.

NOTE: 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.

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

- View, add, enable, edit, or delete the OpenManage Enterprise users.
  NOTE: You cannot enable, disable, or delete the admin/system/root users. You can change the password by clicking Edit in the right pane.
- View details about the logged-in users, and then end (terminate) a user session.
- Manage Directory Services.
- Import and manage users from Active Directory.

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. 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 and Disable OpenManage Enterprise users.
- **ROLE**: Indicates the user role in using OpenManage Enterprise. For example, OpenManage Enterprise administrator and Device Manager. See OpenManage Enterprise user role types.

Related tasks

Delete Directory services
Delete OpenManage Enterprise users
Ending user sessions

Related reference

Disable OpenManage Enterprise users
Enable OpenManage Enterprise users

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
Delete OpenManage Enterprise users
Ending user sessions

Related information

Manage OpenManage Enterprise users

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
Delete OpenManage Enterprise users
Ending user sessions

Related information

Manage OpenManage Enterprise users

Delete OpenManage Enterprise users

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

Related reference

Disable OpenManage Enterprise users

Enable OpenManage Enterprise users

Related information

Manage OpenManage Enterprise users

Delete Directory services

Select the check box corresponding to the Directory Services to be deleted, and then click **Delete**.

Related reference

Disable OpenManage Enterprise users
Enable OpenManage Enterprise users

Related information

Managing OpenManage Enterprise appliance settings
Manage OpenManage Enterprise users

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 reference

Disable OpenManage Enterprise users
Enable OpenManage Enterprise users

Related information

Manage OpenManage Enterprise users

Role-based OpenManage Enterprise user privileges

Users are assigned roles which determine their level of access to the console settings and device management features. This is termed as Role-Based Access Control (RBAC). This is a common list of RBAC for users based on their roles and OpenManage Enterprise features. However, where required, an individual task-level user RBAC list is provided in respective sections for quick reference. Therefore, the console enforces one role per account. For more information about managing users on OpenManage Enterprise, see Manage OpenManage Enterprise users.

Table 14. Role-based user privileges in OpenManage Enterprise

OpenManage Enterprise features	User levels for accessing OpenManage Enterprise		
	Admin	Device Manager	Viewer
Run reports	Y	Y	Y
View	Y	Y	Y
Manage Baseline	Y	Y	N
Configure device	Y	Y	N
Update device	Y	Y	N
Manage jobs	Y	Y	N
Create monitoring policies	Y	Y	N

OpenManage Enterprise features	User levels for accessing OpenManage Enterprise		
	Admin	Device Manager	Viewer
Deploy OS	Y	Y	N
Power control	Y	Y	N
Manage reports	Y	Y	N
Manage templates	Y	Y	N
Set up the OpenManage Enterprise appliance	Y	N	N
Manage discovery	Y	N	N
Manage groups	Y	N	N
Refresh inventory	Y	N	N
Set up security	Y	N	N
Manage traps	Y	N	N

Related tasks

Deploying and managing OpenManage Enterprise

Related reference

OpenManage Enterprise user role types

Add and edit OpenManage Enterprise users

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

NOTE: 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.

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. For adding Directory users, see Add or edit Active Directory groups to be used with Directory Services.

1. Click **Users** > **Add**.
2. In the **Add New User** dialog box:
   a) Enter the user credentials.
      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.
   b) From the **User Role** drop-down menu, select a role:
      - **Administrator**: Has unlimited access to configure and manage all devices and device groups managed by OpenManage Enterprise. Grants access to Device Manager to manage device groups.
      - **Device Manager**: Manages OpenManage Enterprise and designated devices and groups. Administrator must assign groups before they can be managed by the Device Manager. For more information, see Role-based OpenManage Enterprise user privileges. Any number of groups can be assigned to a DM. When selected, the **Select Groups** link is displayed. Select the device group that the new user must manage. For information about selecting groups, see Select device groups for Group Manager.
      - **Viewer**: Can only view info about all the groups and devices. However, role permissions restrict the tasks a user perform on the devices.

      By default, the **Enabled** check box is selected to indicate that the user privileges currently being set up are enabled for a user.
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.

Select device groups for Group Manager

1. In the **Add New User** dialog box, from the **User Role** drop-down menu, select **Device Manager**.
   The **Select Groups** button is displayed.
2. In the **Select Device Groups** dialog box, in the left pane, select the device group that the user must be provided access to.
   Alternately, you can select a group in the left pane, and then select device(s) that the user must be provided access to.
3. Click **Finish**.
   The user is provided access to the selected device group or device(s) and a job is created in the Jobs list.

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 users.
   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.

Import AD and LDAP groups

NOTE: The users with administrator rights cannot enable or disable the Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) users.

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.
   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-based OpenManage Enterprise user privileges.
   b) Click **Assign**.
   The users in the group under the selected directory service are assigned with the selected user roles.

   NOTE: For groups assigned to the Device Manager (DM) role, the group assignment for that DM must be completed after completing these tasks by using the steps for editing a local user and assigning groups for a device manager. See Add or edit Active Directory groups to be used with Directory Services.
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, the user 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.

Directory services integration in OpenManage Enterprise

Directory Services allows you to import directory groups from AD or LDAP for use on the console. To use Directory Services:

- Add a directory connection. See Add or edit Active Directory groups to be used with Directory Services.
- Import directory groups and map all users in the group to a specific role. See Import AD and LDAP groups.
- For DM users, edit the directory group to add the groups the DM can manage. See Add and edit OpenManage Enterprise users.

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.

   a) Enter the AD directory name to be connected to.
   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, 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.
   b) Enter the network timeout and search timeout duration in seconds.
   c) To upload an SSL certificate, select **Certificate Validation** and click **Select a file**.

   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.
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.

   a) Enter the LDAP directory name to be connected to.
   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, use a comma separated list.

c) Enter the LDAP Binder Distinguished Name (DN) and password.

3. In the **Advanced Options** section:
   a) By default, LDAP port number of 636 is populated. To change, enter a port number.
   b) To match the LDAP configuration on the server, enter the group base DN to search for.
   c) Enter the user attribute to search for. If it is not configured, use UID. 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.
   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.
   f) To upload an SSL certificate, select **Certificate Validation** and click **Select a file**.

   The **Test connection** tab is enabled.
4. Click **Test connection**.
5. In the dialog box, enter the username and password of the domain to be connected to.
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.

Set the login security properties

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

NOTE: 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.

By clicking **OpenManage Enterprise** > **Application Settings** > **Security**, you can secure your OpenManage Enterprise either by specifying login IP range or login lockout policy.

- Expand **Login IP Range**:
  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 range of IP addresses separated by a comma.
  3. Click **Apply**. To reset to default properties, click **Discard**.
- 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**.

Related reference

Security Certificates

Security Certificates

By clicking **OpenManage Enterprise** > **Application Settings** > **Security** > **Certifciates**, you can view information about the currently available SLL certificate for the device.

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

To generate a Certificate Signing Request (CSR), see Generate and download the certificate signing request.

Related information

Set the login security properties

Generate and download the certificate signing request

To generate a Certificate Signing Request (CSR) for your device, and then apply for an SSL:

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**.

Manage Console preferences

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

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.

- To set the maximum number of rows (reports) that you can view on OpenManage Enterprise:
  1. Expand **Report Settings**.
  2. Enter a number in the **Reports row limit** box. Maximum rows permitted=1000.
  3. Click **Apply**. A job is run and the setting is applied.
- To set the time after which the health of devices must be automatically monitored and updated on the OpenManage Enterprise Dashboard:
  1. Expand **Device Health**.
  2. Enter the frequency at which the device health must be recorded and data stored.
  3. Select:
     - **Last Known**: Display the latest recorded device health when the power connection was lost.
     - **Unknown**: Display the latest recorded device health when the device status moved to 'unknown'. A device becomes unknown to OpenManage Enterprise when the connection with iDRAC is lost and the device is not anymore monitored by OpenManage Enterprise.
  4. Click **Apply**.
  5. To reset the settings to default attributes, click **Discard**.
- To set the mode by using which the device must be discovered. For example, DNS name and hostname:
  1. Expand **Discovery Setting**.
  2. To use DNS settings for discovering a device, select the **Prefer DNS** check box. For NetBIOS, select the **Prefer NetBIOS** check box.
  3. To use the system hostname for discovering a device, select the **Prefer System Hostname** check box.
  4. To discover a device by using the system hostname through iDRAC, select the **Prefer iDRAC Hostname** check box.

5. Expand **Advance Settings**:
   - Enter one or more invalid hostname separated by a comma in **Invalid Device Hostname**. By default, a list of invalid device hostname is populated.
   - Enter the common MAC addresses separated by a comma in **Common MAC Addresses**. By default, a list of common MAC addresses is populated.
6. Click **Apply**.
7. To reset the settings to default attributes, click **Discard**.

- Set the devices that must be displayed in the **All Devices** view.
  1. Expand **All devices View Setting**.
  2. From the **Show unknown devices** drop-down menu, select:
     - **False**: On the Dashboard page, do not display the unknown devices in the list of all devices and device groups.
     - **True**: Display the unknown devices in the list.
  3. Click **Apply**.
  4. To reset the settings to default attributes, click **Discard**.
- In the **SMB Setting** section, select the Server Message Block (SMB) version that must be used for network communication. By default, **Version2** (SMBv3) is enabled.

  NOTE: To enable SMBv1, or use features such as template deployment or Diagnostic reports, download from the Dell.com site.
- To set the address of the user who is sending an email message:
  1. Expand **Email Sender Settings**.
  2. Enter a email address and click **Apply**.
- To set the trap forwarding format:
  1. Expand **Trap Forwarding Format**.
  2. To retain the trap data as-is, select **Original Format**. To normalize, select **Normalized**.
  3. Click **Apply**.

Manage incoming alerts

NOTE: To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role-based OpenManage Enterprise user privileges.

By clicking **OpenManage Enterprise** > **Application Settings** > **Incoming Alerts**, you can define the properties of the user who receives incoming alerts by using SNMP3 protocol. You can also set the TrapForward properties.

- 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 161. 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 to OpenManage Enterprise version 3.0, you have to reconfigure the settings by providing the username, authentication passphrase, and privacy passphrase to continue receiving the alerts.

- To apply the TrapForward settings:
  1. Expand **TrapForward Settings**.

- To forward the trap, select **AS_IS**.
- To forward the normalized trap, select **Normalized**.

2. Click **Apply**.
3. To reset the settings to default attributes, click **Discard**.

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

By clicking **OpenManage Enterprise** > **Application Settings** > **Warranty Settings**, you can enable the warranty scoreboard notification which is present in the OpenManage Enterprise header by doing the following. All the parameters or settings on this page determine the logic for the count of the warranty scoreboard. By default, the user is alerted 90 days before the warranty expires. To edit the number of days:

1. Select the **Enable Warranty Scoreboard Notifications** check box.
2. To edit this value, enter in the **When Expiry less than** box. The **Warranty Expiry less than** field on the OpenManage Enterprise dashboard displays the warranties that match this criterion.
3. To send a message after the warranty expires, select the **When Warranty expired** check box. When selected, the OpenManage Enterprise dashboard (Widgets) displays the number of warranties that have expired.
4. Click **Apply**.
   To reset the settings to default attributes, click **Discard**.

   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.

Check and update the OpenManage Enterprise version

By clicking **OpenManage Enterprise** > **Application Settings** > **Console Update**, you can view the current version of your OpenManage Enterprise, check if any updated version is available, and then update the OpenManage Enterprise version. A checklist you can follow for pre and post update tasks is here: See Process map for checking and updating the OpenManage Enterprise version.

- Allocate at least an hour for the update process. Allocate additional time if the update must be downloaded by using a slower network connection.
- Ensure no device configuration tasks or deployment tasks are running or are scheduled to run during the planned downtime.
- Notify other console users of the impending scheduled update.
- Take a VM snapshot of the console as a backup in case something unexpected occurs. (Allocate additional downtime for this, if necessary).
- Select the update source:
  - Updating directly from Dell.com: Make sure the console can access Dell.com and the expected update. On the **Console Updates** page, click **Online**, and then click **Check Now**. Check for the expected target version and description of any available updates.
    NOTE: The user is automatically alerted about the availability of a new update package or Warranty information on the Home portal.
  - Updating from an internal NFS: Download the applicable files and save on a network share that can be accessed by the console. On the **Console Updates** page, click **Offline**, and then click **Check Now**. Check for the expected target version and description of any available updates.

NOTE: Not automatically connected to Dell.com. You must set up a local share and manually download the update package. An audit log is created after every manual attempt to find an update.

NOTE: Select Automatic to display information about an available updated version. Updates are automatically checked after every week. This frequency cannot be changed.

- Click **Update Now** and perform an update.
- Log in after the update and confirm that the product works as expected. Check the audit log for any warnings or errors related to the update. If any errors, export the audit log and save for tech support.

  NOTE: When you update OpenManage Enterprise-Tech Release with more than 5500 discovered devices to OpenManage Enterprise version 3.0, 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.

NOTE: Before updating to OpenManage Enterprise version 3.0, it is recommended that OpenManage Enterprise-Tech Release is configured with minimum of 16 GB memory. For more information, see Minimum recommended hardware.

NOTE: After the OpenManage Enterprise version is successfully updated, the status of the associated job on the Job Details page is displayed as Stopped. However, it implies that the actual job status is Completed.

NOTE: Currently, an audit log is not created after the OpenManage Enterprise version update process is successful or unsuccessful.

Table 15. The role-based access privileges for updating the OpenManage Enterprise version

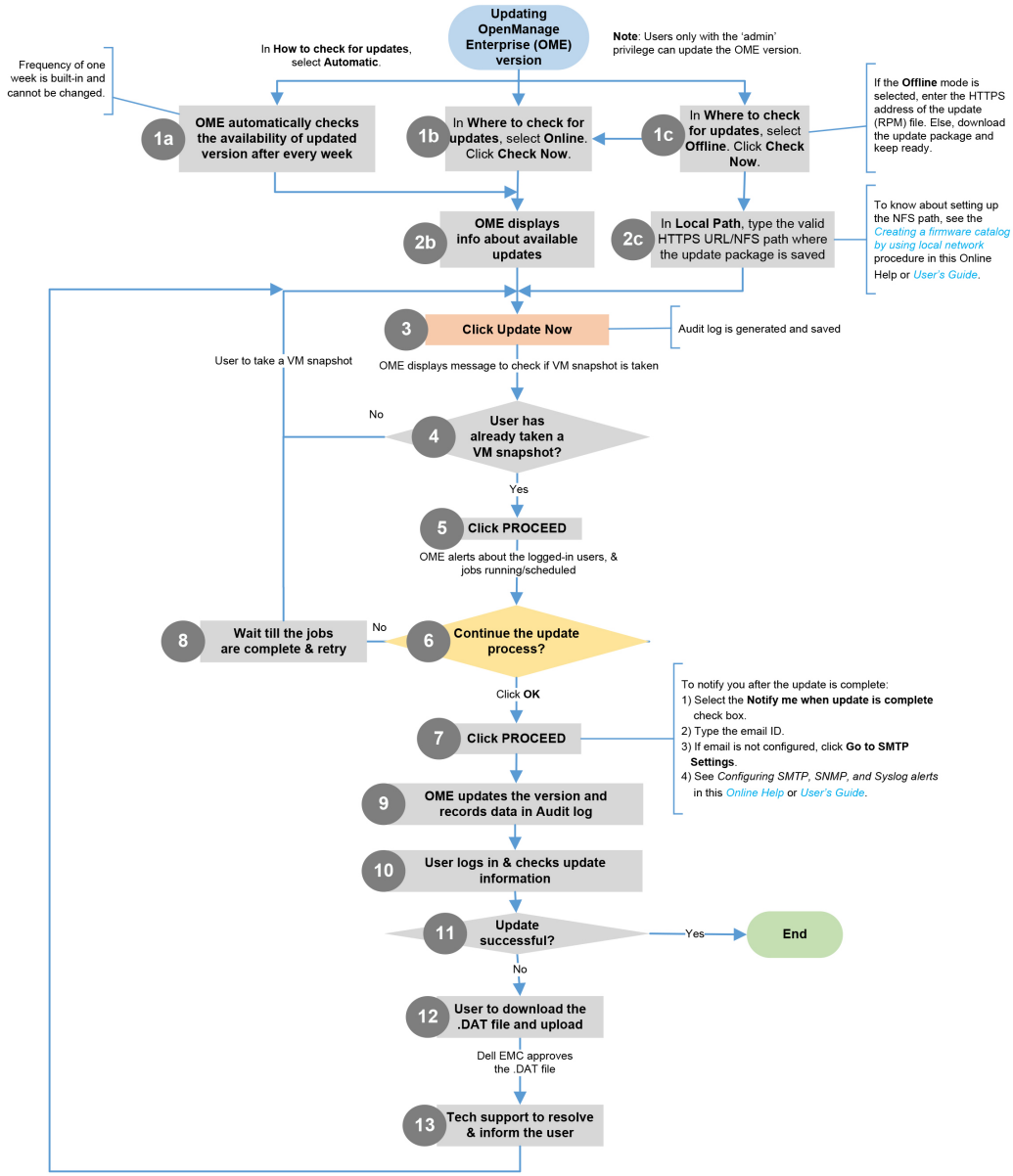
User with this role...	Can...
Administrator	View the current OpenManage Enterprise version and update the version
Device Manger and Viewer	Only view the current OpenManage Enterprise version

NOTE: If an updated version of OpenManage Enterprise is available, a message is displayed on the Dashboard. Users with all privileges (Administrator, Device Manager, and Viewer) can view the message, but only an administrator can choose to reminder later or dismiss the message.

Checking for OpenManage Enterprise VM updates

See Check and update the OpenManage Enterprise version.

Process map for checking and updating the OpenManage Enterprise version



Related information

Deploying and managing OpenManage Enterprise

Execute remote commands and scripts

When you get an SNMP trap, you can run a script on OpenManage Enterprise to set up a policy that opens a ticket on your third party ticketing system for alert management. You can create and store only four remote commands for running immediately or at a later time.

1. Enter the following in the **Remote Command Setting** dialog box:
   a) Script name which helps you in selecting and running a correct script at a later time.
   b) IP address of the OpenManage Enterprise server that runs the command.
   c) Credentials to log in to the OpenManage Enterprise server.
   d) Command that must be run on the OpenManage Enterprise server to open a ticket. For example, `./RCE.sh $IP $MODEL $DATE $ASSETTAG $SERVICETAG`

2. Click **Save**.

   The command is saved. You can set and run these commands also while setting your alert policies. See Creating alert policies.

   NOTE:

   - **You can run only one executable or script at a time.**
   - **The executable or script can be saved on a server that is not necessarily discovered or managed by OpenManage Enterprise—not necessarily discovered by OpenManage Enterprise.**
   - **Script can have a maximum of 1024 characters.**
   - **OpenManage Enterprise supports token substitution that may be helpful to the script or ticketing system. Supported tokens: `$IP`, `$MSG`, `$HOSTNAME`, `$SEVERITY`, `$SERVICETAG`, `$RESOLUTION`, `$CATEGORY`, `$ASSETTAG`, `$DATE`, `$TIME`, and `$MODEL`.**
   - **If an invalid token type is entered, the output appears blank.**
   - **Example command: `./RCE.sh $IP $MODEL $DATE $ASSETTAG $SERVICETAG`**

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
Enable or disable OpenManage Mobile subscribers
Delete an OpenManage Mobile subscriber
View the alert notification service status
Troubleshooting OpenManage Mobile

Related information

Enable or disable alert notifications for OpenManage Mobile
Enable or disable OpenManage Mobile subscribers
Troubleshooting OpenManage Mobile

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

Related information

OpenManage Mobile settings
Delete an OpenManage Mobile subscriber

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.

NOTE: 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.

NOTE: 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

Related information

OpenManage Mobile settings
Delete an OpenManage Mobile subscriber

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
Enable or disable OpenManage Mobile subscribers
Delete an OpenManage Mobile subscriber
View the alert notification service status

Related information

OpenManage Mobile settings
Delete an OpenManage Mobile subscriber

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

Related information

OpenManage Mobile settings
Delete an OpenManage Mobile subscriber
View the alert notification service status

Notification service status

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

Table 16. 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 17. 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.

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

Troubleshooting OpenManage Mobile

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

Table 18. 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.

Problem	Reason	Resolution
		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

Related information

OpenManage Mobile settings

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 baseline.
- **CATALOG**: The firmware catalog to which the firmware baseline belongs to. See Manage firmware Catalogs.
- **LAST RUN TIME**: The time when the baseline compliance report is last run. See Check the compliance of a device firmware against its baseline.

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.

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.
2. Install or grant signed FSD DAT.ini file. See Install or grant a signed FSD DAT.ini file.
3. Invoke FSD. See Invoke FSD.
4. Disable FSD. See Disable FSD.

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.

RELEASE DATE: Date when the catalog file is released for use.