Tables

1

About Dell EMC OpenManage Enterprise

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

- Discover devices in a data center environment.
- View hardware inventory and monitor health of devices.
- View and manage alerts received by the appliance and configure alert policies.
- Monitor firmware / driver versions and Manage firmware / driver updates on devices with firmware baselines.
- Manage remote tasks (such as power control) on devices.
- Manage configuration settings across devices using deployment templates.
- Manage virtual identity settings across devices using intelligent identity pools.
- Detect and remediate configuration deviations across devices using configuration baselines.
- Retrieve and monitor warranty information for devices.
- Group devices into static or dynamic groups.
- Create and manage OpenManage Enterprise users.

ⓘ NOTE:

- OpenManage Enterprise's system management and monitoring is best suited for enterprise LANs and is not recommended for usage over WANs.
- For information about supported browsers, see the *OpenManage Enterprise Support Matrix* available on the support site.

Some of the security features of OpenManage Enterprise are:

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

OpenManage Enterprise has a domain-task-based GUI, where the navigation is designed by considering the sequence of tasks that are predominately used by an administrator and device manager. When you add a device to an environment, OpenManage Enterprise automatically detects the device properties, places it under relevant device group, and enables you to manage the device. The typical sequence of tasks performed by OpenManage Enterprise users:

- Install OpenManage Enterprise on page 22
- Configure OpenManage Enterprise by using Text User Interface on page 29
- Discovering devices for monitoring or management on page 43
- Manage devices and device groups on page 58
- Monitor devices by using the OpenManage Enterprise dashboard on page 40
- Organize devices into groups on page 58
- Manage the device firmware and drivers on page 80
- View and configure individual devices on page 72
- Monitor and Manage device alerts on page 124
- View and renew device warranty on page 145
- Manage device deployment templates on page 90
- Managing the device configuration compliance on page 116
- Manage compliance templates on page 117
- Monitor audit logs on page 133
- Managing OpenManage Enterprise appliance settings on page 156
- Run an inventory job now on page 78

- Manage the device warranty on page 145
- Reports on page 147
- Managing MIB files on page 153
- Role and scope-based access control in OpenManage Enterprise on page 18
- Directory services integration in OpenManage Enterprise on page 165

Topics:

OpenManage Enterprise Advanced license

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

The *OpenManage Enterprise Advanced* license is a perpetual license that is valid for the life of a server, and can be bound to the Service Tag of only one server at a time. OpenManage Enterprise provides a built-in report to view the list of devices and their licenses. Select **OpenManage Enterprise** > **Monitor** > **Reports** > **License Report**, and then click **Run**. See Run reports on page 148.

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

OpenManage Enterprise Advanced license—Supported servers

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

- YX3X servers having the iDRAC8 2.50.50.50 or later firmware versions. The YX3X firmware versions are backward compatible and are installable on YX2X hardware. See Generic naming convention for Dell EMC PowerEdge servers on page 197.
- YX4X servers having the iDRAC9 3.10.10.10 or later firmware versions. See Generic naming convention for Dell EMC PowerEdge servers on page 197

Purchase OpenManage Enterprise Advanced license

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

Verify license information

OpenManage Enterprise provides a built-in report to view the list of devices monitored by OpenManage Enterprise, and their licenses. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **License Report**. Click **Run**. See Run reports on page 148.

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

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

License-based features in OpenManage Enterprise

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

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

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

2

Security features in OpenManage Enterprise

Some of the security features of OpenManage Enterprise are:

- Role-based access control allows different device management functionality for different user roles (Administrator, Device Manager, Viewer).
- Scope-based access control allows an administrator to determine the device groups that the device managers are expected to manage.
- Hardened appliance with Security-Enhanced Linux (SELinux) and an internal firewall.
- Encryption of sensitive data in an internal database.
- 'Use of encrypted communication outside the appliance (HTTPS).
- Only browsers with 256-bit encryption are supported. for more information refer, Minimum system requirements for deploying OpenManage Enterprise on page 23

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

ⓘ NOTE:

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

Topics:

OpenManage Enterprise user role types

ⓘ NOTE:

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

Table 1. 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

Table 1. OpenManage Enterprise User role types (continued)

User with this role...	Has the following user privileges
	- Change the user password
Device Manager (DM)	- Run tasks, policies, and other actions on the devices (scope) assigned by the Administrator. - Can only view and manage entities (jobs, firmware or configuration templates and baselines, alert policies, profiles, and so on) that they have created or have assigned ownership.
Viewer	- Can only view information displayed on OpenManage Enterprise and run reports. - By default, has read-only access to the console and all groups. - Cannot run tasks or create and manage policies.

NOTE:

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

Related information

Role and scope-based access control in OpenManage Enterprise on page 18

Role and scope-based access control in OpenManage Enterprise

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

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

Users are assigned roles which determine their level of access to the appliance settings and device management features. This feature is termed as Role-Based Access Control (RBAC). The console enforces the privilege required for a certain action before allowing the action. For more information about managing users on OpenManage Enterprise, see Manage OpenManage Enterprise users on page 157.

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

Table 2. Role-based user privileges in OpenManage Enterprise

OpenManage Enterprise features	Privilege Description	User levels for accessing OpenManage Enterprise		
		Admin	Device Manager	Viewer
Appliance setup	Global appliance settings involving setting up of the appliance.	Y	N	N
Security setup	Appliance security settings	Y	N	N

Table 2. Role-based user privileges in OpenManage Enterprise (continued)

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

Scope-Based Access Control (SBAC) in OpenManage Enterprise

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

While creating or updating a Device Manager (DM) user, administrators can assign scope to restrict operational access of DM to one or more system groups, custom groups, and / or plugin groups.

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

Scope can be implemented as follows:

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

For more information about managing users, see Manage OpenManage Enterprise users on page 157.

A natural outcome of the SBAC functionality is the Restricted View feature. With Restricted View, particularly the Device Managers will see only the following:

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

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

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

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

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

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

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

SBAC for Local users:

While creating or editing a local user with DM role, admin can select one or more device groups that defines the scope for the DM.

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

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

For example, you (as an administrator) create another DM user named dm2 and assign the same group *g1* present under custom groups. If dm2 creates configuration template, configuration baselines, or profiles for the devices in *g1*, then dm1 will not have access to those entities and vice versa.

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

SBAC for AD/LDAP users:

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

For example,

- User dm1 is a member of two AD groups (*RR5-Floor1-LabAdmins* and *RR5-Floor3-LabAdmins*). Both AD groups have been assigned the DM role, with scope assignments for the AD groups are as follows: *RR5-Floor1-LabAdmins* gets *ptlab-servers* and *RR5-Floor3-LabAdmins* gets *smdlab-servers*. Now the scope of the DM dm1 is the union of *ptlab-servers* and *smdlab-servers*.

- User dm1 is a member of two AD groups (*adg1* and *adg2*). Both AD groups have been assigned the DM role, with scope assignments for the AD groups as follows: *adg1* is given access to *g1* and *adg2* is given access to *g2*. If *g1* is the superset of *g2*, then the scope of dm1 is the larger scope (*g1*, all its child groups, and all leaf devices).

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

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

SBAC for OIDC users:

Scope assignment for OIDC users does not happen within the OME console. You can assign scopes for OIDC users at an OIDC provider during user configuration. When the user logs in with OIDC provider credentials, the role and scope assignment will be available to OME. For more information about configuring user roles and scopes, see Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 170.

ⓘ **NOTE:** If PingFederate is being used as the OIDC provider, then only administrator roles can be used. For more information, see Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 170 and the Release Notes at https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Transfer ownership : The administrator can transfer owned resources from a device manager (source) to another device manager. For example, an administrator can transfer all the resources assigned from a source dm1 to dm2. A device manager with owned entities such as firmware and/or configuration baselines, configuration templates, alert policies, and profiles is considered an eligible source user. Transfer of ownership transfers only the entities and not the device groups (scope) owned by a device manager to another. For more information see, Transfer of ownership of Device Manager entities on page 164.

Related references

OpenManage Enterprise user role types on page 17

Install OpenManage Enterprise

Dell EMC OpenManage Enterprise is provided as an appliance that you can install on a hypervisor and manage resources to minimize downtime. The virtual appliance can be configured from the application web console after initial network provisioning in the Text User Interface (TUI). For steps to view and update the console version, see Check and update the version of the OpenManage Enterprise and the available plugins on page 178. 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.

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.

Hardware requirements

Lists the minimum hardware requirements for the OpenManage Enterprise appliance.

Table 3. Hardware requirements

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

Minimum system requirements for deploying OpenManage Enterprise

Table 4. Minimum requirements

Particulars	Minimum requirements
Supported hypervisors	- VMware vSphere versions: ○ vSphere ESXi 5.5 onwards - Microsoft Hyper-V supported on: ○ Windows Server 2012 R2 onwards - KVM supported on: ○ Red Hat Enterprise Linux 6.5 onwards
Network	Available virtual NIC which has access to the management networks of all the devices which is managed from OpenManage Enterprise.
Supported browsers	- Internet Explorer (64-bit) 11 and later - Mozilla Firefox 52 and later - Google Chrome 58 and later - Microsoft Edge version 41.16299 and later
User interface	HTML 5, JS based

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

Deploy OpenManage Enterprise on VMware vSphere

Prerequisites

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

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

Steps

1. Download the `openmanage_enterprise_ovf_format.zip` file from the support site and extract the file to a location accessible by VMware vSphere Client. It is recommended to use a local drive or CD/DVD, because installing from a network location can take up to 30 minutes.
2. Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select Deploy OVF Template.
3. On the **Select an OVF template** page, specify the location of the source OVF template and click **Next**.

   ⓘ **NOTE:** If you are using VMware vSphere v6.0 or the earlier versions, you must install the Client Integration plug-in before you deploy an OVF template. Then, in vSphere Client select **File** > **Deploy OVF Template**.

   The **Deploy OVF Template** wizard is displayed.
4. On the **Source** page, click **Browse**, and then select the OVF package. Click **Next**.
5. On the **OVF Template Details** page, review the information that is displayed. Click **Next**.
6. On the **End User License Agreement** page, read the license agreement and click **Accept**. To continue, click **Next**.
7. 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**.
8. 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.

9. 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**.
10. On the **Disk Format** page, click **Thick provision** to pre-allocate physical storage space to VMs at the time a drive is created.
11. 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

Prerequisites

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

Steps

1. Download the `openmanage_enterprise_vhd_format.zip` file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager** in the Windows Server 2012 R2 or an earlier version. The Windows Hyper-V should be displayed under the Hyper-V Manager. If not, right-click **Hyper-V Manager**, and then select **Connect to Server**.
3. Click **Actions** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.
5. On the **Specify Name and Location page**
    - provide the **Virtual machine name.**
    - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

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

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

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

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

ⓘ NOTE: Make sure to have a minimum storage size of 20 GB

12. Open the **Settings** of the newly created VM and power on the VM.
13. On the TUI screen, accept the EULA and when prompted, change the password of the appliance and set network parameters to the IP of the appliance.

Deploy OpenManage Enterprise on Hyper-V 2016 host

Prerequisites

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

Steps

1. Download the **openmanage_enterprise_vhd_format.zip** file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager** in the Windows server 2016. The Windows Hyper-V should be displayed under the Hyper-V Manager. If not, right-click **Hyper-V Manager**, and then select **Connect to Server**.
3. Click **Actions** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.
5. On the **Specify Name and Location page**
   - provide the **Virtual machine name.**
   - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

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

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

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

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

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

Deploy OpenManage Enterprise on Hyper-V 2019 or Windows 2022 host

Prerequisites

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

Steps

1. Download the **openmanage_enterprise_vhd_format.zip** file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager**. The Windows Hyper-V should be displayed under the Hyper-V Manager. If not, right-click **Hyper-V Manager**, and then select **Connect to Server**.
3. Click **Actions** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.
5. On the **Specify Name and Location page**
   - provide the **Virtual machine name.**
   - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

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

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

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

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

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

Deploy OpenManage Enterprise by using Kernel-based Virtual Machine

Prerequisites

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.

Steps

1. Install the required virtualization packages while installing the operating system.
2. Download the `openmanage_enterprise_kvm_format.zip` file from the support site. Extract the file to an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
3. Start the virtual manager and select **File** > **Properties**.
4. On the **Network Interfaces** page, click **Add**.
5. Select **Bridge** as the interface type and click **Forward**.
6. Set the start mode to **onboot** and select the **Activate now** check box.
7. Select the interface to bridge from the list and ensure the properties match with the host device, and then click **Finish**.
   A virtual interface is now created, and you can configure the firewall settings by using the terminal.
8. On the Virtual Machine Manager, click **File** > **New**.
9. Enter a name for the VM and select the **Import existing disk image** option, and then click **Forward**.
10. Navigate the file system and select the QCOW2 file that is downloaded in step 1, and then click **Forward**.
11. Assign 16 GB as the memory and select two processor cores, and then click **Forward**.
12. Assign the required disk space for the VM and click **Forward**.
13. Under **Advanced options**, ensure that the bridged host device network is selected and KVM is selected as the Virt Type.
14. Click **Finish**.
    OpenManage Enterprise appliance is now deployed by using the KVM. To get started with OpenManage Enterprise, see Log in to OpenManage Enterprise on page 29.

Deploy OpenManage Enterprise programmatically

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

Prerequisites

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

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

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

To programmatically deploy OpenManage Enterprise, do the following:

Steps

1. Download and extract the `openmanage_enterprise_ovf_format.zip` file or download the following OVF files individually from the support site:
   - `openmanage_enterprise.x86_64-0.0.1-disk1.vmdk`
   - `openmanage_enterprise.x86_64-0.0.1.mf`

- `openmanage_enterprise.x86_64-0.0.1.ovf`
- `openmanage_enterprise.x86_64-0.0.1.vmx`
- `ovf_properties.config`
- `update_ovf_property.py`

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

Table 5. Parameters used in `ovf_properties.config`

Parameter	Accepted Values	Description
bEULATxt	true or false	By setting this value to true, you agree to the terms and conditions in the End-User License Agreement (EULA). The EULA is available at the bottom of the ovf_properties.config file.
adminPassword	Must contain at least one character in: uppercase, lowercase, digit, and special character. For example, Dell123$	Type a new administrator password for the OpenManage Enterprise.
bEnableDHCP	true or false	Set to true if you want the appliance to enable IPv4 DHCP and to ignore the static IPv4.
bEnableIpv6AutoConfig	true or false	Set to true if you want the appliance to enable IPv6 auto configuration and to ignore the static IPv6.
staticIP	static IP in CIDR format	Can be IPv4 or IPv6. (You cannot set both the IPv4 and IPv6 types at a time.)
gateway	IPv4 or IPv6	You cannot set static Gateway as IPv4 and IPv6 types at a time.

3. Run the `update_ovf_property.py` script.

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

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

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

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

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

4

Get started with OpenManage Enterprise

Topics:

Log in to OpenManage Enterprise

About this task

When you boot the system for the first time from the Text User Interface (TUI), you are prompted to accept the EULA, and then change the administrator password. If you are logging in to OpenManage Enterprise for the first time, you must set the user credentials through the TUI. See Configure OpenManage Enterprise by using Text User Interface on page 29.

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

Steps

1. Start the supported browser.
2. In the **Address** box, enter the OpenManage Enterprise appliance IP address.

   On the login page, OpenManage Enterprise logo and a security notice stating 'By accessing the computer, you confirm that such access complies with your organization's security policy,' is displayed. The security notice can be customized by the administrators using API. For more information, see the OpenManage Enterprise API Guide.
3. Type the login credentials, and then click **Log in**.

   ⓘ NOTE: The default user name is `admin`.

Next steps

If you are logging in to OpenManage Enterprise for the first time, the **Welcome to OpenManage Enterprise** page is displayed. Click **Initial Settings**, and complete the basic configuration setup. See Configure OpenManage Enterprise on page 33. To discover the devices, click **Discover Devices**.

ⓘ NOTE: By default, after three failed login attempts, your OpenManage Enterprise account gets locked and you cannot log in until the account lockout duration is over. The account lockout duration is 900 seconds by default. To change this duration, see Set the login security properties on page 175.

Configure OpenManage Enterprise by using Text User Interface

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

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

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

ⓘ NOTE:

- To configure IPv6, ensure that it is already configured by a vCenter server.
- By default, the last discovered IP of a device is used by OpenManage Enterprise for performing all operations. To make any IP change effective, you must rediscover the device.

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

Table 6. Text User Interface options

Options	Descriptions
Change the Admin Password	Select **Change the Admin Password** screen to enter a new password and confirm the password. For the first time, you must change the password by using the TUI screen.
Display Current Appliance Status	Select **Display Current Appliance Status** to view the URL and the status of the appliance. You can also view statuses of the Task Execution, Event Processing, Tomcat, Database, and Monitoring services.
Display Current Network Configuration	Select **Display Current Network Configuration** to view the IP configuration details. **Choose Network Adapter** menu lists all the available network adapters. Clicking on a network adapter will display its current settings.
Set Appliance Hostname	Select **Set Appliance Hostname** to configure the appliance hostname on the DNS. This field supports the following valid characters for host names: alphanumeric (a-z, A-Z, 0-9), periods (.), and dashes (-). ⓘ **NOTE:** Using periods will designate domain name information. If the appliance DNS information is configured statically rather than getting domain details from DHCP, you must configure the hostname using the fully qualified domain name (FQDN) so that the domain search information can be populated.
Set Networking Parameters	Select **Set Networking Parameters** to reconfigure the network adapters. **Choose Network Adapter** menu lists all the available networks adapters. Select a network adapter, reconfigure its network parameters, and select **Apply** to save the changes to the appropriate interface. By default, only IPv4 is enabled on primary network interface with a private static IP in the appliance. However, if a new network interface is added, both IPv4 and IPv6 are enabled for multihoming. If the OpenManage Enterprise appliance fails to acquire a IPv6 address, check if the environment is configured for router advertisements to have the managed bit (M) turned on. Network Manager from current Linux distributions causes a link failure when this bit is on, but DHCPv6 is not available. Ensure that DHCPv6 is enabled on the network or disable the managed flag for router advertisements. ⓘ **NOTE:**

Table 6. Text User Interface options (continued)

Options	Descriptions
	• DNS configuration is only available on the primary network interface. If DNS resolution is wanted on this interface, all host names must be resolvable by the DNS server configured on the primary interface. • For more information about multihoming, see the *Multihoming on OpenManage Enterprise* technical whitepaper on the Dell OpenManage Enterprise support site.
Select Primary Network Interface	**Select Primary Network Interface** allows you to designate a primary network. Primary interface selection gives priority to the selected interface in terms of routing and is used as the default route. This interface will have the routing priority if there is any ambiguity. The primary interface is also expected to be the 'public facing' interface which allows for corporate network/ internet connectivity. Different firewall rules are applied to the primary interface, which allow for tighter access control such as access restriction by IP range. ⓘ **NOTE:** If multihoming is enabled, the appliance can be accessed from two networks. In this case, the primary interface is used by the appliance for all external communication and when proxy settings are used. For more information about multihoming, see the *Multihoming on OpenManage Enterprise* technical whitepaper on the Dell OpenManage Enterprise support site.
Configure Static Routes	Select **Configure Static Routes** if the networks require a static route to be configured to reach a specific subnet over the IPv4 and IPv6 networks. ⓘ **NOTE:** A maximum of 20 static routes per interface is supported.
Configure Server Initiated Discovery	Select **Configure Server Initiated Discovery** to allow the appliance to automatically register the required records with the configured DNS server. ⓘ **NOTE:** • Ensure that the appliance is registered with DNS, and can dynamically update records. • The target systems must be configured to request registration details from DNS. • To change the DNS Domain Name, ensure Dynamic DNS registration is enabled on the DNS server. Also, for appliance to be registered on the DNS server, select the **Nonsecure and secure** option under Dynamic updates.
Configure Appliance Disk Size	Select **Configure Appliance Disk Size** to scan for the availability of disk space or new disk(s) and then allocate the additional disk space or disk(s) for the appliance if required. ⓘ **NOTE:** • It is highly recommended to take a VM snapshot of the console as a backup before applying any disk configuration changes. • Post addition of the disk space, deletion or reduction of the expanded disk space is not supported. To

Table 6. Text User Interface options (continued)

Options	Descriptions
	remove a newly added disk or to reverse the increase in size of an existing disk you must revert to prior VM snapshot. - If the initial scan detects no unallocated space, then allocate additional disk space or disks to the console on your hypervisor and rescan. - Scanning and allocation of disk space is limited to a maximum of four disks.
Enable Field Service Debug (FSD) Mode	Select **Enable Field Service Debug (FSD) Mode** (default) for console debugging using HTTPS. For more information, see Field service debug workflow on page 194.
Restart Services	Select **Restart Services** with the following options to restart the services and networking: - **Restart All Services** - **Restart Networking**
Setup Debug Logging	Select **Setup Debug Logging** using the following options : - **Enable All Debug Logs** ○ to collect the Debug logs of the all the application monitoring tasks, events, the task execution history, and installed plugins. - **Disable All Debug Logs** ○ to disable all the Debug logs. - **Configure Debug Logging** ○ To selectively enable debug logging for appliance and plugin services. ○ Use the **Options** menu to select all services, clear all selections or restore state prior to making any modifications. - **Enable SCP Retention**—to collect the template .XML files. ⓘ **NOTE:** SCP file retention is not applicable for MX7000 chassis templates. - **Disable SCP Retention**—to disable the SCP retention. You can create a console log archive from the **Monitor** > **Audit Logs** page by clicking **Troubleshoot** > **Create Console Log Archive**. To download the archived console log, click **Troubleshoot** > **Download Archived Console Logs**.
Enable CIFS share for FSD (emergency use only)	Select **Enable CIFS share for FSD (emergency use only)** for console debugging using CIFS share. For more information, see Field service debug workflow on page 194.
Change keyboard layout	Select **Change keyboard layout** to change the keyboard layout if needed.
Reboot the Appliance	Select **Reboot the Appliance** to restart the appliance. ⓘ **NOTE:** After running a command to restart the services, the TUI may display the following message: `NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439].` The soft lockup issue likely occurs as a result of the hypervisor being overloaded. In such situations, it is recommended to have at least 16 GB of RAM and CPU of 8000 MHz reserved to the OpenManage Enterprise appliance. It is also recommended that the OpenManage

Table 6. Text User Interface options (continued)

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

Configure OpenManage Enterprise

About this task

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

Steps

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

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

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

Results

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

Recommended scalability and performance settings for optimal usage of OpenManage Enterprise

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

Table 7. Scalability and performance considerations of OpenManage Enterprise

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

Supported protocols and ports in OpenManage Enterprise

Supported protocols and ports on management stations

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

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

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

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

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

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

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

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

Supported protocols and ports on managed nodes

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

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

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

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

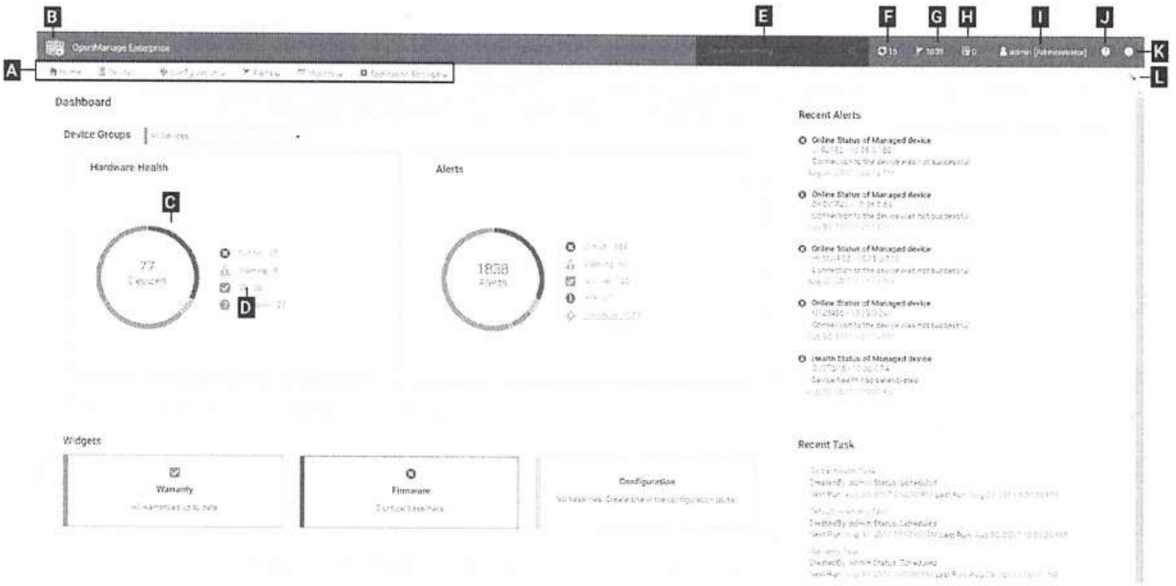
Table 10. Use case links for the supported protocols and ports in OpenManage Enterprise

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

5

OpenManage Enterprise Graphical User Interface overview

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



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

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

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

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

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

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

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

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

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

OpenManage Enterprise Home portal

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

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

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

Topics:

Monitor devices by using the OpenManage Enterprise dashboard

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Donut chart

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

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

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

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

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

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

ⓘ **NOTE:** The compliance level of the selected device 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 11. Device health statuses in OpenManage Enterprise

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

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

7

Discovering devices for monitoring or management

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

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise you must have necessary role-based user privileges and scope-based operational access to the devices. See Role and scope-based access control in OpenManage Enterprise on page 18.
- In order to support discovery with domain credentials, OpenManage Enterprise (version 3.2 and later) uses the OpenSSH protocol instead of the WSMAN protocol used in the previous versions. Hence, all the Windows and Hyper-V devices discovered prior to updating the appliance have to be deleted and re-discovered using their OpenSSH credentials. Refer the Microsoft documentation to enable OpenSSH on Windows and Hyper-V.
- On the **Discovery and Inventory Schedules** pages, the status of a scheduled job is indicated as **Queued** in the **STATUS** column. However, the same status is indicated as **Scheduled** on the **Jobs** page.
- By default, the last discovered IP of a device is used by OpenManage Enterprise for performing all operations. To make any IP change effective, you must rediscover the device.
- For third party devices, you might see duplicate entries if they are discovered using multiple protocols. This duplication can be corrected by deleting the entries and rediscovering the device(s) using only the IPMI protocol.

By using the Discovery feature, you can:

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

Related tasks

Delete a device discovery job on page 56

View device discovery job details on page 49

Stop a device discovery job on page 50

Run a device discovery job on page 50

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

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

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

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

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

Edit a device discovery job on page 50

Topics:

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

Discover servers automatically by using the server-initiated discovery feature

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

Prerequisites

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

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

About this task

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

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

Steps

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

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

     - To create hostname record

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

     - To add records for server-initiated discovery

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

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

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

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

- To create hostname record

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

- To add records for server-initiated discovery

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

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

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

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

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

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

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

Steps

1. **Import**—To import the server credentials:
   a. Click **Import**.
   b. In the Import From File wizard, click **Upload Service Tags File** to navigate and select the .csv file.

      To view a sample CSV file of the server credentials, click **Download sample CSV file**.
   c. Click **Finish**
2. **Discover**—To manually discover the servers in 'Ready to Discover' status:
   a. Select the servers listed on the Server-Initiated Discovery page which are in 'Ready to Discover' Status.
   b. Click **Discover**.

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

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

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

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

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

Create a device discovery job

About this task

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

To discover a device:

Steps

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

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

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

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

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

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

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

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

Results

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

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

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

Onboarding devices

About this task

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

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

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

ⓘ **NOTE:**

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

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

Steps

1. From the **OpenManage Enterprise** menu, under **Devices**, click **All Devices**.
   A Donut chart indicates status of all devices in the working pane. See the Donut chart. The table lists the properties of devices selected along with their following onboarding status:
   - **Error**: Device cannot be onboarded. Try by logging in by using the recommended privileges. See Role and scope-based access control in OpenManage Enterprise on page 18.
   - **Managed**: Device successfully onboarded, and can be managed by the OpenManage Enterprise console.
   - **Monitored**: Device does not have management option (such as the one discovered by using SNMP).
   - **Managed with alerts**: Device is successfully onboarded, and the OpenManage Enterprise console has successfully registered its IP address with the device as a trap destination during discovery.
2. In the working pane, select a check box corresponding to the device(s), click **More Actions** > **Onboarding**.

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

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

3. In the **Onboarding** dialog box, enter the WS-Man credentials—username and password.
4. In the **Connection Settings** section:
   a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
   b. In the **Timeout** box, enter the time after which a job must stop running.

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

   c. In the **Port** box, enter the port number that the job must use to discover.
   d. Optional field. Select **Enable Common Name (CN) check**.
   e. Optional field. Select **Enable Certificate Authority (CA) check** and browse to the certificate file.
5. Click **Finish**.

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

Protocol support matrix for discovering devices

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

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

Table 12. Protocol support matrix for discovery

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

Table 12. Protocol support matrix for discovery (continued)

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

View device discovery job details

About this task

Steps

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

Related information

Discovering devices for monitoring or management on page 43

Edit a device discovery job

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

Steps

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

Related information

Discovering devices for monitoring or management on page 43

Run a device discovery job

About this task

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

To run a device discovery job:

Steps

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

Related information

Discovering devices for monitoring or management on page 43

Stop a device discovery job

About this task

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

Steps

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

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

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

Related information

Discovering devices for monitoring or management on page 43

Specify multiple devices by importing data from the .csv file

About this task

Steps

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

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

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

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

Global exclusion of ranges

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

About this task

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

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

Steps

1. To activate the Global Exclusion of Ranges wizard, you can do one of the following:
   - From the All Devices page (**OpenManage Enteprise** > **Devices**), **Discovery** drop-down menu, click **Edit Exclude Ranges**.
   - From the **Monitor** > **Discovery** , click the **Global Exclusion List** on the top right corner.
2. In the **Global Exclusion of Ranges** dialog box:
   a. In the **Description of Exclude Range** box, enter the information about the range that is being excluded.
   b. In the **Enter Ranges to Exclude** box, enter address(es) or range of devices to be excluded. The box can take up to 1000 address entries at a time, but separated by a line break. Meaning, every exclusion range must be entered in different lines inside the box.
   The range that can be excluded is same as the supported ranges that are applicable while discovering a device. See Create a device discovery job on page 46.

   NOTE:

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

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

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

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

Results

NOTE:

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

.

Specify discovery mode for creating a server discovery job

About this task

Steps

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

Related information

Discovering devices for monitoring or management on page 43

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

About this task

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

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

Steps

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

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

2. To **Discover using IPMI (non-Dell via OOB)**
   a. In the Credentials section, enter **User Name** and **Password**.
   b. In the **Connection Settings** section:
   - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
   - In the **Timeout** box, enter the time after which a job must stop running.
   - In the **KgKey** box, enter an appropriate value.
3. To **Discover using SSH (Linux, Windows, Hyper-V)**

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

   a. In the Credentials section, enter **User Name** and **Password**.
   b. In the **Connection Settings** section:
   - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
   - In the **Timeout** box, enter the time after which a job must stop running.
   - Enter in the **Port** box to edit the port number. By default, 22 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 34
   - Select the **Verify the known Host key** check box to validate host against known host keys.

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

     ⓘ **NOTE:** For sudo accounts to work, the server(s) `/etc/sudoer` file must be configured to use NOPASSWD.
4. To **Discover using ESXi (VMware)**
   a. In the Credentials section, enter **User Name** and **Password**.
   b. In the **Connection Settings** section:
   - In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
   - In the **Timeout** box, enter the time after which a job must stop running.
   - Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 34
   - Select the **Enable Common Name (CN)** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
   - Select the **Enable Certificate Authority (CA)** check box, if needed.

Related information

Discovering devices for monitoring or management on page 43

Specify discovery mode for creating a chassis discovery job

Steps

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

Results

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

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

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

About this task

In the **Additional Settings** dialog box:

Steps

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

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

2. Enter username and password of the chassis to be detected.
3. In the **Connection Settings** section:
   a. In the **Retries** box, enter the number of repeated attempts that must be made to discover a server.
   b. In the **Timeout** box, enter the time after which a job must stop running.
   c. Enter in the **Port** box to edit the port number. By default, 443 is used to connect to the device. For supported port numbers, see Supported protocols and ports in OpenManage Enterprise on page 34.
   d. Select the **Enable Common Name (CN) check** check box if the common name of device is same as the host name used to access the OpenManage Enterprise.
   e. Select the **Enable Certificate Authority (CA) check** check box.
4. To discover IO modules, select the **Discover IO Modules with chassis** check box.

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

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

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

        ⓘ NOTE: Known host keys are added via */DeviceService/HostKeys REST API* service. Please refer to the *OpenManage Enterprise RESTful API Guide* for more information on how to manage host keys.
      - Select **Use SUDO Option** if needed.
5. Click **Finish**.
6. Complete the tasks in Create a device discovery job on page 46.

Specify discovery mode for creating a Dell storage discovery job

Steps

1. From the **Device Type** drop-down menu, select **DELL STORAGE**.
2. When prompted, select:
   - PowerVault ME: To discover the storage devices using the HTTPS protocol like the PowerVault ME.
   - Others: To discover storage devices which use SNMP protocol.

   Based on your selection, the fields change under **Settings**.
3. Enter the IP address, host name, or IP range in **IP/Hostname/Range**.
4. Under **Settings**, depending on your initial selection — enter the **User Name** and **Password** for Storage HTTPS or enter the **SNMP version** and the **community type** of the device to be detected.
5. Click **Additional Settings** to customize the respective discover protocol. See Creating customized device discovery job template for SNMP devices or see Create customized device discovery job protocol HTTPS storage devices -Additional settings for discovery protocols on page 55.
6. Complete the tasks in Create a device discovery job on page 46.

Related information

Discovering devices for monitoring or management on page 43

Specify discovery mode for creating a network switch discovery job

Steps

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

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

About this task

In the **Additional Settings** dialog box:

Steps

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

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

Create customized device discovery job protocol for SNMP devices

About this task

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

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

Steps

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

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

Related information

Discovering devices for monitoring or management on page 43

Specify discovery mode for creating a MULTIPLE protocol discovery job

Steps

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

Related information

Discovering devices for monitoring or management on page 43

Delete a device discovery job

About this task

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

To delete a device discovery job:

Steps

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

Results

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

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

Related information

Discovering devices for monitoring or management on page 43

8

Manage devices and device groups

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

The left pane displays the device groups as follows:

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

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

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

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

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

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

ⓘ NOTE:

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

Topics:

Organize devices into groups

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

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

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