- A message that describes the alert.

b. Click **Finish**.
The trap is edited and the updated trap list is displayed.

ⓘ NOTE: You cannot edit more than one alert at a time. The traps imported to OpenManage Enterprise cannot be edited.

3. In the **Report Definition** dialog box, edit the settings. See Creating reports.
4. Click **Save**.
The updated information is saved.

Remove MIB files

About this task

ⓘ NOTE: You cannot remove a MIB file that has trap definitions used by any of the alert policies. See Alert policies on page 126.

ⓘ NOTE: Events that are received before removing a MIB will not be affected by the associated MIB removal. However, events generated after the removal will have unformatted traps.

Steps

1. In the **MIB FILENAME** column, expand the folder, and select the MIB files.
2. Click **Remove MIB**.
3. In the **Remove MIB** dialog box, select the check boxes of the MIBs to be removed.
4. Click **Remove**.
The MIB files are removed and the MIB table is updated.

Resolve MIB types

About this task

Steps

1. Import the MIB files. See Import MIB files on page 153.
If the MIB type is unresolved, the **Unresolved Types** dialog box lists MIB type(s) indicating that the MIB type(s) will be imported only if resolved.
2. Click **Resolve Types**.
3. In the **Resolve Types** dialog box, click **Select Files**, and then select the missing file(s).
4. In the **Import MIB** dialog box, click **Next**. If there are still missing MIB types, the **Unresolved Types** dialog box again lists the missing MIB types. Repeat steps 1-3.
5. After all the unresolved MIB types are resolved, click **Finish**. Complete the importing process. See Import MIB files on page 153.

Download an OpenManage Enterprise MIB file

Steps

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

ⓘ NOTE: You can download only the OpenManage Enterprise-related MIB files.

20

Managing OpenManage Enterprise appliance settings

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

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

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

- Configure and manage the OpenManage Enterprise network settings such as IPv4, IPv6, time, and proxy settings. See Configuring network settings.
- Add, enable, edit, and delete users. See Managing users.
- Set the device health and dashboard monitoring properties. See Managing Console preferences.
- Manage user login and lockout policies. See Setting login security properties.
- View current SSL certificate, and then generate a CSR request. See Generate and download the certificate signing request on page 173.
- Configure emails, SNMP, and Syslog properties for alert management. See Configure SMTP, SNMP, and Syslog alerts on page 129.
- Set the SNMP listener and Trap Forward settings. See Managing incoming alerts.
- Set the credentials and time to receive notification about warranty expiry. See Managing warranty settings.
- Set the properties to check for availability of updated version and then update the OpenManage Enterprise version. See Check and update the version of the OpenManage Enterprise and the available plugins on page 178.
- Set the user credentials to run remote command by using RACADM, and IPMI. See Executing remote commands & scripts.
- Set and receive alert notifications on your mobile phone. See OpenManage Mobile settings on page 185.

Related tasks

Delete Directory services on page 168

Topics:

Configure OpenManage Enterprise network settings

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.

Steps

1. To only view the current network settings of all the active network connections of OpenManage Enterprise such as DNS domain name, FQDN, and IPv4 and IPv6 settings, expand **Current Settings**.
2. To configure the session timeouts and the maximum number of sessions for the OpenManage Enterprise API and web interface users, expand **Session Inactivity Timeout Configuration** and do the following:
   a. Select the **Enable** check box to activate the Universal Timeout and enter the **Inactivity timeout (1-1440)** value. Inactivity timeout value can be set between 1 minute to 1440 minutes (24 hours). By default the Universal timeout is grayed out. Enabling the Universal timeout disables the API and Web Interface fields.
   b. Change the API **Inactivity timeout (1-1440)** and the **Maximum number of sessions (1-100)** values. These attributes are by default set as 30 minutes and 100 respectively.
   c. Change the Web Interface **Inactivity timeout (1-1440)** and the **Maximum number of sessions (1-100)** values. These attributes are by default set as 30 minutes and 100 respectively.
   d. Click **Apply** to save the settings or click **Discard** to retain the default values.
3. The current system time and the source—local time zone or NTP server IP are displayed. To configure the system time zone, date, time, and NTP server synchronization, expand **Time Configuration**.
   a. Select the time zone from the drop-down list.
   b. Enter the date or click the **Calendar** icon to select the date.
   c. Enter the time in hh:mm:ss format.
   d. To synchronize with an NTP server, select the **Use NTP** check box, and enter the server address of the primary NTP server.

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

      ⓘ NOTE: The **Date** and **Time** options are not available when the **Use NTP** option is selected.

   e. Click **Apply**.
   f. To reset the settings to default attributes, click **Discard**.
4. To configure the OpenManage Enterprise proxy settings, expand **Proxy Configuration**.
   a. Select the **Enable HTTP Proxy Settings** check box to configure the HTTP proxy, and then enter HTTP proxy address and HTTP port number.
   b. Select the **Enable Proxy Authentication** check box to enable proxy credentials, and then enter the username and password.
   c. Select the **Ignore Certificate Validation** check box if the configured proxy intercepts SSL traffic and does not use a trusted third-party certificate. Using this option will ignore the built-in certificate checks used for the warranty and catalog synchronization.
   d. Click **Apply**.
   e. To reset the settings to default attributes, click **Discard**.

Results

To understand all the tasks that you can perform by using the Application Settings feature, see Managing OpenManage Enterprise appliance settings on page 156.

Manage OpenManage Enterprise users

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 18.
- Any change to the user role will not affect the active session of the impacted user(s) and will take effect from subsequent login.

> - If a Device Manager user is demoted to a Viewer, that DM will lose access to all the owned entities such as jobs, firmware or configuration templates and baselines, alert policies, and profiles. These entities can be managed only by the administrator and can't be restored even when the same user is 'promoted' from a Viewer to DM.

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

- View, add, enable, edit, disable, or delete the OpenManage Enterprise local users. For more information, see Add and edit OpenManage Enterprise local users
- Assign OpenManage Enterprise roles to Active Directory users by importing the directory groups. AD and LDAP directory users can assigned an Admin, or a Device Manager, or a Viewer role in OpenManage Enterprise. For more information, see Import AD and LDAP groups on page 163
- View details about the logged-in users, and then end (terminate) a user session.
- Manage Directory Services. For more information, see Add or edit Active Directory groups to be used with Directory Services on page 166
- View, add, enable, edit, disable, or delete OpenID connect providers (PingFederate and/or Key Cloak). For more information, see OpenManage Enterprise login using OpenID Connect providers on page 168

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

- **USERNAME**: Along with the users you created, OpenManage Enterprise displays the following default user roles that cannot be edited or deleted: admin, system, and root. However, you can edit the login credentials by selecting the default username and clicking **Edit**. See Enable OpenManage Enterprise users on page 162. The recommended characters for user names are as follows:
    - 0–9
    - A–Z
    - a–z
    - - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >
    - The recommended characters for passwords are as follows:
        - 0–9
        - A–Z
        - a–z
        - ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >
- **USER TYPE**: Indicates if the user logged in locally or remotely.
- **ENABLED**: Indicates with a tick mark when the user is enabled to perform OpenManage Enterprise management tasks. See Enable OpenManage Enterprise users on page 162 and Disable OpenManage Enterprise users on page 162.
- **ROLE**: Indicates the user role in using OpenManage Enterprise. For example, OpenManage Enterprise administrator and Device Manager. See OpenManage Enterprise user role types on page 17.

Related references

Disable OpenManage Enterprise users on page 162

Enable OpenManage Enterprise users on page 162

Related tasks

Delete Directory services on page 168

Delete OpenManage Enterprise users on page 163

Ending user sessions on page 165

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 26. Role-based user privileges in OpenManage Enterprise

OpenManage Enterprise features	Privilege Description	User levels for accessing OpenManage Enterprise		
		Admin	**Device Manager**	**Viewer**
Appliance setup	Global appliance settings involving setting up of the appliance.	Y	N	N
Security setup	Appliance security settings	Y	N	N
Alert management	Alerts actions / management	Y	N	N
Fabric management	Fabric actions / management	Y	N	N
Network management	Network actions / management	Y	N	N
Group management	Create, read, update and delete (CRUD) for static and dynamic groups	Y	N	N
Discovery management	CRUD for discovery tasks, run discovery tasks	Y	N	N
Inventory management	CRUD for inventory tasks, run inventory tasks	Y	N	N
Trap management	Import MIB, Edit trap	Y	N	N
Auto-deploy management	Manage auto-deploy configuration operations	Y	N	N
Monitoring setup	Alerting policies, forwarding, 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

Add and edit OpenManage Enterprise local users

About this task

This procedure is specific to only adding and editing the local users. While editing local users, you can edit all the user properties. However, for Directory Users, only the role and device groups (in the case of a Device Manager) can be edited. To integrate Directory Services in OpenManage Enterprise and to import the Directory users, see Directory services integration in OpenManage Enterprise on page 165 and Import AD and LDAP groups on page 163.

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

Steps

1. Select **Application Settings** > **Users** > **Users** > **Add**.
2. In the **Add New User** dialog box:
   a. Under **User Details**, select Administrator, Device Manager, or Viewer from the **User Role** drop-down menu.
   For more information, see Role and scope-based access control in OpenManage Enterprise on page 18.

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

b. For the Device Manager roles, the scope is defaulted to **All Devices** (unrestricted scope), however, the administrator can restrict the scope by choosing the **Select Groups** option followed by selecting the device group(s).

c. Under **User Credentials**, enter **Username**, **Password**, and reenter the password in the **Confirm Password** fields.

> ⓘ NOTE: The username must contain only alphanumeric characters (but underscore is allowed) and the password must contain at least one character in: uppercase, lowercase, digit, and special character.

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

Edit OpenManage Enterprise user properties

Steps

1. On the **Application Settings** page, under **Users**, select the check box corresponding to the user.
2. Complete the tasks in Add and edit OpenManage Enterprise local users on page 161.
   The updated data is saved.

> ⓘ NOTE: When you change the role of a user, the privileges available for the new role automatically get applied.
> For example, if you change a device manager to an administrator, the access rights and privileges provided for an administrator will be automatically enabled for the device manager.

Enable OpenManage Enterprise users

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

Related tasks

Delete Directory services on page 168
Delete OpenManage Enterprise users on page 163
Ending user sessions on page 165

Related information

Manage OpenManage Enterprise users on page 157

Disable OpenManage Enterprise users

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

Related tasks

Delete Directory services on page 168
Delete OpenManage Enterprise users on page 163
Ending user sessions on page 165

Related information

Manage OpenManage Enterprise users on page 157

Delete OpenManage Enterprise users

Steps

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

Related references

Disable OpenManage Enterprise users on page 162

Enable OpenManage Enterprise users on page 162

Related information

Manage OpenManage Enterprise users on page 157

Import AD and LDAP groups

Prerequisites

ⓘ NOTE:

- The users without Administrator rights cannot enable or disable the Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) users.
- Before importing AD groups in OpenManage Enterprise, you must include the user groups in a UNIVERSAL GROUP while configuring the AD.
- AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Admin, DeviceManager, or Viewer). The Single-Sign-On (SSO) feature stops at login to the console. Actions run on the devices require a privileged account on the device.

About this task

Steps

1. Click **Import Directory Group**.
2. In the **Import Active Directory** dialog box:
   a. From the **Directory Source** drop-down menu, select an AD or LDAP source that must be imported for adding groups. For adding directories, see Add or edit Active Directory groups to be used with Directory Services on page 166.
   b. Click **Input Credentials**.
   c. In the dialog box, type the username and password of the domain where the directory is saved. Use tool tips to enter the correct syntax.
   d. Click **Finish**.
3. In the **Available Groups** section:
   a. In the **Find a Group** box, enter the initial few letters of the group name available in the tested directory. All the groups names that begin with the entered text are listed under GROUP NAME.
   b. Select the check boxes corresponding to the groups be imported, and then click the **>>** or **<<** buttons to add or remove the groups.
4. In the **Groups to be Imported** section:
   a. Select the check boxes of the groups, and then select a role from the Assign Group Role drop-down menu. For more information about the role-based access, see Role and scope-based access control in OpenManage Enterprise on page 18.
   b. Click **Assign Role**.
   The users in the group under the selected directory service are assigned with the selected user roles.
   c. For the Device Manager role, the scope is defaulted to **All Devices**, however, the administrator can restrict the scope by choosing the **Assign Scope** option followed by selecting the device group(s).
5. Repeat steps 3 and 4, if necessary.
6. Click **Import**.

The directory groups are imported and displayed in the Users list. However, all users in those groups will log in to OpenManage Enterprise by using their domain username and credentials.

Example

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

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

Transfer of ownership of Device Manager entities

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

Prerequisites

> NOTE:
>
> - To perform this task on OpenManage Enterprise you must have the administrator user privileges. Role and scope-based access control in OpenManage Enterprise on page 18.
> - 'Transfer of ownership' transfers only the entities and not the device groups (scope) owned by a device manager to another.
> - Before a transfer of ownership of entities is initiated, the administrator must first reassign the device groups owned by the former device manager to the device manager who will be taking over.
> - If the ownership of the entities is transferred to an Active Directory user group, then the ownership is transferred to all the members of that AD group.
> - The new Device Manager must reschedule any tasks that were scheduled by the former Device Manager, such as the tasks for firmware updates and Deployment of templates, after the transfer of ownership.

About this task

To transfer the ownership of entities such as jobs, firmware or configuration templates and baselines, alert policies, and profiles from one device manager to another do the following:

Steps

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

   > NOTE: The Source User will only list the local, active directory, OIDC, or deleted device managers who have entities such as jobs, FW or configuration templates, alerts policies and profiles associated with them.

3. From the **Target User** drop-down list, select the device manager to whom the entities will be transferred.
4. Click **Finish** and then click **Yes** at the prompt message.

Results

All the owned entities such as jobs, firmware or configuration templates, alert policies, and profiles are transferred from the 'source' device manager to the 'target' device manager.

Ending user sessions

Steps

1. Select the check box corresponding to the username, and then click **Terminate**.
2. When prompted to confirm, click **YES**.
   The selected user session is ended and the user is logged out.

Related references

Disable OpenManage Enterprise users on page 162

Enable OpenManage Enterprise users on page 162

Related information

Manage OpenManage Enterprise users on page 157

Directory services integration in OpenManage Enterprise

Directory Services enables you to import directory groups from AD or LDAP for use on the console. OpenManage Enterprise supports integration of the following directory services:

1. Windows Active Directory
2. Windows AD/LDS
3. OpenLDAP
4. PHP LDAP

Pre-requisites/supported attributes for LDAP Integration

Table 27. OpenManage Enterprise Pre-requisites/supported attributes for LDAP Integration

	Attribute of User Login	Attribute of Group Membership	Certificate Requirement
AD/LDAP	Cn, sAMAccountName	Member	• Subject to Domain Controller Certificate needs to have FQDN. SAN field can have IPv4 and/or IPv6 or FQDN. • Only Base64 certificate format is supported
OpenLDAP	uid, sn	Uniquemember	Only PEM certificate format is supported
PHP LDAP	uid	MemberUid	

User pre-requisites for directory service integration

You must ensure that the following user pre-requisites are met before you begin with the directory service integration:

1. BindDN user and user used for 'Test connection' should be the same.
2. If Attribute of User Login is provided, only the corresponding username value assigned to the attribute is allowed for appliance login.
3. User used for Test connection should be part of any non-default group in LDAP
4. Attribute of Group Membership should have either the 'userDN' or the short name (used for logging in) of the user.
5. When MemberUid is used as 'Attribute of Group Membership,' the username used in appliance login will be considered case sensitive in some LDAP configurations.

6. When search filter is used in LDAP configuration, user login is not allowed for those users who is not part of the search criteria mentioned.
7. Group search will work only if the groups have users assigned under the provided Attribute of Group Membership .

> **NOTE:** If the OpenManage Enterprise is hosted on an IPv6 network, the SSL authentication against domain controller using FQDN would fail if IPv4 is set as preferred address in DNS. To avoid this failure, do one of the following:
>
> - DNS should be set to return IPv6 as preferred address when queried with FQDN.
> - DC certificate needs to have IPv6 in SAN field.

To use the Directory Services:

- Add a directory connection. See Add or edit Active Directory groups to be used with Directory Services on page 166.
- Import directory groups and map all users in the group to a specific role. See Import AD and LDAP groups on page 163.
- For DM users, edit the directory group to add the groups the DM can manage. See Add and edit OpenManage Enterprise local users on page 161.

Add or edit Active Directory groups to be used with Directory Services

About this task

Steps

1. Click **Application Settings** > **Users** > **Directory Services**, and then click **Add**.
2. In the **Connect to Directory Service** dialog box, by default, **AD** is selected to indicate that directory type is Active Directory (AD):

   > **NOTE:** To create an LDAP user group by using Directory Services, see Add or edit Lightweight Directory Access Protocol groups to be used with Directory Services on page 167.

   a. Enter a desired name for the AD directory.
   b. Select the Domain Controller Lookup method:
      - **DNS**: In the **Method** box, enter the domain name to query DNS for the domain controllers.
      - **Manual**: In the **Method** box, enter the FQDN or the IP address of the domain controller. For multiple servers, a maximum of three servers are supported, use a comma-separated list.

   c. In the **Group Domain** box, enter the group domain as suggested in the tool tip syntax.
3. In the **Advanced Options** section:

   a. By default, Global Catalog Address port number 3269 is populated. For the Domain Controller Access, enter 636 as the port number.

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

   b. Enter the network timeout and search timeout duration in seconds. The maximum timeout duration supported is 300 seconds.
   c. To upload an SSL certificate, select **Certificate Validation** and click **Select a file**. The certificate should be a Root CA Certificate encoded in Base64 format.

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

   > **NOTE:** The **username** must be entered in either the UPN (username@domain) or in the NetBIOS (domain\username) format.
6. Click **Test connection**.
   In the **Directory Service Information** dialog box, a message is displayed to indicate successful connection.
7. Click **Ok**.
8. Click **Finish**.
   A job is created and run to add the requested directory in the Directory Services list.

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

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

Add or edit Lightweight Directory Access Protocol groups to be used with Directory Services

About this task

Steps

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

   NOTE: To create an AD user group by using Directory Services, see Add or edit Active Directory groups to be used with Directory Services on page 166.

   a. Enter a desired name for the LDAP directory.

   b. Select the Domain Controller Lookup method:
   - **DNS**: In the **Method** box, enter the domain name to query DNS for the domain controllers.
   - **Manual**: In the **Method** box, enter the FQDN or the IP address of the domain controller. For multiple servers, a maximum of three servers are supported, use a comma-separated list.

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

   NOTE: Anonymous bind is not supported for AD LDS.
3. In the **Advanced Options** section:

   a. By default, LDAP port number of 636 is populated. To change, enter a port number.

   NOTE: Only LDAPS ports are supported.

   b. To match the LDAP configuration on the server, enter the group base DN to search for.

   c. Enter the **User attributes** already configured in the LDAP system. It is recommended that this is unique within the selected Base DN. Else, configure a search filter to ensure that it is unique. If the user DN cannot be uniquely identified by the search combination of attribute and search filter, the login operation fails.

   NOTE: The user attributes should be configured in the LDAP system used to query before integrating on the directory services.

   NOTE: You need to enter the user attributes as **cn** or **sAMAccountName** for AD LDS configuration and **UID** for LDAP configuration

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

   e. Enter the network timeout and search timeout duration in seconds. The maximum timeout duration supported is 300 seconds.

   f. To upload an SSL certificate, select **Certificate Validation** and click **Select a file**. The certificate should be a Root CA Certificate encoded in Base64 format.

   The **Test connection** button is enabled.
4. Click **Test connection**, and then enter the bind user credentials of the domain to be connected to.

   NOTE: While testing the connection, ensure that the **Test username** is the value of the **Attribute of User Login** entered previously.
5. Click **Test connection**.
   In the **Directory Service Information** dialog box, a message is displayed to indicate successful connection.
6. Click **Ok**.
7. Click **Finish**.
   A job is created and run to add the requested directory in the Directory Services list.

Editing LDAP groups to be used with Directory Services

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

Delete Directory services

About this task

Steps

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

Related references

Disable OpenManage Enterprise users on page 162
Enable OpenManage Enterprise users on page 162

Related information

Managing OpenManage Enterprise appliance settings on page 156
Manage OpenManage Enterprise users on page 157

OpenManage Enterprise login using OpenID Connect providers

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

⚠ WARNING: **User roles and scopes are reset to 'default' on client re-registration with OIDC provider PingFederate (PingIdentity). This issue might lead to resetting of the privileges and scope of non-admin roles (DM and Viewer) to that of the Administrator. Re-registration of the appliance console with OIDC provider is triggered in the event of an appliance upgrade, change in network configuration, or change in SSL certificate.**

To avoid security concerns post any of the above-mentioned re-registration events, the administrator must reconfigure all the OpenManage Enterprise Client IDs on the PingFederate site. Also, it is highly recommended that Client IDs are created only for Administrator users with Pingfederate till this issue is resolved.

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have the necessary user privileges. See Role and scope based access control in OpenManage Enterprise on page 18.
- Only a maximum of four OpenID Connect provider IDs can be added in the appliance.

Prerequisites:

Before enabling an OpenID Connect provider login you must:

1. **Add an OIDC provider in the OpenManage Enterprise**: In OpenManage Enterprise Application Settings, add an OpenID Connect provider. When you add the OpenID Connect provider, a **Client ID** is generated for the OpenID Connect provider. For more information, see: Add an OpenID Connect provider to OpenManage Enterprise on page 169.
2. **Configure the OpenID Connect provider using the Client ID**: In the OpenID Connect provider, locate the Client ID and define a login role (Administrator, Device Manager or Viewer) by adding and mapping the scope called **dxcua** (Dell extended claim for user authentication). For more information, see:
   - Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 170
   - Configure an OpenID Connect provider policy in Keycloak for role-based access to OpenManage Enterprise on page 170

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

- Name - The OpenID Connect provider's name when it was added in the appliance
- Enabled - A 'check' on this field indicates that the OpenID Connect provider is enabled in the appliance
- Discovery URI - The URI (Uniform Resource Identifier) of the OpenID Connect provider
- Registration Status - Can be one of the following:
  - Successful - Indicates a successful registration with the OpenID Connect provider
  - Failed - Indicates an unsuccessful registration with the OpenID Connect provider. The 'Failed' OpenID Connect provider registration will not be allowed even when they are enabled.
  - In Progress - This status is displayed when the appliance tries to register with OpenID Connect provider.

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

On the **Application Settings** > **Users** > **OpenID Connect Providers** page you can do the following:

- Add an OpenID Connect provider to OpenManage Enterprise on page 169
- Edit an OpenID Connect provider details in OpenManage Enterprise on page 171
- Test the registration status of OpenManage Enterprise with the OpenID Connect provider on page 171
- Enable OpenID Connect providers on page 172
- Disable OpenID Connect providers on page 172
- Delete OpenID Connect providers on page 172

Add an OpenID Connect provider to OpenManage Enterprise

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

About this task

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

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

Steps

1. Click **Add** to activate the Add New OpenID Connect Provider page.
2. Fill the following information in the respective fields:
   a. Name - Name for the OIDC client.
   b. Discovery URI - Uniform Resource Identifier of the OIDC provider
   c. Authentication type - Choose from one of the following methods the access token must use to access the appliance:
      i. Initial Access Token - Provide the Initial access token
      ii. Username and Password - Provide the username and password
   d. (Optional) Certificate Validation check box - You can select the check box and upload the OIDC provider's certificate by clicking **Browse** and locating the certificate or by dragging and dropping the certificate in the 'broken line' box.
   e. (Optional) Test connection - Click **Test URI and SSL Connection** to test the connection with the OpenID Connect provider.

      ⓘ NOTE: Test connection does not depend on the username and password or the initial access token details, as it only checks for the validity of the Discovery URI provided.
   f. (Optional) Enabled check box - You can select the check box to allow the authorized client access tokens to login to the appliance.
3. Click **Finish**.

Results

The newly added OpenID Connect provider is listed on the Application Settings > Users > OpenID Connect providers page and the Client ID can be located on the right pane.

Next steps:

Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 170

Configure an OpenID Connect provider policy in Keycloak for role-based access to OpenManage Enterprise on page 170

Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise

To enable OpenManage Enterprise OpenID Connect login using PingFederate, you must add and map a scope **dxcua** (Dell extended claim for user authentication) to the Client ID and define the user privileges as follows:

About this task

WARNING: **User roles and scopes are reset to 'default' on client re-registration with OIDC provider PingFederate (PingIdentity). This issue might reset the privileges and scope of non-admin roles (DM and Viewer) to that of the Administrator. Re-registration of the appliance console with OIDC provider is triggered in the event of an appliance upgrade, change in network configuration, or change in SSL certificate.**

To avoid security concerns post any of the above-mentioned re-registration events, the administrator must reconfigure all the OpenManage Enterprise Client IDs on the PingFederate site. Also, it is highly recommended that Client IDs are created only for Administrator users with Pingfederate till this issue is resolved.

NOTE:

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

Steps

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

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

        iii. Viewer: `dxcua : [{"Role": "VE"}]`
    d. If an 'exclusive' scope is configured after the client registration in OpenManage Enterprise, edit the configured client in PingFederate and enable the created 'dxcua' exclusive scope.
3. **Dynamic client registration** should be enabled in PingFederate for OpenManage Enterprise client registration. If the 'Require Initial access token' option is unselected in OpenID Connect provider client settings, the registration will work with Username and password. If the option is enabled, then the registration will work only with the Initial Access token.

Configure an OpenID Connect provider policy in Keycloak for role-based access to OpenManage Enterprise

To enable OpenManage Enterprise OpenID Connect login using Keycloak, you must first add and map a scope **dxcua** to the Client ID and define the user privileges as follows:

About this task

NOTE: The Discovery URI specified in the OpenID Connect provider configuration wizard should have a valid endpoint of the provider listed.

Steps

1. In the Attributes section of Keycloak Users, define the 'Key and Value' for OpenManage Enterprise login roles using one of the following attributes:
    - Administrator : `dxcua : [{"Role": "AD"}]`

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

  ⓘ **NOTE:** To restrict access of the device manager to select device groups, say G1 and G2, in OpenManage Enterprise use `dxcua : [{"Role": "DM", "Entity":"G1, G2"}]`
- Viewer: `dxcua : [{"Role": "VE"}]`

2. Once the client is registered in Keycloak, in the Mappers section, add a "User Attribute" mapper type with below values:
   - Name: dxcua
   - Mapper Type: User Attribute
   - User Attribute: dxcua
   - Token Claim Name: dxcua
   - Claim Json Type: String
   - Add to ID Token: enable
   - Add to access Token: Enable
   - Add to user info: Enable

Test the registration status of OpenManage Enterprise with the OpenID Connect provider

About this task

On the **Application Settings** > **Users** > **OpenID Connect Providers** page do the following:

Steps

1. Select an OpenID Connect provider.
2. On the right pane, click **Test Registration Status**.

   ⓘ **NOTE:** Test connection does not depend on the username and password or the initial access token details, as it only checks for the validity of the Discovery URI.

Results

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

Edit an OpenID Connect provider details in OpenManage Enterprise

About this task

On the **Application Settings** > **Users** > **OpenID Connect Providers** page do the following:

Steps

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

Enable OpenID Connect providers

If an OpenID Connect provider's login was not enabled at the time when it was added to the appliance, then to activate the login you must 'enable' it in the appliance.

About this task

On the **Application Settings** > **Users** > **OpenID Connect providers** page do the following:

Steps

1. Select the OpenID Connect provider(s).
2. Click **Enable**.

Results

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

Delete OpenID Connect providers

About this task

On the **Application Settings** > **Users** > **OpenID Connect Providers** page do the following:

Steps

1. Select the OpenID Connect provider(s).
2. Click **Delete**.

Disable OpenID Connect providers

About this task

On the **Application Settings** > **Users** > **OpenID Connect providers** page do the following:

Steps

1. Select the OpenID Connect provider(s).
2. Click **Disable**.

Results

The client access token from the 'disabled' OIDC providers will be rejected by the appliance.

Security Certificates

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

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

To generate a Certificate Signing Request (CSR), see Generate and download the certificate signing request on page 173.

Generate and download the certificate signing request

About this task

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

ⓘ NOTE: You must generate the CSR from within the OpenManage Enterprise appliance only.

Steps

1. Click **Generate Certificate Signing Request**.
2. In the **Generate Certificate Signing Request** dialog box, enter information in the fields.
3. Click **Generate**.
   A CSR is created and displayed in the **Certificate Signing Request** dialog box. A copy of the CSR is also sent to the email address you provided in your request.
4. In the **Certificate Signing Request** dialog box, copy the CSR data and submit it to the Certificate Authority (CA) while applying for an SSL certificate.
   - To download the CSR, click **Download Certificate Signing Request**.
   - Click **Finish**.

Assigning a webserver certificate to OpenManage Enterprise using the Microsoft Certificate Services

Steps

1. Generate and download the Certificate Signing Request (CSR) in OpenManage Enterprise. See Generate and download the certificate signing request on page 173
2. Open a web session to the certification server (https://x.x.x.x/certsrv) and click on the **Request a certificate** link .
3. On the Request a Certificate page, click on the **submit an advanced certificate request** link.
4. On the Advanced Certificate Request page, click on the **Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS#7 file** link.
5. On the Submit a Certificate Request or Renewal Request page do the following:
   a. In the **base-64-encoded cerficate request (CMC or PKCS#10 file or PKCS#7)** field, copy and paste the entire content of downloaded CSR.
   b. For **Certificate Template** select **Web Server**.
   c. Click **Submit** to issue a certificate.
6. On the Certificate Issued page, select the option **Base 64 encoded** and then click the **Download Certificate** link to download the certificate.
7. Upload the certificate in OpenManage by navigating to the **Application Settings** > **Security** > **Certificates**page and then clicking **Upload**.

Manage Console preferences

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

By clicking **OpenManage Enterprise** > **Application Settings** > **Console Preferences**, you can set the default properties of the OpenManage Enterprise GUI. For example, default time after which a device health is automatically checked and updated on the dashboard, and preferred settings used for discovering a device. The following options are available:

1. **Report Settings**: To set the maximum number of rows that you can view on OpenManage Enterprise reports:
   a. Expand **Report Settings**.
   b. Enter a number in the **Reports row limit** box. The default limit is set at 1,000 rows, however, the maximum rows permitted is 2,000,000,000.
   c. Click **Apply**. A job is run and the setting is applied.
2. **Device Health**: To set the time after which the health of the devices must be automatically monitored and updated on the OpenManage Enterprise Dashboard:

a. Expand **Device Health**.

b. Enter the frequency at which the device health must be recorded and data stored.

c. Select:

- **Last Known**: Display the latest recorded device health when the power connection was lost.
- **Unknown**: Display the latest recorded device health when the device status moved to 'unknown'. A device becomes unknown to OpenManage Enterprise when the connection with iDRAC is lost and the device is not anymore monitored by OpenManage Enterprise.

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

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

> NOTE: The device naming choices in the General Device Naming and the Server Device Naming are independent of each other and they do not affect each other.

a. **General Device Naming** applies to all the discovered devices other than the iDRACs. Select from one of the following naming modes:

- **DNS** to use the DNS name.
- **Instrumentation (NetBIOS)** to use the NetBIOS name.

> NOTE:
> - The default setting for General Device Naming is **DNS**.
> - If any of the discovered devices do not have the DNS name or the NetBIOS name to satisfy the setting, then the appliance identifies such devices with their IP addresses.
> - When the **Instrumentation(NetBios)** option is selected in **General Device Naming**, for chassis devices the **Chassis name** is displayed as the device name entry on the All Devices page.

b. **Server Device Naming** applies to iDRACs only. Select from one of the following naming modes for the discovered iDRACs:

- **iDRAC Hostname** to use the iDRAC hostname.
- **System Hostname** to use the system hostname.

> NOTE:
> - The default naming preference for iDRAC devices is the **System Hostname** .
> - If any of the iDRACs do not have the iDRAC hostname or the System hostname to satisfy the setting, then the appliance identifies such iDRACs using their IP addresses.

c. To specify the invalid device hostnames and the common MAC addresses expand the **Advance Settings**

i. Enter one or more invalid hostnames separated by a comma in **Invalid Device Hostname**. By default, a list of invalid device hostname is populated.

ii. Enter the common MAC addresses separated by a comma in **Common MAC Addresses**. By default, a list of common MAC addresses is populated.

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

4. **Server Initiated Discovery**. Select one of the following discovery-approval policies:

- **Automatic**: To allow servers with iDRAC Firmware version 4.00.00.00, which are on the same network as the console, to be discovered automatically by the console.
- **Manual**: For the servers to be discovered by the user manually.
- Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.

5. **MX7000 Onboarding Preferences**: Specify one of the following alert-forwarding behavior on MX7000 chassis when they are onboarded:

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

6. **Built-in Appliance Share**: Select one of the following external network share options that the appliance must access to complete operations such as updating of the device firmware and/or drivers, extraction and deployment of templates and profiles, and for downloading of the diagnostic and technical support reports:

> NOTE: The share type or the credentials of an active network share cannot be changed if the appliance tasks are using that network share.

- **CIFS**(Default):
  - **Enable V1**: To enable SMBv1.
  - **Enable V2**(Default): To enable SMBv2.

> NOTE: Ensure to enable SMBv1 in the **SMB Settings** before you begin any tasks which need communication with any chassis or the PowerEdge YX2X and YX3X servers that have iDRAC version 2.50.50.50 and earlier. For

more information, see the Openmanage Enterprise Support Matrix and Generic naming convention for Dell EMC PowerEdge servers on page 197.

- **HTTPS**: To shut the default CIFS and to enable HTTPS.

  ⓘ NOTE:

  - Device operations using HTTPS may fail on PowerEdge servers with older iDRAC firmware versions that don't support HTTPS. See Firmware and DSU requirement for HTTPS on page 191.
  - When the internal share uses HTTPS, then, template creation, template deployment, Boot to Network ISO, and firmware updation are not supported on FX2, VRTX, and M1000e chassis.
  - When the internal share uses HTTPS, then, template creation and deployment, and firmware updates are not supported on the MX7000 chassis and proxied sleds.
  - The credentials to the HTTPS share is automatically rotated every 6 hours.

7. **Email Sender Settings**: To set the address of the user who is sending an email message:
   a. Enter an email address in the **Sender Email ID** box.
   b. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.
8. **Trap Forwarding Format**: To set the trap forwarding format —
   a. Select one of the following options
      - **Original Format (Valid for SNMP traps only)**: To retain the trap data as-is.
      - **Normalized (Valid for all events)**: To normalize the trap data. When the Trap-forwarding format is set to 'Normalized,' the receiving agent such as the Syslog receives a tag containing the device IP from which the alert was forwarded.

   b. Click **Apply** to save the changes or click **Discard** to reset the settings to the default attributes.
9. **Metrics Collection Settings**: To set the frequency of the PowerManager extension data maintenance and purging do the following:
   a. In the **Data purge interval** box, enter the frequency to delete the PowerManager data. You can enter values within 30 to 365 days.
   b. Click **Apply** to save changes or click **Discard** to reset the settings to the default attributes.

Set the login security properties

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: AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Admin, DeviceManager, or Viewer).

About this task

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

- Expand **Restrict Allowed IP Range**:

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

  1. To specify the IP address range that must be allowed to access OpenManage Enterprise, select the **Enable IP Range** check box.
  2. In the **IP Range Address (CIDR)** box, enter the IP address range.

     ⓘ NOTE: Only one IP range is allowed.
  3. Click **Apply**. To reset to default properties, click **Discard**.

     ⓘ NOTE: **Apply** button will not be enabled if multiple IP ranges are entered in the **IP Range Address (CIDR) box**.
- Expand **Login Lockout Policy** :
  1. Select the **By User Name** check box to prevent a specific user name from logging in to OpenManage Enterprise.
  2. Select the **By IP address** check box to prevent a specific IP address from logging in to OpenManage Enterprise.

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

Customize the alert display

Steps

1. Click **OpenManage Enterprise** > **Application Settings>Alerts** and expand the **Alert Display Settings**.
2. Select one of the following:
   a. **All** — to enable the display of both acknowledged and unacknowledged alerts.
   b. **Unacknowledged** — to enable the display of only the unacknowledged alerts.

      ⓘ NOTE: By default, the **Alert Display Settings** is set as **Unacknowledged**.

   c. **Acknowledged** — to enable the display of only the acknowledged alerts.
3. Click **Apply**.

   Changes to the Alert Display Settings would be impact the following OpenManage Enterprise pages:
   - The upper-right corner of all the OpenManage Enterprise pages. See OpenManage Enterprise Graphical User Interface overview on page 38.
   - The Dashboard page. See Monitor devices by using the OpenManage Enterprise dashboard on page 40.
   - The Devices page. See Donut chart on page 41.
   - The **Alert Log** table under the Alerts page. See View alert logs on page 124.

Configure SMTP, SNMP, and Syslog alerts

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

To configure and authenticate the SMTP server that manages the email communication between the users and OpenManage Enterprise:

1. Expand **Email Configuration**.
2. Enter the SMTP server network address that sends email messages.
3. To authenticate the SMTP server, select the **Enable Authentication** check box and enter the username and password.
4. By default, the SMTP port number to be accessed is 25. Edit if necessary.
5. Select the **Use SSL** check box to secure your SMTP transaction.
6. To test if the SMTP server is working properly, click on the **Send Test Email** check box and enter an **Email Recipient**.
7. Click **Apply**.
8. To reset the settings to default attributes, click **Discard**.

To configure the SNMP alert forwarding configuration:

1. Expand **SNMP Alert Forwarding Configuration**.
2. Select the **ENABLED** check box to enable the respective SNMP traps to send alerts in case of predefined events.
3. In the **DESTINATION ADDRESS** box, enter the IP address of the destination device that must receive the alert.

   ⓘ NOTE: Entering of the console IP is disallowed to avoid duplication of alerts.
4. From the **SNMP VERSION** menu select the SNMP version type as SNMPv1, SNMPv2, or SNMPv3 and fill the following fields:
   a. In the COMMUNITY STRING box, enter the SNMP community string of the device that must receive the alert.
   b. Edit the PORT NUMBER if needed. Default port number for SNMP traps=162. See Supported protocols and ports in OpenManage Enterprise on page 34.
   c. If SNMPv3 is selected, provide the following additional details:
      i. USERNAME: Provide a username.

   ii. AUTHENTICATION TYPE : From the drop down list select SHA, MD_5, or None.
   iii. AUTHENTICATION PASSPHRASE: Provide an authentication passphrase having a minimum of eight characters.
   iv. PRIVACY TYPE: From the drop down list select DES, AES_128, or None.
   v. PRIVACY PASSPHRASE: Provide a privacy passphrase containing a minimum of eight characters.
5. To test an SNMP message, click the **Send** button of the corresponding trap.
6. Click **Apply**. To reset the settings to default attributes, click **Discard**.

To update the Syslog forwarding configuration:

1. Expand **Syslog Forwarding Configuration**.
2. Select the check box to enable the Syslog feature on the respective server in the **SERVER** column.
3. In the **DESTINATION ADDRESS/HOST NAME** box, enter the IP address of the device that receives the Syslog messages.
4. Default port number by using UDP=514. Edit if necessary by entering or selecting from the box. See Supported protocols and ports in OpenManage Enterprise on page 34.
5. Click **Apply**.
6. To reset the settings to default attributes, click **Discard**.

Manage incoming alerts

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.

About this task

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

- To set the SNMP credentials for incoming alerts:

Steps

1. Select the **SNMPV3 Enable** check box.
2. Click **Credentials**.
3. In the **SNMP Credentials** dialog box:
   a. In the **User Name** box, enter the login ID of the user who manages the OpenManage Enterprise settings.
   b. From the **Authentication Type** drop-down menu, select either the **SHA** or **MD_5** algorithm as the authentication type.
   c. In the **Authentication Passphrase** box, enter the passphrase pertaining to SHA or MD_5 based on your selection.
   d. From the **Privacy Type** drop-down menu, select either DES or AES_128 as your encryption standard.
   e. In the **Privacy Passphrase** box, enter the passphrase based on your privacy type.
   f. Click **Save**.
4. In the **Community** box, enter the community string to receive the SNMP traps.
5. By default, the SNMP port number for the incoming traps is 162. Edit to change the port number.
6. Click **Apply**.
   The SNMP credentials and settings are saved.
7. To reset the settings to default attributes, click **Discard**.

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

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

Set SNMP Credentials

About this task

Steps

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

Manage warranty settings

Warranty settings determine the display of warranty statistics by the OpenManage Enterprise on the home page Alert widget, scoreboard across all pages, the Warranty page, and the reports.

About this task

To change the warranty settings:

Steps

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

Check and update the version of the OpenManage Enterprise and the available plugins

From the **Console and Plugins** page, you can check and update the OpenManage Enterprise version and install and update plugins. To go to the **Console and Plugins** page, click **Application Settings** > **Console and Plugins**.

On the **Console and Plugins** page, you can do the following:

- View the current version of your OpenManage Enterprise, check if updates are available, and then upgrade to a newer version. You can click the **Update Settings** button to:
  - Choose to check for the updates Automatically or Manually.
  - Choose from the Dell.com (Online) or Network Share (Offline) modes of updating the appliance.

  For more information about upgrading from dell.com or network share, see Configure and upgrade OpenManage Enterprise using online method on page 179 or Configure OpenManage Enterprise and perform offline upgrade using network share on page 181 respectively.
- Click **Install** for the plugin you want to install to enhance the functionality of the appliance. For more information about installing plugins, see plugin.

  ⓘ NOTE:
  - The OpenManage Enterprise Advanced license is required for the plugins to be fully functional after installation. For more in-depth information about the plugins, refer the respective documentation available on the Dell Support site.
  - Installing a plugin on OpenManage Enterprise restarts the appliance services.
- With the already-installed plugins you can do the following:

- Disable the plugin. See Disable a plugin on page 183
- Enable the plugin. See Enable plugin on page 184
- Uninstall the plugin. See Uninstall a plugin on page 184

Upgrade Recommendations and Prerequisites

Administrators must consider the following before updating to the latest version:

- Take a VM snapshot of the console as a backup in case something unexpected occurs. Allocate more downtime for this if necessary.
- Allocate at least an hour for the update process. Allocate more time if the update must be downloaded by using a slower network connection.
- Check the storage utilization percentage in the Resource Utilization home screen widget. If the storage utilization is more than 33%, it is recommended to add twice the size of current hard disk size using the **Configure Appliance Disk Size** option in the Text User Interface (TUI). For example, consider expanding the available HD space to 300 GB if the initial allocation is 100 GB.
- Ensure that no device configuration, deployment, or extension (plug-in) tasks are running or are scheduled to run during the planned downtime. Any active or scheduled tasks or policies are terminated without further warning during the update.
- Post deletion of devices, a restart of services using TUI is recommended before initiating a console upgrade. Otherwise, the upgrade may fail and the console would reboot with the previous working state of the appliance.
- Notify other console users of the impending scheduled update.
- If the upgrade fails, the appliance would restart. It is recommended to revert the VM snapshot and upgrade again.

> ⓘ NOTE:
>
> - Only OpenManage Enterprise versions starting 3.6 and later can be directly updated to version 3.8 by the **Automatic** > **Online** method.
> - OpenManage Enterprise versions earlier than version 3.6, for example, version 3.5.x and version 3.4.x, must first be updated to version 3.6.x before considering an upgrade to version 3.8.x.
> - OpenManage Enterprise—Tech Release version should be first upgraded to OpenManage Enterprise either version 3.0 or 3.1.
> - When you update OpenManage Enterprise with up to 8000 discovered devices, the update task completes in two to three hours. During this time, the services might become unresponsive. It is then recommended to gracefully reboot the appliance. After the reboot, normal functionality of the appliance is restored.
> - Upgrade time for an appliance with Power Manager plugin installed, might be between 1 and 10 hours depending on the number of devices being monitored by Power Manager.
> - Adding a second network interface should be done only after the completion of the post-console upgrade tasks. Attempt to add a second NIC while the post-upgrade task is in progress would be ineffective.
> - You can log in immediately after the appliance is updated and do not have to wait until the entire inventory is discovered. Post update, the discovery task will run in the background and you can see the progress occasionally.
> - Clicking **Update** would initiate an Upgrade Bundle Download job. This job finishes automatically after all the update files are downloaded and cannot be terminated by the user.

Configure and upgrade OpenManage Enterprise using online method

OpenManage Enterprise can be upgraded online, either automatically or manually, from Dell.com (https://downloads.dell.com/openmanage_enterprise).

Prerequisites

- You must have the administrator privileges to perform the upgrade. For more information about privileges, see Role and scope based access control in OpenManage Enterprise on page 18.
- You must ensure that the OpenManage Enterprise appliance can access Dell.com and the expected update.

About this task

Upgrading OpenManage Enterprise is a two-step process. First, Configure the appliance for online update on page 180 to specify how to get the updates and specify the update method, and then Upgrade OpenManage Enterprise using online method on page 180 from the Console and Plugins page. Configuring the Update Settings is a one-time process. Once the update settings are configured, you can click the refresh icon in the Update section to see if an updated version is available to download.

Configure the appliance for online update

Steps

1. Click **Application Settings** > **Console and Extension** > **Update Settings**.
2. In **How to check for updates** , select one of the following options:
   - **Automatic**: The appliance checks for the availability of the updates automatically every Monday from the source specified in the **Where to check for updates**.
   - **Manual**: User has to manually check for the availability of the update from the source specified in the **Where to check for updates** by clicking the Refresh list icon in the Updates section on the Console and Plugins page.
3. In **Where to check for updates**, select **dell.com** to specify the location from where the appliance will check for updates.
4. Optional: Select the **Automatically start the console update when downloads are complete** check box to initiate an installation of the console update immediately after the update package is downloaded. Otherwise, the update can be initiated manually.
5. Click **Apply**.

   The appliance checks for updates directly from https://downloads.dell.com/openmanage_enterprise.

Next steps

Update the appliance using online method.

Upgrade OpenManage Enterprise using online method

Prerequisites

Before you begin the update from dell.com, ensure the following:

- Ensure the update settings is configured for online update. See Configure and upgrade OpenManage Enterprise using online method on page 179.
- Ensure that you have gone through all the upgrade prerequisites and recommendations as mentioned in Upgrade Recommendations and Prerequisites on page 179.
- Ensure to take a VM snapshot of the console as a backup in case something unexpected occurs. Allocate more downtime for this if necessary.

Steps

1. Based on the update settings, the appliance checks for the availability of an update and if a new version is available, a banner with the new upgrade version information is displayed. On the banner, the administrator can choose to dismiss the notification, be reminded later, or can click **View Now** to know details such as the version and size of the update available on the **Application Settings** > **Console and Plugins** page. The OpenManage Enterprise section of the Console and Plugins page displays all the new features and enhancements of the available update.
2. Click **Update** and then click **Download Console** to download the package from the specified source.

   NOTE:

   - Clicking **Update** initiates an Upgrade Bundle Download job. This job finishes by itself after all the update files are downloaded and cannot be terminated.
   - If the upgrade fails, the appliance would restart. It is recommended to revert the VM snapshot and upgrade again
3. If the **Automatically start the console update when downloads are complete** check box is selected in the Update settings, the upgrade will start automatically·after the update package is downloaded. Otherwise, click **Update Console** to perform the update.

Configure OpenManage Enterprise and perform offline upgrade using network share

You must set up a local network share and manually download the update package when you are not automatically connected to Dell.com. An audit log is created after every manual attempt to find an update.

Prerequisites

Before you begin the update from a network share:

- You must have the administrator privileges to perform the upgrade. For more information about privileges, see Role and scope-based access control in OpenManage Enterprise on page 18.
- Ensure that you have read the general upgrade recommendations and prerequisites as mentioned in Upgrade Recommendations and Prerequisites on page 179.
- For the offline updates (Network Share), the Administrator should create appropriate folder structures depending on whether a minimal or a full upgrade is needed and then download the applicable files from https://downloads.dell.com and save on the network share. For more information about updating OpenManage Enterprise to the latest version and permissible folder structure for updates, see the Upgrade the Dell EMC OpenManage Enterprise appliance version (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) technical white paper on the support site.
- Take a VM snapshot of the console as a backup in case something unexpected occurs. (Allocate more downtime for this, if necessary).
- If the upgrade fails, the appliance would restart. It is recommended to revert the VM snapshot and upgrade again.
- Adding a second network interface should be done only after the completion of the post-console upgrade tasks. Attempt to add a second NIC while the post-upgrade task is in progress would be ineffective.
- You must ensure that the security certificates are signed by a trusted third-party certificate authority when using the HTTPS method of update.

About this task

ⓘ **NOTE:** OpenManage Enterprise versions earlier than version 3.6, for example, version 3.5 and version 3.4.x, must first be updated to version 3.6.x before considering an upgrade to 3.8.x through a shared Network File Share (NFS).

Upgrading OpenManage Enterprise from a network share is a two-step process. First, Configure the appliance to update from a network share on page 181 to specify how to get the updates and the update method and then Update the appliance from a network share on page 182 from the Console and Plugins page.

Configure the appliance to update from a network share

Steps

1. Download the applicable files from https://downloads.dell.com and save on a network share preserving the same folder structure that can be accessed by the console.

   For more information about updating OpenManage Enterprise to the latest version and permissible folder structure for updates, see the Upgrade the Dell EMC OpenManage Enterprise appliance version (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) technical white paper on the support site.
2. Click **Application Settings** > **Console and Extension** > **Update Settings**.
3. In **How to check for updates**, select one of the following options:
   - **Automatic**: The appliance checks for the availability of the updates automatically every Monday from the source specified in the **Where to check for updates**.
   - **Manual**: User has to manually check for the availability of the update from the source specified in the **Where to check for updates** by clicking the Refresh list icon in the Updates section on the Console and Plugins page.
4. In **Where to check for updates**, select **Network Share** option to specify the location from where the appliance will check for updates.
   a. In **Local Path**, specify an NFS, HTTP, or HTTPS path that contains the downloaded files. The format of a network share is: `nfs://<IP Address>/<Folder_Name>, http://<IP Address>/<Folder_Name>, or https://<IP Address>/<Folder_Name>`.
   b. To verify the connection to the specified network share, click **Test Now**.

5. Optional: Select the **Automatically start the console update when downloads are complete** check box to initiate an installation of the console update immediately after the update package is downloaded. Otherwise, the update can be initiated manually.
6. Click **Apply**.

Update the appliance from a network share

Prerequisites

- Ensure that you have read the prerequisites and recommendations as mentioned in the Upgrade Recommendations and Prerequisites on page 179.
- Make sure the update settings is configured for update from a network share. See *Configure the appliance to update from a network share*.

Steps

1. Based on the update settings, the appliance checks for the availability of an update and if a new version is available, a banner with the new upgrade version information is displayed. On the banner, the administrator can choose to dismiss the notification, and be reminded later, or can click **View Now** to know details such as the version and size of the update available on the **Application Settings** > **Console and Plugins** page. The OpenManage Enterprise section of the Console and Plugins page displays all the new features and enhancements of the available update.
2. Click **Update** and then click **Download Console** to download the package from the specified source.

   ⓘ NOTE:

   - Clicking **Update** initiates an Upgrade Bundle Download job. This job finishes by itself after all the update files are downloaded and cannot be terminated.
   - If the upgrade download has a problem connecting through proxy, uncheck the proxy settings and then download.
3. If **Automatically start the console update when downloads are complete** check box is selected in the Update settings, the upgrade will start automatically after the update package is downloaded. Otherwise, click **Update Console** to perform the update.

Next steps

Log in after the update and confirm that the product works as expected. Check the audit log for any warnings or errors that are related to the update. If any errors, export the audit log and save for tech support.

After the appliance is updated:

- Clear the browser cache. Not clearing the browser cache, may cause failing of new tasks post update.
- If upgrading from OpenManage Enterprise version 3.1, it is recommended that you re-configure or import the Active Directory groups for enhanced performance.
- You can log in immediately after the appliance is updated and don't have to wait till the entire inventory is discovered. Post update, the discovery task will run in the background and you can see the progress occasionally.

Install a plugin

You can install the CloudIQ, Power Manager, OpenManage Enterprise Services (formerly SupportAssist-Enterprise), and Update Manager plugins based on your requirements to enhance the functionality of OpenManage Enterprise.

Prerequisites

- To install OpenManage Enterprise plugins from Dell.com, ensure that the OpenManage Enterprise appliance can access downloads.dell.com.
- To install OpenManage Enterprise plugins from a local network share, you must manually download the package to your network share and update the location on the Update Settings page in OpenManage Enterprise.

For more information about Update Settings configuration, see Check and update the version of the OpenManage Enterprise and the available plugins on page 178.

About this task

ⓘ NOTE: Installing a plugin on OpenManage Enterprise restarts the appliance services.

To install a plugin, perform the following steps:

Steps

1. In OpenManage Enterprise, click **Application Settings** > **Console and plugins**
   The **Console and Plugins** page is displayed.
2. In the **Plugins** section, click **Install** for the plugin you want to install.
   The **Install Plugin** wizard is displayed.
3. From the **Available Version(s)** list, select the version that you want to install.
4. Review and ensure that you meet the list of prerequisites that are mentioned under the **Prerequisite** section, and then click **Download Plugin**.

   ⓘ NOTE: The lists of prerequisites change as you select the version of plugin that you want to install.

   The install operation validates the prerequisites to install the plugin. If installation prerequisites are not fulfilled, an appropriate error message is displayed.

   After the plugin is downloaded successfully, the status that appears on the top of the plugin changes from **Available** to **Downloaded**.
5. To install the OpenManage Enterprise plugin, in the **Install Plugin** wizard, click **Install Plugin**.
6. A consent form is displayed to inform you about the End User License Agreement (EULA). Click **Accept** to continue to install the plugin.
   The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirmation** dialog box.
7. To confirm the installation, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action** option, and then click **Confirm Install**.
   The status of installation operation is displayed. After the successful installation of the plugin, the status that appears on the top of the plugin section changes from **Available** or **Downloaded** to **Installed**.

Disable a plugin

Disables all the functionality of the plugin on OpenManage Enterprise.

About this task

ⓘ NOTE: Disabling a plugin on OpenManage Enterprise restarts the appliance services.

Steps

1. In OpenManage Enterprise, click **Application Settings** > **Console and Plugins**.
   The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Disable** for the plugin you want to disable.
   The **Disable Plugin** wizard is displayed.
3. To disable the plugin, click **Disable Plugin**.
   The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirmation** dialog box.
4. To confirm, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action.** option, and then click **Confirm Disable**.

Results

ⓘ NOTE: After disabling the plugin, you cannot see any information or pages related to the plugin on OpenManage Enterprise.

Uninstall a plugin

Uninstalls and deletes all the data that is collected by the plugin.

Steps

1. In OpenManage Enterprise, click **Application Settings** > **Console and Plugins**.
   The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Uninstall** for the plugin you want to uninstall.
   The **Uninstall Plugin** wizard is displayed.
3. To uninstall the plugin from the OpenManage Enterprise, click **Uninstall Plugin**.
   The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirmation** dialog box.
4. To confirm the uninstall, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action.** option, and then click **Confirm Uninstall**.

Results

All functionality and data associated with the plugin will be uninstalled.

Enable plugin

About this task

All plugin pages are displayed on OpenManage Enterprise and plugin functionality is enabled on OpenManage Enterprise.

ⓘ NOTE: Enabling a plugin on OpenManage Enterprise restarts the appliance services.

Steps

1. In OpenManage Enterprise, click **Application Settings** > **Console and Plugins**.
   The **Console and Plugins** tab is displayed.
2. In the **Plugins** section, click **Enable** for the plugin you want to enable.
   The **Enable Plugin** wizard is displayed.
3. To enable the plugin, click **Enable Plugin**.
   The details of the number of users logged in to OpenManage Enterprise, tasks in progress, and schedule jobs are displayed in the **Confirmation** dialog box.
4. To confirm, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action.** option, and then click **Confirm Enable**.

Update a plugin

Based on the update settings, the appliance checks for the availability of an update of the installed plugins. If a new version is available, a banner with the new upgrade version information is displayed. On the banner, the administrator can choose to dismiss the notification, be reminded later, or can click **View Now** to know details such as the version and size of the update available on the **Application Settings** > **Console and Plugins** page. The Plugin section of the Console and Plugins page displays all the new features and enhancements of the available plugin update.

Prerequisites

Before you update a plugin, ensure that the update settings is configured as mentioned in Check and update the version of the OpenManage Enterprise and the available plugins on page 178.

Steps

To update a plugin, do the following:

1. In the Plugin section, click **Update Available** for the plugin you want to update.
   The **Update Plugin** page is displayed.
2. Select the plugin version, and then click **Download Plugin**.
   The plug-in is downloaded, and the status of the download is displayed on a green color band.

3. To update the plugin, click **Update Plugin**.
   In the **Confirmation** window, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action** option, and then click **Update**.

Results

After update operation is complete, the version is displayed in the plugin section.

Execute remote commands and scripts

About this task

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

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

Steps

1. Click **Application Settings** > **Script Execution**.
2. In the **Remote Command Setting** section, do the following:
   a. To add a remote command, click **Create**.
   b. In the **Command Name** box, enter the command name.
   c. Select any one of the following command type:
      i. Script
      ii. RACADM
      iii. IPMI Tool
   d. If you select **Script**, do the following:
      i. In the **IP Address** box, enter the IP address.
      ii. Select the authentication method: **Password** or **SSH Key**.
      iii. Enter the **user name** and **password** or the **SSH Key**.
      iv. In the **Command** box, type the commands.
         - Up to 100 commands can be typed with each command required to be on a new line.
         - Token substitution in scripts is possible. See Token substitution in remote scripts and alert policy on page 194
      v. Click **Finish**.
   e. If you select **RACADM**, do the following:
      i. In the **Command Name** box, enter the command name.
      ii. In the **Command** box, type the commands. Up to 100 commands can be typed with each command required to be on a new line.
      iii. Click **Finish**
   f. If you select **IPMI Tool**, do the following:
      i. In the **Command Name** box, enter the command name.
      ii. In the **Command** box, type the commands. Up to 100 commands can be typed with each command required to be on a new line.
      iii. Click **Finish**
3. To edit a remote command setting, select the command, and then click **Edit**.
4. To delete a remote command setting, select the command, and then click **Delete**.

OpenManage Mobile settings

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

- Receive alert notifications from OpenManage Enterprise.
- View the group, device, alert, and log information.

- Turn on, turn off, or restart a server.

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

ⓘ NOTE: For information about installing and using OMM, see the *OpenManage Mobile User's Guide* at Dell.com/OpenManageManuals.

Related tasks

Enable or disable alert notifications for OpenManage Mobile on page 186

Enable or disable OpenManage Mobile subscribers on page 186

Delete an OpenManage Mobile subscriber on page 187

View the alert notification service status on page 187

Troubleshooting OpenManage Mobile on page 189

Related information

Enable or disable alert notifications for OpenManage Mobile on page 186

Enable or disable OpenManage Mobile subscribers on page 186

Troubleshooting OpenManage Mobile on page 189

Enable or disable alert notifications for OpenManage Mobile

About this task

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

ⓘ NOTE: The administrator rights are required for enabling or disabling alert notifications for OpenManage Mobile.

ⓘ NOTE: For OpenManage Enterprise to send alert notifications to OpenManage Mobile, ensure that the OpenManage Enterprise server has outbound (HTTPS) Internet access.

To enable or disable alert notifications from OpenManage Enterprise to OpenManage Mobile:

Steps

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

Related tasks

OpenManage Mobile settings on page 185

Related information

OpenManage Mobile settings on page 185

Delete an OpenManage Mobile subscriber on page 187

Enable or disable OpenManage Mobile subscribers

About this task

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

ⓘ NOTE:

- The administrator rights are required for enabling or disabling OpenManage Mobile subscribers.
- OpenManage Mobile subscribers may be automatically disabled by OpenManage Enterprise if their mobile service provider push notification service indicates that the device is permanently unreachable.

- Even if an OpenManage Mobile subscriber is enabled in the **Mobile Subscribers** list, they can disable receiving alert notifications in their OpenManage Mobile application settings.

To enable or disable alert notifications to the OpenManage Mobile subscribers:

Steps

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

   You can select more than one subscriber at a time.

Related tasks

OpenManage Mobile settings on page 185

Related information

OpenManage Mobile settings on page 185
Delete an OpenManage Mobile subscriber on page 187

Delete an OpenManage Mobile subscriber

About this task

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

ⓘ **NOTE:** The administrator rights are required for deleting an OpenManage Mobile subscriber.

To delete an OpenManage Mobile subscriber:

Steps

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

Related tasks

Enable or disable alert notifications for OpenManage Mobile on page 186
Enable or disable OpenManage Mobile subscribers on page 186
Delete an OpenManage Mobile subscriber on page 187
View the alert notification service status on page 187

Related information

OpenManage Mobile settings on page 185
Delete an OpenManage Mobile subscriber on page 187

View the alert notification service status

About this task

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

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

Related tasks

View the alert notification service status on page 187

Related information

OpenManage Mobile settings on page 185
Delete an OpenManage Mobile subscriber on page 187
View the alert notification service status on page 187

Notification service status

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

Table 28. Notification service status

Status Icon	Status Description
✓	The service is running and operating normally. ⓘ NOTE: This service status only reflects successful communication with the platform notification service. If the device of the subscriber is not connected to the Internet or a cellular data service, notifications will not be delivered until the connection is restored.
⚠	The service experienced an error delivering a message which may be of a temporary nature. If the issue persists, follow troubleshooting procedures or contact technical support.
✖	The service experienced an error delivering a message. Follow troubleshooting procedures or contact technical support as necessary.

View information about OpenManage Mobile subscribers

About this task

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

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

OpenManage Mobile subscriber information

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

Table 29. OpenManage Mobile subscriber information

Field	Description
ENABLED	Select or clear the check box, and then click **Enable** or **Disable** respectively to enable or disable the alert notifications to an OpenManage Mobile subscriber.
STATUS	Displays the status of the subscriber, indicating whether or not OpenManage Enterprise is able to send alert notifications successfully to the Alert Forwarding Service.
STATUS MESSAGE	Status description of the status message.