

OpenManage Enterprise Power Manager 3.0

Security Configuration Guide

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Figures.....	4
Tables.....	5
Chapter 1: PREFACE.....	6
Chapter 2: Legal disclaimers.....	7
Chapter 3: Deployment models.....	8
Chapter 4: Product and Subsystem Security	9
Security controls map.....	9
Authentication.....	9
Rest API security.....	9
Login security settings.....	9
User and credential management.....	10
Role and scope-based access control in OpenManage Enterprise	10
Data security.....	13
Cryptography.....	13
Auditing and logging.....	14
Alerting.....	14
Chapter 5: Contacting Dell.....	15

1	Security control map for Power Manager plugin.....	9
---	--	---

1	Role-based user privileges for Power Manager.....	10
---	---	----

PREFACE

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document. This document was accurate at publication time. To ensure that you are using the latest version of this document, go to <https://www.dell.com/support>

Scope of the document

This document includes information about security features and capabilities of OpenManage Enterprise Power Manager. Also, use this document to:

- Understand the security features and capabilities of the product.
- Know how to modify the configuration of the product to maximize the security posture in your environment.
- Be aware of the capabilities Dell EMC has available for secure remote and on-site serviceability.
- Be informed of the expectations Dell EMC has of the environment in which the product is deployed.

Document references

In addition to this guide, you can access other documents of OpenManage Enterprise Power Manager available at **<https://www.dell.com/support>**.

- *OpenManage Enterprise Power Manager User's Guide*
- *OpenManage Enterprise Power Manager Release Notes*
- *OpenManage Enterprise Power Manager API Guide*
- *OpenManage Enterprise User's Guide*
- *OpenManage Enterprise Release Notes*
- *OpenManage Enterprise API Guide*
- *OpenManage Enterprise Support Matrix*

Getting help

In addition to the above mentioned guides, see the OpenManage Enterprise Power Manager Online Help and OpenManage Enterprise Online Help integrated in the product.

Legal disclaimers

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages.

The Security Configuration Guide intends to be a reference. The guidance is provided based on a diverse set of installed systems and may not represent the actual risk/guidance to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. All aspects of this Security Configuration Guide are subject to change without notice and on a case-by-case basis. Your use of the information contained in this document or materials linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

Deployment models

You can download and install Power Manager plug-in from dell.com (online) or from an already downloaded package in a network share (offline). You can configure this setting in OpenManage Enterprise (**Application Settings > Console and Plugins > Update Settings**). For more information, see the *Update settings in OpenManage Enterprise* section in OpenManage Enterprise User's Guide.

Prerequisites

Ensure that your connectivity to the repository is successful:

- To connect to an online repository, connect to `downloads.dell.com` portal through proxy server, if any, for a secure connection.
- To connect to an offline repository, ensure that the offline server is configured with required plugin catalog and plugin installation files.

For more details, see OpenManage Enterprise User's Guide.

- Ensure that you have the compatible version of OpenManage Enterprise to install the latest version of Power Manager. For more information, see Dell EMC OpenManage Enterprise Power Manager User's Guide.

Steps

1. Launch Dell EMC OpenManage Enterprise, and then click **Application Settings > Console and Plugins**.
The **Console and Plugins** page is displayed.
2. In the **Power Manager** section, click **Install**.
The **Install Plugin** page is displayed.
3. Select the plugin version (if there are multiple versions of the plugin that is supported on existing OpenManage Enterprise version) from the **Available Version(s)** drop-down menu and review to ensure that you meet the list of prerequisites that are mentioned in the **Prerequisites** section.

 **NOTE:** Only the versions of the plugin that is supported on the installed version of OpenManage Enterprise is listed in the **Available Version(s)** drop-down menu.

4. Click **Download plugin**.
The progress of download is displayed, and then the plugin is downloaded and the status of the plugin is updated to **Downloaded** on the **Console and Plugins** page.
5. In **Install Details** page, click **Install plugin**.
The **Install Plugin** window is displayed.

Product and Subsystem Security

Topics:

- [Security controls map](#)
- [Authentication](#)
- [Rest API security](#)
- [Login security settings](#)
- [User and credential management](#)
- [Role and scope-based access control in OpenManage Enterprise](#)
- [Data security](#)
- [Cryptography](#)
- [Auditing and logging](#)

Security controls map

Power Manager uses fine-grained instrumentation to provide increased visibility to power consumption, anomalies, and utilization. Power Manager alerts and reports about power and thermal events in servers, chassis, and custom groups consisting of servers and chassis. This reporting enables increased control, faster response times, greater accuracy, and broader decision-making intelligence than is otherwise possible.

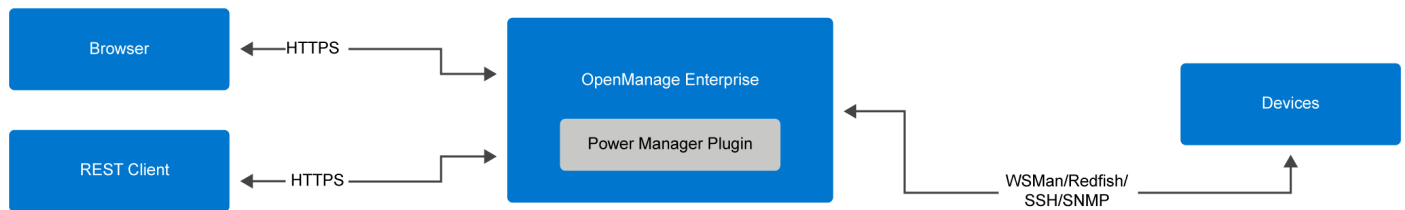


Figure 1. Security control map for Power Manager plugin

Authentication

Access control settings provide protection of resources against unauthorized access. Only Administrators, Device Managers, and Viewers have access to Power Manager plug-in features with appropriate roles and privileges configured. For feature-based access details, see the OpenManage Enterprise Power Manager and OpenManage Enterprise User's Guide.

Rest API security

For the rest API security-related information, see the *Security* section in OpenManage Enterprise Power Manager RESTful API Guide.

Login security settings

There are various security configurations available in OpenManage Enterprise which when applied in OpenManage Enterprise gets automatically applied to Power Manager plug-in. For example, you can provide an IP range where only the devices that are specified in the IP range can access OpenManage Enterprise, block a user by specifying the username or an IP address, or lock a user for a specific duration after multiple failed attempts. For more details, see the *Set the login security properties* topic in OpenManage Enterprise User's Guide.

User and credential management

Each user is assigned certain privileges that determine their access level in OpenManage Enterprise. For information about the user roles and feature-based access privileges for OpenManage Enterprise and Power Manager, see the Dell EMC OpenManage Enterprise User's Guide and Dell EMC OpenManage Enterprise Power Manager User's Guide.

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.

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

Table 1. Role-based user privileges for Power Manager

Features	Administrator	Device Manager (scope for assigned groups)	Device Manager (scope for non-assigned groups)	Viewer
Install Power Manager	Yes	No	No	No
Upgrade Power Manager	Yes	No	No	No
Enable Power Manager	Yes	No	No	No
Disable Power Manager	Yes	No	No	No
Uninstall Power Manager	Yes	No	No	No
Add or remove supported devices from Power Manager	Yes	Yes	No	No
Add or remove static groups from Power Manager	Yes	Yes	No	No
Add or remove unmonitored devices from Power Manager	Yes	No	No	No
Add or remove Power Distribution Units (PDUs) from Power Manager	Yes	No	No	No
Monitor PDUs	Yes	Yes	No	Yes
Create, edit, or delete Physical Groups	Yes	No	No	No

Table 1. Role-based user privileges for Power Manager (continued)

Features	Administrator	Device Manager (scope for assigned groups)	Device Manager (scope for non-assigned groups)	Viewer
Import physical groups through CSV file	Yes	No	No	No
Manage the devices in rack	Yes	No	No	No
Monitor metrics	Yes	Yes	No	Yes
Manage power policies for devices	Yes	Yes	No	No
Manage power policies for groups	Yes	Yes	No	No
Manage temperature-triggered policies for group	Yes	Yes	No	No
Manage alert thresholds for devices	Yes	Yes	No	No
Manage alert thresholds for groups	Yes	Yes	No	No
View alert thresholds in Power Manager	Yes	Yes	No	Yes
Modify Power Manager Settings	Yes	No	No	No
View Settings	Yes	Yes	Yes	Yes
Manage Power Manager Emergency Power Reduction (EPR) for devices	Yes	Yes	No	No
Manage EPR for groups	Yes	Yes	No	No
Run and view reports for devices and groups	Yes	Yes	No	Yes
Manage custom reports for devices	Yes	Yes	No	No
Manage custom reports for groups	Yes	Yes	No	No
View events	Yes	Yes	No	Yes
Dashboard	Yes	Yes	No	Yes
Create, edit, or delete VM Groups	Yes	No	No	No
Analyze usage metrics	Yes	Yes	No	Yes
Automatically create physical hierarchy	Yes	No	No	No
View maximum and minimum power consumption of VMs on the Overview page	Yes	Yes	No	Yes

Table 1. Role-based user privileges for Power Manager (continued)

Features	Administrator	Device Manager (scope for assigned groups)	Device Manager (scope for non-assigned groups)	Viewer
Disable LCS Event-triggered EPR	Yes	No	No	No
Enable and disable Liquid cooling system alert policy	Yes	No	No	No
View maximum and minimum power consumption of VM groups on the Overview page	Yes	Yes	Yes	Yes
Update device location in device console	Yes	No	No	No
View idle servers	Yes	Yes	No	Yes

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

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*.

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* section in OpenManage Enterprise User's Guide.

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* section in OpenManage Enterprise User's Guide.

Data security

The data that is maintained by Power Manager is stored and secured in internal databases within the appliance and it cannot be accessed from outside. The data that is transferred through Power Manager is secured by secure communication channel.

Cryptography

Sensitive data is encrypted and stored in an internal database. For more information, see the *Security features in OpenManage Enterprise* section in OpenManage Enterprise User's Guide.

Auditing and logging

Power Manager lists all the actions that are performed on the monitored devices in audit logs. Use the OpenManage Enterprise console to generate the audit logs with all the relevant information. You can export the audit log files to a CSV file format.

Alerting

Automate your actions for the alerts generated, manage the alerts and forward the alerts that are generated in OpenManage Enterprise. For more information, see the *Alert policies* section in OpenManage Enterprise User's Guide.

Contacting Dell

Prerequisites

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

About this task

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

Steps

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