Dell EMC OpenManage Enterprise Update Manager 1.2

Security Configuration Guide

October 2021
Rev. A00

Notes, cautions, and warnings

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

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

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

Contents

Tables

1

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 Update 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 Update Manager available at **https://www.dell.com/support**.

- *OpenManage Enterprise Update Manager User's Guide*
- *OpenManage Enterprise Update Manager Release Notes*
- *OpenManage Enterprise Update 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 Update Manager Online Help and OpenManage Enterprise Online Help integrated in the product.

2

Deployment models

You can download and install Update 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 you are using OpenManage Enterprise version 3.6 or above.

Steps

1. Launch Dell EMC OpenManage Enterprise.
2. In **Application Settings**, click **Console and Plugins**.
3. In the **Plugins** section, click the **Install** option for Update Manager.
   The **Install Plugin** window is displayed.
4. Check for the latest available versions of update manager.
5. Click **Download Plugin**.
   Wait for the plug-in to download. The plug-in is downloaded, and the status of the download is displayed on a green color band on the top-right corner.
6. Click **Install Plugin**.

   Capture a snapshot of the OpenManage Enterprise appliance VM.

Example

For more information about installation prerequisites and installation steps, see the OpenManage Enterprise Update Manager 1.2 User's Guide.

3

Product and Subsystem Security

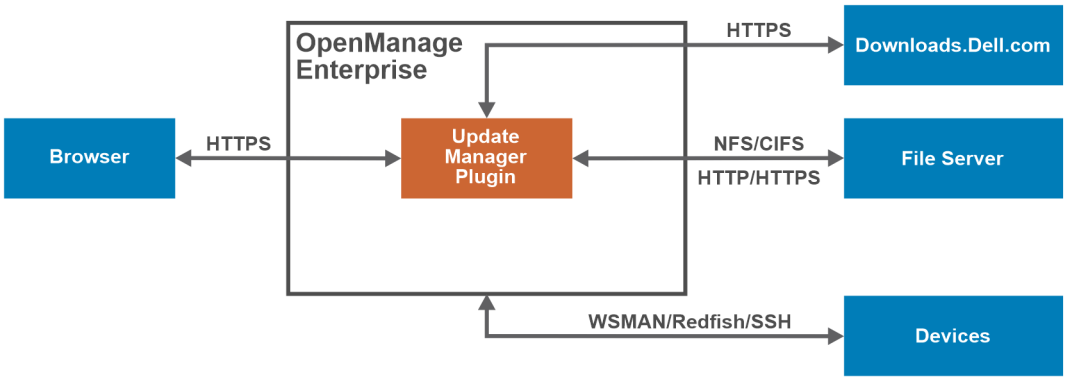
Topics:

Security controls map

Using Update Manager create and manage custom repositories for the PowerEdge devices that are discovered and managed in OpenManage Enterprise. Interact with the Update Manager UI through a browser using HTTPS protocol.

Update Manager interacts with `downloads.dell.com` through HTTPS protocol and with any network share or file server through the CIFS or NFS or HTTP or HTTPS protocols.

The following figure displays the Update Manager security controls map:



Authentication

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

Login security settings

There are various security configurations available in OpenManage Enterprise which when applied gets automatically applied to Update 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.

Failed login behavior

By default, after three unsuccessful logins, the OpenManage account is locked for 900 seconds. For more information, see *Set the login security properties* topic in OpenManage Enterprise User's Guide.

Emergency user lockout

You can block users from logging into OpenManage Enterprise, based on various parameters. For more information, see the *Set the login security properties* topic in OpenManage Enterprise User's Guide. To disable a user account, see the *Disable OpenManage Enterprise users* section 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 more information about the user roles and feature-based access privileges, see the Dell EMC OpenManage Enterprise User's Guide.

Password complexity

For information about the strength of the username and recommended password complexity, see the guidelines that are displayed on the OpenManage Enterprise user interface. For more details, see the *Configure OpenManage Enterprise by using Text User Interface* in Dell EMC OpenManage Enterprise User's Guide.

RBAC privileges

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 one role per account.

The following table lists the permissions of the Update Manager user roles.

Table 1. Role-based privileges for Update Manager

Functions	Administrator	Device Manager (DM)	Viewers
Install or uninstall Update Manager	Allowed	Not Allowed	Not Allowed
Enable or disable Update Manager	Allowed	Not Allowed	Not Allowed
Configure proxy	Allowed	Not Allowed	Not Allowed
Configure preferences	Allowed	Not Allowed	Not Allowed
Create repository	Allowed	Allowed	Not allowed
Import update package	Allowed	Allowed (Owned by DM)	Not allowed
Delete repository or bundles or update packages	Allowed	Allowed (Owned by DM)	Not allowed
Repository refresh	Allowed	Allowed (Owned by DM)	Not allowed
View repository dashboard	Allowed	Allowed (Owned by DM)	Allowed
View repositories	Allowed	Allowed (Owned by DM)	Allowed
View or edit baseline compliance report from the **Repository** page.	Allowed	Allowed (Owned by DM)	Not allowed

Also, Update Manager users use some of the OpenManage Enterprise features, the following table lists out the OpenManage Enterprise features.

Table 2. Role-based privileges for OpenManage Enterprise

Functions	Administrator	Device Manager	Viewers
Update firmware with baseline compliance report	Allowed	Allowed (Owned by DM)	Not allowed
Update Settings	Allowed	Not allowed	Not allowed
Create alert policy	Allowed	Allowed (Owned by DM)	Not allowed

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.

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:

Data security

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

You can set the storage space for Update Manager within 1 GB to 10 GB range in the **Alert when storage exceeds** field. After the data exceeds the specified space, Update Manager generates alerts to delete the existing content to create repositories. For more information, see the **Configure Update Manager preferences** section in OpenManage Enterprise Update Manager User's Guide.

Cryptography

The SHA256 signing algorithm is used to verify the signature of update packages.

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

Update 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. The following table lists all the EEMI message details that are used in Update Manager.

Table 3. EEMI messages in Update Manager

Message ID	Message Description
CUMP0001	The repository <repoName> is refreshed successfully.
CUMP0002	Unable to refresh the repository <repoName>.
CUMP0003	Repository has exceeded the configured storage limit.
CUMP0004	Unable to create the repository <repoName>.
CUMP0005	Unable to delete the repository <repoName>.
CUMP0008	Unable to import the update package into the repository <repoName>.
CUMP0011	The repository <repoName> is created successfully.
CUMP0012	The repository <repoName> is updated successfully.
CUMP0013	The repository <repoName> is deleted successfully.
CUMP0014	The configuration data is successfully updated.
CUMP0015	An update package is available for the selected catalog.
CUMP0016	An update package is unavailable for the selected catalog.
CUMP0017	The catalog <catalogName> is updated successfully.
CUMP0018	Unable to update the catalog <catalogName>.
CUMP0019	The storage space has reached or exceeded 80% of the configured value.
CUMP0020	Unable to create the repository version because the maximum number of versions are already created.
CUMP0021	The repository version <version number> of repository <repository name> is deleted successfully.
CUMP0022	The repository bundle(s) or component(s) of repository <repository name> is deleted successfully.

Table 3. EEMI messages in Update Manager (continued)

Message ID	Message Description
CUMP0023	The repository version <version number> of repository <repository name> is created successfully after performing the <task name> operation.
CUMP0024	The repository <repository name> is edited successfully.

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.

Serviceability

The support website `https://www.dell.com/support` provides access to the licensing information, product documentation, advisories, downloads, and troubleshooting information. This information helps you to resolve a product issue before you contact support team.

Ensure that you install security patches and other updates when they are available.

4

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.