

Dell EMC OpenManage Enterprise SupportAssist version 1.1

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

Chapter 1: Preface	4
Legal disclaimers	4
Scope of document	4
Audience	4
Related Documentation	4
Chapter 2: Deployment models	5
Chapter 3: Product and Subsystem Security	6
Security controls map	6
Access control	6
Login security settings	7
Failed login behavior	7
Emergency user lockout	7
User and credential management	7
Username and Password complexity	7
Role and scope-based access control in OpenManage Enterprise	7
Data security	9
Cryptography	10
Auditing and logging	10
Serviceability	10
Chapter 4: Contacting Dell	11
Chapter 5: Accessing support content from the Dell EMC support site	12

Preface

Topics:

- [Legal disclaimers](#)
- [Scope of document](#)
- [Audience](#)
- [Related Documentation](#)

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.

Scope of document

This document includes information about the security features and capabilities of OpenManage Enterprise SupportAssist.

Audience

This document is intended for individuals who are responsible for managing security for OpenManage Enterprise SupportAssist.

Related Documentation

In addition to this guide, you can access the other guides available at <https://www.dell.com/OpenManageEnterprise/ServicesPlugin>.

- Dell EMC OpenManage Enterprise SupportAssist Version 1.1 Release Notes
- Dell EMC OpenManage Enterprise SupportAssist Version 1.1 Support Matrix
- Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide
- Dell EMC OpenManage Enterprise SupportAssist Version 1.1 Reportable Items

You can find RESTful APIs exposed by OpenManage Enterprise SupportAssist at <https://api-marketplace.dell.com/>

Deployment models

You can download and install OpenManage Enterprise SupportAssist 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 about how to configure update settings, see *Dell EMC OpenManage Enterprise User's Guide*.

To install the OpenManage Enterprise SupportAssist within OpenManage Enterprise, do the following:

1. Start Dell EMC OpenManage Enterprise.
2. From the **Application Settings** menu, select **Console and Plugins**.

The **Console and Plugins** page is displayed.

3. On the **Console and Plugins** page, in the **SupportAssist** section, click **Install**.

For more information about installation prerequisites and installation steps, see the *Dell EMC OpenManage Enterprise User's Guide* available at <https://www.dell.com/OpenManageEnterprise/ServicesPlugin>

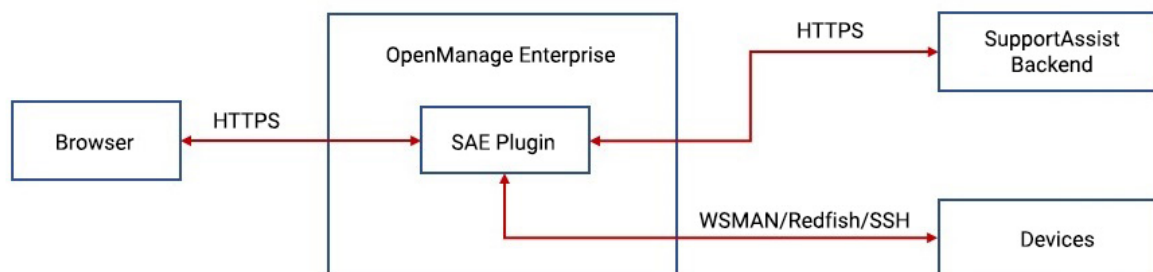
Product and Subsystem Security

Topics:

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

Security controls map

The following figure describes the OpenManage Enterprise SupportAssist security controls map.



Access control

Access control settings provide protection to the resources against unauthorized access. Monitoring and managing resources in OpenManage Enterprise SupportAssist requires necessary OpenManage Enterprise user privileges. For more information, see the section "Security features in OpenManage Enterprise" in *Dell EMC OpenManage Enterprise User's Guide*.

Login security settings

Failed login behavior

For failed login behavior, see the section "Set the login security properties" in *Dell OpenManage Enterprise User's Guide*.

Emergency user logout

For emergency user logout behavior, see the section "Ending user sessions" in *Dell OpenManage Enterprise User's Guide*.

User and credential management

For information about the user and credential management, see *Dell EMC OpenManage Enterprise User's Guide*.

Username and Password complexity

For the recommended complexity and strength of username, see the section "Add and edit OpenManage Enterprise users" in *Dell EMC OpenManage Enterprise User's Guide*.

The complexity and strength of passwords must be as per the OpenManage Enterprise recommendation. That is, as per the recommendation that is provided in the message that is displayed on the OpenManage Enterprise user interface when you enter a password that does not fulfill the required complexity and strength.

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.

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* cannot 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 us 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 that are 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.

The following table lists the SupportAssist features and their permissions based on the role that is assigned to a user. For the Device Manager role, the table also lists the permissions to the features based on the device group scope assigned. For the list of users roles and scope that you can assign to a Device Manager role for appliance settings and device management features in OpenManage Enterprise, see *Dell EMC OpenManage Enterprise User's Guide* available at <https://www.dell.com/esmmanuals>.

Table 1. Role-based and scope-based access control in OpenManage Enterprise SupportAssist

Features	Admin	Device Manager (scope for assigned device groups)	Device Manager (scope for non-assigned device groups)	Viewer
Installation	Yes	No	No	No
Update	Yes	No	No	No
Registration	Yes	No	No	No
Edit Settings	Yes	No	No	No
View Settings	Yes	Yes	Yes	Yes
Site Health	Yes	Yes (only for devices within the device group scope)	No	No
Connection Test	Yes	No	No	No

Table 1. Role-based and scope-based access control in OpenManage Enterprise SupportAssist (continued)

Features	Admin	Device Manager (scope for assigned device groups)	Device Manager (scope for non-assigned device groups)	Viewer
Cases				
Case (View and Filter)	Yes	Yes (only for devices within the device group scope)	No	Yes
Case Operation (Suspend, Resume, Request for closure)	Yes	Yes (only for devices within the device group scope)	No	No
Collections				
Collection View	Yes	No	No	Yes
Start Collection	Yes	No	No	No
Start Group Collection	Yes	No	No	No
Cancel Collection	Yes	No	No	No
Upload Collection	Yes	No	No	No
Download Collection	Yes	No	No	No
SupportAssist Device Groups				
Enable SupportAssist Maintenance Mode	Yes	Yes (only for device groups within the scope)	No	No
View Device Groups	Yes	Yes (only for devices within the device group scope)	No	Yes
Create, Delete, Edit Group	Yes	No	No	No
Device Specific Operations				
Enable SupportAssist Maintenance Mode	Yes	Yes (only for devices within the device group scope)	No	No
Start Collections	Yes	No	No	No

Data security

By default, SupportAssist collects device identification information such as the complete configuration snapshot of systems, hosts, and network devices that can contain host identification and network configuration data. Usually, part or all this data is required to properly diagnose issues. If the security policy of your company restricts sending identity data outside of the network, you can disable SupportAssist from collecting such data. For more information about how to disable SupportAssist from collecting device identification information, see the section "Enable or disable collection of identity information" in *Dell EMC OpenManage Enterprise SupportAssist User's Guide*.

The SupportAssist maintenance mode functionality suspends the alert processing and automatic case creation capability of SupportAssist, thereby preventing the creation of unnecessary support cases during an alert storm or a planned maintenance activity. You can also enable the maintenance mode functionality before a planned maintenance activity to temporarily suspend the automatic case creation capability. For more information about SupportAssist maintenance mode, see the section "SupportAssist maintenance mode" *Dell EMC OpenManage Enterprise SupportAssist User's Guide*.

Cryptography

OpenManage Enterprise SupportAssist applies cryptography in the following components.

- Access control
- Authentication
- Digital signatures

For more information, see *Dell EMC OpenManage Enterprise User's Guide*

Auditing and logging


Audit logs lists the actions that were performed on the devices that are monitored by OpenManage Enterprise. Log data help you or Dell EMC Support teams in troubleshooting and analysis. The audit log files can be exported to the CSV file format. For more information about how to export logs, see the section "Manage audit logs" in *Dell EMC OpenManage Enterprise User's Guide*.

Serviceability

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

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.

Accessing support content from the Dell EMC support site

Access supporting content related to an array of systems management tools using direct links, going to the Dell EMC support site, or using a search engine.

- Direct links:
 - For Dell EMC Enterprise Systems Management and Dell EMC Remote Enterprise Systems Management—<https://www.dell.com/esmmanuals>
 - For Dell EMC Virtualization Solutions—<https://www.dell.com/SoftwareManuals>
 - For Dell EMC OpenManage—<https://www.dell.com/openmanagemanuals>
 - For iDRAC—<https://www.dell.com/idracmanuals>
 - For Dell EMC OpenManage Connections Enterprise Systems Management—<https://www.dell.com/OMConnectionsEnterpriseSystemsManagement>
 - For Dell EMC Serviceability Tools—<https://www.dell.com/serviceabilitytools>
- Dell EMC support site:
 1. Go to <https://www.dell.com/support>.
 2. Click **Browse all products**.
 3. From the **All products** page, click **Software**, and then click the required link.
 4. Click the required product and then click the required version.

Using search engines, type the name and version of the document in the search box.