Dell EMC OpenManage Integration Version 1.2 with ServiceNow

Security Configuration Guide

June 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

Figures

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**.

Purpose

This document includes information about security features and capabilities of Dell EMC OpenManage Integration with ServiceNow

Audience

This document is intended for individuals who are responsible for managing security for ServiceNow.

Revision History

The following table presents the revision history of this document.

Table 1. Revision History

Revision	Date	Description
A00_1.2	June 2021	Initial release of the OpenManage Integration for Dell EMC OpenManage Integration Version 1.2 with ServiceNow

Related documentation

The complete documentation set for OpenManage Integration with ServiceNow (OMISNOW) is available at **https://www.dell.com/support**. Click **Browse all products**, then click **Software** > **Enterprise System Management**. Click **OpenManage Integration with ServiceNow** to access the following documents:

- *OpenManage Integration with ServiceNow 1.2 User's Guide*
- *OpenManage Integration with ServiceNow 1.2 Release Notes*
- *OpenManage Integration with ServiceNow 1.2 Installation Guide*

You can find the technical artifacts including white papers at **https://www.dell.com/support**.

2

Deployment models

OpenManage Enterprise Integration for ServiceNow is an application that is imported into ServiceNow SaaS instance which uses the MID Server (Management Instrument and Discovery) to collect information from OpenManage Enterprise, SupportAssist Enterprise Plugin, and SupportAssist Enterprise into the Configuration management database (CMDB). ServiceNow Applications include scripts (that either run on ServiceNow instance or those that run on MID Server), UI controls (User Interface), forms, mappings, CI definitions (Configuration Items) and so on. The Application is installed on ServiceNow instance, and ServiceNow publishes the relevant artifacts to MID Server as needed.

For more information on the installation procedure of OpenManage Integration with ServiceNow, see installation guide for ServiceNow at *support.dell.com*

3

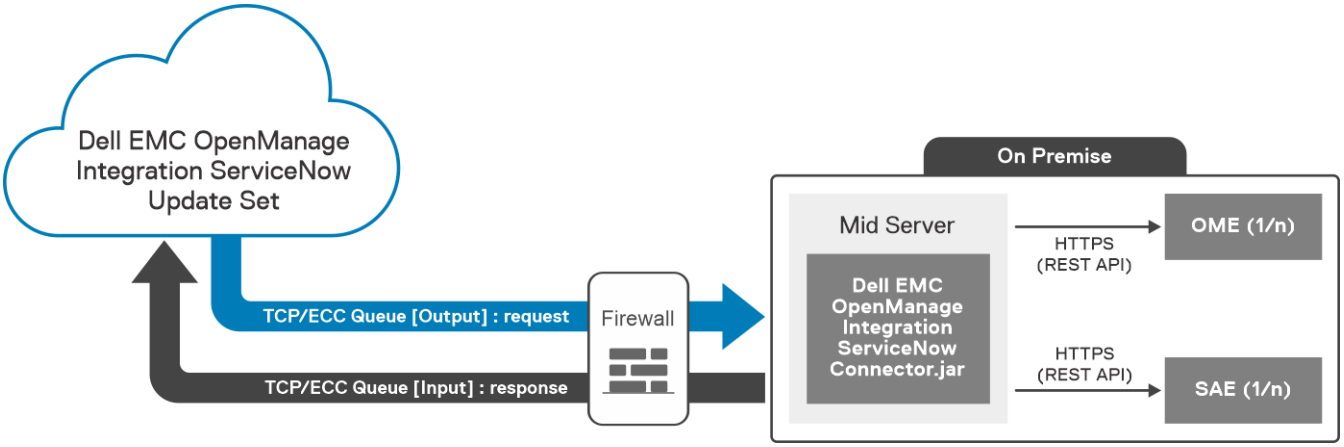
Product and Subsystem Security

Topics:

Security controls map

The following figure displays the ServiceNow security controls map:

Figure 1. Security Controls Map



Authentication

This chapter provides user an information on how authentication of user login works in ServiceNow instance.

About this task

Authentication is handled in OpenManage Integration for ServiceNow in following ways:

Steps

1. User needs to login to the ServiceNow instance using user credentials.
   The login authentication is handled by ServiceNow.
2. Once connection is established with ServiceNow instances, user should provide OME and SAE details like IP Address or hostname, username and password. OMISNOW uses these details to establish a connection with OME/SAE.

Results

The user credentials are then saved in ServiceNow instance using AES 128 or AES 256 encryption.

Required user privileges

The OpenManage Integration with ServiceNow application installs the following set of user roles in a ServiceNow instance:

- `x_310922_omisnow.OMISNOW Operator` for the OpenManage Integration Operator role.
- `x_310922_omisnow.OMISNOW User` for the OpenManage Integration User role.

Ensure that appropriate roles and privileges are assigned to the ServiceNow users to use the OpenManage Integration with ServiceNow application. If required, additional users can be created in ServiceNow and assign them OpenManage Integration Operator and User roles.

Table 2. Required user privileges

OpenManage Integration with ServiceNow features	ServiceNow Administrator	OpenManage Integration with ServiceNow Operator	OpenManage Integration with ServiceNow User
Upload the OpenManage Integration with ServiceNow update set to ServiceNow	Allowed	Not allowed	Not allowed
Deploy OpenManage Integration with ServiceNow connector .jar on a MID Server	Allowed	Not allowed	Not allowed
Create, Modify, or Delete OpenMange Enterprise connection profiles	Allowed	Allowed	Not allowed
Create, Modify, or Delete SupportAssist Enterprise connection profiles	Allowed	Allowed	Not allowed
Retrieve the server and chassis inventory information from OpenManage Enterprise instances	Allowed	Allowed	Not allowed
Retrieve all the server and chassis events from OpenManage Enterprise	Allowed	Allowed	Not allowed
Retrieve cases from SupportAssist Enterprise	Allowed	Allowed	Not allowed
View the application logs in ServiceNow	Allowed	Not allowed	Not allowed
Schedule the OME inventory collection, OME Event Collection, Server Health Collection, SAE Plugin Case Collection, SAE Case Collection intervals	Allowed	Allowed	Not allowed
View the alerts and incidents created for the retrieved events	Allowed	Allowed	Allowed

Table 2. Required user privileges (continued)

OpenManage Integration with ServiceNow features	ServiceNow Administrator	OpenManage Integration with ServiceNow Operator	OpenManage Integration with ServiceNow User
from OpenManage Enterprise			
Update the alerts and incidents	Allowed	Allowed	Not allowed
Enable or disable alert management rule	Allowed	Not allowed	Not allowed
Enable or disable alert correlation rule	Allowed	Not allowed	Not allowed
Delete OpenManage Integration application from ServiceNow	Allowed	Not allowed	Not allowed
Create or edit alert correlation rules	Allowed	Not allowed	Not allowed
Assign incidents to OME and SAE groups	Allowed	Allowed	Not allowed
Activate and deactivate transform maps	Allowed	Allowed	Not allowed
Configure parallel queues, Devices per basic inventory request, Devices per detailed inventory request	Allowed	Allowed	Not allowed
Acknowledging the OME events once incidents are created	Allowed	Allowed	Not Allowed
To log application logs in work notes	Allowed	Allowed	Not Allowed
To view, configure and delete inbound webservices	Allowed	Not Allowed	Not Allowed
To view, configure and delete staging table	Allowed	Not Allowed	Not Allowed
System Scheduler	Allowed	Not Allowed	Not Allowed
OpenManage Device health sync	Allowed	Allowed	Not Allowed
SupportAssist Plugin case sync	Allowed	Allowed	Not Allowed
Viewing and editing of dashboard	Allowed	Allowed	Allowed (View only)

User Credential Management

OpenManage Enterprise or SupportAssist Enterprise connection profiles are stored securely using AES encryption.

Login security settings

The initial login to SNOW instance is handled by SNOW .The connection with the OME/SAE instance are done with respective credentials. Session or token based authentication is used to communicate with OpenManage and SupportAssist Enterprise.

Network security

The communication from OMISNOW application happens two ways:

1. The SNOW instance communicates with MID server using ECC queue.
2. The OMISNOW connector jar(MID server) communicates with OME and SAE using HTTPS.

NOTE: User is given an option to approve SSL certificate. Once its approved, the certificate will be installed in the trust store which is used in all the subsequent calls.

Validating jar file

Jar file validation is performed to check the integrity of the file.

jarsigner.exe - verify [OMISNOW jar path]

Path of jarsigner : C:\Program Files\Java\jdk-<version>\bin>jarsigner.exe

If jar is signed we will get message **jar verified** ,else **jar is unsigned**

Table 3. Lists of ports

Communication Channel	Port number
ECC	443
HTTPS	443

Data security

- The monitoring data is fetched from OME and the data is stored in SNOW CMDB. Data is secured by SNOW.
- The OpenManage Enterprise and SupportAssist Enterprise user credentials are encrypted and stored in SNOW CMDB.
- The data which is in the transit through OMISNOW is secured by HTTPS.

Signature file verification

Signature file verification is used to verify the integrity of the update set xml file.

About this task

Following are the steps to verify signature file:

Steps

1. Download GPG3 public key from http://linux.dell.com/files/pgp_pubkeys/0x1285491434D8786F.asc).
2. Import the public key in the system using GPG. `gpg --import 0x1285491434D8786F.asc`
3. Upon running `gpg --list-key`, it lists the key ID 34D8786F.
4. Validate signature file using `gpg --verify <FileName>.tar.gz.sign <FileName>.tar.gz` or `gpg -v --verify <FileName>.tar.gz.sign <FileName>.tar.gz`
   Verification is successful if you see the following output:

```
gpg: Signature made Fri 17 Nov 2017 03:40:10 PM IST using RSA key ID 34D8786F
gpg: using PGP trust model
gpg: Good signature from "Dell Inc., PGRE 2012 (PG Release Engineering Build Group
```

```
2012) <PG_Release_Engineering@Dell.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4255 0ABD 1E80 D7C1 BC0B  AD85 1285 4914 34D8 786F
gpg: binary signature, digest algorithm SHA512
```