OpenManage Enterprise Power Manager 3.4

Security Configuration Guide

January 2025
Rev. A01

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 Technologies 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 in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell Technologies 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 Dell support site.

Scope of the document

This guide provides an overview of the security configuration controls and settings available in OpenManage Enterprise Power Manager. This guide is intended to help facilitate secure deployment, usage, and maintenance of the software and hardware used in OpenManage Enterprise Power Manager.

Security information for other products or subcomponents that might be deployed with OpenManage Enterprise Power Manager are covered in their own security configuration guides.

Document references

In addition to this guide, you can access other documents of OpenManage Enterprise Power Manager available at Dell support site.

- *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

See the OpenManage Enterprise Power Manager Online Help and OpenManage Enterprise Online Help integrated in the product.

2

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.

3

Deployment models

You can download and install the 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 the OpenManage Enterprise section in OpenManage Enterprise User's Guide.

Prerequisites

Ensure that your connectivity to the repository is successful:

- 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 the required plug-in catalog and plug-in installation files. For more details, see the OpenManage Enterprise User's Guide.
- Ensure that you have the compatible or latest version of OpenManage Enterprise. To see the list of compatible OpenManage Enterprise versions with Power Manager, see Compatibility matrix of Power Manager and OpenManage Enterprise.

About this task

ⓘ **NOTE:** Installing a plug-in on OpenManage Enterprise restarts the appliance services.

To install the plug-in, perform the following steps:

Steps

1. In OpenManage Enterprise, click **Application Settings** > **Console and plugins**.
   The **Console and Plugins** screen is displayed.
2. In the **Plugins** section, click **Install** for the plug-in you want to install.
   The **Install and update multiple plugins** wizard is displayed.
3. From the **Plugins available for install** list, select the plugins that you want to install, and then click **Next**.
4. View the progress of the plug-in that you selected to install under the **Download** section, and then click **Next** on completion.

   ⓘ **NOTE:** If you leave the wizard, the download continues .

5. Click **End User License Agreement** > **Accept** > **Next**.
6. To confirm the installation, select **I agree that I have captured a backup of the OpenManage Enterprise appliance prior to performing a plugin action** option, and then click **Finish**.
   The status of installation operation is displayed. After the successful installation of the plug-in, the status that appears on the top of the plug-in section changes from **Available** or **Downloaded** to **Installed**.
7. To instantly view the latest list of devices and groups that are part of Power Manager as a result of any license changes made on the target devices, click **Run Inventory** in OpenManage Enterprise, and then click **Refresh Power Manager capabilities** on the Power Manager Devices page.

   View the count of overall power-capable devices from the **Power Manager Devices Statistics** section of the OpenManage Enterprise dashboard.

Topics:

Versions of Power Manager compatible with OpenManage Enterprise

The following table shows Power Manager and OpenManage Enterprise version compatibility.

Table 1. Compatibility matrix of Power Manager and OpenManage Enterprise

Power Manager Version	OpenManage Enterprise Version
Power Manager 1.0	● OpenManage Enterprise 3.2 ● OpenManage Enterprise 3.2.1 ● OpenManage Enterprise 3.3 ● OpenManage Enterprise 3.3.1
Power Manager 1.1 and 1.2	● OpenManage Enterprise 3.4 ● OpenManage Enterprise 3.4.1 ● OpenManage Enterprise 3.5
Power Manager 2.0	● OpenManage Enterprise 3.6 ● OpenManage Enterprise 3.7 ● OpenManage Enterprise 3.8 ● OpenManage Enterprise 3.8.2 ● OpenManage Enterprise 3.8.3
Power Manager 3.0	● OpenManage Enterprise 3.9 ● OpenManage Enterprise 3.9.2
Power Manager 3.1	● OpenManage Enterprise 3.10 ● OpenManage Enterprise 3.10.1 ● OpenManage Enterprise 3.10.2
Power Manager 3.2	● OpenManage Enterprise 4.0.x ● OpenManage Enterprise 4.1.x
Power Manager 3.3	● OpenManage Enterprise 4.1 ● OpenManage Enterprise 4.2
Power Manager 3.4	OpenManage Enterprise 4.3.x

4

Product and Subsystem Security

Topics:

Verify integrity of downloaded files by GPG signature verification

Verify that a Linux RPM package file is signed by Dell Technologies and has not changed since the signing.

Prerequisites

Ensure that you have access to Linux system.

About this task

Linux RPM uses GPG to sign packages. GPG does not rely on a network of Certificate Authorities (CA), but on individual signatures and peer trust. To verify the signature of an RPM, you must first import the Dell OpenManage Enterprise Power Manager public key into the GPG keyring, and then verify the RPM.

Steps

1. Download the Power Manager artifacts to a Linux server from the following location: Artifacts.
2. Open a terminal window or shell session.
3. Change the directory to the location where the files are downloaded.
4. Extract the files using the following command:

   ```
   tar -xf ome_powermanager_1.(3.3.0).tar.gz
   ```

   The RPM files are displayed.
5. Verify the signature of each RPM package by running the following command:

   ```
   rpm --checksig -v package
   ```

   Where the package is the package file name.

   For example,

   ```
   rpm --checksig -v dell-pmp-business-powermgrgrpext-3.3.0.82-1.x86_64.rpm
   ```

If the Dell OpenManage Enterprise Power Manager public key is not added to the keyring of the system, the following output is displayed:

```
Header V4 RSA/SHA1 Signature, key ID 19b55d20: NOKEY
Header SHA1 digest: OK
V4 RSA/SHA1 Signature, key ID 19b55d20: NOKEY
MD5 digest: OK
```

The NOKEY messages indicate that the Linux system does not recognize the signing key.

6. Save the following Dell OpenManage Enterprise Power Manager public key in a text file on Linux system. Ensure that no additional characters are added to or removed from the key.

Table 2. OpenManage Enterprise Power Manager public key

GPG key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

mQINBF7QKiIBEACaEeovHfPxmgH2CADkgN4RTZx+5WY2zU+rz4YazU8dp/V1Evwc
QhIvWSYCeRnTFnwQ05dOHnMIiMtpOEmoWVRDyUQQFH06KRbk3s63r2a9x6uNPlvv
r8OuB6sTlWZbZMK0AeBh7STHh37wpyXdudtSas3PDhI2428a8Z9YhQh+jXoV9E4J
VmMLToWTc9S37jYonMHpDMKuL1cYJp+lZnZMG21VYmsAW1BftqISx/zcDR9lIGbg
MN/S04CDBN5BLduIvoJxNQfbRMlrAaVhqmCNYmK+98LFVT0HrJkqzR6NZN4j2mV2
+1M81Qu/ZVXJ5+i9Rs38GgtwDUF9Ule7MB06PVSDbu0PLYqRJI/H1uy6Lsn8pkit
f6rdjS0Ch58M1g2bi5FERVye7mdON0AYnIzjq7KN+Ibe/8KZJSIj1OwBpLUInRqI
vxNMS5wUens3rSI0jO30QHlYFk5LIHgy+vONW+rKHkU/4HZVTvUvmK93yXL7nmOy
Mm9nAI9IgKlwFFY80LIg88ygjLWm4xKbOCjuf90DQVFC6PDu9o6UxoxueLGV2jXk
1U1VFdrFJMLSWL2Qs3nUkGSA+6dYVL06hHH64es6lyz8GlUWbAcraXlr3xKpT1Cc
K3OKXolsIKnpMw+WbAtilUAui2f/5MfC3QY0vCG31I7ZTCTmHtkCwkZUEwARAQAB
tF5EZWxsIEluYy4sIFBNUCBQR1JFIDIwMjAgKFBHIENvbnNvbGUgRW5naW5lZXJp
bmcgR3JvdXAgMjAyMCkgPFBHX1JlbGVhc2VfRW5naW5lZXJpbmdARGVsbC5jb20+
iQI5BBMBAgAjBQJe0CoiAhsvBwsJCAcDAgEGFQgCCQoLBBYCAwECHgECF4AACgkQ
2wGYJRm1XSBPeQ//fGCL+OWU+7+q2308XgbudLk7mvAhkG363OXPV7xjqI2YEQSD
vEYZt6GeBCItp13/IQg51vpOOj/zKvMSFubERiMvRnrZJbScJbEQNCf93i6hYbrD
vmZAetzXSS7H1h37LFvkYMCBcg+DAUsKT6wZm3HhNMo2aJtcIdfMaVQi3zJ6IwqY
2zGu/72lSDpkH/J3P5PtjjPq8PQdTmv1z0DNe2LQTn3G1BF3T98B+XZGbAVqW1FL
rMAdWACokEckOjap3EvfaiYi525ueZW6anAquq/c82IrWs62WTeFtzMpJLX9no6G
D4laKAMkRWBcS2LTH2TYHAWvZkdZbx8lYagsSHHh/f4ioec5C8wiFPTRKkkVEjTt
TKdy9qsVWRVpU5JhogS13DKPbGmwEaJlKYNHWugkInNC7GLC/u7q4srPTVWk/BYA
Gr4pGFSRtf5/YxUZiR1hBQ9urhfHDkFKx3a0rTMmTwBz+a+rFIiHYvaVG/IQRTYF
VEYeFAkXw5MnDZuv0ZSZxGGYKjbe5iCQmNoMj937PArkfZ8+4V67ldmdy/Nn4fg0
ByBG5SL2xWQ6FUBBtzvYoByU0m6MCcMfL39FkD9JoZOV3mZCGCJZdvxUJx7qemDN
Mc8W32jNDVAy/bzv6vXlIzUngvSXKyOXiLNfpwFKQtNHqwtCE27tza4T32a5Ag0E
XtAqIgEQAN36JZAEhnl5eXWUVWrJQY3KoPkVW+t5jkJXyzJlhlsfXJPjHrosvGQR
g3VuyEiroQxPpXpRgwmcF9uSpFDZ59LtnvwNY3wWdxhh8Rlu1ccT7mQdGVzmnem2
ltJI/e/Zafcu71o91UFYm2e6Od2e6/Xwx4w9V198fJVSaieglR2KkKA+eVQPG9oO
aoEG9dGDxI1U7D6kpI9pikd6//ENKNEriXBjtL8z/sO93qBRbEfEqELsScLnTIXy
fTEQYNifNLHBxa4NbbNXyR5/8ik3mQpOmR1WkZmWLNxJO8oRgOS0Aw/8FHeQBmW1
FAEsw6CqKIg2WcrY6P3qhmgbc0DYH9x1AxpQN6uaqBf4MR4wsreYN3dQLOfSQk+d
qSLnT3MMNQlEJvJxrpk7bTa3j0TUpWGlO6aXZFn6Qf4W3R6t2RWU9N7uDvdYF0wU
SbdRyouEW2jZDjEMbQ0RAteojdnhFnNurRsVKA7Z+3+xZody/ARnV9bnJLnQ9IaG
oFsvLB1212Jdsf/WFsOilmQqU7jyvt0IRM9FbZ/BGZiC1r0EmCnDCxdWVi5Ae3av
fSeJHXcgJ/GY02V2ejy8d2XKLDutkFCFnJyrGItMYjlWyeGGy6VUmEFYxFXgkJu6
Y/r9tpPa93JwqlNAt8O4zrjHiH5uNTJeWdE8KbHkVrFBzLI7lQyZABEBAAGJAh8E
GAECAAkFAl7QKiICGwwACgkQ2wGYJRm1XSDKOQ//YsPBGQFDu+lOeJ2ZiO6MDRhX
44uxP9uHY2mPGmfM+7ZgmjKJx7ohOGB/0kw4wNm8zUriTTkbOGAVMPWtmsw1/L/L
l4aAmpq9Hm/rQfDgfJYk8yaqgDCinNynr9M+vY7b8/UtJpwb8RtX1EgWLgpR96cZ
SG72GAsvWTqKNM6OxXgPJBKKHNetGNMjAtggI+8v8STOteeW9ii4H67ZeWfd3uTh
5YTPAThlmQggEIjCuZmyBcBK5ZgIqmsXLuwjfXJhSZK6mN2NSO6MYxEFkjjMkZc6
rvaldvuDanxLZcwlcu96kCw8iQizMq7Wsw4NUVN5q3qVKFjvqhNTDHSAC5WvijcU
iREr5f4sLu738CjhhtyxzXsxaIZm6MH/NdfrcJaru8Yys3V/dExVFOb3A63aIkgw
l2f527xbjIaet4r73rcOKvUbjskJt46PhKp8WKvK6McU8i5P23XiDn37e10nxQ7A
pLUZLQD6N07L6nO6gS2iB/LM95OWroxL4fstzULXc4DyHSh7aI0+EusaOfPhm1En
m4oKu0qQecMBDJbSmC8+b8pTcE6hBNqnAUiMfbIXovTTKQw+74ZqL4L8otD5NsuZ
vnVDkq+XlKM9HirbQh6CfwwRYUtW40vBetUHqnne28GNaGT2oFgWUeUQB8AjOJ+D
8EiGrqBliHLd1DqDASY=
=F3zT
-----END PGP PUBLIC KEY BLOCK-----
```

7. Import the public key using the following command:

   ```
   rpm --import keyfile
   ```

   Where keyfile is the text file which has the public key.

8. After importing the key, verify the RPM package files for a valid signature by running the following command:

   ```
   rpm --checksig -v package
   ```

   Where the package is the package file name.

   For example,

   ```
   rpm --checksig -v dell-pmp-business-powermgrgrpext-3.3.0.82-1.x86_64.rpm
   ```

   .

   The following response confirms that the files are signed by Dell Technologies and not tampered.

   ```
   Header V4 RSA/SHA1 Signature, key ID 19b55d20: OK
   Header SHA1 digest: OK
   V4 RSA/SHA1 Signature, key ID 19b55d20: OK
   MD5 digest: OK
   ```

   The OK messages indicate that the Linux server recognizes that the package is signed by a trusted key.

9. Run the following command to verify all the RPM package files in a directory:

   ```
   find rpmFileLocation -type f -name \*.rpm -exec rpm --checksig -v {} ';'
   ```

   where rpmFileLocation is the path where all RPM files exist.

   For example,

   ```
   find . -type f -name \*.rpm -exec rpm --checksig -v {} ';'
   ```

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.

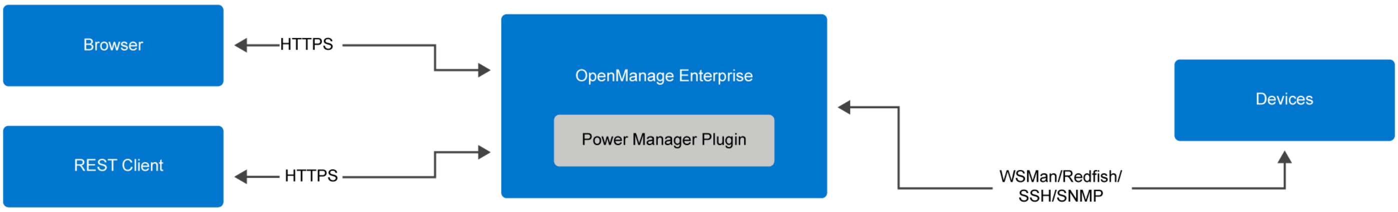

Figure 1. Security control map for Power Manager plug-in

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 that are 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 the 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 the 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 OpenManage Enterprise User's Guide and OpenManage Enterprise Power Manager User's Guide.

Role and scope-based access

Role-Based Access Control (RBAC) defines the user privileges into three categories: Administrator, Device Manager, and Viewer. Scope-Based Access Control (SBAC) enables administrators to limit the device groups that a device manager can access. The following topics further explain the RBAC and SBAC features.

Role-based access control (RBAC) privileges

Users are assigned roles that 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 that is required for a certain action before allowing the action.

The privileges for the custom roles created by an administrator are assigned at the time the role is created.

The table below lists the privileges of each role.

Table 3. Role-based user privileges for Power Manager

Privilege	Administrator	Device Manager (scope for assigned groups)	Device Manager (scope for nonassigned 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	Yes	Yes	No	No
Add or remove static groups	Yes	Yes	No	No

Table 3. Role-based user privileges for Power Manager (continued)

Privilege	Administrator	Device Manager (scope for assigned groups)	Device Manager (scope for nonassigned groups)	Viewer
Add or remove unmonitored devices	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
Import physical groups through CSV file.	Yes	No	No	No
Manage the devices in the 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

Table 3. Role-based user privileges for Power Manager (continued)

Privilege	Administrator	Device Manager (scope for assigned groups)	Device Manager (scope for nonassigned groups)	Viewer
Create, edit, or delete VM groups.	Yes	No	No	No
Analyze usage metrics.	Yes	Yes	No	Yes
Automatically create a physical hierarchy.	Yes	No	No	No
View maximum and minimum power consumption of VMs on the Overview screen.	Yes	Yes	No	Yes
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 screen	Yes	Yes	Yes	Yes
Update device location in device console	Yes	No	No	No
View idle servers.	Yes	Yes	No	Yes
Add or remove Uninterruptible Power Supply (UPS).	Yes	No	No	No
Monitor UPS	Yes	Yes	No	Yes
Monitor GPU	Yes	Yes	No	Yes
Monitor PSU	Yes	Yes	No	Yes
Analyze multivariate metrics.	Yes	Yes	No	Yes
View devices associated with system and workload profiles	Yes	Yes	No	Yes

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 the 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 the OpenManage Enterprise User's Guide.

5

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.