

Dell EMC OpenManage Enterprise SupportAssist Version 1.1

User's 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

Tables	5
Chapter 1: About OpenManage Enterprise SupportAssist	6
How SupportAssist works	6
Device information collected by SupportAssist	6
Chapter 2: What is new	8
Chapter 3: OpenManage Enterprise SupportAssist capabilities available with Dell service contracts	9
Chapter 4: OpenManage Enterprise SupportAssist support matrix	11
Chapter 5: Role and scope-based access control in OpenManage Enterprise	12
Chapter 6: Installing OpenManage Enterprise SupportAssist	15
Chapter 7: Getting started with OpenManage Enterprise SupportAssist	17
Register OpenManage Enterprise SupportAssist.....	17
Chapter 8: Site Health	19
Run connectivity test.....	19
Chapter 9: Group devices for effective management and monitoring	21
Predefined device groups	21
View devices in staging and maintenance—in a specific group.....	22
View device groups	22
Creating a device group	22
View and update device group information	23
Delete a device group	24
Chapter 10: OpenManage Enterprise SupportAssist cases	25
View Cases	25
Request to suspend case activities for 24 hours	27
Request to resume support activities	27
Request to close a support case	27
View support cases for a specific device	28
Chapter 11: OpenManage Enterprise SupportAssist device collections	29
View collections.....	29
Using SupportAssist to collect and send system information	30
Manually collect device information from a device.....	30
Manually collect system information from a device group.....	31
Upload collection from disconnected site.....	31

Download and view multiple device collections	32
Download and view collection from a specific device.....	32
Configuring collection settings on OpenManage Enterprise SupportAssist.....	33
Prerequisites for collecting system information.....	33
Enable or disable automatic collection of system information on support case creation.....	33
Enable or disable periodic validation of device inventory	34
Enable or disable periodic collection of system information.....	34
Enable or disable collection of identity information.....	34
Filter components of device collections.....	35
Chapter 12: Configuring OpenManage Enterprise SupportAssist settings	36
Configure proxy server settings.....	36
Enable or disable SupportAssist maintenance mode	37
Enable or disable group-level SupportAssist maintenance mode	37
Enable or disable device-level SupportAssist maintenance mode	37
Collection preferences	38
Contact Details	38
Configure contact information	38
Configure Shipping Details	39
Schedule collection and inventory validation.....	40
Configure email notification settings	40
Types of email notifications.....	40
Chapter 13: OpenManage Enterprise SupportAssist product information	42
Chapter 14: Disable OpenManage Enterprise SupportAssist	43
Chapter 15: Uninstall OpenManage Enterprise SupportAssist.....	44
Chapter 16: SupportAssist maintenance mode	45
Global-level SupportAssist maintenance mode	45
Group-level SupportAssist maintenance mode	45
Device-level SupportAssist maintenance mode	45
Chapter 17: Alert policies in OpenManage Enterprise SupportAssist	47
Which hardware faults does SupportAssist monitor?	47
What happens when a hardware issue is detected by SupportAssist?.....	47
How and where am I notified by OpenManage Enterprise SupportAssist about device alerts?.....	47
What is the response time for resolving my OpenManage Enterprise SupportAssist case?.....	48
What alerts open predictive support cases in advance of hardware failures?	48
What if I require assistance for deploying installing OpenManage Enterprise SupportAssist?.....	48
Alert threshold	48
First occurrence policies	49
Repeat occurrence policies	49
Chapter 18: Error code appendix.....	50
Chapter 19: Accessing support content from the Dell EMC support site.....	65

1	OpenManage Enterprise SupportAssist capabilities available with Dell service contracts.....	9
2	Role-based and scope-based access control in OpenManage Enterprise SupportAssist.....	13
3	Types of email notifications.....	40
4	Error code appendix.....	50

About OpenManage Enterprise SupportAssist

Dell EMC OpenManage Enterprise SupportAssist is a plugin to the Dell EMC OpenManage Enterprise console that enables proactive and predictive monitoring and management support for your devices with ProSupport and ProSupport Plus entitlements. OpenManage Enterprise with SupportAssist provides a single, unified solution for your complete device lifecycle management and proactive and predictive support experience. SupportAssist improves the data center efficiency by enabling the administrator to seamlessly manage hardware failure incidents, reducing the time spent by Dell EMC Technical Support, and improving the turnaround and downtime in resolving the hardware issues.

The key benefits of SupportAssist are:

- Monitors your devices, proactively detects hardware issues, and accelerates resolution by creating Technical Support cases automatically to Dell EMC.
- Enables you to provide your support and dispatch contacts (primary, secondary, and group) to Dell EMC.
- Improves productivity by replacing manual routine operations with automated support.
- Predictive issue detection by using the periodic hardware telemetry collections, which enables you to take preventive measures to avoid data loss in future.
- Expedites dispatch process.

When an issue is detected, SupportAssist collects and uploads the system information required for troubleshooting an issue. The collected system information helps Technical Support to provide you an enhanced, personalized, and efficient support experience. SupportAssist also provides predictive support and reporting by using the periodic hardware telemetry collections. The periodic collections enable Dell EMC to perform advanced analytics, predict future failures, and inform you about the due time to back up and resolve failures in advance.

Topics:

- [How SupportAssist works](#)
- [Device information collected by SupportAssist](#)

How SupportAssist works

SupportAssist receives an alert whenever a hardware event occurs on a device. The alert is filtered using various policies to determine if the alert qualifies for creating a support case or for updating an existing support case. All qualifying alerts are sent securely to the backend for creating a support case or for updating an existing support case. After the support case is created or updated, SupportAssist collects device information from the device and sends it to the Dell EMC backend. Also, some of the devices send the information directly to the backend when an alert is generated. Dell EMC Technical Support uses the system information to troubleshoot the issue and provide an appropriate solution. For more information about how SupportAssist processes alerts and automatically creates support cases, see [Alert policies in OpenManage Enterprise SupportAssist](#) on page 47.

NOTE: To experience the automatic case creation and system information collection capabilities of SupportAssist, you must complete the registration.

NOTE: SupportAssist does not create a support case for every alert received from a monitored device. A support case is created only for a device that has an active service contract, and if the alert type and number of alerts received from the device match the predefined criteria for support case creation.

NOTE: SupportAssist sends you automatic email notifications about registration, support cases, network connectivity status, and so on.

Device information collected by SupportAssist

SupportAssist continually monitors the configuration and usage information of the hardware and software devices managed using SupportAssist. While Dell EMC does not anticipate accessing or collecting personal information, such as your personal files, web browsing history, or cookies in connection with this program, any personal system information inadvertently collected

or viewed is treated in accordance with the Dell Privacy Policy available for review at <https://www.dell.com/learn/us/en/uscorp1/policies-privacy>

The information encrypted in the collected system information log contains the following categories of data:

- Hardware and software inventory—Installed devices, processors, memory, network devices, usage, and Service Tag
- Software configuration for servers—Operating system and installed applications
- Configuration information—Interfaces, VLAN, Data Center Bridging (DCB), spanning tree, and stacking
- Identity information—System name, domain name, and IP address
- Event data—Windows event logs, core dump, and debug logs

By default, SupportAssist collects system information from all devices, irrespective of the service contract of the devices, and sends the device information securely to the backend. Device information is collected from one device at a time based on the predefined collection start day and time specified on the **Schedule Tasks** page. To start the collection on a different day, see [Enable or disable periodic collection of system information](#) on page 34.

 **NOTE:** If the security policy of your company restricts sending some of the collected system information outside of your company network, you can configure SupportAssist to exclude the collection of certain system information from your devices. For information about excluding the collection of certain system information, see [Enable or disable collection of identity information](#) on page 34.

What is new

The release adds support for:

- Support for Scope-Based Access Control (SBAC). An admin can use SBAC to restrict a user with Device Manager role only to a subset of device groups.
- Support for the latest iDRAC9 based PowerEdge servers. See *Dell EMC OpenManage Enterprise SupportAssist Support Matrix* available at [OpenManage Enterprise SupportAssist](#) page in support site.
- Support for SNMP v3 traps to receive and process alerts and automate case creation.

OpenManage Enterprise SupportAssist capabilities available with Dell service contracts

The following table provides a comparison of the OpenManage Enterprise SupportAssist capabilities available with the ProSupport and ProSupport Plus service contracts.

Table 1. OpenManage Enterprise SupportAssist capabilities available with Dell service contracts

OpenManage Enterprise SupportAssist capabilities	Description	Basic Hardware	ProSupport	ProSupport Plus
Proactive detection of hardware failures	SupportAssist receives alerts for hardware events that occur in monitored devices and proactively determines if the alerts indicate a hardware failure.	Supported	Supported	Supported
Predictive detection of hardware failures	Intelligent analysis of data collected from a monitored device is used to predict hardware failures that may occur in future.	Not supported	Not supported	Supported
Automated data collection	Data required for troubleshooting a hardware failure is automatically collected from the monitored device and sent securely to Dell.	Supported	Supported	Supported
Automated support case creation	When a hardware failure is detected either proactively or predictively, a Service Request is automatically created with Dell Technical Support.	Not supported	Supported	Supported
Automated email notification	An email notification about the support case or issue is automatically sent to your company's primary and secondary SupportAssist contacts.	Not supported	Supported	Supported
Proactive response from Dell Technical Support	A Dell Technical Support agent contacts you proactively about the support case and	Not supported	Supported	Supported

Table 1. OpenManage Enterprise SupportAssist capabilities available with Dell service contracts (continued)

OpenManage Enterprise SupportAssist capabilities	Description	Basic Hardware	ProSupport	ProSupport Plus
	helps you resolve the issue.			
Expedited parts dispatch	After the verification of the collected system information, if the Dell Technical Support agent determines that a part requires a replacement to resolve the issue, a replacement part is dispatched to you based on the dispatch preferences that you configure in SupportAssist.	Not supported	Supported	Supported

OpenManage Enterprise SupportAssist support matrix

For the complete list of compatible devices, hypervisors, and operating systems, see *Dell EMC OpenManage Enterprise SupportAssist Support Matrix* available at [OpenManage Enterprise SupportAssist](#) page in support site.

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 2. 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
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				

Table 2. 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
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

Installing OpenManage Enterprise SupportAssist

Prerequisites

- Ensure that you logged in to OpenManage Enterprise as an **Admin**. Only the user with Admin role can install plugins in OpenManage Enterprise.
- While you deploy OpenManage Enterprise SupportAssist plugin within OpenManage Enterprise, which is the recommended solution for proactive and predictive monitoring, ensure that:
 - If SupportAssist Enterprise (SAE) standalone application 2.0.50 or lower deployed in your data center, delete the OpenManage Enterprise adapter from the SAE application to avoid duplicate management and serviceability functions.
 - If SAE standalone virtual appliance 4.x deployed in your data center, delete the OpenManage Enterprise adapter from the SAE virtual appliance to avoid duplicate management and serviceability functions.

However, if you have deployed SAE application 2.0.60 and later, the standalone SAE application ensures no duplicate management and serviceability functions even if OpenManage Enterprise SupportAssist plugin and SAE 2.0.60 application co-exist. In this case, OpenManage Enterprise SupportAssist plugin takes precedence in alert processing and case creation.

- Ensure that minimum requirements for installing and using OpenManage Enterprise SupportAssist are fulfilled. For the list of hardware, networking and ports, and operating system requirements, see *Dell EMC OpenManage Enterprise SupportAssist Support Matrix* available at [OpenManage Enterprise SupportAssist](#) page in support site.
- You can download and install OpenManage Enterprise SupportAssist plugin 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 OpenManage Enterprise SupportAssist from `dell.com`, you must ensure that the OpenManage Enterprise appliance can access downloads.dell.com.
 - To install OpenManage Enterprise SupportAssist from a local network share, you must manually download the package to your network share and update the location on the **Update Settings** page in OpenManage Enterprise.
- If OpenManage Enterprise uses OpenID Connect (OIDC) for OAuth token-based authorization, ensure that:
 - The DNS server configured in OpenManage Enterprise can resolve the OIDC provider and Dell EMC Secure Remote Services (SRS) backend.
 - The OIDC provider and Dell EMC Secure Remote Services (SRS) backend are in the same DNS domain.

Steps

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**. The **Install Plugin** window is displayed.
4. On the **Install Plugin** window, from the **Available Version(s)** list, select the OpenManage Enterprise SupportAssist version.
5. Review and ensure that you meet the list of prerequisites that are mentioned in the **Prerequisite** section, and then click **Download Plugin**. After OpenManage Enterprise SupportAssist is downloaded successfully, the status that appears on the top of the **SupportAssist** section changes from **Available** to **Downloaded**.
6. On the **Install Plugin** window, click **Install Plugin**. The install operation validates the prerequisites to install SupportAssist. If installation prerequisites are not fulfilled, an appropriate error message is displayed.
7. On the **END USER LICENSE AGREEMENT** page, read the license agreement, and click **Accept**.
8. On the **INFRASTRUCTURE TELEMETRY NOTICE** page, read the telemetry notice, and click **Accept**.
9. On the **Confirmation** window, select the **I agree that I have captured a snapshot of the OpenManage Enterprise appliance prior to performing a plugin action** option, and then click **Confirm Install**.

The status of installation operation is displayed. After the successful installation of SupportAssist, the status that appears on the top of the **SupportAssist** section changes from **Available** to **Installed**.

Next steps

Register OpenManage Enterprise SupportAssist to monitor your devices for hardware issues and automatically collect device information. See [Register OpenManage Enterprise SupportAssist](#) on page 17.

Getting started with OpenManage Enterprise SupportAssist

Register OpenManage Enterprise SupportAssist to monitor your devices for hardware issues and automatically collect device information.

Topics:

- [Register OpenManage Enterprise SupportAssist](#)

Register OpenManage Enterprise SupportAssist

About this task

When you access OpenManage Enterprise SupportAssist for the first time, a banner message is displayed that you have not registered the SupportAssist. You must register SupportAssist to monitor your devices for hardware issues and automatically collect device information. To register SupportAssist:

Steps

1. In the banner message, click the **Register Now** link.
2. Click **Add Proxy**, enter the following information, and then click **Apply**.
The **Add Proxy** page is displayed only when SupportAssist is not able to establish a network connection with the Dell EMC.
 - a. To use HTTP Proxy, select **Enable HTTP Proxy Settings**.
 - b. Enter the hostname or IP address and port number of the proxy server.
 - c. If the proxy server requires authentication, select **Requires Proxy Authentication**.
 - d. Enter the username and password of the proxy server.
3. On the **Connectivity** page, enter the access key and PIN, and then click **Next**. If you do not have the access key and PIN, do one of the following:
 - On the **Connectivity** page (in the SupportAssist plugin registration wizard), click **Generate Access Key**.
 - Go to the [OpenManage Enterprise SupportAssist](#) support site page. On the **Overview** tab, under **Quick Links**, click **Generate Access key**.

NOTE: The access key generated by using the links provided for other SupportAssist products cannot be used for SupportAssist plugin.
4. On the **Contact Details** page, enter the primary contact information, and then click **Next**.

NOTE: After registering SupportAssist, you can update the primary contact information and provide a secondary contact on the **Settings > Contact Details** page. If the primary contact is unavailable, Dell EMC contacts your company through the secondary contact. If both the primary and secondary contacts are configured with valid email addresses, an email is sent to both the contacts.
5. Optionally, on the **Expedited Dispatch (Optional)** page, perform the following and click **Next**.
 - If you want Dell EMC to automatically ship the replacement parts for your servers, select **I want Dell EMC to expedite dispatch of the replacement parts**.
 - If you want an onsite technician to replace the dispatched hardware component, select **I want a technician to replace the parts onsite if the service is included in the service plan**.
6. Optionally, on the **Shipping Details** page, enter the primary and secondary shipping contact details, shipping address, and click **Next**.

NOTE: If the primary shipping contact information are same as the contact details, click **copy contact details**.

7. Optionally, to view asset information and manage SupportAssist alerts and part dispatches by using TechDirect, sign in to TechDirect using your company's administrator account and enter the One-Time Password (OTP). To sign in to TechDirect, on the **TechDirect Integration (Optional)** page, click **Launch TechDirect**.
8. Click **Next**.
The **Summary** page is displayed.
9. Click **Finish**.
The **Site Health** page is displayed.

Site Health

The **Site Health** page enables you to identify and prioritize the most important issues on your site.

You can view the following on the **Site Health** page.

- The number of devices in the following statuses:
 - **NOTE:** If you are logged in with a Device Manager role, the device count that is displayed for Managed Devices, Staging Devices, and Unmanaged Devices includes devices only from the device groups that are within your scope.
 - **Managed Devices**—Displays the number of monitored devices. Click to view the number of monitored devices according to the device type.
 - **NOTE:** The **Managed Devices** tab is selected by default.
 - **NOTE:** The OpenManage Enterprise SupportAssist version supports only IPv4 devices.
 - **Staging Devices**— Displays the number of devices that are discovered partially while you tried to add them because of certain requirements were not met. Click to view the number of devices listed based on the reason and remediation. To view the host name of the devices that are in staging, click **Export**. The staging details are exported to Excel.
 - **Unmanaged Devices**—Displays the number of devices that are not supported. Click to view the number of devices that are not supported grouped according to the device type. To view the host name of the devices that are not managed, click **Export**. The details of unmanaged devices are exported to Excel.
- In the **Connectivity to Dell EMC** section, you can view the following:
 - **Online Status**—Displays the SupportAssist Internet connectivity status. Internet connection is required to communicate with Dell EMC.
 - **Enterprise Servers**—Displays the status of SupportAssist connectivity to the Dell EMC Enterprise Servers.
 - **Connectivity Tests**—Click the link to run the connectivity tests to check the connectivity to the Internet, Dell EMC Enterprise Servers, and to validate the case creation capability. For more information about the connectivity tests, see [Run connectivity test](#) on page 19.

Topics:

- [Run connectivity test](#)

Run connectivity test

By default, SupportAssist automatically tests connectivity to the dependent resources every day at 11 p.m. If there is an issue with connectivity to a dependent resource, an email is sent to your primary and secondary contacts. You can also test the SupportAssist connectivity to the dependent servers at any time.

To run the connectivity tests:

1. On the **Site Health** page, click **Connectivity Tests** link in the **Connectivity** section. The **Connectivity Tests** page is displayed.
2. To check if the SupportAssist can connect to the Dell EMC Enterprise Servers, in the **Network Connectivity Test** section, click **Test Connectivity**. To check the status of the connectivity test, click the arrow next to **Enterprise Server**. The connectivity status is displayed in a table as follows:
 - **Hostname**—Lists the SupportAssist enterprise servers hosted by Dell EMC.
 - **Ping Time (ms)**—Displays the ping time of the SupportAssist enterprise servers in milliseconds.
 - **Ping Status**—Displays the ping status of the SupportAssist enterprise servers. A green tick mark indicates that SupportAssist can reach the enterprise servers.
 - **Port 443**—The port 443 must be open on the firewall to establish a secure HTTPS connection to the Dell EMC backend. Displays a green tick mark if port 443 is open.
 - **Port 8443**—The port 8443 must be open on the firewall to enable Dell EMC technical support to access the devices remotely over SSH. Displays a green tick mark if port 8443 is open.

- **Proxy Status**—Displays the details of the proxy server if SupportAssist connects to the Internet through a proxy server. If SupportAssist is connected to the Internet through a proxy server, the status is displayed as **Proxy enabled**. Else, the status is displayed as **Proxy not enabled**.
 - **Last Verified**—Displays the date and time the connectivity status was last verified.
3. To ensure that SupportAssist can automatically create a support case for an alert, in the **Case Creation Ability Test** section, click **Test Connectivity**.

The possible statuses are:

- **Validated**—The support case creation task is successfully validated.
- **Not Validated**—The support case creation task is not validated.
- **Unknown**—Unable to retrieve the status of SupportAssist case creation capability because the case creation service is down.

Group devices for effective management and monitoring

SupportAssist has two predefined device groups—**Maintenance** and **Staging**—that help you in managing the devices that you add. Depending on your requirement, you can also create custom device groups to manage certain devices as a group. For example, you can create device groups that may include devices based on the following:

- Device type (server or chassis)
- The individual who manages the devices (Administrator group)
- Organization or business unit (Marketing, Operations, Finance, and so on)
- Physical location of the devices (shipping address)
- Alerting or notification (individuals who must be notified if an issue is detected on certain devices)

After you create a device group, you can:

- Add or remove devices from the device group
- Configure the contact information and parts dispatch information for the device group.
- Edit the device group details or delete the device group

NOTE: Grouping of devices is optional. Device grouping does not have an impact on the monitoring and automatic case creation capabilities of SupportAssist.

NOTE: The credentials, contact information, or parts dispatch information configured for a device group will override the default credentials, contact information, and parts dispatch information configured using **Settings** pages. For example, if you have created a device group and configured the primary contact for the device group, all SupportAssist notifications for issues with any device included in the device group are sent to the primary contact assigned to that device group.

Topics:

- [Predefined device groups](#)
- [View devices in staging and maintenance—in a specific group](#)
- [View device groups](#)
- [Creating a device group](#)
- [View and update device group information](#)
- [Delete a device group](#)

Predefined device groups

The predefined device groups in OpenManage Enterprise SupportAssist enables you to group devices that are monitored by SupportAssist, group all devices in maintenance mode, and group devices in staging for effective monitoring. When monitoring devices as an administrator, you can make use of the SupportAssist, Maintenance, and Staging groups that are predefined.

The predefined device groups available in SupportAssist plugin are as follows:

- **SupportAssist** default group—By default, all devices that are supported by SupportAssist are assigned to this group unless you assign the device to any other group.
- **Maintenance** group—Contains devices that are placed in SupportAssist maintenance mode.
- **Staging** group—Contains devices that were only discovered partially while you tried to add them because certain requirements were not met. Devices in this group are automatically moved to the Default group when you revalidate them after the requirements for SupportAssist to monitor are fulfilled. SupportAssist capabilities are not available for devices that are present in this group. Typically, a device is added to the staging group in the following cases:
 - For PowerEdge servers or iDRAC that do not have the required service contracts.
 - Prerequisites for monitoring the device are not fulfilled. To identify the reason why SupportAssist cannot monitor a staging device, go to the **Site Health** page and click **Staging Devices** pane. A list displays the reason and remediation to resolve the issue with the staging devices. The resolution and remediation are grouped according to the type of issue in one or more devices. For information, see [Site Health](#) on page 19.

View devices in staging and maintenance—in a specific group

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. On the left pane, expand the **PLUGIN GROUPS** section, and click a SupportAssist group. The **Staging** and **Maintenance** legends of the doughnut chart displayed on the upper-right corner shows the number of devices that are in staging and maintenance, respectively in the group.
NOTE: If you are logged in with a Device Manager role, you can view only the device groups that are within your scope.
3. To view the list of devices that are in staging and maintenance, click a color band on the doughnut chart. The **Devices** dialog box is displayed.
4. On the **Devices** dialog box, perform the following:
 - To view the devices that are in staging, click **Staging** tab.
 - To view the devices that are in maintenance, click **Maintenance** tab.

View device groups

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. In the left pane, in the **PLUGIN GROUPS** section, expand the **SupportAssist** category. The list of custom device groups are listed under SupportAssist group, along with the predefined groups, Maintenance and Staging.
NOTE: If you are logged in with a Device Manager role, you can view only the device groups that are within your scope.

Creating a device group

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. In the left pane, in the **PLUGIN GROUPS** section, click the three vertical dots next to the **SupportAssist** group category, and then click **Create SupportAssist Group** from the list. The **Create/Edit SupportAssist Group** dialog box is displayed.
3. On the **General** page, type the group name and a description for the group, and click **Next**.
4. On the **Group Contact** page, do the following:
 - a. Select **Contact Details**.
 - b. Select the **Primary** option and enter the following primary contact details:
NOTE: If the primary and secondary contact information is same as the contact details, click **copy contact details**.
 - i. Type your first name, last name, phone number, alternate phone number, and email address in the appropriate fields.
 - ii. Select the preferred contact method, preferred contact hours, and time zone.
 - c. Optionally, select the **Secondary** option and enter the following secondary contact details:
 - i. Type your first name, last name, phone number, alternate phone number, and email address in the appropriate fields
 - ii. Select the preferred contact method, preferred contact hours, and time zone.
5. Optionally, on the **Expedited Dispatch (Optional)** page, perform the following and click **Next**.
 - a. If you want Dell EMC to automatically ship the replacement parts for your servers, select **I want Dell EMC to expedite dispatch of the replacement parts**.
 - b. On the **Shipping Details** page, enter the primary and secondary shipping contact information, shipping address, and click **Next**.

NOTE: If the primary shipping contact information is same as the group contact information, click **copy contact details**

6. On the **Devices** page, click **Select Devices**.
7. In the **All Devices** dialog box, select the devices to add to the group, and then click **Add Selected**.
To filter the devices, click **Advanced Filters** and select or enter data in the filter boxes. You can filter the devices by Health State, Power State, Connection State, Name, IP Address, Service Tag, Model, and Type. To disable the filter, click **Clear All Filters**.
To view the devices added to the group, click the **All Selected Devices** tab. The number suffixed to the **All Selected Devices <number>** tab title indicates the number of devices in the group.
8. Click **Finish**.

Results

The device group that you created is listed under the **SupportAssist** group title.

View and update device group information

About this task

You can view or edit the group name and description, contact information, preferred contact method and time, the parts dispatch information of a device group, and add or remove devices from a group.

Updating the contact information for a device group enables SupportAssist to send notifications to the device group contact.

NOTE: The device group parts dispatch information overrides the default parts dispatch information that you configured on the **Settings > Contact Information** page. If resolving a problem requires replacing a part, the replacement part is shipped with your consent to the device group parts dispatch address (not the default parts dispatch address).

NOTE: If the Technical Support staff determines that a part must be replaced in your system to resolve a support case, the replacement part is dispatched with your consent to the provided address.

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. In the left pane, in the **PLUGIN GROUPS** section, expand the **SupportAssist** category.
3. Click the three vertical ellipses next to the device group.
4. From the list, click **Edit SupportAssist Group**.
The **Create/Edit SupportAssist Group** dialog box is displayed.
5. On the **General** page, edit the group name and a description for the group, and click **Next**.
6. On the **Group Contact** page, perform the following steps:
 - a. Select **Contact Details**.
 - b. Select the **Primary** option and edit the following primary contact details:

NOTE: If the primary and secondary contact information is same as the contact details, click **copy contact details**.

 - i. Type your first name, last name, phone number, alternate phone number, and email address in the appropriate fields.
 - ii. Select the preferred contact method, preferred contact hours, and time zone.
 - c. Optionally, select the **Secondary** option and edit the following secondary contact details:
 - i. Type your first name, last name, phone number, alternate phone number, and email address in the appropriate fields.
 - ii. Select the preferred contact method, preferred contact hours, and time zone.
7. Optionally, on the **Expedited Dispatch (Optional)** page, perform the following and click **Next**:
 - a. If you want Dell EMC to automatically ship the replacement parts for your servers, select **I want Dell EMC to expedite dispatch of the replacement parts**.
 - b. On the **Shipping Details** page, enter the primary and secondary shipping contact details, shipping address, and then click **Next**.

NOTE: If the primary shipping contact details are same as the group contact information, click **copy contact details**
8. On the **Devices** page, perform the following steps:
 - a. Click **Device(s) Selected**.
 - b. In the **All Devices** dialog box, add or remove devices from the device group, and then click **Add Selected**.

To filter the devices, click **Advanced Filters** and select or enter data in the filter boxes. You can filter the devices by Health State, Power State, Connection State, Name, IP Address, Service Tag, Model, and Type. To disable the filter, click **Clear All Filters**.

To view the devices added to the group, click the **All Selected Devices** tab. The number suffixed to the **All Selected Devices <number>** tab title indicates the number of devices in the group.

9. Click **Finish**.

Results

The device group is updated based on the devices that you have added or removed.

Delete a device group

About this task

You can delete device groups based on your preference.

 **NOTE:** Deleting a device group removes only the device group and contact information.

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. In the left pane, in the **PLUGIN GROUPS** section, expand the **SupportAssist** category.
3. To delete a device group, click the vertical ellipses next to the device group, and then click **Delete SupportAssist Group** from the list.

OpenManage Enterprise SupportAssist cases

A support case is automatically created when an issue is detected on devices that are monitored by SupportAssist. The **Cases** page displays all cases that are created by SupportAssist.

NOTE:

- SupportAssist automatically creates support cases for the issues detected on all monitored devices irrespective of the role and scope of the user logged in to OpenManage Enterprise.
- SupportAssist does not create a support case for every alert that is received from a monitored device. SupportAssist collects evidence file from the device and sends it to Dell EMC backend for alert processing. A support case is created only if the alert type and number of alerts that are received from the device match with the criteria that are defined by Dell EMC for support case creation. For more information about how SupportAssist processes alerts and automatically creates support cases, see [Alert policies in OpenManage Enterprise SupportAssist](#) on page 47.

If SupportAssist is connected to the Dell support case and service contract databases over the Internet, support case information is automatically available for the supported devices that have valid Service Tags. The support case information is refreshed only when you:

- Open the **Cases** page.
- Click **Refresh** the **Cases** page.
- The **Cases** page is open and you refresh the web browser window.

You can also request Technical Support to perform the following activities by using the available case management options:

- Suspend activities that are related to a support case.
- Resume activities that are related to a support case.
- Request to close a support case.

The case management options are applicable only for support cases that were opened automatically by SupportAssist for the devices listed in *Dell EMC OpenManage Enterprise SupportAssist Support Matrix* available at [OpenManage Enterprise SupportAssist](#) page in support site.

For information about the fields and data that are displayed on the **Cases** page, see [View Cases](#) on page 25.

Topics:

- [View Cases](#)
- [Request to suspend case activities for 24 hours](#)
- [Request to resume support activities](#)
- [Request to close a support case](#)
- [View support cases for a specific device](#)

View Cases

The **Cases** page displays the support cases for your devices that are monitored by SupportAssist. By default, the displayed support cases are grouped under their respective device name or device IP address.

 **NOTE:** If you are logged in with a Device Manager role, you can view the support cases created for devices from the device groups that are within your scope.

To view the **Cases** page, from the **Plugins** menu, select **SupportAssist > Cases**. To view the support cases that are opened for a specific device, see [View support cases for a specific device](#) on page 28.

The following options and support case information are displayed on the **Cases** page.

- **Advanced Filters**—The **Advanced Filters** option is in the upper-left corner of the cases list. To filter the cases, click **Advanced Filters** and select or enter data in the filter boxes. You can filter the cases by case number, service contract, Service Tag, and source type. To disable filter, click **Clear All Filters**.
- To sort the case list display data by column name, click any column header. The report refreshes to display the data in an ascending or descending order of the column header you clicked.

- Case Options (**Suspend, Resume, Request To Close**)—The options to manage support cases that were opened by SupportAssist based on your requirement. The available options are:
 - **Suspend**—Request Technical Support to stop activities that are related to a support case for 24 hours. After 24 hours, Technical Support automatically resumes activities that are related to the support case. See [Request to suspend case activities for 24 hours](#) on page 27.
 - **Resume**—Request Technical Support to resume activities that are related to a support case. See [Request to resume support activities](#) on page 27.
 - ① **NOTE:** The **Resume** option is enabled only if you had previously requested to suspend activities that are related to a support case.
 - **Request To Close**—Request Technical Support to close a support case. See [Request to close a support case](#) on page 27.
- The Refresh icon—The Refresh icon is in the upper-right corner of the cases list. Click the icon to refresh the case list displayed.
- **IP ADDRESS**—Displays the IP address of the device associated with the support case.
- **CASE NUMBER**—Numeric identifier that is assigned to the support case.
- **CASE STATUS** —Displays the current state of the support case. The possible statuses are:
 - **Submitted**—SupportAssist has submitted the support case.
 - **Open**—Technical Support has opened the submitted support case.
 - **InProgress**—Technical Support is working on the support case.
 - **Assigning**—The support case is not yet assigned to a technical support agent.
 - **Customer Deferred**—Technical support has deferred the support case on your request.
 - **Reopened**—The support case was previously closed but is currently reopened.
 - **Suspended**—Technical Support has suspended activities that are related to the support case for 24 hours based on your request.
 - **ReqForClosure**—You have requested technical support to close the support case.
 - **Closed**—The support case is closed.
 - **Not Applicable**—SupportAssist detected an issue, but a support case was not created because the device has either an expired warranty or Basic Hardware warranty.
 - **Unavailable**—The support case status could not be retrieved from Dell.
 - **Unknown**—SupportAssist is unable to determine the status of the support case.
- **CASE TITLE**—The support case name, which identifies:
 - Support case generation method
 - Device model
 - Device operating system
 - Alert ID, if available
 - Alert description, if available
 - Device warranty status
 - Resolution description
- **DATE OPENED**—The date and time the support case was opened.
- **SERVICE CONTRACT**—The Dell EMC service contract level under which the device is covered. The **Service Contract** column may display:
 - **ProSupport Flex**—The device is covered under a Dell EMC ProSupport Flex service contract.
 - **ProSupport Plus**—The device is covered under a Dell EMC ProSupport Plus service contract.
 - **ProSupport**—The device is covered under a Dell EMC ProSupport service contract.
 - **Basic**—The device is covered under a Dell EMC Basic Hardware service contract.
 - **ExpiredWarranty**—The service contract of the device has expired.
- **SERVICE TAG**—Unique, alphanumeric identifier that enables Dell EMC to recognize the device.
- **SOURCE TYPE**—Identifies the source from which the support case is opened. The possible source types are:
 - **Phone**
 - **Email**
 - **Chat**
 - **SupportAssist**
 - **TechDirect**
 - **HelpDesk**
 - **Others**

Request to suspend case activities for 24 hours

About this task

You can request Technical Support to stop activities that are related to a support case for 24 hours, if necessary. For example, you may want the Technical Support team to stop the activities for a support case in the following cases:

- To resolve the issue without any assistance from Technical Support.
 - Not to receive any notifications that are related to the support case from Dell EMC during a planned maintenance activity.
-  **NOTE:** You can request Technical Support to stop activities that are related to a support case only if the support case is opened by SupportAssist.

Steps

1. From the **Plugins** menu, select **SupportAssist > Cases**.
The **Cases** page displays the list of all cases that were opened by SupportAssist.
2. Select the support case that you want to suspend and click **Suspend**.
 **NOTE:** The **Suspend** option is disabled if you have already requested to suspend the selected support case.
3. Optionally, enter your reason for requesting to suspend activities for the support case.
4. Click **OK**.
The support case displays the appropriate status.
 **NOTE:** If SupportAssist is unable to process your request, an appropriate message is displayed. In such a case, you can run the case creation test to verify connectivity to Dell EMC, and then retry the operation. See [Run connectivity test](#) on page 19.

Request to resume support activities

About this task

If you had previously requested to suspend support activities for the support case, you can request Technical Support to resume activities for a support case.

Steps

1. From the **Plugins** menu, select **SupportAssist > Cases**.
The **Cases** page displays the list of all cases that were opened by SupportAssist.
2. Select the support case that you want Technical Support to resume case activities and click **Resume**.
 **NOTE:** The **Resume** option is enabled only if you had previously requested to suspend the selected support case.
3. Optionally, enter the reason for requesting to resume activities for the support case.
4. Click **OK**.
The support case displays the appropriate status.
 **NOTE:** If SupportAssist is unable to process your request, an appropriate error message is displayed. In such a case, you can run the cases creation test to verify connectivity to Dell EMC, and then retry. See [Run connectivity test](#) on page 19.

Request to close a support case

About this task

If you have resolved an issue with a device, you can request Technical Support to close the support case.

-  **NOTE:** You can request Technical Support to close a support case only if the support case was opened by SupportAssist.
-  **NOTE:** You can request Technical Support to close a support case that is in any status, except the case for which the request for closure is in progress.

Steps

1. From the **Plugins** menu, select **SupportAssist > Cases**.
The **Cases** page displays the list of all cases that were opened by SupportAssist.
2. Select the support case that you want to suspend and click **Request To Close**.
3. Optionally, enter your reason for requesting to close the support case.
4. Click **OK**.
The support case displays the appropriate status.
 - NOTE:** After you request to close a support case, Technical Support may contact you to get more information before closing the support case.
 - NOTE:** If SupportAssist is unable to process your request, an appropriate error message is displayed. In such a case, you can run the case creation test to verify connectivity to Dell EMC, and then retry the operation. See [Run connectivity test](#) on page 19.

View support cases for a specific device

About this task

You can view the open support cases for a specific device monitored by SupportAssist.

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. To view the open support cases for a device, in the **All Devices** list, click the device name.
3. On the <device name> page, click **SupportAssist > Cases**.
 - If support cases are available for the device, all the support cases for the device are listed on the **Cases** page.
 - OpenManage Enterprise SupportAssist displays a message when SupportAssist is unable to retrieve support case information.

OpenManage Enterprise SupportAssist device collections

Collections are files that contain information of the SupportAssist managed devices. SupportAssist collects device information from each device that you added, and then uploads the information securely to Dell EMC.

The purge collections task runs automatically every day at 10 p.m. (time as on the server where SupportAssist is installed). System information collections that are 30 days or older and collections that are older than the last 5 collections within the last 30 days are automatically purged.

NOTE: To collect system information from the device, OpenManage Server Administrator (OMSA) must be installed and running on the managed PowerEdge devices.

The system information is collected in following ways:

- **Periodically**—The device collection is performed periodically at regular intervals, depending on the predefined collection start date specified in the **Settings > Schedule Tasks** page. For more information, see [Enable or disable periodic collection of system information](#) on page 34.
- **On case creation**—The device collection is performed when a support case is created for an issue that is detected by SupportAssist.
- **Manually (on demand)**—If Technical Support requests you to upload the device collection, you can initiate the collection of device information from one or more devices at any time.

You can manually upload a collection to the backend or SupportAssist can automatically initiate a collection for the devices listed in *Dell EMC OpenManage Enterprise SupportAssist Support Matrix* available at [OpenManage Enterprise SupportAssist](#) page in support site.

You can view, upload, and download collections by using the **Collections** page. See [View collections](#) on page 29.

Topics:

- [View collections](#)
- [Using SupportAssist to collect and send system information](#)
- [Configuring collection settings on OpenManage Enterprise SupportAssist](#)

View collections

The **Collections** page lists the collections of your devices. To view the collections that are specific for a device, see [Manually collect device information from a device](#) on page 30. To view the **Collections** page, from the **Plugins** menu, select **SupportAssist > Collections**.

The following options and collection information is displayed on the **Collections** page.

- **Advanced Filters**—To filter the collections, click **Advanced Filters** in the upper-left corner of the **Collections** page, and select or enter data in the filter boxes. You can filter collections by collection purpose, collection status, collection type, and filter collections within a specified start and end dates. To remove filter, click **Clear All Filters**.
- The Refresh icon—The Refresh icon in the upper-right corner of the **Collections** page. Click the icon to refresh the collection list displayed.
- To sort the collection list display data by column name, click any column header. The report refreshes to display the data in an ascending or descending order of the column header you clicked.
- **NAME**—The unique name that identifies the collection.
- **COLLECTION DATE**—Displays the date and time of the collection.
- **UPLOAD STATUS**—Displays the upload status of the collection. The possible statuses are:
 - **Not Initiated**
 - **Not Applicable**
 - **In Progress**
 - **Completed**

- **Failed**
- **COLLECTION STATUS**—Displays the status of the collection. The possible statuses are:
 - **Initiated**
 - **In Progress**
 - **Completed**
 - **Completed With Warnings**
 - **Completed Partially**
 - **Partial**
 - **Execution Failed**
 - **Cancel Initiated**
 - **Cancel In Progress**
 - **Cancelled**
 - **Aborted**
- **PERCENTAGE COMPLETE**—The collection completing status in percentage.
- **COLLECTION PURPOSE**—Displays the purpose of the collection.
- **CASE NUMBER**—Identifies the case that is associated with this collection.
- **COLLECTION TYPE**—Identifies the type of the collection. The possible types are **Manual**, **Periodic**, and **Alert Based**.
- Detailed collection pane—The detailed collection pane on the right side of the **Collections** page displays the following data for each collection. To view the detailed information about a collection, click the collection record on the **Collections** page.
 - Collection name
 - Upload Status
 - Upload Date
 - Lists the Hostname/ IP Address of the devices in the collection.
 - List the Service Tag of the devices in the collection.
 - Collection status of each device in the collection. The possible statuses are:
 - **Initiated**
 - **In Progress**
 - **Completed**
 - **Completed With Warnings**
 - **Completed Partially**
 - **Execution Failed**
 - **Cancel Initiated**
 - **Cancel In Progress**
 - **Cancelled**
 - **Aborted**

 **NOTE:** The **Cancelled** status is displayed when you cancel the collection on the user interface. The **Aborted** status is displayed if device collection is stopped unexpectedly due to service failures in the backend.

Using SupportAssist to collect and send system information

SupportAssist automates the collection of system information from your devices both periodically and on case creation. If required, you can also manually start the collection and upload of system information to Dell EMC at any time. You can choose to start the collection of device information from one or more devices or from a device group.

Manually collect device information from a device

About this task

When a support case is opened or updated for a device, SupportAssist automatically collects and uploads the system information to the backend. If necessary, you can also manually start the collection of system information from a device.

You may manually start the collection:

- If an issue occurs during automatic collection and upload of system information
- If requested by Technical Support

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. To collect the device information from a device, in the **All Devices** list, click the device name.
3. On the <device name> page, click the **SupportAssist** tab, and then click **Collections**.
4. On the **Collections**, click **Start Collection**.
The device collection will be automatically listed on the **Collections** page. See [View collections](#) on page 29.

Manually collect system information from a device group

About this task

When a support case is opened or updated for a device, SupportAssist automatically collects and uploads the system information to the backend. If necessary, you can also manually start the collection from devices in a group.

 **NOTE:** The collection operations are not supported for **Staging** group.

You may manually start the collection:

- If an issue occurs during automatic collection and upload of system information
- If requested by Technical Support

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. In the left pane, in the **PLUGIN GROUPS** section, expand the **SupportAssist** group.
3. To start the collection from a device group, click the vertical ellipses next to the group, and click **Start Collection** from the list.

 **NOTE:** If there are more than 100 devices in a group, the collection will be initiated in batches of 200 devices.

4. In the list, click **Start Collection**.
The **Start Collection** dialog box is displayed.
5. On the **Collection Purpose** page, select one of the following purposes for which the device details are collected, and then click **Next**.
 - **Deployment**
 - **System Maintenance**
 - **Consulting**
 - **Technical Support**

 **NOTE:** The **Deployment** option is selected by default for the collection purpose.

6. Optionally, on the **Collection Details** page, enter the name for the collection, case number associated with this collection, Dell EMC Technical email address, and project ID.
7. To upload the collection after the collection is successfully completed, select **Upload Collection**.
The device collection is automatically listed on the **Collections** page. See [View collections](#) on page 29

Upload collection from disconnected site

When Internet connectivity is available, SupportAssist automatically collects and sends system information from your devices to the Dell EMC backend. If the server where OpenManage Enterprise is deployed does not have Internet connection, you can manually upload collections. You may opt to upload a collection in the following cases:

- The collection is successful, but the collection could not be successfully uploaded.
- You want to reupload a collection to the backend.

Upload multiple collections

Steps

1. From the **Plugins** menu, select **SupportAssist > Collections**.
The **Collections** page displays the list of all collections.

2. Select the collections that you want to send to Dell EMC and click **Upload**.
To upload a collection for a specific device, see [Upload collection for a specific device](#) on page 32.

Upload collection for a specific device

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. To collect the device information from a device, in the **All Devices** list, click the device name.
3. On the <device name> page, click **SupportAssist > Collections**.
4. Select the collections that you want to send to Dell EMC backend and click **Upload**.
To upload multiple collections, see [Upload multiple collections](#) on page 31.

Download and view multiple device collections

About this task

If you have performed a collection for one or more devices or for a device group, you can download and view the device information that is collected for each device using a web browser.

Steps

1. From the **Plugins** menu, select **SupportAssist > Collections**.
The **Collections** page displays the list of all collections.
2. Select the collection that you want to download.
 **NOTE:** You can download only one collection at a time.
3. Click **Download** and save the collection file.
4. To view the device information for each device, extract the files and open the `index.html` file in a web browser.
To download and view collection for a specific device, see [Download and view collection from a specific device](#) on page 32.

Download and view collection from a specific device

About this task

If you have performed a collection for a specific device, you can download and view device data about the device by doing the following in the OpenManage enterprise console.

Steps

1. From the OpenManage Enterprise menu, select **Devices**.
2. In the **All Devices** list, click the device name from which you want to collect the device information.
3. On the <device name> page, click **SupportAssist > Collections**.
4. Select the collection that you want to download.
5. Click **Download** and save the collection file.
6. To view the device information, extract the file and open the `index.html` file.
To download and view device information for each device in a multiple collection [Download and view multiple device collections](#) on page 32

Configuring collection settings on OpenManage Enterprise SupportAssist

SupportAssist automatically collects system information from all devices at periodic intervals. SupportAssist also collects system information automatically from a device when a support case is created or an issue is created in a device. Based on your preferences, you can configure the following:

- Automatic collection of system information when a support case is created or updated. See [Enable or disable automatic collection of system information on support case creation](#) on page 33.
- Periodic collection of system information. See [Enable or disable periodic collection of system information](#) on page 34.
- Collection of identity information. See [Enable or disable collection of identity information](#) on page 34.
- Collection of software information and the system log. See [Filter components of device collections](#) on page 35.

Prerequisites for collecting system information

- The local system must have sufficient disk space to save the collected system information.
- The local system and remote devices must fulfill the network port requirements.
- If you have added a server using the operating system, IP address, or hostname (agent-based monitoring):
 - To collect system information from the device, OpenManage Server Administrator (OMSA) must be installed and running on the managed PowerEdge devices.
 - If the server is running a Linux operating system:
 - The device credentials that you have entered in SupportAssist must have administrator-level rights on the device.
 - No resource (network share, drive, or ISO image file) must be mounted on the `/tmp` folder.
 - If OMSA is installed on the device, the latest version of OpenSSL must also be installed on the device. For more information about OpenSSL, see the resolution for OpenSSL CCS injection vulnerability (CVE-2014-0224) available on the respective vendor support website of the operating system.
- If you have added by using the iDRAC IP address (agentless monitoring), the iDRAC credentials that you entered must have administrator privileges.
- The local system must have Internet connection for uploading the collected system information to the backend.
- For collecting system information from ESX and ESXi only, ensure that Small Footprint CIM Broker (SFCB) daemon and CIM Object Manager (CIMOM) are enabled.

Enable or disable automatic collection of system information on support case creation

About this task

By default, SupportAssist automatically collects system information from the device when a support case is created and sends the information securely to Dell EMC. If required, you can enable or disable the automatic collection based on your preference.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
The **Settings** page is displayed.
2. On the **Settings** tab, select **Collection**.
The **Collection** page is displayed.
3. In the **Upload Collection** section, select or clear **Collect and send system state information to Dell EMC**.

 **NOTE:** By default, this option is selected.

4. Click **Apply**.

Results

The automatic collection feature is enabled and the collection data is automatically sent to Dell EMC Support team when a device case is created.

Enable or disable periodic validation of device inventory

About this task

By default, the device inventory validation is scheduled on a randomly determined day of every month at 11 PM. If necessary, you can change the schedule based on your requirement.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
The **Settings** page is displayed.
2. On the **Settings** tab, select **Schedule Tasks**.
The **Schedule Tasks** page is displayed.
3. Perform one of the following in the **Validate Device Inventory** section:
 - To enable periodic validation of device inventory, select the **On day <select a date> of every month at 11 PM** check box, and select a date to validate the device inventory.
 - To disable periodic device inventory validation, clear the **On day <select a date> of every month at 11 PM** check box.
4. Click **Apply**.

Enable or disable periodic collection of system information

About this task

By default, SupportAssist starts collecting system information from all monitored devices at periodic intervals and sends it to the backend. The collection start time is a user-defined day of every month at 11 p.m. If required, you can enable or disable the periodic collection of system information from all monitored devices based on your preference.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
The **Settings** page is displayed.
2. On the **Settings** tab, select **Schedule Tasks**.
The **Schedule Tasks** page is displayed.
3. Perform one of the following in the **Collect system state information** section:
 - To enable periodic collection, select the **On day <select a date> of every month at 11 PM** check box, and select a date to collect device state information from the supported devices.
 - To disable periodic collection, clear the **On day <select a date> of every month at 11 PM** check box.
4. Click **Apply**. To reset to default connection settings, click **Discard**.

Enable or disable collection of identity information

About this task

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 your company's security policy restricts sending identity data outside of the company network, you can disable SupportAssist from collecting such data.

The following identity information can be filtered when collecting the system information from a device:

- Host name
- IP address
- Subnet mask
- Default gateway
- MAC address
- DHCP server
- DNS server
- Processes
- Environment variables
- Registry

- Logs
- iSCSI data
- Fibre Channel data—Displays the WWN of the host device and port.

NOTE: When you disable collection of identification information, some of the data about your company network (including the system log and SMART log) is not transmitted to the backend. This may prevent technical support from resolving issues that may occur on your devices.

NOTE: If you have disabled the collection of identity information from the devices, the identity information such as hostname and IP address are replaced by tokenized values. The tokenized values are represented as TOKEN n. For example, TOKEN0, TOKEN1, or TOKEN2.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
The **Settings** page is displayed.
2. On the **Settings** tab, select **Collection**.
The **Collection** page is displayed.
3. By default, the **Include device identification information in data sent to Dell EMC** check box in the **Identification Information Settings** section is selected. Depending on your requirement, select or clear the check box.

NOTE: If you disable collection of device identification information, the settings for collection of logs, diagnostic data, and support data are disabled automatically. Therefore, collections that are sent to the Dell EMC from your devices do not include certain categories of data.
4. Click **Apply**.

Filter components of device collections

About this task

By default, the system information that is collected and sent to the Dell EMC by SupportAssist includes software information and system logs. If required, you can configure SupportAssist to filter the components of the collection being uploaded to Dell EMC.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
The **Settings** page is displayed.
2. On the **Settings** tab, select **Collection**.
The **Collection** page is displayed.
3. In the **Server/Hypervisor** section, to filter the following components of the device collection, clear the corresponding check boxes.
 - **Software Details**
 - **System Logs**
 - **SMART Logs**
4. Click **Apply**.

Configuring OpenManage Enterprise SupportAssist settings

The **Settings** tab enables you to configure the following:

- Internet connection settings for the servers on which OpenManage Enterprise SupportAssist is deployed
- Enable SupportAssist maintenance mode for all devices monitored using SupportAssist
- Collection of system information
- Contact and shipping information
- TechDirect integration
- Schedule device telemetry collection and device inventory validation
- Email notifications

Topics:

- [Configure proxy server settings](#)
- [Enable or disable SupportAssist maintenance mode](#)
- [Enable or disable group-level SupportAssist maintenance mode](#)
- [Enable or disable device-level SupportAssist maintenance mode](#)
- [Collection preferences](#)
- [Contact Details](#)
- [Configure contact information](#)
- [Configure Shipping Details](#)
- [Schedule collection and inventory validation](#)
- [Configure email notification settings](#)

Configure proxy server settings

About this task

The OpenManage Enterprise SupportAssist uses the same proxy server that is configured on OpenManage Enterprise to connect to the Internet. If a proxy is configured on OpenManage Enterprise server, the same proxy settings are applied to SupportAssist Plugin, by default. To add or edit the proxy settings for both OpenManage Enterprise and OpenManage Enterprise SupportAssist, perform the following steps.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
2. On the **Settings** page, click **Add/Edit Proxy**.
3. On the **Add/Edit Proxy** page, perform one of the following:
 - If proxy is not configured on OpenManage Enterprise, the **Add Proxy Settings** link is displayed. To configure the proxy settings for both OpenManage Enterprise and SupportAssist Plugin, click **Add Proxy Settings**.
 - If proxy is configured on OpenManage Enterprise, the same proxy details are displayed in the **Add/Edit Proxy** page. To edit the proxy settings, click **Edit Proxy Settings**.

a. Select **Enable HTTP Proxy Settings**.

The proxy server fields are enabled.

b. Enter the IP address or hostname of the proxy server.

c. Enter the port number of the proxy server.

d. If a username and password are required to connect to the proxy server, select **Enable Proxy Authentication**.

 **NOTE:** If you do not provide the username and password, SupportAssist connects to the proxy server as an anonymous user.

4. Click **Apply**.
The proxy settings are saved.

Enable or disable SupportAssist maintenance mode

About this task

SupportAssist maintenance mode places all monitored devices in maintenance mode, suspends alert processing and automatic case creation. However, SupportAssist does not restrict other operations such as periodic and manual collections, connectivity check, and so on. In this mode, a yellow Maintenance Mode banner is displayed on top of the page. Enable this mode to prevent the creation of support cases during downtime or a routine maintenance activity. For more information about SupportAssist maintenance mode, see [SupportAssist maintenance mode](#) on page 45.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
2. On the **Settings** page, click **SupportAssist Maintenance**.
3. To enable maintenance mode, select **Suspend SupportAssist activities (including case creation and collection) for all supported devices**.
4. To place all monitored devices in maintenance mode, on the confirmation message displayed, click **Yes**.

Results

If SupportAssist Maintenance Mode is enabled, a Maintenance mode banner is displayed on the OpenManage Enterprise SupportAssist user interface.

Enable or disable group-level SupportAssist maintenance mode

About this task

If you have a planned maintenance activity for a device group and do not want SupportAssist to process alerts from the devices in the group, you can place that device group in maintenance mode. After the maintenance activity is completed, you can remove the device group from the maintenance mode, enabling SupportAssist to process alerts from the device normally. For more information about SupportAssist maintenance mode, see [SupportAssist maintenance mode](#) on page 45.

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. In the left pane, in the **PLUGIN GROUPS** section, expand the **SupportAssist** group.
3. To place a device group in SupportAssist Maintenance mode, click the vertical ellipses next the group, and click **Enable SupportAssist Maintenance mode** from the list. To disable the SupportAssist Maintenance mode, click **Disable SupportAssist Maintenance mode**.

Enable or disable device-level SupportAssist maintenance mode

About this task

If you have a planned maintenance activity for a specific device and do not want SupportAssist to process alerts from that device, you can place the device in maintenance mode. After the maintenance activity is completed, you can remove device from maintenance mode, enabling SupportAssist to process alerts from the device normally. For more information about SupportAssist maintenance mode, see [SupportAssist maintenance mode](#) on page 45.

Steps

1. From the OpenManage Enterprise menu, click **Devices**.
2. In the **All Devices** list, click the device name that you want to place it in SupportAssist Maintenance mode.
3. On the <device name> page, click **SupportAssist > Device Info**.
4. On the **Device Info** page, click **Enable SupportAssist Maintenance**.
5. To place the device in maintenance mode, in the confirmation message displayed, click **Yes**.
A banner message is displayed that the device is in SupportAssist maintenance mode. To disable the SupportAssist maintenance mode for the device, click **Disable** in the banner message.

Collection preferences

The **Collection** page enables you to configure collection preferences. To open the **Collection** page, from the **Plugins** menu, select **SupportAssist > Settings**. On the **Settings** page, click **Collection**.

On the **Collection** page, you can configure the following collection preferences:

- **Server/Hypervisor**—Do the following:
 - To collect software-related information from the device, select **Software Details**.
 - To collect logs from the device, select **System Logs**.
 - To collect smart CTL logs from the device, select **SMART Logs**.
- **Upload Collection**—Select **Collect and send system state information to Dell EMC** to enable SupportAssist to automatically upload collections to the backend.
- **Identification Information Settings**—Select **Include device identification information in data sent to Dell EMC** to enable SupportAssist to send the system identification information along with other data to the backend. Else, the device identification information values are masked when the collections are uploaded to the Dell EMC

Contact Details

The **Contact Details** page enables you to view and edit the primary and secondary contact information.

- To configure your contact information, see [Configure contact information](#) on page 38.
- To configure your parts dispatch preferences, see [Configure Shipping Details](#) on page 39.

Configure contact information

About this task

Enter or update your primary and secondary contact information after you register SupportAssist. If the primary contact is unavailable, Dell EMC contacts your company through the secondary contact. If both the primary and secondary contacts are configured with valid email addresses, both receive the SupportAssist emails.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
2. On the **Settings** page, click **Contact Details**.
3. In the **Primary Contact Details** section, perform the following:
 - a. Enter the company name, first name, last name, phone number, alternate phone number, and email address.
 - b. Select the preferred contact method, contact hours, and time zone.
4. In the **Secondary Contact Information** section, perform the following:
 - a. Enter the first name, last name, phone number, alternate phone number, and email address.
 - b. Select the preferred contact method, contact hours, and time zone.
5. Click **Apply**.

Configure Shipping Details

About this task

Entering your dispatch preferences and shipping information enables Dell EMC to dispatch a replacement part for your device.

 **NOTE:** If a device is moved to a different location, ensure that the dispatch preferences and shipping information are updated.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
2. On the **Settings** page, click **Shipping Details**.
3. If you do not want to automatically receive the replacement parts, clear the **I want Dell EMC to expedite dispatch of the replacement parts** check box. By default, the **I want Dell EMC to expedite dispatch of the replacement parts** check box is selected.
4. In the **Primary Shipping Contact Details** section, perform the following:
 - a. Enter first name, last name, phone number, email address, and select the time zone.
 **NOTE:** If the primary shipping contact details are same as the contact details, click **copy contact details**.
 - b. Select the preferred contact hours.
 **NOTE:** If you enter your preferences and shipping information during the registration, the information is automatically displayed on the **Shipping Details** page. You can edit the information, if required.
5. In the **Secondary shipping contact** section, enter the first name, last name, phone number, and email address.
 **NOTE:** Contact details of the primary and secondary contact must be unique.
6. In the **Shipping Address** section, perform the following:
 - a. Enter the shipping address.
 - b. In the **Dispatch notes** section, enter dispatch-related information.
 - c. If you want a technician to replace the parts onsite, select **I want a technician to replace the parts onsite if the service is included in the service plan**. Replacement of the parts onsite service is available only if the service is included in your service plan.
 **NOTE:** The availability of parts to dispatch and policies may vary based on your region and country.
7. Optionally, to view asset information and manage SupportAssist alerts and part dispatches by using TechDirect, sign in to TechDirect using your company's administrator account and enter the One-Time Password (OTP). To sign in to TechDirect, click **Launch TechDirect**, and then do the following.
 **NOTE:** To manage SupportAssist and part dispatches by using TechDirect, you must provide the primary contact information, and primary and secondary shipping information.
 - a. Click **Sign In**.
The **Dell Account Sign In** window is displayed.
 - b. Enter the email address and password, and then click **Sign In**.
The OTP is displayed.
 - c. Enter the OTP and click **Validate OTP**.
The TechDirect account is verified and a message is displayed that your TechDirect account is integrated with SupportAssist. To integrate SupportAssist with a different TechDirect account, click **SwitchAccount**.
8. Click **Apply**.

Schedule collection and inventory validation

About this task

By default, periodic collection and inventory validation is scheduled on a randomly determined day on every month at 11 p.m. If necessary, you can change the schedule (day) based on your requirement.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
2. On the **Settings** page, click **Schedule Tasks**.
3. To select or change the date to collect the system state information, in the **Collect System State Information** section, select **On day <day> of every month at 11 PM**, and then select the day from the drop-down.
4. To select or change the change the date to perform device inventory validation, in the **Validate Device Inventory** section, select **On day <day> of every month at 11 PM**, and then select the day from the drop-down.
5. Click **Apply**.

Configure email notification settings

About this task

By default, SupportAssist is configured to send an email notification when a support case is created automatically. SupportAssist can also send email notifications about maintenance mode, device status, and network connectivity status. For information about the different types of SupportAssist Enterprise email notifications, see [Types of email notifications](#) on page 40.

Depending on your preference, you can perform the following:

Enable or disable automatic email notification from SupportAssist and also select the preferred language for email notifications.

Steps

1. From the **Plugins** menu, select **SupportAssist > Settings**.
2. On the **Settings** page, click **Email Notification**.
The **Email Notification** page is displayed.
3. To receive email whenever a support case is created, select **Receive email notification when a new support case is opened**.
4. From the **Preferred Email Language** list, select a language in which you want to receive email notifications.
5. Click **Apply**.

Types of email notifications

The following table provides a summary of the different types of email notifications that are sent by Dell EMC backend.

Table 3. Types of email notifications

Email notification type	When the email notification is sent
Registration confirmation and welcome email	After the registration of SupportAssist is completed successfully.
Case created	After a hardware issue is detected and a support case is created.
Unable to create a case	After a hardware issue is detected, but a support case could not be created because of technical difficulties.
Device warranty expired	After a hardware issue is detected, but a support case could not be created because the device is out of warranty and does not have an active ProSupport or ProSupport Plus service contract.

Table 3. Types of email notifications (continued)

Email notification type	When the email notification is sent
Unable to collect system information	After a support case is created automatically for a device, but SupportAssist is unable to system information from the device.
Unable to send the collected system information to Dell EMC	After a support case is created automatically for a device, but SupportAssist is unable to send the collected system information from the device to Dell EMC.
Devices added for the first time	After the devices are added to the SupportAssist for the first time.
Inactive notification	If SupportAssist is not monitoring any device and no device has been added in the past 30 days.
Disable SupportAssist alert	If you disable SupportAssist on OpenManage Enterprise.
TechDirect token expiry notification	When the TechDirect token expires.
Parts dispatch notification and address validation	When SupportAssist has detected a hardware issue on one of your devices and a part replacement is required to resolve the issue.
Parts dispatch address confirmation	After the replacement part is ready to be dispatched.

OpenManage Enterprise SupportAssist product information

The **About** page displays the OpenManage Enterprise SupportAssist version, publisher name, registration ID, serial number, and product overview.

To access the **About** page, from the **Plugins** menu, click **SupportAssist > About**.

Disable OpenManage Enterprise SupportAssist

About this task

Disables all the functionality of SupportAssist on OpenManage Enterprise.

NOTE: Ensure that you logged in to OpenManage Enterprise as an **Admin**. Only the user with Admin role can disable plugins in OpenManage Enterprise.

NOTE: Disabling an plugin in OpenManage Enterprise restarts the appliance services.

Steps

1. From the OpenManage Enterprise menu, click **Application Settings > Console and Plugins**.
The **Console and Plugins** tab is displayed.
2. In the SupportAssist section, click the **Disable** option.
The **Disable Plugin** page is displayed.
3. To disable SupportAssist on OpenManage Enterprise, click **Disable Plugin**.

Results

After disabling SupportAssist, you cannot see any information or pages that are related to Support Assist in OpenManage Enterprise.

Uninstall OpenManage Enterprise SupportAssist

About this task

You can uninstall SupportAssist from OpenManage Enterprise and remove all data associated with SupportAssist.

 **NOTE:** Ensure that you logged in to OpenManage Enterprise as an **Admin**. Only the user with Admin role can uninstall plugins in OpenManage Enterprise.

Steps

1. From the OpenManage Enterprise menu, click **Application Settings > Console and Plugins**.
The **Console and Plugins** tab is displayed.
2. In the SupportAssist section, click the **Uninstall** option.
The **Uninstall Plugin** page is displayed.
3. To uninstall SupportAssist from OpenManage Enterprise, click **Uninstall Plugin**.

SupportAssist maintenance mode

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. The following sections provide more information about the maintenance mode functionality:

Topics:

- [Global-level SupportAssist maintenance mode](#)
- [Group-level SupportAssist maintenance mode](#)
- [Device-level SupportAssist maintenance mode](#)

Global-level SupportAssist maintenance mode

Global-level SupportAssist maintenance mode places all monitored devices in maintenance mode, suspending alert processing and automatic case creation for all devices. While in global-level maintenance mode, SupportAssist displays a yellow Maintenance Mode banner at the top of the page. You can enable global-level maintenance mode to prevent the creation of unnecessary support cases during downtime or a routine maintenance activity. For instructions to enable global-level maintenance mode, see [Enable or disable SupportAssist maintenance mode](#) on page 37.

Group-level SupportAssist maintenance mode

Group-level SupportAssist maintenance mode suspends alert processing and automatic case creation for a device group. For all other monitored devices and device groups SupportAssist continues to process alerts and create support cases, if the alerts qualify for case creation.

The global-level and group-level SupportAssist maintenance mode functionalities work independent of each other. If a device group is placed in SupportAssist maintenance mode, the devices in group continues to remain in SupportAssist maintenance mode even if global-level maintenance mode is enabled and then disabled. For the instructions on how to enable or disable Group-level SupportAssist maintenance mode, see [Enable or disable group-level SupportAssist maintenance mode](#) on page 37.

Device-level SupportAssist maintenance mode

Device-level SupportAssist maintenance mode suspends alert processing and automatic case creation for a specific device. For all other monitored devices, SupportAssist continues to process alerts and create support cases, if the alerts qualify for case creation. Device-level SupportAssist maintenance mode is implemented as follows:

- **Automated device-level maintenance mode**—By default, if SupportAssist receives 10 or more valid hardware alerts within 60 minutes from a specific device, SupportAssist automatically places that device in maintenance mode. The device remains in maintenance mode for 30 minutes, enabling you to resolve the issue without creating additional support cases for the device. An email notification is also sent to the primary and secondary contacts, and the device displays the maintenance mode icon. After 30 minutes, the device is automatically removed from the maintenance mode, enabling SupportAssist to resume normal alert processing for the device. If required, you can retain the device in maintenance mode until you resolve the issue, by manually enabling maintenance mode. You can also remove a device from automated maintenance mode before the 30-minute period. For instructions to enable or disable the device-level maintenance mode, see [Enable or disable device-level SupportAssist maintenance mode](#) on page 37.
- **Manual device-level maintenance mode**—If you have a planned maintenance activity for a device, and do not want SupportAssist to automatically create support cases, you can place that device in maintenance mode. After the maintenance activity is completed, you can remove the device from the maintenance mode, enabling SupportAssist to resume processing alerts from the device normally. For instructions to enable device-level maintenance mode, see [Enable or disable device-level SupportAssist maintenance mode](#) on page 37.

The global-level and device-level SupportAssist maintenance modes work independent of each other. For example:

- If a device is placed in manual maintenance mode, the device continues to remain in manual maintenance mode even if global-level maintenance mode is enabled and then disabled.
- If a device is placed in automated maintenance mode, the device continues to remain in automated maintenance mode for 30 minutes even if the global-level maintenance mode is enabled and then disabled.

For the instructions on how to enable or disable Device-level SupportAssist maintenance mode, see [Enable or disable device-level SupportAssist maintenance mode](#) on page 37

Alert policies in OpenManage Enterprise SupportAssist

This chapter provides details on how SupportAssist processes alerts and automatically creates support cases.

Topics:

- Which hardware faults does SupportAssist monitor?
- What happens when a hardware issue is detected by SupportAssist?
- How and where am I notified by OpenManage Enterprise SupportAssist about device alerts?
- What is the response time for resolving my OpenManage Enterprise SupportAssist case?
- What alerts open predictive support cases in advance of hardware failures?
- What if I require assistance for deploying installing OpenManage Enterprise SupportAssist?
- Alert threshold
- First occurrence policies
- Repeat occurrence policies

Which hardware faults does SupportAssist monitor?

SupportAssist has a smart hardware fault monitoring algorithm with thresholds to avoid false positives and duplication of actions. Not all hardware faults have immediate response actions. They are compared to persistent fault threshold values prior to responding with defined actions. Defined response actions include case creation, diagnostic execution, and log attachment.

- On Dell EMC PowerEdge servers, SupportAssist monitors for hardware faults, including memory, disk, power supply, controller, and other component failures.
- On Dell EMC Storage devices such as MD Series, PS Series, and SC Series, SupportAssist can integrate with OpenManage Essentials to monitor faults such as disks, controllers, power supplies, cache batteries, and other component failures.
- On Dell EMC Networking switches previously known as PowerConnect and Force10, SupportAssist can monitor faults such as link failures or rising temperatures.

What happens when a hardware issue is detected by SupportAssist?

When a fault occurs on a device with an active ProSupport or ProSupport Plus service entitlement, SupportAssist creates a new support case with Dell EMC Technical Support. You receive an email notification containing the case number for that Dell EMC Service Tag, and then a support technician contacts you to resolve the issue. All subsequent faults on that Service Tag are appended to the same support case until the issues are resolved and the case is closed.

When a fault occurs on a system that does not have a ProSupport or ProSupport Plus service entitlement, SupportAssist does not create a new case with Dell EMC Technical Support. However, you receive an email notification stating that an error has occurred for a Service Tag, and that you may want to contact Dell EMC Technical Support for assistance.

How and where am I notified by OpenManage Enterprise SupportAssist about device alerts?

For devices that are managed by a systems management console, alert notifications are displayed within the systems management console. You can also set up OpenManage Essentials or SCOM to send alert notifications automatically to you by email. For more information on setting up alert notifications in OpenManage Essentials, see the "Managing Alerts" and "Alerts - Reference" chapters in the Dell OpenManage Essentials User's Guide at Dell.com/OpenManageManuals.

Alert notifications in SupportAssist occur through automatic email notifications from Dell EMC Technical Support. If the device that generated the alert has a ProSupport or ProSupport Plus service entitlement, Dell Technical Support will also contact you by phone to assist you in resolving the issue. SupportAssist automates support case creation with Dell EMC. If the alerts generated by a device exceed the Dell EMC Support Services predefined alert threshold, a support case is automatically created. For information on the predefined alert thresholds, see [Alert threshold](#) on page 48

NOTE: SupportAssist sends automatic email notifications only for hardware alerts that would most likely create a support case when you contact Dell EMC Technical Support by phone or via Dell EMC TechDirect online case management.

What is the response time for resolving my OpenManage Enterprise SupportAssist case?

A service request to open a support case with Dell EMC is created by SupportAssist at the time a given alert goes beyond the predefined threshold. The service request is created automatically, without you necessarily noticing the issue and then contacting Dell EMC. These service requests are then automatically sent and assigned to a Dell EMC Technical Support agent. The agent accepts the service request and starts the resolution process

The response time for a support case created by SupportAssist is generally faster than that of a support case created by contacting Dell EMC Technical Support over phone. The support case is created at severity level which is important, but not urgent. If you consider that the support case requires more urgent attention, you may contact Dell EMC Technical Support.

For more information on the Dell Support agreement, see the [Service Descriptions](#).

What alerts open predictive support cases in advance of hardware failures?

Predictive alerts are based on scheduled collections that are sent to Dell EMC. These collections are analyzed and compared so we can determine that a failure will occur with a high degree of certainty. Customers using SupportAssist will receive automated predictive case creation for server hardware (hard disk, backplane and expanders), provided the server has an active ProSupport Plus service entitlement.

What if I require assistance for deploying installing OpenManage Enterprise SupportAssist?

Many customers download and install OpenManage Enterprise SupportAssist without assistance from Dell EMC. For those wanting assistance, the [ProDeploy](#) Enterprise suite of services includes the enablement and configuration of OpenManage Enterprise SupportAssist.

Alert threshold

The SupportAssist alert threshold specifies the criteria that must be satisfied for a support case to be created (or appended) in the Dell EMC Technical Support case management system.

Currently, there are two types of policies for determining the criteria for creating or appending a support case:

- First occurrence policies—These policies create or append a support case each time a specific alert is detected
- Repeat occurrence policies—These policies create or append a support case when a specific alert is detected a specific number of times within a specific duration

SupportAssist processes all alerts from OpenManage Essentials and SCOM, but a support case is created only if:

- SupportAssist policies qualify the alert for creating a support case
- SupportAssist is configured correctly to automatically create support cases
- The Service Tag has an active ProSupport, ProSupport Plus, ProSupport Flex for Data Center, and ProSupport One for Data Center service entitlement at the time of the alert

For SupportAssist to create a support case, the alert must match a criteria in the alert policy defined in SupportAssist. Dell EMC may change a policy for a specific alert within the alert policy for either the SupportAssist application or the back-end

infrastructure at Dell EMC. This may be done from time to time, as Dell EMC Technical Support and Engineering continue to incorporate experience from support case data with all customers.

First occurrence policies

The first occurrence policies represent all hardware-related events. These events can be characterized as follows:

- Hardware issues that impact you from accessing applications or data
- Hardware issues that require a part replacement
- Hardware issues that may result in your data being lost or corrupted
- Violation of critical threshold values for sensors (fan, temperature, power, and so on)

Repeat occurrence policies

These policies represent critical, warning, or informational events. These events result in a support case, if the alert occurs several times within a specified duration.

Warning events

Typically, Dell EMC Technical Support monitors for warning and critical events that are redundant. A warning event indicates that you should schedule time to address the issue. These events can be characterized as follows:

- Hardware issues that have limited impact on your access to applications or data
- Missing devices
- Predictive events that indicate that the hardware is at a risk of failing
- Redundancy loss or degradation (typically 2 or less occurrences)
- Violation of warning threshold values for sensors (fan, temperature, power, and so on). These items typically have threshold < 5 occurrences within a short time span
- Events that result in minor performance degradation in your applications or access to data
- Greater than 5 occurrences (high frequency of occurrence within a short time span)
 - Events in which the system fails to complete a requested action (utilization > 80%)
 - Network type of events

Informational events

- Hardware issues that have minimal impact on your access to applications or data
- Events which you can easily work around
- Error recovery events
- Hardware inventory changes
- System and device setting changes
- Infrequent self-correcting events such as disk media errors or single-bit ECC

After a support case is created, SupportAssist collects system state information from the device and uploads it to Dell EMC.

 **NOTE:** For devices that are covered by a Dell EMC Basic Support service entitlement or with an expired entitlement, a support case is not created, but the system state information is collected and uploaded to Dell EMC, provided SupportAssist is configured correctly.

Error code appendix

The following table lists the error codes, error messages, and possible resolutions.

Table 4. Error code appendix

Error code	Error message	Possible resolution
Registration		
SAE-010001	This request has an invalid status.	The only available statuses are ENABLE or DISABLE.
SAE-010002	Invalid request.	The format of this request body must be a JSON.
SAE-010003	Registration for this client is already in progress.	Contact your network administrator for more information.
SAE-010006	Encountered an error while trying to register SupportAssist.	Reenter your access key and PIN and try to register again.
SAE-010007	Unable to register SupportAssist because of an invalid access key and PIN.	Reenter your access key and PIN, then try to register again.
SAE-010008	The access key and PIN have already expired.	Request for new access key and PIN, and then try again.
SAE-010009	The access key and PIN have already been used.	Request for new access key and PIN, and then try again.
SAE-010010	An error occurred while trying to register SupportAssist.	Enter a new access key and PIN, and then try to register again.
SAE-010011	An error occurred while trying to register SupportAssist.	Reenter your access key and PIN, then try to register again.
SAE-010012	This client is already authenticated with Dell EMC backend.	Try again later. If the problem persists, contact technical support.
SAE-010013	An error occurred while updating your connectivity status.	Try again later, and if the issue persists, contact technical support.
SAE-010015	An error occurred while updating your registration status of the gateway.	Try again later, and if the issue persists, contact technical support.
SAE-010019	Cannot change your registration status until your access key and PIN have been authenticated.	Complete the authentication, and then try again.
SAE-010020	Unable to retrieve the properties file.	Try again. If the issue persists, contact technical support.
SAE-010021	An unknown error occurred while updating the registration.	Try again. If the issue persists, contact technical support.
SAE-010022	This request has an invalid status.	The only available statuses are ENABLED, DISABLED, or DEREGISTERED.
SAE-010023	Cannot complete this operation until registration is completed.	Complete the registration, and then try again.
SAE-010024	Registration failed. An invalid client ID was sent from the client.	Check your request inputs, and then try again.
SAE-010026	This client is already registered.	Try again later. If the problem persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-010027	This request is blocked until the client has completed registration with Dell EMC backend.	Wait for the registration to complete and try again. If the problem persists, contact technical support.
SAE-010032	An error occurred while trying to log in to TechDirect.	Check your connection to the Internet, and then try again.
SAE-010033	An error occurred while trying to reach your gateway.	Check your connection to the Internet, and then try again. If the problem persists, contact technical support.
SAE-010034	The TechDirect integration failed due to an invalid input.	Check the details that are entered and try again.
SAE-010035	This OTP is no longer valid.	Request a new OTP and try again.
SAE-010036	The TechDirect integration failed because of an IDM service issue.	Try again later. If the problem persists, contact technical support.
SAE-010039	Cannot perform this action until this gateway is integrated with your Service Intelligence account.	Integrate the gateway with your Service Intelligence account and try again.
SAE-010040	Cannot complete this operation until SupportAssist is registered.	Complete the registration, and then try again.
SAE-010041	The refresh token has expired.	Log in again.
SAE-010046	The gateway server returned an empty response for this request.	Review the request details and try again.
SAE-010047	A database error occurred while saving the registration ID.	Try again later, and if the issue persists, contact technical support.
SAE-010060	Could not complete this operation due to an unknown database error.	Try again later, and if the issue persists, contact technical support.
SAE-010063	Could not complete your client validation because of a server error.	Try again later, and if the problem persists, contact technical support.
SAE-010064	Encountered an error and could not complete this action.	Try again later, and if the issue persists, contact technical support.
SAE-010065	Could not validate this Access Key and PIN because the company name returned from this request was blank or invalid.	Check your entries and try again. If the issue persists, contact technical support.
SAE-010066	Editing the name of a company is not allowed.	Try again later. If the problem persists, contact technical support.
SAE-010068	An error occurred during validation.	Check your entries and try again. If the issue persists, contact technical support.
SAE-010069	This client is already registered.	Try again later. If the problem persists, contact technical support.
SAE-010070	Unable to validate your contact details with your gateway.	Check your entries and try again. If the problem persists, contact technical support.
SAE-010071	Unable to validate your shipping details.	Try again. If the problem persists, contact technical support.
SAE-010074	Unable to complete this operation because the SupportAssist plug-in was already removed from your gateway.	Register and enable the plug-in, and then try again.
SAE-010080	Cannot change this registration status of the gateway until its initial registration is finished.	Complete your registration, and then try again.
SAE-010081	Unable to complete this operation because of an error with the Dell EMC backend servers.	Try again later. If the issue persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-010082	Unable to complete this operation because of a certificate error.	Restart the service, and then try again. If the issue persists, contact technical support.
SAE-010083	Unable to attempt this operation because connectivity is disabled.	Verify that your plug-in is enabled and try again. If the issue persists, contact technical support.
SAE-010084	Unable to complete this operation because of an unknown error.	Try again later, and if the issue persists, contact technical support.
SAE-010085	Unable to complete this operation because of an unknown error.	Check if your registration has completed, and then restart the service and try again. If the issue persists, contact technical support.
SAE-010086	Unable to complete this operation because of a certificate error.	Restart the service, and then try again. If the issue persists, contact technical support.
SAE-010087	Could not register SupportAssist because unable to reach the Dell EMC backend servers.	Check your Internet connection and try again. If the issue persists, contact technical support.
SAE-010088	Unable to register because this access key is not associated with this model.	Request an access key specific for this model and try again.
SAE-010089	Unable to continue with the the registration because an error occurred during your gateway deployment.	Start your deployment again. If the problem persists, contact technical support.
SAE-010090	Unable to continue with your registration because an error occurred during your gateway deployment.	Restart the host system or virtual machine for your gateway and try again. If the problem persists, contact technical support.
SAE-010091	An error occurred during registration.	Contact technical support for assistance.
SAE-010092	An error occurred during registration because of a server issue.	Enter a new access key and PIN, and then try again.
SAE-010111	Received an error from TechDirect and could not complete this action.	Try again later. If the problem persists, contact technical support.
SAE-010114	Received an error from TechDirect and could not complete this action.	Try again later. If the problem persists, contact technical support.
SAE-010116	Unable to retrieve the state information because of an invalid country code.	Enter a valid country code and try again.
SAE-010117	Unable to retrieve the city information because of an invalid country code.	Enter a valid country code and try again.
SAE-010118	Unable to retrieve the shipping information because of an invalid country code.	Enter a valid country code and try again.
SAE-010119	Cannot continue with the operation because of too many failed attempts.	Wait for 15 minutes and try again.
Collections		
SAE-030001	Operation failed. Unable to perform the operation because an error occurred in the gateway.	Try again later. If the problem persists, contact technical support.
SAE-030002	Collection failed. The gateway could not attempt to collect this telemetry due to insufficient disk space.	Free the space and try again. If the problem persists, contact technical support.
SAE-030003	Operation failed. This query failed to run in the database.	Try again later. If the problem persists, contact technical support.
SAE-030004	Operation failed. These queries failed to run in the database.	Try again later. If the problem persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-030005	Collection failed. Unable to collect the device telemetry from the device.	Unable to collect the device telemetry from the device because the device is not available.
SAE-030006	Collection failed.	Retry the collection after a few minutes.
SAE-030007	Operation failed. The gateway could not update the status of this collection in the database.	Try again later. If the problem persists, contact technical support.
SAE-030008	The gateway could not start this collection.	The "purpose" field is required for multidevice collections, and the current value is either missing or invalid. Check your value, and try again.
SAE-030009	Unable to run this collection.	Move this device out of the Staging group, then try again.
SAE-030010	Collection failed.	This device is not available, so unable to attempt to collect telemetry from it.
SAE-030011	This device does not support telemetry collection.	Try again later. If the problem persists, contact technical support.
SAE-030012	Operation failed. There are no associated records for this Job ID, so there is nothing to return.	Check your Job ID values and try again.
SAE-030013	There are no collections in progress available to cancel for this device.	Try again later. If the problem persists, contact technical support.
SAE-030014	No records were found matching your search criteria.	Update your search criteria and try again.
SAE-030015	Operation failed. The gateway could not update the result of this collection in the database.	If the problem persists, contact technical support.
SAE-030016	Operation failed. The gateway could not update the record of this collection in the database.	If the problem persists, contact technical support.
SAE-030017	Operation failed. The gateway could not update the device-specific record of this collection in the database.	If the problem persists, contact technical support.
SAE-030018	The gateway failed to cancel this collection of telemetry.	Try again later. If the problem persists, contact technical support.
SAE-030019	Operation failed.	The gateway could not locate a record for this collection.
SAE-030020	The gateway has successfully canceled this collection of telemetry.	Try again later. If the problem persists, contact technical support.
SAE-030021	The gateway cannot attempt this operation without a collection age.	Enter one, and then try again.
SAE-030022	The gateway cannot attempt this operation without a valid collection age.	Ensure that the entry is not a null value, and then try again.
SAE-030023	Operation failed. The start or end date is missing.	Enter the start and end date, and then try again.
SAE-030024	Operation failed. No matching records were found for your search criteria.	Update your criteria and try again.
SAE-030025	Unable to retrieve your telemetry due to an internal database error.	Try again later. If the problem persists, contact technical support.
SAE-030026	Operation failed. The device ID is missing.	Try again later. If the problem persists, contact technical support.
SAE-030027	Operation failed. The collection ID is missing.	Try again later. If the problem persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-030028	Operation failed. The gateway cannot reach the Discovery Service.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030029	Operation failed because unable to retrieve the current customer registration details.	Try again later. If the problem persists, contact technical support.
SAE-030030	Operation failed. The gateway cannot communicate with the Registration Service.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030031	Operation failed. The gateway cannot retrieve collection settings from application preferences.	Try again later. If the problem persists, contact technical support.
SAE-030032	Operation failed. The gateway cannot reach the Preferences Service.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030033	Operation failed. The gateway could not reach the Inventory Service.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030034	Operation failed. The gateway could not retrieve device details from the Inventory Service.	Try again later. If the problem persists, contact technical support.
SAE-030035	Operation failed. The gateway could not retrieve collections using the collection ID.	
SAE-030036	Operation failed. The gateway could not retrieve these outdated collections.	
SAE-030037	Operation failed. The gateway cannot retrieve the device ID from the collection device map.	
SAE-030038	Collection removal failed. The gateway could not delete these collections using their ID.	
SAE-030039	Collection removal failed. The gateway could not delete the collections from their file system.	
SAE-030040	Collection removal failed. The gateway could not delete the .zip files from the reports directory.	
SAE-030041	Operation failed. The gateway could not retrieve the collection using the device ID.	
SAE-030042	Operation failed. The gateway could not update the upload status of this collection in the database.	
SAE-030043	Collection upload failed.	
SAE-030044	Collection upload failed. The report size exceeds the maximum limit.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030045	Collection failed. The gateway encountered an error creating a record in the database.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030046	Collection failed. The gateway could not update the status of this record in the database.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030047	Collection failed. The gateway could not retrieve this record due to an internal database error.	Try again later. If the problem persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-030048	Collection failed. The gateway could not delete this record due to an internal database error.	Try again later. If the problem persists, contact technical support.
SAE-030049	Collection upload failed. The gateway could not upload the collection results file to our servers.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030050	Collection upload failed. The gateway cannot check the collection upload status.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030051	Collection upload failed. The upload failed because of a server issue.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030052	Collection upload failed. The collection results upload timed out.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030053	Collection upload failed. The collection results file is unavailable.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030054	Collection upload failed. The gateway could not finish uploading the collection results.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030055	Collection upload failed. The gateway could not check the collection upload status.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030056	Collection upload failed. The collection report file is not available in our servers.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030057	Collection failed. The gateway cannot reach the Connectivity Service.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030058	Operation failed. The gateway cannot retrieve the collection attribute details for tree view.	Try again later. If the problem persists, contact technical support.
SAE-030059	Operation failed. The gateway cannot retrieve the collection attribute details because the object ID is missing.	
SAE-030060	Operation failed. Unable to find data associated with this collection.	
SAE-030061	Operation failed. The gateway cannot retrieve the collection components for tree view.	
SAE-030062	Operation failed. The gateway cannot retrieve the structured logs for tree view.	
SAE-030063	Operation failed. The gateway cannot retrieve the structured logs because the object ID is missing.	
SAE-030064	Unable to start a new collection because either the collection is in progress or the collection was performed in last 24 hours.	Ensure that the collection is not in progress and try again.
SAE-030065	Able to start this alert-based collection.	Try again later. If the problem persists, contact technical support.
SAE-030066	Collection failed. The gateway could not update the plug-in task ID in the database.	Try again later. If the problem persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-030067	Collection failed. The gateway could not update the collection progress in the database.	
SAE-030068	Collection failed. The gateway could not update the error code for device collection.	
SAE-030069	Collection failed. The gateway could not complete an evidence collection.	
SAE-030070	Operation failed. An invalid evidence collection request.	
SAE-030071	The gateway could not retrieve the current status from the periodic collection table.	
SAE-030072	The gateway could not retrieve the start time for this periodic collection.	
SAE-030073	The gateway could not retrieve the device collection status from the collection device map table.	
SAE-030074	Operation failed. The gateway encountered an error updating the status of this collection in the database.	
SAE-030075	A scheduled periodic collection is already in progress.	Try again later. If the problem persists, contact technical support.
SAE-030076	The scheduled periodic collection has already run for this month.	Try again later. If the problem persists, contact technical support.
SAE-030077	The gateway failed to delete the data from this periodic collection.	Try again later. If the problem persists, contact technical support.
SAE-030078	The gateway failed to create a data entry from this periodic collection.	
SAE-030079	Operation failed. The gateway could not retrieve the asset list from the Inventory Service.	
SAE-030080	Collection failed. The gateway could not start this periodic collection.	
SAE-030081	Collection failed. The gateway received a null status from the plug-in service.	
SAE-030082	Collection failed. The gateway could not retrieve details on task progress for this collection.	
SAE-030083	Cannot perform this operation because of an invalid date range.	
SAE-030084	Operation failed. The format for start date or end date is invalid.	
SAE-030085	The gateway cannot perform this operation because of an invalid collection type filter.	
SAE-030086	Operation failed. The device type filter is invalid.	
SAE-030087	Operation failed. The collection purpose filter is invalid.	
SAE-030088	Operation failed. The collection status filter is invalid.	
SAE-030089	Operation failed. The "sort by" parameter is invalid.	

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-030090	Operation failed. The "order by" parameter is invalid.	
SAE-030091	Operation failed. The service tag value is invalid.	Enter a valid service tag, and then try again.
SAE-030092	Operation failed. The hostname or IP address is invalid.	Enter a valid hostname and IP address, and then try again.
SAE-030093	Operation failed. Invalid limit parameter.	Change the limit parameter, and then try again.
SAE-030094	Operation failed. Invalid offset parameter.	Change the offset parameter, and then try again.
SAE-030095	Operation failed. Invalid index parameter.	Change your index parameter, and then try again.
SAE-030096	Operation failed. The gateway could not interact with the Case Domain Service.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030097	Operation failed. The gateway could not transfer the collection file to MFT.	Try again later. If the problem persists, contact technical support for assistance.
SAE-030098	Operation failed. The gateway could not retrieve the job ID from the periodic collection table.	
SAE-030099	Operation failed. The gateway could not retrieve asset IDs from the periodic collection table.	
SAE-030199	The gateway is collecting telemetry from this device.	Try again once it is completed.
SAE-030101	The upload of collected telemetry data has not started.	Wait for a few minutes. If the problem persists, contact technical support for assistance.
SAE-030103	The report for collected telemetry has been updated.	Try again later. If the problem persists, contact technical support.
SAE-030104	Operation failed. The gateway could not reach a required server to upload the file.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030105	Operation failed. The gateway could not reach a required server to check the status of the uploaded file.	Check the gateway connectivity to Dell EMC backed. If the problem persists, contact technical support for assistance.
SAE-030106	An error occurred while parsing the certificate.	Try again later. If the problem persists, contact technical support for assistance.
SAE-030107	The device certificate is required and cannot be null or empty.	Try again later. If the problem persists, contact technical support.
SAE-030200	An upgrade is in progress.	Try again once it is completed.
SAE-030201	Upload failed. An upgrade is currently in progress.	Try again once it is completed. .
SAE-030300	A scheduled data analytics collection is already in progress.	Try again once it is completed.
SAE-030301	Operation failed. The column filter parameter is invalid.	Enter a valid column filter and try again.
SAE-030302	Unable to run this operation because no assets can run frequent collections.	Try again later. If the problem persists, contact technical support.
SAE-030303	Unable to start data analytics collection. There was an unexpected error occurred.	Try again later. If the problem persists, contact technical support for assistance.
SAE-030304	Unable to start data analytics collection. The gateway could not retrieve assets by property.	Try again later. If the problem persists, contact technical support for assistance.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-030400	The gateway could not start this download.	The file is not available.
SAE-030401	The gateway could not start this download.	The file type is not supported.
SAE-030402	The gateway could not start this download. A file detail parameter is required to download this file.	Enter one, and then retry this request.
SAE-030500	Collection failed. This device is not reachable.	Check if you can reach this device from the gateway. If you can access this device, retry the collection. To retry the collection, select the device, and then click Start Collection .
SAE-030501	Collection failed. This device has an invalid IP address.	Enter a valid IP address for this device in the gateway. To retry the collection, select the device, and then click Start Collection .
SAE-030502	Collection failed. This device is not reachable.	Check if you can reach this device from the gateway. If you can access this device, retry the collection. To retry the collection, select the device, and then click Start Collection .
SAE-030503	Collection failed. This device has an invalid IP address.	Enter a valid IP address for this device in the gateway. To retry the collection, select the device, and then click Start Collection .
SAE-030504	Collection failed. The gateway could not download a certificate file from this device.	Check your firewall and network settings and ensure that you can download certificate files, and then retry the collection. To retry the collection, select the device, and then click Start Collection .
SAE-030505	The gateway cannot gather telemetry from this device.	The SSL encryption level of the device is set to 256 bits or higher.
SAE-030507	The gateway cannot gather some telemetry from this device.	The view the list of sections that may have incomplete information, download the collection file and click the Section Status tab.
SAE-030508	The gateway cannot collect all telemetry data from this device because the collection process exceeded the time limit.	Retry the collection. To retry the collection, select the device, and then click Start Collection .
SAE-030509	The gateway has successfully collected all telemetry from this device.	Retry the collection. To retry the collection, select the device, and then click Start Collection . If the problem persists, contact technical support for assistance.
SAE-030510	Unknown error. The gateway could not package telemetry from this device.	Try again later. If the problem persists, contact technical support for assistance.
SAE-030511	Collection error. The gateway could not collect telemetry from this device because of an unknown error.	Retry the collection. To retry the collection, select the device, and then click Start Collection . If the problem persists, contact technical support for assistance.
SAE-030512	Connection error. The gateway could not connect to the device.	Check your login credentials for the device in the gateway and that their associated user has admin or elevated privileges on the device.
SAE-030513	Connection error. The gateway could not connect to the device.	Check your login credentials for the device in the gateway and that their associated user has admin or elevated privileges on the device and then retry the collection. To retry the collection, select the device, and then click Start Collection . If the problem persists, contact technical support for assistance.
SAE-030514	Collection failed. This device either has incorrect credentials, or restricted privileges.	Check the login and password for this device in the gateway and ensure that the user account has

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
		admin/root privileges for the device. To retry the collection, select the device, and then click Start Collection .
SAE-030515	Connection error. The gateway could not connect to the device.	Check your login credentials for the device in the gateway and that their associated user has admin or elevated privileges on the device and then retry the collection. To retry the collection, select the device, and then click Start Collection . If the problem persists, contact technical support for assistance.
SAE-030518	Connection error. The gateway could not connect to the device.	Check your login credentials for the device in the gateway and that their associated user has admin or elevated privileges on the device and then retry the collection. To retry the collection, select the device, and then click Start Collection . If the problem persists, contact technical support for assistance.
SAE-030520	Connection error. The gateway could not connect to the device.	Check your login credentials for the device in the gateway and that their associated user has admin or elevated privileges on the device and then retry the collection. To retry the collection, select the device, and then click Start Collection . If the problem persists, contact technical support for assistance.
SAE-030521	Connection error. The gateway could not connect to the device.	Check that the SSH service is running on the device and retry the collection. To retry the collection, select the device, and then click Start Collection . If the problem persists, contact technical support for assistance.
SAE-030522	Collection failed. Unable to reach the device.	Check the login and password for this device in the gateway and ensure that the user account has admin/root privileges for the device. To retry the collection, select the device, and then click Start Collection .
SAE-030523	Collection failed. The gateway could not validate the SSH host key validation.	Try again later. If the problem persists, contact technical support for assistance.
SAE-030524	Collection failed. The optional credentials of the device are not present.	Update your device credentials and retry the collection. To retry the collection, select the device, and then click Start Collection .
SAE-030525	Collection failed. The gateway could not retrieve telemetry from this device because of a bad request.	Try again later. If the problem persists, contact technical support for assistance.
SAE-030526	Collection failed. The gateway could not connect to this device because the required ports are not open.	
SAE-030527	Collection failed. Device identification failed.	
SAE-030528	Collection failed. The type that is chosen for this device is incorrect.	Update the device type and retry the collection. To retry the collection, select the device, and then click Start Collection .
SAE-030529	Collection failed. The type for this device is null or missing.	
SAE-030530	Collection failed. The type of device does not support collection of telemetry.	
SAE-030531	Collection failed. The gateway could not find the request URI.	Try again later. If the problem persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-030532	Collection failed. The gateway requires proxy authentication to reach this device.	Check your proxy details for this device, then rerun the collection by selecting this device and clicking "Start Collection."
SAE-030533	Collection failed. The gateway could not retrieve telemetry from this device because of a bad request.	Try again later. If the problem persists, contact technical support for assistance.
SAE-030534	Collection failed. The gateway could not retrieve telemetry from one or more devices.	For more information about the failure, download the collection file and click the Section Status tab.
Cases		
SAE-071000	Register your installation of SupportAssist to view current alerts.	Try again later. If the problem persists, contact technical support.
SAE-070000	Your request has an invalid name entry.	Check your values and try again. For more information about RESTful APIs exposed by OpenManage Enterprise SupportAssist, see Dell Developer Portal .
SAE-070001	Your request has an invalid offset entry.	
SAE-070002	Your request has an invalid limit.	
SAE-070003	Your request has an invalid index value.	
SAE-070004	Your request has an invalid sort query.	
SAE-070005	Your request has an invalid order query.	
SAE-070006	Your request has an invalid device type.	
SAE-070007	Your request has an invalid event source.	
SAE-070008	Your request has an invalid service contract.	
SAE-070009	Your request has an invalid Service Tag.	
SAE-070010	Your request has an invalid case number.	
SAE-070011	Your request has an invalid case status.	
SAE-070012	Your request has an invalid hostname/IP address.	
SAE-070013	Your request has an invalid attributes name.	
SAE-070014	Your request has an invalid case title.	
SAE-070015	Your request had some invalid inputs.	
SAE-070016	Your request included an invalid case operation.	
SAE-070017	Remove any invalid characters in the notes section.	For more information about RESTful APIs exposed by OpenManage Enterprise SupportAssist, see Dell Developer Portal .
SAE-070101	An unexpected error occurred.	Try again later. If the problem persists, contact Tech Support for assistance.
SAE-070102		
SAE-070103		
SAE-070104		
SAE-070105		
SAE-070106		
SAE-070107		
SAE-070108		
SAE-070109		
SAE-070110		

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-070111 SAE-070112 SAE-070113 SAE-070114 SAE-070115 SAE-070116 SAE-070153 SAE-070154 SAE-070155 SAE-070156 SAE-070157 SAE-070158		
SAE-070201	Enter a valid Operation Type to continue.	For more information about RESTful APIs exposed by OpenManage Enterprise SupportAssist, see Dell Developer Portal .
SAE-070202	Enter a valid case ID to continue.	For more information about RESTful APIs exposed by OpenManage Enterprise SupportAssist, see Dell Developer Portal .
SAE-070203	The character limit has exceeded the max limit of 7500.	Remove some characters to continue.
SAE-070204	An unknown error is occurred.	Try again after a few minutes. If problem persists, contact technical support.
SAE-070205	This action is not allowed for a case with this current status.	Refresh to see the current status of the case and try again.
SAE-070206	It is not supported because the source of this event is not SupportAssist.	For more information about RESTful APIs exposed by OpenManage Enterprise SupportAssist, see Dell Developer Portal .
SAE-070207	This action is not available on a closed case.	None.
SAE-070208	Issue with your connection.	Check your Internet connection and proxy settings, and then try again. If the problem persists, contact technical support.
SAE-070209	This action is not allowed on a dummy case.	None.
SAE-070214	An unexpected error occurred.	Try again later. If the problem persists, contact technical support.
SAE-070301 SAE-070302 SAE-070303 SAE-070304 SAE-070305 SAE-070306 SAE-070307 SAE-070308 SAE-070309	An unexpected error occurred.	Try again later. If the problem persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-070310 SAE-070311 SAE-070312 SAE-070313 SAE-070314 SAE-070315 SAE-070316		
SAE-070317	Request timed out. Either the server is not reachable or there is an issue with your connection.	Check your Internet connection and proxy settings, and then try again. If the problem persists, contact technical support.
SAE-070400 SAE-070401 SAE-070402 SAE-070403 SAE-070404 SAE-070405 SAE-070406 SAE-070407 SAE-070408	An unexpected error occurred.	Try again later. If the problem persists, contact technical support.
SAE-070500 SAE-070501 SAE-070502 SAE-070503 SAE-070504 SAE-070505 SAE-070506 SAE-070507 SAE-070508 SAE-070509 SAE-070510 SAE-070511 SAE-070512 SAE-070513 SAE-070514 SAE-070515	An unexpected error occurred.	Try again later. If the problem persists, contact technical support.
SAE-071001 SAE-071002	An unexpected error occurred.	Try again later. If the problem persists, contact technical support.
SAE-071004	Unable to complete the operation. Request timed out.	Try again. If the problem persists, contact technical support.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-071005	Unable to retrieve one or more cases.	Try again later. If the problem persists, contact technical support.
SAE-074001	Asset not found. Received an alert from a device that is not currently monitored by SupportAssist.	To monitor the device from which you receive the alert, add the device.
SAE-074002	Alert that is received from an inactive or staging device.	Move this device back to an active state to reenale monitoring for it.
SAE-074003	An error occurred while displaying this alert.	Try again later. If the problem persists, contact technical support.
SAE-074004	An error occurred while displaying this alert.	Try and update the configuration of SupportAssist to avoid this issue in the future.
SAE-074005	An error occurred while displaying this alert.	Try again later. If the problem persists, contact technical support.
SAE-074006		
SAE-074007	An error occurred while displaying this alert.	Disable maintenance mode to avoid this error.
SAE-074008	This alert was not available because monitoring is disabled on this device.	Enable monitoring on the device and try again.
SAE-074009	This alert was not available because it is not present in the policy file.	None.
SAE-074009	This alert cannot be viewed until your installation of SupportAssist is registered.	Register SupportAssist with Dell EMC backend and try again.
SAE-074010	An unknown error occurred.	Try again after a few minutes. If the problem persists, contact technical support.
SAE-074011	Encountered an error that is related to maintenance mode.	Disable the maintenance mode to avoid similar type of errors.
SAE-074012	An unknown error occurred.	Try again after a few minutes. If the problem persists, contact technical support.
SAE-074013		
SAE-074014		
SAE-074015		
SAE-074016		
SAE-074017		
SAE-074018		
SAE-074019		
SAE-074020		
SAE-074021		
SAE-074022	Case status in progress	None.
SAE-074023	Case status in success	None.
SAE-074024	A connection issue has occurred.	Check your Internet connection and proxy settings, and then try again. If the problem persists, contact technical support.
SAE-074025	Unable to create a case.	Contact technical support to manually create a case.
SAE-074026	Unable to create a case.	Contact technical support check the status of your service tag.
SAE-074027	Unable to create a case.	Contact technical support to manually create a case.

Table 4. Error code appendix (continued)

Error code	Error message	Possible resolution
SAE-074028	Unable to create a case.	Contact technical support to check the status of your service tag.
SAE-074029	An error related to maintenance mode has occurred.	Disable maintenance mode to avoid similar type of errors.
SAE-074600 SAE-074601	An unknown error occurred.	Try again after a few minutes. If the problem persists, contact technical support.

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—www.dell.com/virtualizationsolutions
 - 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.