

# Dell EMC SupportAssist Enterprise Version 1.0 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

<b>1 Overview.....</b>	<b>9</b>
Overview of supported device types.....	9
How SupportAssist Enterprise works.....	10
SupportAssist Enterprise capabilities available with Dell service contracts.....	10
Data collected by SupportAssist Enterprise.....	11
<b>2 Getting started with SupportAssist Enterprise .....</b>	<b>13</b>
Setting up SupportAssist Enterprise for the local system.....	13
Setting up SupportAssist Enterprise for remote devices.....	13
Evaluating SupportAssist Enterprise.....	14
Evaluating the monitoring capability.....	14
Evaluating the data collection capability.....	14
Downloading the SupportAssist Enterprise installation package.....	14
Minimum requirements for installing and using SupportAssist Enterprise.....	15
Hardware requirements.....	15
Software requirements.....	15
Network requirements.....	16
Installing SupportAssist Enterprise.....	18
Installing SupportAssist Enterprise (Windows).....	18
Installing SupportAssist Enterprise (Linux).....	19
Installing SupportAssist Enterprise in silent mode (Linux).....	20
Migrating to SupportAssist Enterprise.....	21
Migrating to SupportAssist Enterprise (Windows).....	21
Migrating to SupportAssist Enterprise (Linux).....	22
Using SupportAssist Enterprise without registration.....	22
Registering SupportAssist Enterprise.....	23
Setting up an SELinux enabled system to receive alerts.....	25
Opening the SupportAssist Enterprise user interface.....	26
Logging in to SupportAssist Enterprise.....	26
Logging out of SupportAssist Enterprise.....	26
<b>3 Adding devices.....</b>	<b>28</b>
Device types and applicable devices.....	28
Adding a single device.....	29
Adding a server or hypervisor.....	29
Adding an iDRAC.....	32
Adding a chassis.....	33
Adding a Dell Networking device.....	35
Adding a PowerVault MD Series storage array.....	36
Adding a Dell EqualLogic PS Series storage array.....	37
Adding a Dell Compellent SC Series storage solution.....	38
Adding a Dell Fluid File System (FluidFS) NAS device.....	39

Adding a device by duplication.....	40
Importing multiple devices.....	41
Exporting details of devices that were not imported.....	45
Revalidating a device.....	45
<b>4 Viewing cases and devices.....</b>	<b>47</b>
Viewing all support cases.....	47
Case management options.....	48
Requesting to suspend case activities for 24 hours.....	48
Requesting to resume support activities.....	49
Requesting to close a support case.....	49
Viewing the device inventory.....	50
Viewing the device overview pane.....	51
Refining the displayed data.....	52
Filtering the displayed data.....	52
Clearing the data filter.....	52
Sorting the displayed data.....	52
Checking support cases for a specific device.....	52
<b>5 Device grouping.....</b>	<b>55</b>
Predefined device groups.....	55
Viewing device groups.....	56
Creating a device group.....	56
Managing devices in a device group.....	56
Managing the credentials of a device group.....	57
Viewing and updating the contact information of a device group.....	58
Editing device group details.....	59
Deleting a device group.....	59
<b>6 Understanding maintenance mode.....</b>	<b>61</b>
Global-level maintenance mode.....	61
Device-level maintenance mode.....	61
Enabling or disabling global-level maintenance mode.....	62
Enabling or disabling device-level maintenance mode.....	62
<b>7 Maintaining SupportAssist Enterprise capability.....</b>	<b>64</b>
Enabling or disabling monitoring of a device.....	64
Editing device credentials.....	65
Installing or upgrading OMSA by using SupportAssist Enterprise.....	66
Configuring SNMP settings by using SupportAssist Enterprise.....	67
Viewing and updating the contact information.....	69
Configuring proxy server settings.....	69
Connectivity test.....	70
Viewing the connectivity status.....	70
Performing the connectivity test.....	71
Testing the case creation capability.....	71

Clearing the System Event Log (SEL).....	72
Automatic update.....	73
Enabling or disabling automatic updates.....	73
Deleting a device.....	73
Opting in or opting out from ProSupport Plus server recommendation report emails.....	74
<b>8 Configuring email notifications.....</b>	<b>76</b>
Configuring email notification settings.....	76
Configuring SMTP server settings.....	76
Types of email notifications.....	77
<b>9 Configuring data collection settings.....</b>	<b>79</b>
Prerequisites for collecting system information.....	79
Enabling or disabling the automatic collection of system information on case creation.....	80
Enabling or disabling the periodic collection of system information from all devices.....	80
Customizing the schedule for periodic collection of system information.....	81
Default schedule for collection of system information.....	81
Disabling the periodic collection of system information from specific devices.....	82
Enabling or disabling the collection of identity information.....	82
Enabling or disabling the collection of software information and the system log.....	83
<b>10 Viewing collections.....</b>	<b>84</b>
Viewing a collection from the Devices page.....	84
Viewing a collection from the Collections page.....	85
Configuration Viewer.....	86
Data views.....	87
Log types.....	87
Items reported in periodic collections from servers.....	88
Downloading and viewing a multiple device collection.....	90
Multiple device configuration viewer.....	91
<b>11 Using SupportAssist Enterprise to collect and send system information.....</b>	<b>93</b>
Setting up SupportAssist Enterprise for collecting and sending system information.....	93
Starting the collection of system information from a single device.....	93
Starting the collection of system information from multiple devices.....	95
Uploading a collection.....	96
Uploading a collection from a disconnected site.....	97
<b>12 SupportAssist Enterprise user groups.....</b>	<b>98</b>
SupportAssist Enterprise functions and user privileges.....	98
Granting elevated or administrative privileges to users.....	99
Adding users to the SupportAssist Enterprise user groups (Windows).....	100
Adding users to the SupportAssist Enterprise user groups (Linux).....	100
<b>13 Manually configuring SNMP settings.....</b>	<b>101</b>
Manually configuring the alert destination of a server.....	101

Manually configuring the alert destination of a server by using the script file (Windows).....	101
Manually configuring the alert destination of a server (Windows).....	102
Manually configuring the alert destination of a server by using the script file (Linux).....	102
Manually configuring the alert destination of a server (Linux).....	103
Manually configuring the alert destination of iDRAC by using the web interface.....	104
Manually configuring the alert destination of a chassis by using the web interface.....	104
Manually configuring the alert destination of a networking device.....	105

## **14 Other useful information..... 106**

Monitoring servers for hardware issues.....	106
Benefits of agent-based monitoring.....	106
Support for automatically installing or upgrading OMSA.....	106
Support for automatically configuring SNMP settings.....	107
Device correlation.....	108
Detection of hardware issues in attached storage devices.....	108
Support for Dell OEM servers.....	108
Installing Net-SNMP (Linux only).....	108
Configuring sudo access for SupportAssist Enterprise (Linux).....	109
Ensuring successful communication between the SupportAssist Enterprise application and the SupportAssist server..	109
Accessing the SupportAssist Enterprise application logs.....	110
Event storm handling.....	110
Accessing the context-sensitive help.....	110
Viewing SupportAssist Enterprise product information.....	110
Uninstalling SupportAssist Enterprise.....	111
Uninstalling SupportAssist Enterprise (Windows).....	111
Uninstalling SupportAssist Enterprise (Linux).....	111
Uninstalling SupportAssist Enterprise in silent mode (Linux).....	112
Identifying the generation of a Dell PowerEdge server.....	112

## **15 Troubleshooting..... 113**

Installing SupportAssist Enterprise .....	113
SupportAssist Enterprise registration.....	113
Opening the SupportAssist Enterprise user interface.....	113
Logging in to SupportAssist Enterprise .....	114
Unable to add device.....	114
Servers.....	115
Storage.....	115
Networking.....	115
Chassis.....	116
Importing multiple devices.....	116
OMSA not installed.....	116
SNMP not configured.....	116
New version of OMSA available.....	116
Unable to configure SNMP.....	117
Unable to verify SNMP configuration.....	117
Unable to install OMSA.....	117

Unable to verify OMSA version.....	118
OMSA not supported.....	118
Unable to reach device.....	118
Unable to gather system information.....	118
Servers.....	119
Storage.....	119
Networking.....	119
Chassis.....	120
Insufficient storage space to gather system information.....	120
Unable to export collection.....	120
Unable to send system information.....	120
Authentication failed.....	120
Server.....	120
Storage.....	121
Networking.....	121
Chassis.....	121
Clearing System Event Log failed.....	121
Clearing the System Event Log by using iDRAC.....	121
Clearing the System Event Log by using OMSA.....	122
Maintenance mode.....	122
Auto update.....	122
Unable to edit device credentials.....	122
Servers.....	123
Storage.....	123
Networking.....	123
Chassis.....	123
Automatic case creation.....	124
Scheduled tasks.....	124
SupportAssist service.....	124
Verifying the SupportAssist service status (Windows).....	125
Verifying the SupportAssist service status (Linux).....	125
Other services.....	125
WMI service.....	125
SSH service.....	125
Security.....	126

**16 SupportAssist Enterprise user interface..... 127**

SupportAssist Enterprise Registration Wizard.....	128
Welcome.....	128
Proxy Settings.....	129
Registration.....	129
Summary.....	129
Login page.....	129
Cases page.....	130
Devices page.....	132
Add Single Device or Import Multiple Devices window.....	136

Device Import pane.....	139
Device overview pane.....	140
Multiple Device Collection window.....	141
Multiple Device Collection pane.....	141
Device Groups page.....	141
Manage Devices.....	142
Manage Credentials.....	142
Manage Contacts.....	143
Edit/Delete Device Group.....	143
Collections page.....	144
Collection overview pane.....	144
Settings.....	145
Collection Schedules.....	145
Proxy Settings.....	146
Preferences.....	147
Contact Information.....	148
SMTP Settings.....	149
Network Connectivity Test.....	150
Test SupportAssist Enterprise.....	151

**17 Error code appendix..... 152**


**18 Related documents and resources..... 165**

Video tutorials.....	165
SupportAssist Enterprise community.....	166
Dell Remote Consulting Service.....	166
Accessing documents from Dell support site.....	166
Contacting Dell.....	166

# Overview


Dell EMC SupportAssist Enterprise is an application that automates technical support for your Dell server, storage, and networking devices. SupportAssist Enterprise monitors your Dell devices and proactively detects hardware issues that may occur. When a hardware issue is detected, SupportAssist Enterprise automatically opens a support case with Dell Technical Support and sends you an email notification. Data required for troubleshooting the issue is automatically collected by SupportAssist Enterprise and sent securely to Dell Technical Support. The collected data helps Dell Technical Support to provide you an enhanced, personalized, and efficient support experience. SupportAssist Enterprise capability also includes a proactive response from Dell Technical Support to help you resolve the issue.

 **NOTE: SupportAssist Enterprise can monitor hardware issues that occur in Dell server and Dell networking devices. For Dell storage devices, SupportAssist Enterprise can only collect and send system information.**

 **NOTE: SupportAssist Enterprise capabilities available for a device vary depending on the Dell service contract of the device. The primary capabilities of SupportAssist Enterprise are available only for devices with an active ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract. For a summary of the SupportAssist Enterprise capabilities and Dell service contracts, see [SupportAssist Enterprise capabilities available with Dell service contracts](#).**

This document provides information about installing and setting up SupportAssist Enterprise to:

- Monitor devices for hardware issues
- Automatically create a support case when an issue is detected
- Collect and send system information from your devices periodically and as needed


 **NOTE: In this document, the term *local system* refers to the server where SupportAssist Enterprise is installed; *remote device* refers to any other device that you want SupportAssist Enterprise to monitor for hardware issues and collect system information, or to only collect system information.**

## Related links

[Data collected by SupportAssist Enterprise](#)

## Overview of supported device types

SupportAssist Enterprise is compatible with Dell server, storage, networking, and chassis devices. The following is an overview of the device types that are compatible with SupportAssist Enterprise.

 **NOTE: SupportAssist Enterprise may not be compatible with all device models of a supported device type. For the complete list of supported device types and device models, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).**

- Servers
  - Dell's 9th to 13th generation of PowerEdge servers
  - Dell PowerEdge C Series servers
  - Dell XC Series of Web-scale Hyper-converged Appliances
  - Dell Datacenter Scalable Solutions
  - Dell PowerVault NX devices
  - Dell PowerVault DL devices
  - Dell OEM-ready servers
- Storage

- Dell EqualLogic storage arrays
- Dell PowerVault MD Series storage arrays
- Dell Compellent storage arrays
- Dell network attached storage (NAS) devices
- Networking
  - Dell PowerConnect switches
  - Dell Force10 switches
  - Dell Networking switches
  - Dell Networking X-Series switches
  - Dell Networking Wireless Controllers Mobility Series
- Chassis
  - Dell PowerEdge FX2/FX2s
  - Dell PowerEdge VRTX
  - Dell PowerEdge M1000e


#### Related links


[Identifying the generation of a Dell PowerEdge server](#)

## How SupportAssist Enterprise works

When SupportAssist Enterprise is setup and the devices to be monitored are configured correctly, SupportAssist Enterprise receives an alert whenever a hardware event occurs on any monitored device. The received alerts are filtered by using various policies to determine if the alerts qualify for creating a new support case or for updating an existing support case. All qualifying alerts are sent securely to the SupportAssist server hosted by Dell, for creating a new support case or for updating an existing support case. After the support case is created or updated, SupportAssist Enterprise collects system information from the device that generated the alert and sends the information securely to Dell. The system information is used by Dell Technical Support to troubleshoot the issue and provide an appropriate solution.

You can also use SupportAssist Enterprise to only collect and send system information from your devices to Dell. By default, SupportAssist Enterprise automatically collects and sends system information from your devices at periodic intervals and on case creation. If required, you can also manually start the collection and upload of system information to Dell.

 **NOTE: To experience the automatic case creation and data collection capabilities of SupportAssist Enterprise, you must complete the registration. Without registration, you can only use SupportAssist Enterprise to manually start the collection and upload of data from your devices to Dell. For more information about the restrictions that apply when using SupportAssist Enterprise without registration, see [Using SupportAssist Enterprise without registration](#).**

 **NOTE: SupportAssist Enterprise 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 entitlement, and if the alert type and number of alerts received from the device match with the predefined criteria for support case creation. For more information about how SupportAssist Enterprise processes alerts and automatically creates support cases, see the *Dell SupportAssist Alert Policy* technical document at [Dell.com/SupportAssistGroup](http://Dell.com/SupportAssistGroup).**

 **NOTE: SupportAssist Enterprise sends you automatic email notifications about support cases, device status, network connectivity status, and so on. For information about the various email notifications, see [Types of email notifications](#).**


## SupportAssist Enterprise capabilities available with Dell service contracts

The following table provides a comparison of the SupportAssist Enterprise capabilities available with the ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contracts.

 **NOTE: Completing the registration is a prerequisite to receive the full benefits of SupportAssist Enterprise for your Dell devices. For information on registering SupportAssist Enterprise, see [Registering SupportAssist Enterprise](#).**

**Table 1. SupportAssist Enterprise capabilities and Dell service contracts**

SupportAssist Enterprise capability	Description	Basic Hardware	ProSupport	ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center
Proactive detection of hardware failures	SupportAssist Enterprise receives alerts for hardware events that occur in monitored devices and proactively determines if the alerts indicate a hardware failure.	✓	✓	✓
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.	✗	✗	✓
Automated data collection	Data required for troubleshooting a hardware failure is automatically collected from the monitored device and sent securely to Dell.	✓	✓	✓
Automated support case creation	When a hardware failure is detected either proactively or predictively, a Service Request is automatically created with Dell Technical Support.	✗	✓	✓
Automated email notification	An email notification about the support case or issue is automatically sent to your company's primary and secondary SupportAssist Enterprise contacts.	✗	✓	✓
Proactive response from Dell Technical Support	A Dell Technical Support agent contacts you proactively about the support case and helps you resolve the issue.	✗	✓	✓
Proactive parts dispatch	Based on examination of the collected system information, if the Dell Technical Support agent determines that a part needs to be replaced to resolve the issue, a replacement part is dispatched to you with your consent.	✗	✓	✓
ProSupport Plus reporting	Data collected periodically by SupportAssist Enterprise enables Dell to provide you an insight into your company's as-maintained environment configuration with proactive firmware recommendations and other reports.	✗	✗	✓

 **NOTE: SupportAssist Enterprise also detects hardware issues in devices with a Dell Basic Hardware service contract. However, a support case is not created automatically for devices with a Basic Hardware service contract.**

\* Predictive detection of hardware failures is applicable only for the hard drives, backplanes, and expanders of Dell's 12th and 13th generation of PowerEdge servers that have PowerEdge RAID Controller (PERC) Series 5 to 9. Predictive detection of hardware failures is available only when SupportAssist Enterprise is configured to periodically collect and send system information from your devices to Dell.

## Data collected by SupportAssist Enterprise


SupportAssist Enterprise continually monitors the configuration data and usage information of managed Dell hardware and software. While Dell 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 data inadvertently collected or viewed will be treated in accordance with the Dell Privacy Policy available for review at [Dell.com/privacy](http://Dell.com/privacy).

The information encrypted in the data log sent to Dell 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

You can also access and view the data collected by SupportAssist Enterprise. For information on viewing the collected data, see [Viewing the collected system information](#).

By default, SupportAssist Enterprise collects data from all devices, irrespective of the service contract of the devices, and sends the data securely to Dell. The collection of data is staggered, and the data is collected from 10 devices at a time. For information about the default frequency of data collection, see [Default schedule for collection of system information](#).

 **NOTE: If the security policy of your company restricts sending some of the collected data outside of your company network, you can configure SupportAssist Enterprise to exclude the collection of certain data from your devices. For information on excluding the collection of certain data, see [Enabling or disabling the collection of identity information](#) and [Enabling or disabling the collection of software information and the system log](#).**

 **NOTE: For more information about the data collected by SupportAssist Enterprise and how the collected data is used by Dell, see the *Dell SupportAssist: Security Considerations* technical document at [Dell.com/SupportAssistGroup](http://Dell.com/SupportAssistGroup).**

# Getting started with SupportAssist Enterprise

Dell EMC SupportAssist Enterprise automates technical support from Dell for your Dell devices. Depending on your requirement, you can install and set up SupportAssist Enterprise to automate technical support for one or more of your devices.

## Setting up SupportAssist Enterprise for the local system

Installing SupportAssist Enterprise enables you to start the collection and upload of system information from the local system (server where SupportAssist Enterprise is installed). To allow SupportAssist Enterprise to monitor the local system for hardware issues, you must complete the registration and perform additional tasks.

To set up SupportAssist Enterprise for the local system:

1. Download the SupportAssist Enterprise installation package. See [Downloading the SupportAssist Enterprise installation package](#).
2. Review the requirements for installing SupportAssist Enterprise. See [Minimum requirements for installing and using SupportAssist Enterprise](#).
3. Perform one of the following:
  - Install SupportAssist Enterprise. See [Installing SupportAssist Enterprise](#).
  - If you are already using Dell SupportAssist for Servers, migrate to SupportAssist Enterprise. See [Migrating to SupportAssist Enterprise](#).
4. (Optional) Complete the registration of SupportAssist Enterprise. See [Registering SupportAssist Enterprise](#).
 

**⚠ CAUTION: Completing the registration is a prerequisite to experience the full benefits of SupportAssist Enterprise. Without registration, you can only use SupportAssist Enterprise to manually start the collection and upload of system information from your devices to Dell. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.**
5. Perform the following if you want SupportAssist Enterprise to monitor the local system for hardware issues:
  - a. Install or upgrade Dell OpenManage Server Administrator (OMSA) on the local system. See [Installing or upgrading OMSA by using SupportAssist Enterprise](#).
  - b. Configure the SNMP settings of the local system. See [Configuring SNMP settings by using SupportAssist Enterprise](#).
  - c. Enable SupportAssist Enterprise to monitor hardware issues that may occur on the local system. See [Enabling or disabling monitoring of a device](#).
6. (Optional) Update the contact information to include a secondary SupportAssist Enterprise contact and a parts dispatch address. See [Viewing and updating the contact information](#).

## Setting up SupportAssist Enterprise for remote devices

Adding remote device in SupportAssist Enterprise prepares SupportAssist Enterprise to monitor hardware issues and collect system information from those devices.

To set up SupportAssist Enterprise for remote devices:

1. Ensure that you have completed the steps listed in [Basic setup](#).
2. (Optional) If you want to manage a set of devices as a group, create one or more device groups based on your preference. See [Device grouping](#).
3. Add devices in SupportAssist Enterprise. See [Adding devices](#).
4. (Optional) If your company utilizes an SMTP server (email server), configure the SMTP server settings in SupportAssist Enterprise. See [Configuring the SMTP server settings](#).

# Evaluating SupportAssist Enterprise

SupportAssist Enterprise has several configuration settings that you can enable or disable to evaluate the monitoring and data collection capabilities.

## Evaluating the monitoring capability

You can disable SupportAssist Enterprise from monitoring some specific devices or all devices.

When you disable monitoring of a specific device, SupportAssist Enterprise does not process alerts that are received from that device. Therefore, even if a hardware issue may occur on the device, SupportAssist Enterprise does not open a support case automatically. For instructions to disable monitoring of a specific device, see [Enabling or disabling monitoring of a device](#).

You can also temporarily disable monitoring of a specific device by placing the device in maintenance mode. Placing a device in maintenance mode ensures that SupportAssist Enterprise does not process alerts received from the device during a planned maintenance activity. For instructions to place a device in maintenance mode, see [Enabling or disabling device-level maintenance mode](#).

If necessary, you can disable SupportAssist Enterprise from monitoring all your devices by placing all your devices in maintenance mode. For instructions to place all your devices in maintenance mode, see [Enabling or disabling global-level maintenance mode](#).


## Evaluating the data collection capability

By default, SupportAssist Enterprise automatically collects system information from all devices at periodic intervals, and also when a support case is created. The collected system information is then sent securely to Dell. For information on the data collected by SupportAssist Enterprise from devices, see [Data collected by SupportAssist Enterprise](#).

You can also view the data that is collected by SupportAssist Enterprise. For information on viewing the collected data, see [Viewing the collected system information](#).

If the security policy of your company restricts sending some of the collected data outside of your company network, you can use the following configuration options available in SupportAssist Enterprise:

- You can disable the collection of identity information from all devices. See [Enabling or disabling the collection of identity information](#).
- You can disable the collection of software information and the system log from all devices. See [Enabling or disabling the collection of software information and the system log](#).
- You can disable the periodic collection of system information from all devices. See [Enabling or disabling the periodic collection of system information from all devices](#).
- You can disable the periodic collection of system information from some specific devices. See [Disabling the periodic collection of system information from specific devices](#).
- You can disable the automatic collection of system information when a support case is created. See [Enabling or disabling the automatic collection of system information](#).

 **NOTE: In most cases, part or all of the data collected by SupportAssist Enterprise is required by Dell Technical Support to properly diagnose issues and provide an appropriate resolution. To receive the full benefits of SupportAssist Enterprise, you must enable all the data collection options.**

# Downloading the SupportAssist Enterprise installation package

## Prerequisites

The system must have internet connectivity.

## About this task

Installation of SupportAssist Enterprise is supported on a Dell PowerEdge server running either a Windows or Linux operating system. You can download the appropriate installation package depending on the operating system running on the server where you want to install SupportAssist Enterprise.

## Steps

1. Visit [Dell.com/SupportAssist](https://Dell.com/SupportAssist).

The Dell SupportAssist portal is displayed.

2. In the **Available Versions** section, click the **Learn More** link that is displayed under **SupportAssist for servers, storage and networking**.

The **SupportAssist for servers, storage and networking** page is displayed.

3. In the **Downloads** section, under **SupportAssist Enterprise**, do one of the following based on the installation package that you want to download:

- For the Windows installation package, click the **Windows Management Server** link.
- For the Linux installation package, click the **Linux Management Server** link.

The **Drivers Details** page is displayed in a new web browser window.

4. In the **Available formats** section, click the **Download File** link that is displayed under **File Format: Application**.

Download of the SupportAssist Enterprise installation package is initiated.

## Minimum requirements for installing and using SupportAssist Enterprise

The following sections describe the minimum hardware, software, and networking requirements for installing and using SupportAssist Enterprise.

### Hardware requirements

The hardware requirements for installing and using SupportAssist Enterprise vary depending on:


- The number of devices you want to monitor
- The SupportAssist Enterprise functionality you want to use — data collection only or both monitoring and data collection

You can install SupportAssist Enterprise on any Dell PowerEdge server (9th to 13th generation).

The following table provides a summary of the minimum hardware requirements on the server where you want to install SupportAssist Enterprise.

**Table 2. Hardware requirements**

Hardware	For data collection only from a single device	For monitoring and data collection from up to 20 devices	For monitoring and data collection from up to 100 devices	For monitoring and data collection from up to 300 devices
Processor	1 core	2 cores	4 cores	4 cores
Installed memory (RAM)	4 GB	4 GB	8 GB	8 GB
Hard drive (free space)	1 GB	4 GB	12 GB	32 GB

 **NOTE: For monitoring more than 100 devices in your environment, Dell recommends that you install SupportAssist Enterprise on server that meets the specified hardware requirements. Periodic collections (required for ProSupport Plus reporting) from more than 100 devices may result in a high processor or memory utilization on the monitoring server. This high resource utilization may affect other applications that are running on the monitoring server, if the resources are shared with other applications.**


### Software requirements

You can install SupportAssist Enterprise on a Dell PowerEdge server running a Windows or Linux operating system. After installing SupportAssist Enterprise, you can view the SupportAssist Enterprise user interface by using a web browser. The following section provides information about the operating system requirements for installing and using SupportAssist Enterprise.

## Operating system requirements

The following sections provide the list of Windows and Linux operating systems that support the installation of SupportAssist Enterprise.

### Windows operating systems

 **NOTE: SupportAssist Enterprise can be installed only on 64-bit operating systems.**

- Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise, and Datacenter
- Windows Server 2008 SP2 Standard, Enterprise, and Datacenter
- Windows Server 2012 R2 Standard and Datacenter
- Windows Server 2012 Standard, Essentials, and Datacenter
- Windows Server 2016 Standard, Essentials, and Datacenter
- Small Business Server 2008 Essentials and Standard
- Small Business Server 2011 Essentials and Standard

 **NOTE: In Windows Server 2016, ensure that you select Internet Explorer as the default browser for opening SupportAssist Enterprise.**

 **NOTE: SupportAssist Enterprise can also be installed on a Microsoft Windows domain controller.**

 **NOTE: Installation of SupportAssist Enterprise is not supported on Server Core and Windows Server 2016 Nano Server.**

### Linux operating systems

- Red Hat Enterprise Linux 7.x
- Red Hat Enterprise Linux 6.x
- Red Hat Enterprise Linux 5.x
- CentOS 7.x
- CentOS 6.x
- Novell SUSE Linux Enterprise Server 12 SP1
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 11 SP4
- SUSE Linux Enterprise Server 10 SP4
- Oracle Linux 7.x
- Oracle Linux 6.x

 **NOTE: Installation of SupportAssist Enterprise is not supported on Red Hat Enterprise Linux 6.6.**

## Web browser requirements

To view the SupportAssist Enterprise user interface, one of the following web browsers is required:

- Internet Explorer 10 or later
- Mozilla Firefox 31 or later

 **NOTE: SupportAssist Enterprise is not supported on Microsoft Edge web browser.**

 **NOTE: On Linux operating systems, SupportAssist Enterprise can also be viewed using the native web browser version.**

## Network requirements

The following are the network requirements on the local system (the server where SupportAssist Enterprise is installed) and remote devices.

- Internet connection — standard 1 GbE network.
- The local system must be able to communicate with the SupportAssist server hosted by Dell over HTTPS protocol.

- The local system must be able to connect to the following destinations:
  - <https://apidp.dell.com> and <https://api.dell.com> — end point for the SupportAssist server.
  - <https://is.us.dell.com/FUS/api/2.0/uploadfile> — the file upload server where the collected system information is uploaded.
  - <https://is.us.dell.com/FUSCHUNK/api/1.0/file/uploadChunk> — the file upload server where the collection files greater than 10 MB in size are uploaded.
  - <https://downloads.dell.com/> — for downloading Dell OpenManage Server Administrator (OMSA) and receiving new SupportAssist Enterprise release information, policy files, and product support files.

The following table lists the ports that must be open on the local system.

**Table 3. Network port requirements on the local system**

Port	Direction	Usage
22	Out	For adding the local system running a Linux operating system and for collecting system information
25	Out	For SMTP communication (required for SupportAssist Enterprise to send certain email notifications through the SMTP server utilized by your company)
80	Out	For HTTP communication
135	Out	For Windows Management Instrumentation (WMI) communication
162	In	For receiving alerts (SNMP traps) from remote devices
443	Out	For Secure Socket Layer (SSL) communication, WS-Man communication, and verifying SupportAssist Enterprise update information
1311	Out	For Dell OpenManage Server Administrator (OMSA) communication
5700	In	For opening SupportAssist Enterprise securely (HTTPS) from a remote system
5701, 5702, 5703, and 5704	In	For collecting system information from devices
9099	In	For opening SupportAssist Enterprise (HTTP) from the local system
61616	In	For processing SupportAssist Enterprise tasks

The following table lists the ports that must be open on remote devices that you want to monitor or collect system information by using SupportAssist Enterprise.


**Table 4. Network port requirements on remote devices**

Device Type	Port	Usage
Server / Hypervisor	22	For adding a remote device running a Linux operating system and to collect system information
	135	For adding a remote device running Windows (WMI) and to collect system information
	161	For forwarding alerts (SNMP traps) to the local system
	443	For Secure Socket Layer (SSL), WS-Man, and VMware web services communication
	1311	For OMSA communication
iDRAC	443	For Secure Socket Layer (SSL) and WS-Man communication
	161	For forwarding alerts (SNMP traps) to the local system
EqualLogic	22	For adding the device and to collect system information
	161	For forwarding alerts (SNMP traps) to the local system
PowerVault	2463	For adding the device and to collect system information

Device Type	Port	Usage
Compellent	443	For adding the device and to collect system information
Fluid File System (FluidFS)	22 and 44421	For adding the device and to collect system information
Networking	22	For adding the device and to collect system information
	161	For forwarding alerts (SNMP traps) to the local system
Chassis	22	For adding the device and to collect system information
	161	For forwarding alerts (SNMP traps) to the local system

## Installing SupportAssist Enterprise

You can install SupportAssist Enterprise on a server running a supported Windows or Linux operating system. The following sections provide the instructions to install SupportAssist Enterprise on Windows and Linux operating systems.

 **NOTE: For SupportAssist Enterprise installation on Linux operating systems only: When SupportAssist Enterprise is installed on a server running a Linux operating system, SupportAssist Enterprise can monitor the local system, remote servers running a supported Linux operating system, and other device types. Monitoring remote servers running any other operating system is only possible if you add the iDRAC of the server in SupportAssist Enterprise. For information on adding the iDRAC of a server, see [Adding an iDRAC](#).**


### Installing SupportAssist Enterprise (Windows)

#### Prerequisites

- Download the SupportAssist Enterprise installation package for Windows operating systems. See [Downloading the SupportAssist Enterprise installation package](#).
- Log in to the system with administrator privileges.
- The system must meet the requirements for installing SupportAssist Enterprise. See [Minimum requirements for installing and using SupportAssist Enterprise](#).

#### Steps


1. Right-click the SupportAssist Enterprise installer package and then click **Run as administrator**.

 **NOTE: Microsoft User Access Control (UAC) requires that the installation is performed with elevated privileges that are obtained only through the Run as administrator option. If you are logged in to the system as an administrator, double-click the installer package to install SupportAssist Enterprise. However, ensure that you acknowledge the Open File - Security Warning dialog box to proceed.**

The **Preparing to Install** page is displayed briefly, and then the **Welcome to SupportAssist Enterprise Installer** page is displayed.

2. Click **Next**.

The **License Agreement** page is displayed.

 **NOTE: Installing and using SupportAssist Enterprise requires that you allow Dell to save certain Personally Identifiable Information (PII) such as your contact information, device credentials, and so on. SupportAssist Enterprise installation cannot proceed unless you agree to allow Dell to save your PII.**

3. Read about the information that SupportAssist Enterprise collects from monitored devices, and select **I Agree**.
4. Read the **Dell End User License Agreement**, select **I Agree**, and then click **Install**.

The **Installing SupportAssist Enterprise** page is displayed briefly, and then the **Installation Completed** page is displayed.

 **NOTE: In Windows Server 2016, the User Account Control dialog box may be displayed more than once while the installation is in progress.**

5. Click **Finish** to exit the SupportAssist Enterprise installer.

The **SupportAssist Enterprise** login page opens in a web browser window.

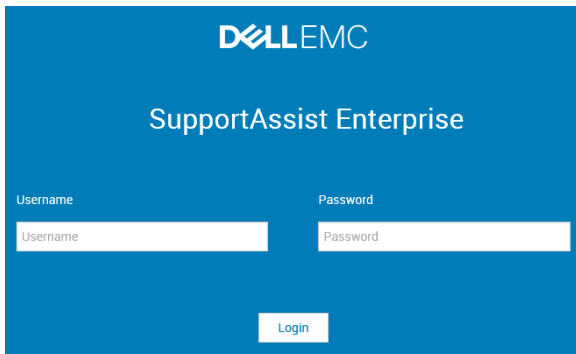




Figure 1. Login page


 **NOTE:** If the initialization of the Dell SupportAssist Service takes longer than expected, an error message is displayed. If this issue occurs, close the web browser and try accessing SupportAssist Enterprise later. For instructions to access SupportAssist Enterprise, see [Opening the SupportAssist Enterprise user interface](#).

 **NOTE:** If the system is a member of a domain, you must enter the login user name in the [Domain\Username] format. For example, MyDomain\MyUsername. You can also use a period [ . ] to indicate the local domain. For example, .\Administrator.

6. Enter the Microsoft Windows operating system user name and password, and then click **Login**.  
The **SupportAssist Enterprise Registration Wizard** is displayed.

#### Next steps

(Optional) Follow the instructions in the **SupportAssist Enterprise Registration Wizard** to complete the registration of SupportAssist Enterprise.

 **CAUTION:** Completing the registration is a prerequisite to experience the full benefits of SupportAssist Enterprise. Without registration, you can only use SupportAssist Enterprise to manually start the collection and upload of system information from your devices to Dell. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.

## Installing SupportAssist Enterprise (Linux)

### Prerequisites

- Download the SupportAssist Enterprise installation package for Linux operating systems. See [Downloading the SupportAssist Enterprise installation package](#).
- Log in to the system with root privileges.
- Net-SNMP must be installed on the system. For information on installing Net-SNMP, see [Installing Net-SNMP \(Linux only\)](#).
-  **NOTE:** If you choose to install Net-SNMP after installing SupportAssist Enterprise, ensure that you run the script file, `snmptrapdServiceConfiguration.sh`, after installing Net-SNMP. The script file will be available at `/opt/dell/supportassist/scripts` after the installation of SupportAssist Enterprise is completed.
- The system must meet the requirements for installing SupportAssist Enterprise. See [Minimum requirements for installing and using SupportAssist Enterprise](#).

### Steps

1. Open the terminal window on the system running the Linux operating system.
2. Browse to the folder where the SupportAssist Enterprise installation package is available.
3. Perform one of the following:
  - Type `chmod 744 supportassist_1.x.x.bin` and press Enter.
  - Type `chmod +x supportassist_1.x.x.bin` and press Enter.
4. Type `./supportassist_1.x.x.bin` and press Enter.  
The **Welcome to the SupportAssist Enterprise Installer** message is displayed.
5. To continue, type `c`.

The **SupportAssist Enterprise License Agreement** is displayed.

6. Read the license agreement and type `y` to start the installation.

After the installation is completed, the **SupportAssist Enterprise** login page opens in a web browser window.

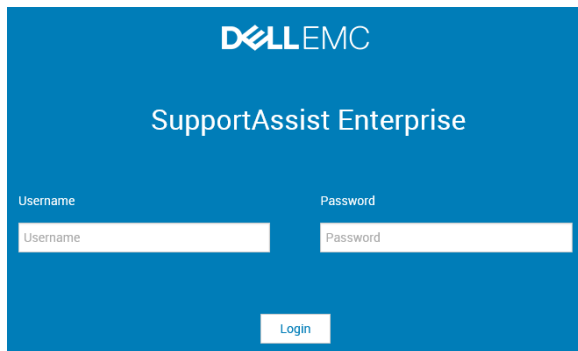





Figure 2. Login page


-  **NOTE:** If the initialization of the Dell SupportAssist Service takes longer than expected, an error message is displayed. If this issue occurs, close the web browser and try accessing SupportAssist Enterprise later. For instructions to access SupportAssist Enterprise, see [Opening the SupportAssist Enterprise user interface](#).
-  **NOTE:** If you are using a Linux terminal emulator such as PuTTY to remotely install SupportAssist Enterprise, the SupportAssist Enterprise login page is not displayed. In such a scenario, you must access the SupportAssist Enterprise login page by using one of the following methods:
  - Log in to a remote system and access the following web address by using a web browser:  
`https://<IP address or host name of the server where SupportAssist Enterprise is installed>:5700/SupportAssist`
  -  **NOTE:** You can access SupportAssist Enterprise from a remote system only if port 5700 is open on the network.
  - Log in to the local system and access the following web address by using a web browser: `http://localhost:9099/SupportAssist`

7. Type the user name and password of a user with root privileges on the system where SupportAssist Enterprise is installed, and then click **Login**.

The **SupportAssist Enterprise Registration Wizard** is displayed.

### Next steps

(Optional) Follow the instructions in the **SupportAssist Enterprise Registration Wizard** to complete the registration of SupportAssist Enterprise.

-  **CAUTION:** Completing the registration is a prerequisite to experience the full benefits of SupportAssist Enterprise. Without registration, you can only use SupportAssist Enterprise to manually start the collection and upload of system information from your devices to Dell. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.

## Installing SupportAssist Enterprise in silent mode (Linux)

### Prerequisites


- Download the SupportAssist Enterprise installation package for Linux operating systems.
- Log in to the system with root privileges.
- Net-SNMP must be installed on the system. For information on installing Net-SNMP, see [Installing Net-SNMP \(Linux only\)](#).
-  **NOTE:** If you choose to install Net-SNMP after installing SupportAssist Enterprise, ensure that you run the script file, `snmptrapdServiceConfiguration.sh`, after installing Net-SNMP. The script file will be available at `/opt/dell/supportassist/scripts` after the installation of SupportAssist Enterprise is completed.
- The system must meet the requirements for installing SupportAssist Enterprise. See [Minimum requirements for installing and using SupportAssist Enterprise](#).

## Steps

1. Open the terminal window on the system running the Linux operating system.
2. Browse to the folder where the SupportAssist Enterprise installation package is available.
3. Perform one of the following:
  - Type `chmod 744 supportassist_1.x.x.bin` and press Enter.
  - Type `chmod +x supportassist_1.x.x.bin` and press Enter.
4. Type `./supportassist_1.x.x.bin silent` and press Enter.

## Next steps

(Optional) Follow the instructions in the **SupportAssist Enterprise Registration Wizard** to complete the registration of SupportAssist Enterprise.

 **CAUTION: Completing the registration is a prerequisite to experience the full benefits of SupportAssist Enterprise. Without registration, you can only use SupportAssist Enterprise to manually start the collection and upload of system information from your devices to Dell. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.**

# Migrating to SupportAssist Enterprise

If you are already using Dell SupportAssist for Servers, you can migrate to SupportAssist Enterprise. When you migrate to SupportAssist Enterprise, the devices, cases, collections, user groups, and settings are migrated. Before you migrate, download the SupportAssist Enterprise Windows or Linux installer package depending on the operating system installed on the server. The following sections provide the information required to migrate from SupportAssist for Servers to SupportAssist Enterprise.

 **NOTE: If auto update is enabled in SupportAssist for Servers version 1.2 or 1.3, you may be automatically migrated to SupportAssist Enterprise. For instructions to access SupportAssist Enterprise after the migration is complete, see [Opening the SupportAssist Enterprise user interface](#).**

## Migrating to SupportAssist Enterprise (Windows)


If you have SupportAssist for Servers version 1.2 or 1.3 installed, you can migrate to SupportAssist Enterprise.

### Prerequisites

Download the SupportAssist Enterprise installation package for Windows operating systems. See [Downloading the SupportAssist Enterprise installation package](#).

### Steps

1. Right-click the SupportAssist Enterprise installer package and click **Run as administrator**.

 **NOTE: Microsoft User Access Control (UAC) requires that the installation is performed with elevated privileges that are obtained only through the Run as administrator option. If you are logged in to the system as an administrator, double-click the installer package to install SupportAssist Enterprise. However, ensure that you acknowledge the Open File - Security Warning dialog box to proceed.**

The **Dell SupportAssist Enterprise - InstallShield Wizard** window is displayed.

2. At the **This setup will perform an upgrade of 'Dell SupportAssist'. Do you want to continue?** prompt, click **Yes**.

The **Preparing to Install** page is displayed briefly, and then the **Welcome to the SupportAssist Enterprise Installer** page is displayed.

3. Click **Upgrade**.

The **Installing SupportAssist Enterprise** page is displayed, and then the **Installation Completed** page is displayed.

4. Click **Finish**.

The **SupportAssist Enterprise** login page opens in a web browser window.

5. Type the Microsoft Windows operating system user name and password, and then click **Login**.

The SupportAssist Enterprise **Devices** page is displayed. Devices that you added in SupportAssist for Servers are displayed in the **Devices** page.

 **NOTE:** For instructions to access SupportAssist Enterprise after the migration is complete, see [Opening the SupportAssist Enterprise user interface](#).

## Migrating to SupportAssist Enterprise (Linux)

If you have SupportAssist for Servers version 1.2 or 1.3 installed, you can migrate to SupportAssist Enterprise.

### Prerequisites

Download the SupportAssist Enterprise installation package for Linux operating systems. See [Downloading the SupportAssist Enterprise installation package](#).

### Steps

1. Open the terminal window on the system running the Linux operating system.
2. Browse to the folder where the SupportAssist Enterprise installation package is available.
3. Perform one of the following:
  - Type `chmod 744 supportassist_1.x.x.bin` and press Enter.
  - Type `chmod +x supportassist_1.x.x.bin` and press Enter.
4. Type `./supportassist_1.x.x.bin` and press Enter.

 **NOTE:** If you want to upgrade SupportAssist Enterprise silently, type `./supportassist_1.x.x.bin silent` and press Enter.


The **Welcome to the SupportAssist Enterprise Installer** message is displayed.


5. To continue, type `c`.

The **SupportAssist Enterprise License Agreement** is displayed.

6. Read the license agreement and type `y` to start the installation.

After the installation is completed, the SupportAssist Enterprise login page opens in a web browser window.

 **NOTE:** If the initialization of the Dell SupportAssist Service takes longer than expected, an error message is displayed. If this issue occurs, close the web browser and try accessing SupportAssist Enterprise later. For instructions to access SupportAssist Enterprise, see [Opening the SupportAssist Enterprise user interface](#).

 **NOTE:** If you are using a Linux terminal emulator such as PuTTY to remotely install SupportAssist Enterprise, the SupportAssist Enterprise login page is not displayed. In such a scenario, you must access the SupportAssist Enterprise login page by using one of the following methods:

- Log in to a remote system and access the following web address by using a web browser:

```
https://<IP address or host name of the server where SupportAssist Enterprise is installed>:5700/SupportAssist
```

 **NOTE:** You can access SupportAssist Enterprise from a remote system only if port 5700 is open on the network.

- Log in to the local system and access the following web address by using a web browser: `http://localhost:9099/SupportAssist`

7. Type the user name and password of a user with root privileges on the system where SupportAssist Enterprise is installed, and then click **Login**.

The **Devices** page is displayed.

## Using SupportAssist Enterprise without registration

Registration of SupportAssist Enterprise is a prerequisite to experience the full benefits of SupportAssist Enterprise and to use all the available features. You can also use SupportAssist Enterprise without registration. However, only certain capabilities or features of SupportAssist Enterprise are available without registration. The following table provides a summary of the availability of capabilities or features without registration.

**Table 5. Availability of capabilities or features without registration**

Capabilities or features that are available	Capabilities or features that are not available
<ul style="list-style-type: none"> <li>· Add devices</li> <li>· Manually start the collection and upload of system information to Dell</li> </ul>	<ul style="list-style-type: none"> <li>· Monitor devices for hardware issues</li> <li>· Automatic case creation on issue detection</li> <li>· Scheduling automated periodic data collection</li> <li>· View support cases that are open for your devices</li> <li>· Opt-in or opt-out from receiving ProSupport Plus Server Recommendation Report by email</li> <li>· Update contact details</li> </ul>


 **NOTE: Registration of SupportAssist Enterprise is optional. However, Dell recommends that you complete the registration to experience the full benefits of the automated support capabilities of SupportAssist Enterprise.**

## Registering SupportAssist Enterprise

### Prerequisites

- If the server where you have installed SupportAssist Enterprise connects to the internet through a proxy server, ensure that you have the details of the proxy server.
- Ensure that you have the details of the contact you want to assign as your company's primary contact for SupportAssist Enterprise.

### About this task

 **CAUTION: Completing the registration is a prerequisite to experience the full benefits of SupportAssist Enterprise. Without registration, you can only use SupportAssist Enterprise to manually start the collection and upload of system information from your devices to Dell. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.**

The **Dell SupportAssist Enterprise Registration Wizard** guides you through configuring the proxy server settings (if applicable) and completing the registration. The registration wizard is displayed when you log in to SupportAssist Enterprise for the first-time. If you do not complete the registration or skip the registration, whenever you log in to SupportAssist Enterprise, the **SupportAssist Enterprise is not registered** banner is displayed at the top of the page. You can click the **Register now** link to open the registration wizard and complete the registration.

 **NOTE: You can also click Register in the About page or on the add devices wizard to open the Dell SupportAssist Enterprise Registration Wizard.**

 **NOTE: In Internet Explorer, if the Internet Explorer Enhanced Security Configuration feature is enabled, the SupportAssist Enterprise Registration Wizard is not displayed.**

### Steps

1. On the **Welcome** page, click **Next**.

SupportAssist Enterprise verifies connectivity to the Internet.

- If SupportAssist Enterprise is able to connect to the Internet, the **Registration** page is displayed.
- If SupportAssist Enterprise is unable to connect to the Internet, a message prompts you to confirm if the system connects to the Internet through a proxy server. If you click **Yes**, the **Proxy Settings** page is displayed.

If the system connects to the Internet directly, but the Internet connectivity issue persists, contact your network administrator for assistance.

2. If the **Proxy Settings** page is displayed:

- a. In the **Address** field, type the IP address or host name of the proxy server.
- b. In the **Port** field, type the port number of the proxy server.
- c. If a user name and password is required to connect to the proxy server, select **Requires authentication**, and type the user name and password in the appropriate fields.
- d. Click **Next**.

SupportAssist Enterprise verifies connectivity to the Internet through the proxy server. If the connection is successful, the **Registration** page is displayed. Else, an error message is displayed. If the proxy server connectivity issue persists, contact your network administrator for assistance.

The screenshot shows the 'Registration' step of the Dell SupportAssist Enterprise wizard. The interface includes a sidebar with 'Welcome', 'Registration', and 'Summary' options. The main content area is titled 'Registration' and contains the following fields:


- Company Information:**
  - \* Name: Text input field
  - \*Country / Territory: Dropdown menu with 'Select a country' option
- Contact Information:**
  - \* First Name: Text input field
  - \* Last Name: Text input field
  - \* Phone Number: Text input field
  - Alternate Phone Number: Text input field
  - \* Email Address: Text input field


At the bottom of the form, it indicates 'Step 2 of 3' and provides 'Back', 'Next', and 'Skip' buttons.

**Figure 3. Registration page**

3. On the **Registration** page, provide the following information:

- **Name** — The name must contain one or more printable characters, and must not exceed 256 characters.
- **Country/Territory** — Select your country or territory.
- **First Name** — The first name can contain letters, quotation marks [ ' ], periods [ . ], spaces, and must not exceed 50 characters.
- **Last Name** — The last name can contain letters, quotation marks [ ' ], periods [ . ], spaces, and must not exceed 50 characters.
- **Phone Number** — The phone number must contain a minimum of 9 characters and must not exceed 50 characters. The phone number can be provided in the international format, including special characters such as + and –.
- **Alternate Phone Number** — Optional, with the same requirements as the **Phone Number**.
- **Email Address** — Provide the email address in the name@company.com format. It must contain a minimum of five characters and not exceed 50 characters.

 **NOTE: Ensure that you use an English keyboard layout to type data in the Phone Number, Alternate Phone Number, and Email Address fields. If a native keyboard layout or non-English language is used to type data in these fields, an error message is displayed.**

 **NOTE: After registering SupportAssist Enterprise, you can update the primary contact information and also provide a secondary contact information. If the primary contact is unavailable, Dell will contact your company through the secondary contact. If both the primary and secondary contacts are configured with valid email addresses, both receive SupportAssist Enterprise emails. For information on updating the contact information, see [Viewing and updating the contact information](#).**

4. Click **Next**.


SupportAssist Enterprise connects to Dell and completes the registration. If the registration is successful, the **Summary** page is displayed. Else, an error message is displayed. If the registration issue persists, contact your network administrator for assistance.

5. Click **Finish**.

The SupportAssist Enterprise **Devices** page is displayed. The local system may display the following status in the **Devices** page:

- **OMSA not installed** — Dell OpenManage Server Administrator (OMSA) is not installed on the local system.

- **SNMP not configured** — SNMP settings of the local system is not configured.

 **CAUTION: Without the installation of OMSA and the configuration of SNMP settings, SupportAssist Enterprise will not be able to monitor hardware issues that may occur on the local system.**

### Next steps

- To allow SupportAssist Enterprise to automatically create a support case when a hardware issue occurs on the local system:
  - a. Install or upgrade Dell OpenManage Server Administrator (OMSA) on the local system. See [Installing or upgrading OMSA by using SupportAssist Enterprise](#).
  - b. Configure the SNMP settings of the local system. See [Configuring SNMP settings by using SupportAssist Enterprise](#).
  - c. Enable SupportAssist Enterprise to monitor hardware issues that may occur on the local system. See [Enabling or disabling monitoring of a device](#).
- If you have installed SupportAssist Enterprise on a server running a Linux operating system that has Security Enhanced Linux (SELinux) enabled, set up the server to receive alerts from remote devices. For more information, see [Setting up an SELinux enabled system to receive alerts](#).
- Add devices in SupportAssist Enterprise. For more information, see [Adding devices](#).
- (Optional) If your company utilizes an SMTP server (email server), configure the SMTP server settings in SupportAssist Enterprise. This enables SupportAssist Enterprise to utilize the SMTP server to send you device status and connectivity status email notifications. For more information, see [Configuring the SMTP server settings](#).
- (Optional) Update the contact details of the primary and secondary SupportAssist Enterprise contacts and provide a parts dispatch address. See [Viewing and updating the contact information](#).
- (Optional) If you want to manage a set of devices as a group, create one or more device groups based on your preference. See [Device grouping](#).

## Setting up an SELinux enabled system to receive alerts

### About this task

Security-Enhanced Linux (SELinux) is a security module that authorizes or prevents operations in Linux operating systems. When SELinux is enabled on the system running SupportAssist Enterprise, alerts (SNMP traps) from remote devices are not received by SupportAssist Enterprise. Without receiving alerts, SupportAssist Enterprise will not be able to identify hardware issues that may occur on remote devices. Therefore, you must perform the following steps on the system running SupportAssist Enterprise to allow SupportAssist Enterprise to receive alerts from remote devices.

 **NOTE: SELinux is enabled by default in the following operating systems:**

- Red Hat Enterprise Linux 6 or 7
- CentOS 6 or 7
- Oracle Enterprise Linux 6 or 7

### Steps

1. Open the terminal window and create a policy file named **supportassistpolicy.te**.
2. Open the policy file (**supportassistpolicy.te**) and type the following:

```
module supportassistpolicy 1.0;

require {
    type websm_port_t;
    type snmpd_t;
    type root_t;
    class tcp_socket name_connect;
    class dir { write add_name };
    class file { write getattr open create };
}

#===== snmpd_t =====

allow snmpd_t websm_port_t:tcp_socket name_connect;
allow snmpd_t root_t:dir write;
allow snmpd_t root_t:dir add_name;
allow snmpd_t root_t:file { write create open getattr };
```

3. Save the policy file.
4. Browse to the folder where you saved the policy file.
5. Type `checkmodule -M -m -o supportassistpolicy.mod supportassistpolicy.te` and press Enter.
6. Type `semodule_package -o supportassistpolicy.pp -m supportassistpolicy.mod` and press Enter.
7. Type `semodule -i supportassistpolicy.pp` and press Enter.

## Opening the SupportAssist Enterprise user interface

You can open the SupportAssist Enterprise user interface by using one of the following methods:

- If you are logged in to the server where SupportAssist Enterprise is installed:
  - If the server is running a Windows operating system, double-click the Dell SupportAssist Enterprise desktop icon.
  - Open a web browser and type the address in the following format:  
`http://localhost:9099/SupportAssist`
- To access SupportAssist Enterprise from a remote system, open a web browser and type the address in the following format:  
`https://<IP address or host name of the server where SupportAssist Enterprise is installed>:5700/SupportAssist.`  
For example, `https://10.25.35.1:5700/SupportAssist.`

 **NOTE:** When typing the address, ensure that you type `SupportAssist` with the `S` and `A` in uppercase.


- If you are using Internet Explorer, the following message is displayed: **There is a problem with this website's security certificate.** To open SupportAssist Enterprise, click **Continue to this website (not recommended).**
- If you are using Mozilla Firefox, the following message is displayed: **This Connection is Untrusted.** To open SupportAssist Enterprise, click **I Understand the Risks,** and then click **Add Exception.** In the **Add Security Exception** window, click **Confirm Security Exception.**


The **SupportAssist Enterprise** login page is displayed in the web browser.

 **NOTE:** The recommended screen resolution for optimally viewing the SupportAssist Enterprise user interface is 1280 x 1024 or higher.

## Logging in to SupportAssist Enterprise

1. In the **SupportAssist Enterprise** login page, type the user name and password in the appropriate fields.

 **NOTE:** You must provide the user name and password of a user account that is a member of the `SupportAssistAdmins` or `SupportAssistUsers` user group. If SupportAssist Enterprise is installed on a Linux operating system, you can also provide the user name and password of a user account that is a member of the `root` or `users` user group. For information on the SupportAssist Enterprise user groups, see [SupportAssist Enterprise user groups](#).

 **NOTE:** If the server where SupportAssist Enterprise is installed is a member of a Windows domain, you must provide the user name in the `[Domain\Username]` format. For example, `MyDomain\MyUsername`. You can also use a period `[.]` to indicate the local domain. For example, `.\Administrator`.

2. Click **Login**.

The SupportAssist Enterprise **Devices** page is displayed.

 **NOTE:** By default, after 14 minutes of inactivity, a **Session Timeout** message is displayed. If you want to continue the session, click **Renew**. If no response is received within a minute, you will be logged out automatically.

## Logging out of SupportAssist Enterprise

1. Click the **user name** link that is displayed at the top-right of the SupportAssist Enterprise header area.
2. In the menu that is displayed, click **Logout**.

The **SupportAssist Enterprise** login page is displayed.

## Adding devices

Adding devices prepares Dell EMC SupportAssist Enterprise to automate support from Dell Technical Support for your Dell devices. To use SupportAssist Enterprise to either monitor hardware issues or collect system information from your devices, you must add your devices in SupportAssist Enterprise.

After the installation of SupportAssist Enterprise, the local system (server where SupportAssist Enterprise is installed) is automatically added in SupportAssist Enterprise. To receive the benefits of SupportAssist Enterprise for your other Dell devices, you must manually add each device in SupportAssist Enterprise.

 **NOTE:** For the complete list of devices types and device models that you can add in SupportAssist Enterprise, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

You can add devices by using one of the following methods:

- Add a single device — Add each device individually by entering details of the device
- Import multiple devices — Add several devices by using a .csv file that contains details of the devices

## Device types and applicable devices

While adding a device in SupportAssist Enterprise, you must select an appropriate device type. The following table lists the devices that you can add by selecting a specific device type.




 **NOTE:** SupportAssist Enterprise may not be compatible with all device models of a supported device type. For the complete list of supported device types and device models, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

Table 6. Selecting a device type

Device Type	Devices that you can add
Chassis	<ul style="list-style-type: none"> <li>• Dell PowerEdge M1000e</li> <li>• Dell PowerEdge VRTX</li> <li>• Dell PowerEdge FX2/FX2s</li> </ul>
Fluid File System (FluidFS)	<ul style="list-style-type: none"> <li>• Dell EqualLogic with FluidFS</li> <li>• Dell PowerVault with FluidFS</li> <li>• Dell Compellent FS with FluidFS</li> </ul>
iDRAC	Dell's 12th and 13th generation of PowerEdge servers   <b>NOTE:</b> To add an iDRAC, you must provide the iDRAC IP address of the server.
Networking	<ul style="list-style-type: none"> <li>• Dell PowerConnect</li> <li>• Dell Force10</li> <li>• Dell Networking</li> <li>• Dell Networking X-Series switches</li> <li>• Dell Networking Wireless Controllers Mobility Series</li> </ul>

Device Type	Devices that you can add
Peer Storage (PS) / EqualLogic	Dell EqualLogic PS Series storage arrays
PowerVault	Dell PowerVault MD series storage arrays
Server / Hypervisor	<p>Dell's 9th to 13th generation of PowerEdge servers running:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> <li>• VMware ESX or ESXi</li> <li>• Citrix XenServer</li> <li>• Oracle Virtual Machine</li> <li>• Microsoft Hyper-V</li> </ul> <p> <b>NOTE: To add a Server / Hypervisor, you must provide the operating system IP address of the server.</b></p>
Storage Center (SC) / Compellent	Dell Compellent SC Series storage solutions

## Adding a single device

You can add a device individually based on the device type. The available device types that you can add are as follows:

- Chassis
- Fluid File System (FluidFS)
- iDRAC
- Networking
- Peer Storage (PS) / EqualLogic
- PowerVault
- Server / Hypervisor
- Storage Center (SC) / Compellent

## Adding a server or hypervisor

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The device must be reachable from the server where SupportAssist Enterprise is installed.
- If the device is running a Microsoft Windows operating system, Windows Management Instrumentation (WMI) service must be running on the device.
- If the device is running a Linux operating system:
  - Secure Shell (SSH) service must be running on the device.
  - SSH password authentication must be enabled (enabled by default).
  - Unzip package must be installed on the server where SupportAssist Enterprise is installed.
- If the device is running VMware ESXi, ESX, Oracle Virtual Machine, Citrix XenServer, or Microsoft Hyper-V:
  - SSH service must be running on the device.
  - Port 22 and 443 must be open on the device.
- Port 1311 must be open on the device for OMSA communication.
- If the device connects to the internet through a proxy server, the following ports must be open on the proxy server firewall: 161, 22 (for adding devices running Linux), 135 (for adding devices running Windows), and 1311.
- Review the requirements for installing OMSA on the device. For more information, see the “Installation Requirements” section in the *Dell OpenManage Server Administrator Installation Guide* at [Dell.com/OpenManageManuals](http://Dell.com/OpenManageManuals).

## About this task

SupportAssist Enterprise can monitor hardware issues and collect system information from Dell servers. You can perform the following steps to add a server running Windows or Linux, or a hypervisor. While adding the device, you can allow SupportAssist Enterprise to automatically perform the following tasks that are required for monitoring hardware issues that may occur on the device:

- Install or upgrade OMSA — OMSA is required to generate alerts for hardware events that occur on the device and also to collect system information from the device.
- Configure SNMP — Configuration of SNMP settings is required to forward alerts from the device to SupportAssist Enterprise.

## Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Click **Add Devices**.  
The **Add Single Device or Import Multiple Devices** wizard is displayed.
3. From the **Device Type** list, select **Server / Hypervisor**.

Add single device or Import multiple devices

Single device  
 Multiple devices

**Add single device**  
Enter the IP address or hostname of the device and click **Next**. Depending on the device configuration, additional information may be required.




Select device type: Server / Hypervisor

IP Address / Hostname: 000.000.000.000  
Name (optional): Name

Enable monitoring (may require additional SNMP settings)  
 Configure SNMP settings (required for receiving alerts from the device)  
 Install or upgrade OMSA (required for alert generation and data collection)

Next Cancel

Figure 4. Add single device window

4. Type the IP address or host name of the device in the appropriate field.  
 **NOTE: Dell recommends that you enter the host name of the device. If the host name is not available, you can enter the IP address of the device.**
5. If desired, type a name for the device in the appropriate field.  
The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.
6. If you want SupportAssist Enterprise to monitor hardware issues that may occur on the device, select the **Enable Monitoring**, **Configure SNMP Settings**, and **Install / Upgrade OMSA** options.  
 **NOTE: If the registration is completed, by default, the Enable Monitoring, Configure SNMP Settings, and Install / Upgrade OMSA options are selected.**  
 **NOTE: If the registration is not completed, when you select the Enable Monitoring option, you are requested to complete the registration. To continue, you can either clear the Enable Monitoring option or click Register to open the registration wizard.**

For SupportAssist Enterprise to monitor hardware issues that may occur on the device, the following dependencies must be met:

- The SNMP settings of the device must be configured to forward SNMP traps (alerts) to the server where SupportAssist Enterprise is installed.

- The recommended version of Dell OpenManage Server Administrator (OMSA) must be installed on the device.

To help you meet these dependencies, SupportAssist Enterprise can configure SNMP trap (alert) forwarding and also install or upgrade OMSA automatically on the device. To allow SupportAssist Enterprise to automatically:

- Configure the device to forward alerts, ensure that the **Configure SNMP Settings** option is selected.
- Install or upgrade OMSA on the device, ensure that the **Install / Upgrade OMSA** option is selected.

Tasks to configure alert forwarding and to install OMSA are initiated after the device is added successfully to the device inventory.

 **NOTE: If you prefer to perform both tasks (configure alert forwarding and install or upgrade OMSA) manually, clear the Configure SNMP Settings and Install / Upgrade OMSA options.**

7. Click **Next**.

The **Device Credentials** page is displayed.

8. Type the administrator or root user name and password of the device in the appropriate fields and click **Next**.

 **NOTE: The user name and password you enter must have:**

- Local administrator or domain administrator rights and WMI access on the device (if the device is running a Windows operating system)
- Root or sudo user rights (if the device is running a Linux operating system). If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist Enterprise. For information on configuring the sudo user, see [Configuring sudo access for SupportAssist Enterprise \(Linux\)](#).

If the device is a member of a Windows domain, you must provide the user name in the [Domain\Username] format. For example, MyDomain\MyUsername. You can also use a period [ . ] to indicate the local domain. For example, .\Administrator.

Example of a Linux user name: root

The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.


9. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.


If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).

10. Click **Finish**.



The device is added to the device inventory and the **Summary** page is displayed.


11. Click **OK** to close the **Add Single Device** wizard.



 **CAUTION: If the SNMP settings of the device is not configured and OMSA is not installed on the device, SupportAssist Enterprise cannot monitor hardware issues that may occur on the device.**

 **NOTE: Installation of OMSA is not supported on devices running CentOS, Oracle Virtual Machine, and Oracle Enterprise Linux. When you add these devices with the Device Type as Server / Hypervisor, SupportAssist Enterprise can only collect and upload system information. To allow SupportAssist Enterprise to monitor these devices for hardware issues, add these devices by selecting the Device Type as iDRAC. For more information on adding an iDRAC, see [Adding an iDRAC](#).**

The device is added to the device inventory with an appropriate status:

- When SupportAssist Enterprise is configuring the SNMP settings, the device displays a  **Configuring SNMP** status.
- When SupportAssist Enterprise is installing or upgrading OMSA, the device displays an  **Installing OMSA** status.

After the installation of OMSA and configuration of SNMP settings are completed, the device status changes to  **OK**. If an issue occurs during the configuration of SNMP or OMSA installation, the device displays an appropriate status in the **Devices** page.

 **NOTE:** If the device displays an  error status, click the error link to see a description of the issue and the possible resolution steps. To retry the OMSA installation or SNMP configuration, you can use the More Tasks list available on the device overview pane.

### Next steps

(Optional) You can also add the server in SupportAssist Enterprise by using the iDRAC details. In this scenario, SupportAssist Enterprise automatically correlates the alerts and collection of system information from both the operating system and the iDRAC. For instructions to add an iDRAC, see [Adding an iDRAC](#). For more information on how SupportAssist Enterprise correlates device information, see [Device correlation](#).

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

### Related links

[Add Single Device](#)

## Adding an iDRAC

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The device must be a 12th or 13th generation Dell PowerEdge server (iDRAC7 or iDRAC8). For information on identifying the generation of a PowerEdge server, see [Identifying the generation of a PowerEdge server](#).
- The device must be reachable from the server where SupportAssist Enterprise is installed.
- If the device connects to the internet through a proxy server, ports 161 and 443 must be open on the proxy server firewall.
- Enterprise or Express license must be installed on the iDRAC. For information on purchasing and installing an Enterprise or Express license, see the "Managing Licenses" section in the *iDRAC User's Guide* at [Dell.com/idracmanuals](http://Dell.com/idracmanuals).

### About this task

SupportAssist Enterprise can monitor hardware issues and collect system information from Dell servers. You can perform the following steps to add Dell's 12th and 13th generation of PowerEdge servers. While adding the device, you can allow SupportAssist Enterprise to automatically configure the SNMP settings of the device. Configuration of SNMP settings is required to forward alerts from the device to SupportAssist Enterprise.


### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Click **Add Devices**.  
The **Add Single Device or Import Multiple Devices** wizard is displayed.
3. From the **Device Type** list, select **iDRAC**.
4. Type the IP address or host name of the device in the appropriate field.

 **NOTE:** Dell recommends that you enter the host name of the device. If the host name is not available, you can enter the IP address of the device.

5. If desired, type a name for the device in the appropriate field.  
The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.
6. If you want SupportAssist Enterprise to monitor hardware issues that may occur on the device, select the **Enable Monitoring** and **Configure SNMP Settings** options.

 **NOTE:** If the registration is completed, by default, the **Enable Monitoring** and **Configure SNMP Settings** options are selected.

 **NOTE: If the registration is not completed, when you select the Enable Monitoring option, you are requested to complete the registration. To continue, you can either clear the Enable Monitoring option or click Register to open the registration wizard.**

For SupportAssist Enterprise to monitor hardware issues that may occur on the device, the device must be configured to forward SNMP traps (alerts) to the server where SupportAssist Enterprise is installed. To help you meet this requirement, SupportAssist Enterprise can configure SNMP trap (alert) forwarding automatically. To allow SupportAssist Enterprise to automatically configure the device to forward alerts, ensure that the **Configure SNMP Settings** option is selected. A task to configure alert forwarding is initiated after the device is added successfully to the device inventory.

 **NOTE: If you prefer to configure alert forwarding manually, clear the Configure SNMP Settings option.**

7. Click **Next**.

The **Device Credentials** page is displayed.

8. Type the iDRAC administrator user name and password in the appropriate fields and click **Next**.

The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.

9. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.

If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).

10. Click **Finish**.


The device is added to the device inventory and the **Summary** page is displayed.



11. Click **OK** to close the **Add Single Device** wizard.

 **CAUTION: If the SNMP settings of the device is not configured to forward alerts to the server where SupportAssist Enterprise is installed, SupportAssist Enterprise cannot monitor hardware issues that may occur on the device.**

The device is added to the device inventory with an appropriate status. When SupportAssist Enterprise is configuring the

SNMP settings, the device displays a  **Configuring SNMP** status. After the configuration of SNMP settings are completed,

the device status changes to  **OK**. If an issue occurs during the configuration of SNMP, the device displays an appropriate status in the **Devices** page.

 **NOTE: If the device displays an  error status, click the error link to view the description of the issue and the possible resolution steps. To retry the SNMP configuration, you can use the More Tasks list available on the device overview pane.**

### Next steps

(Optional) You can also add the server in SupportAssist Enterprise by using the operating system details. In this scenario, SupportAssist Enterprise automatically correlates the alerts and collection of system information from both the operating system and the iDRAC. For instructions to add the server, see [Adding a server or hypervisor](#). For more information on how SupportAssist Enterprise correlates device information, see [Device correlation](#).

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

### Related links

[Add Single Device](#)

## Adding a chassis

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).

- The device must be reachable from the server where SupportAssist Enterprise is installed.
- Ports 22 must be open on the device.
- Secure Shell (SSH) service must be running on the device.

### About this task

SupportAssist Enterprise can monitor hardware issues and collect data from Dell chassis. The chassis that you can add in SupportAssist Enterprise are:

- Dell PowerEdge FX2/FX2s
- Dell PowerEdge VRTX
- Dell PowerEdge M1000e

### Steps

1. Click **Devices**.

The **Devices** page is displayed.

2. Click **Add Devices**.

The **Add Single Device or Import Multiple Devices** wizard is displayed.

3. From the **Device Type** list, select **Chassis**.

4. Type the IP address or host name of the device in the appropriate field.


 **NOTE: Dell recommends that you enter the host name of the device. If the host name is not available, you can enter the IP address of the device.**


5. If desired, type a name for the device in the appropriate field.

The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.

6. If you want SupportAssist Enterprise to monitor hardware issues that may occur on the device, select the **Enable Monitoring** option.

 **NOTE: If the registration is completed, by default, the Enable Monitoring option is selected.**

 **NOTE: If the registration is not completed, when you select the Enable Monitoring option, you are requested to complete the registration. To continue, you can either clear the Enable Monitoring option or click Register to open the registration wizard.**

 **NOTE: SupportAssist Enterprise can monitor hardware issues that may occur on the device only if the device is configured to forward SNMP traps (alerts) to the server where SupportAssist Enterprise is installed. For instructions to configure alert forwarding on a chassis, see [Manually configuring the alert destination of a chassis by using the web interface](#).**

7. Click **Next**.

The **Device Credentials** page is displayed.

8. Type the chassis administrator user name and password in the appropriate fields and click **Next**.

The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.

9. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.

If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).

10. Click **Finish**.

The device is added to the device inventory and the **Summary** page is displayed.

11. Click **OK** to close the **Add Single Device** wizard.

### Next steps

 **CAUTION: If the device is not configured to forward alerts, SupportAssist Enterprise cannot detect hardware issues that may occur on the device.**

For monitoring hardware issues that may occur on the device only — Ensure that the device is configured to forward SNMP traps (alerts) to the server where SupportAssist Enterprise is installed. For instructions to configure alert forwarding, see [Manually configuring the alert destination of a chassis by using the web interface](#).

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

#### Related links

[Add Single Device](#)

## Adding a Dell Networking device

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The device must be reachable from the server where SupportAssist Enterprise is installed.
- Port 22 or 161 must be open on the device.
- Secure Shell (SSH) and SNMP services must be running on the device.

### About this task

SupportAssist Enterprise can monitor hardware issues and collect data from Dell Networking devices. The networking devices that you can add in SupportAssist Enterprise are:

- Dell PowerConnect
- Dell Force10
- Dell Networking
- Dell X-Series switches
- Dell Wireless Controllers Mobility Series

### Steps

1. Click **Devices**.

The **Devices** page is displayed.

2. Click **Add Devices**.

The **Add Single Device or Import Multiple Devices** wizard is displayed.

3. From the **Device Type** list, select **Networking**.

4. Type the IP address or host name of the device in the appropriate field.


 **NOTE: Dell recommends that you enter the host name of the device. If the host name is not available, you can enter the IP address of the device.**


5. If desired, type a name for the device in the appropriate field.

The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.

6. If you want SupportAssist Enterprise to monitor the health status of the device, select the **Enable Monitoring** option.

 **NOTE: If the registration is completed, by default, the Enable Monitoring option is selected.**

 **NOTE: If the registration is not completed, when you select the Enable Monitoring option, you are requested to complete the registration. To continue, you can either clear the Enable Monitoring option or click Register to open the registration wizard.**

 **NOTE: SupportAssist Enterprise can monitor the health status of the device only if the SNMP settings of the device is configured to forward SNMP traps (alerts) to the server where SupportAssist Enterprise is installed. For instructions to configure alert forwarding, see [Manually configuring the alert destination of a networking device](#).**

7. Click **Next**.

The **Device Credentials** page is displayed.

8. Type the user name, password, enable password, and community string of the device in the appropriate fields and click **Next**.  
The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.  
If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
9. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.  
If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).
10. Click **Finish**.  
The device is added to the device inventory and the **Summary** page is displayed.
11. Click **OK** to close the **Add Single Device** wizard.

#### Next steps

 **CAUTION: If the device is not configured to forward alerts, SupportAssist Enterprise cannot detect hardware issues that may occur on the device.**

For monitoring hardware issues that may occur on the device only — Ensure that the device is configured to forward SNMP traps (alerts) to the server where SupportAssist Enterprise is installed. For instructions to configure alert forwarding, see [Manually configuring the alert destination of a networking device](#).

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

#### Related links

[Add Single Device](#)

## Adding a PowerVault MD Series storage array


#### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The device must be reachable from the server where SupportAssist Enterprise is installed.
- Port 2463 must be open on the device.

#### About this task

SupportAssist Enterprise can only collect data from the PowerVault MD Series storage arrays. By adding a PowerVault device, you will be able to collect data on demand and after deployment. You can perform the following steps to add a PowerVault MD Series storage array.

#### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Click **Add Devices**.  
The **Add Single Device or Import Multiple Devices** wizard is displayed.
3. From the **Device Type** list, select **PowerVault**.
4. Type the IP address or host name of the device in the appropriate field.  
 **NOTE: Dell recommends that you enter the host name of the device. If the host name is not available, you can enter the IP address of the device.**
5. If desired, type a name for the device in the appropriate field.  
The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.
6. Click **Next**.  
The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.

7. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.  
If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).
8. Click **Finish**.  
The device is added to the device inventory and the **Summary** page is displayed.
9. Click **OK** to close the **Add Single Device** wizard.

### Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

### Related links

[Add Single Device](#)

## Adding a Dell EqualLogic PS Series storage array

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The device must be reachable from the server where SupportAssist Enterprise is installed.
- Ports 21, 22, and 161 must be open on the device.
- Secure Shell (SSH) and SNMP service must be running on the device.

### About this task

SupportAssist Enterprise can only collect data from the EqualLogic PS Series storage arrays. By adding a Dell EqualLogic device, you will be able to collect data on demand and after deployment. You can perform the following steps to add an EqualLogic PS Series storage array.

### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Click **Add Devices**.  
The **Add Single Device or Import Multiple Devices** wizard is displayed.
3. From the **Device Type** list, select **Peer Storage (PS) / EqualLogic**.
4. Type the IP address or host name of the EqualLogic group in the appropriate field.
5. If desired, type a name for the device in the appropriate field.  
The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.
6. Click **Next**.  
The **Device Credentials** page is displayed.
7. Type the user name, password, and community string of the EqualLogic group in the appropriate fields and click **Next**.  
The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.  
If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
8. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.  
If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).
9. Click **Finish**.  
The device is added to the device inventory and the **Summary** page is displayed.

10. Click **OK** to close the **Add Single Device** wizard.

### Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

### Related links

[Add Single Device](#)

## Adding a Dell Compellent SC Series storage solution

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The device must be reachable from the server where SupportAssist Enterprise is installed.
- Port 443 must be open on the device.
- REST service must be running on the device.
- For collecting system information, SupportAssist must be enabled in the Dell Compellent Enterprise Manager application.

### About this task

SupportAssist Enterprise can only collect data from the Dell Compellent SC Series storage solutions. By adding a Dell Compellent device, you will be able to collect data on demand and after deployment. You can perform the following steps to add a Dell Compellent SC Series storage solution.

### Steps

1. Click **Devices**.

The **Devices** page is displayed.

2. Click **Add Devices**.

The **Add Single Device or Import Multiple Devices** wizard is displayed.

3. From the **Device Type** list, select **Storage Center (SC) / Compellent**.

4. Type the IP address or host name of the device in the appropriate field.



**NOTE: Dell recommends that you enter the host name of the device. If the host name is not available, you can enter the IP address of the device.**

5. If desired, type a name for the device in the appropriate field.

The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.

6. Click **Next**.

The **Device Credentials** page is displayed.

7. Type the user name and password of the device in the appropriate fields and click **Next**.

The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.

8. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.

If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).

9. Click **Finish**.

The device is added to the device inventory and the **Summary** page is displayed.

10. Click **OK** to close the **Add Single Device** wizard.

### Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

#### Related links

[Add Single Device](#)

## Adding a Dell Fluid File System (FluidFS) NAS device

#### Prerequisites


- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The device must be reachable from the server where SupportAssist Enterprise is installed.
- Ports 22 and 44421 must be open on the device.
- Secure Shell (SSH) service must be running on the device.

#### About this task

SupportAssist Enterprise can only collect data from a Dell Fluid File System (FluidFS) network attached storage (NAS) device. By adding a FluidFS NAS device, you will be able to collect data on demand and after deployment. You can perform the following steps to add a FluidFS NAS device. The FluidFS NAS devices that you can add are:

- Dell Compellent
- Dell EqualLogic
- Dell PowerVault

#### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Click **Add Devices**.  
The **Add Single Device or Import Multiple Devices** wizard is displayed.
3. From the **Device Type** list, select **Fluid File System (FluidFS)**.
4. Type the IP address or host name of the device in the appropriate field.  
 **NOTE: Dell recommends that you enter the host name of the device. If the host name is not available, you can enter the IP address of the device.**
5. If desired, type a name for the device in the appropriate field.  
The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.
6. Click **Next**.  
The **Device Credentials** page is displayed.
7. Type the user name and password of the device in the appropriate fields and click **Next**.  
The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.  
If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
8. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.  
If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).
9. Click **Finish**.  
The device is added to the device inventory and the **Summary** page is displayed.
10. Click **OK** to close the **Add Single Device** wizard.

#### Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

**Related links**

[Add Single Device](#)

## Adding a device by duplication

**Prerequisites**

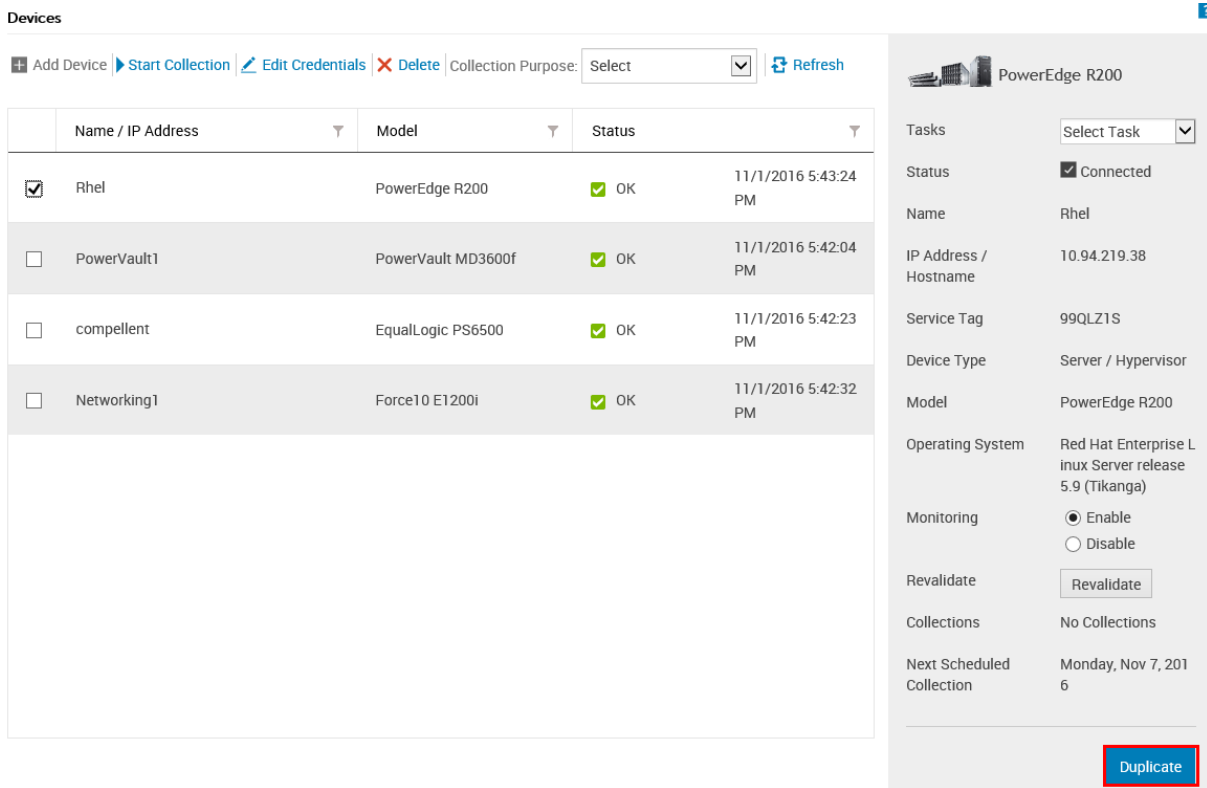
- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The device must be reachable from the server where SupportAssist Enterprise is installed.
- The required network ports must be open on the device. For the network port requirements on the remote device, see [Network requirements](#).

**About this task**

You can use the **Duplicate** feature to quickly add a device that is of the same type as a device that you have already added. For example, if you have already added a remote server, you select that server and click **Duplicate** to start adding another remote server.

**Steps**

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select a device which is of the same type as the device that you want to add.



**Figure 5. Duplicate option**

The device overview pane is displayed at the right side of the **Devices** page.

3. Click **Duplicate**.  
The **Duplicate Device** wizard is displayed.
4. Type the IP address or host name of the device in the appropriate field.

 **NOTE: Dell recommends that you enter the host name of the device. If the host name is not available, you can enter the IP address of the device.**

5. If desired, type a name for the device in the appropriate field.  
The name you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or host name that you have entered is used to represent the device.
6. Depending on the device type and your requirement, select or clear the available options, and click **Next**.  
The **Device Credentials** page is displayed.
7. Enter the credentials of the device and click **Next**.  
The **Discovering Device** page is displayed until SupportAssist identifies the device.  
If the device is discovered successfully, the **Device Options** page is displayed. Otherwise, an appropriate error message is displayed.
8. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.  
If you do not select a device group, the device is assigned to the **Default** device group. For information on the predefined device groups, see [Predefined device groups](#).
9. Click **Finish**.  
The device is added to the device inventory and the **Summary** page is displayed.
10. Click OK to close the **Duplicate Device** wizard.

### Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Revalidate the device. See [Revalidating a device](#).

## Importing multiple devices

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

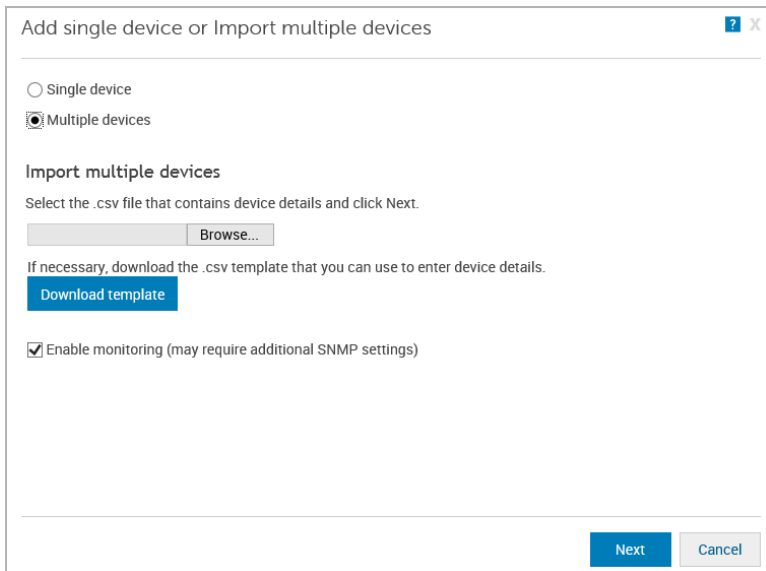
### About this task

You can import multiple devices by using a .csv file that contains details of the devices in a specified format.

 **NOTE: The maximum number of devices that you can import by using a csv file is 300.**

### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Click **Add Devices**.  
The **Add Single Device or Import Multiple Devices** wizard is displayed.
3. Click **Multiple Devices**.



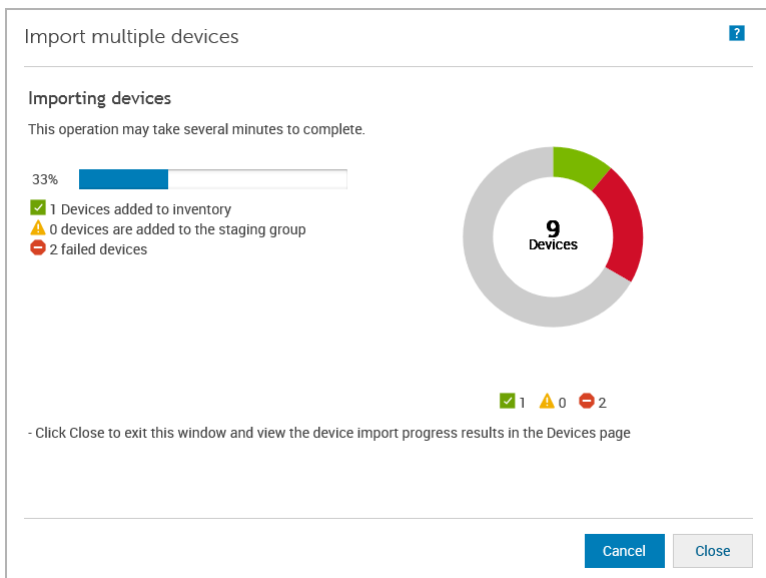
**Figure 6. Import multiple devices window**

4. Click **Download .csv template** and save the .csv file.
5. Open the .csv template and update the details of the devices.

An example of a .csv file with the device details is as follows:

```
Device Type,IP/Hostname,Display Name,Username,Password,Enable Password,Community String,Auto SNMP Config(Yes/No),Auto Push OMSA(Yes/No),Compellent UserName,Compellent Password
Server/hypervisor,10.14.17.14,ServerA.com,Onyx,ak,,,,yes,yes,,
Server/hypervisor,10.14.19.28,Rhel,root,Dell_123$,,,,yes,yes,,
PowerVault,10.14.16.65,PowerVault1,,,,,yes,yes,,
chassis,10.14.100.22,Enclosure,root,calvin,,,yes,yes,,
PeerStorage(PS) / Equallogic,10.94.101.236,compellent,root,admin@321,,public,yes,yes,,
Networking,10.14.26.23,Networking1,Admin,$tores1,$tores1,public,yes,yes,,
iDRAC,10.14.28.18,iDRAC11,root,calvin,,,yes,yes,,
iDRAC,10.14.217.205,,root,calvin,,,yes,yes,,
iDRAC,10.14.217.1,,root,calvin,,,yes,yes,,
```

6. Click **Browse**.  
The **Choose file to Upload** window is displayed.
7. Navigate to the folder that contains the .csv file, select the .csv file, and then click **Open**.
8. If you want SupportAssist Enterprise to monitor the health status of the devices, ensure that the **Enable Monitoring** option is selected.
9. Click **Next**.



**Figure 7. Importing devices window**

The **Importing Devices** window is displayed.

If you click **Cancel** while the device import operation is in progress:

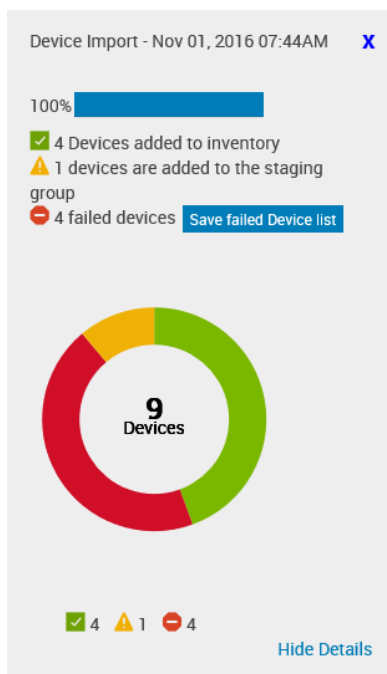
- The import operation is stopped after your confirmation.
- Devices that were already imported are retained in the **Default** or **Staging** group.
- The import operation continues for devices for which discovery has already started.
- Devices for which the initial identification is incomplete are discarded.

While importing devices that are members of one or more domains by using a .csv file, if SupportAssist Enterprise detects that the credentials of two of those devices of a certain domain are incorrect, the import operation is paused for other devices in that domain. The import operation is paused to prevent automatic lockout of the domain account due to repetitive authentication failures. For devices of other domains included in the .csv file, the import process continues normally. If the import process is paused for devices of a certain domain, you can perform one of the following:

- Click **Cancel** to stop the import operation. You can try importing the .csv file again after verifying and updating the device credentials.
- Click **Resume** to continue importing other devices that are members of that domain.

**CAUTION:** Resuming the import operation may result in lockout of the domain account, if other devices in the .csv file use the same credentials.

10. Click **Close**.



**Figure 8. Device Import pane**

The **Device Import** pane is displayed at the right side of the **Devices** page. The result of the device import operation is as follows:

- Devices that were imported successfully are added to the device inventory.
- Devices that were identified, but did not meet certain prerequisites, are added to the **Staging** group. For more information on the **Staging** group, see [Predefined device groups](#).
- Devices that were not identified are notified as failed devices.

### Next steps

- For devices that were added successfully to the device inventory:
  - Verify if the device displays an error status. If an error status is displayed, click the error status to view a detailed description of the error and a possible resolution.
  - You may also have to perform additional tasks that may be required to enable SupportAssist Enterprise to monitor those devices. To allow SupportAssist Enterprise to monitor the device, enable monitoring and ensure that the SNMP settings of the device is configured. For instructions to enabling monitoring, see [Enabling or disabling monitoring of a device](#). For instructions to configure the SNMP settings of a device, see [Configuring SNMP settings by using SupportAssist Enterprise](#) and [Manually configuring SNMP settings](#).
- For devices that were added to the **Staging** group:
  - If the device is an iDRAC, ensure that the iDRAC Enterprise license is installed. For information on purchasing and installing the iDRAC Enterprise license, see the *iDRAC User's Guide* at [Dell.com/idracmanuals](http://Dell.com/idracmanuals).
  - If the device is a Compellent storage array, ensure that SupportAssist is enabled in the Dell Compellent Enterprise Manager application. For information on enabling the SupportAssist in Enterprise Manager, see the *Dell Enterprise Manager Administrator's Guide* at [Dell.com/storagemanuals](http://Dell.com/storagemanuals).
  - Ensure that all prerequisites for adding the device are met. For information on the prerequisites for adding a device, see the "Prerequisites" section in the instructions for adding each device type. See [Adding a single device](#).
  - Revalidate each device. See [Revalidating a device](#).
- For devices notified as failed devices:
  - a. Export the device details to view the issue description and possible resolution. See [Exporting details of devices that were not imported](#).
  - b. Update the device details in the .csv file and try importing the devices again.

## Related links

[Import Multiple Devices](#)

# Exporting details of devices that were not imported

## About this task

You can export the details of the devices that were not imported as a .csv file. The exported file contains the device details, description of the issue, and the possible resolution.

## Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. In the **Device Import** pane, click **Save failed device list**.  
The **Save As** window is displayed.
3. Navigate to the location where you want to save the file and click **Save**.

## Next steps

Open the exported .csv file. The **Status** column displays the error code, description of the issue, and the possible resolution.

# Revalidating a device

## Prerequisites

- The device that you want to revalidate must be in the **Staging** group.
- If the device is an iDRAC, ensure that the iDRAC Enterprise license is installed. For information on purchasing and installing the iDRAC Enterprise license, see the *iDRAC User's Guide* at [Dell.com/idracmanuals](http://Dell.com/idracmanuals).
- If the device is a Compellent storage array, ensure that SupportAssist is enabled in the Dell Compellent Enterprise Manager application. For information on enabling the SupportAssist in Enterprise Manager, see the *Dell Enterprise Manager Administrator's Guide* at [Dell.com/storagemanuals](http://Dell.com/storagemanuals).

## About this task

Revalidating a device enables you to verify if a device present in the **Staging** group meets the requirements for enabling SupportAssist Enterprise capabilities.

## Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. In the **Refine By** pane, select **Staging**.  
The devices in the **Staging** group are displayed.
3. Select the device that you want to revalidate.

**Devices** ?

+ Add Device | 
 ▶ Start Collection | 
 🔗 Edit Credentials | 
 ✖ Delete | 
 Collection Purpose: Select | 
 🔄 Refresh

	Name / IP Address	Model	Status	
<input type="checkbox"/>	Rhel	PowerEdge R200	✔ OK	11/1/2016 5:43:24 PM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	✔ OK	11/1/2016 5:42:04 PM
<input type="checkbox"/>	compellent	EqualLogic PS6500	✔ OK	11/1/2016 5:42:23 PM
<input type="checkbox"/>	Networking1	Force10 E1200i	✔ OK	11/1/2016 5:42:32 PM
<input checked="" type="checkbox"/>	10.94.217.205	PowerEdge R420	✖ Unable to add device	11/1/2016 5:42:51 PM

**PowerEdge R420**

Tasks: Select Task

Status:  Connected

Name: Not Available

IP Address / Hostname: 10.94.217.205

Service Tag: 4FF2G2S

Device Type: iDRAC

Model: PowerEdge R420

Operating System:

Monitoring:  Enable  Disable

Revalidate: Revalidate

Collections: No Collections

Duplicate

**Figure 9. Revalidate option**

The device overview pane is displayed at the right side of the **Devices** page.

**4. Click Revalidate.**

SupportAssist Enterprise identifies the device and verifies if all the requirements for enabling SupportAssist Enterprise capabilities are met. If the revalidation is successful, the device is moved to the **Default** group.

## Viewing cases and devices

The Dell EMC SupportAssist Enterprise user interface displays the devices that you have added and the support cases that are open for those devices. From the **Devices** page, you can perform various device-specific operations such as view collections, enable or disable monitoring, and so on. From the **Cases** page, you can manage cases that were opened by SupportAssist Enterprise.

**NOTE: SupportAssist Enterprise does not create a support case for every alert received from a monitored device. A support case is created only if the alert type and number of alerts received from the device match with the criteria defined by Dell for support case creation.**

## Viewing all support cases

**NOTE: The list of open cases is displayed only if you have completed the registration of SupportAssist.**

To view the support cases that are present for your monitored devices, click **Cases**. A progress indicator may appear on the **Cases** page to indicate that SupportAssist Enterprise is in the process of updating the cache of open support cases.

Refine By:

Device Type:

- Server
- Storage
- Networking
- Chassis

Case Status:

- Open
- Submitted
- In Progress
- Suspended
- Requested for Closure

Service Contract:

- Basic
- ProSupport
- ProSupport Plus
- ProSupport Flex for Data Center
- ProSupport One for Data Center Or ProSupport Flex for Data Center

Source Type:

- Email
- Phone
- Chat
- SupportAssist
- Help Desk
- TechDirect
- Others

Home > Cases

**Cases**

Case Options  Refresh

	Name / IP Address	Number	Status	Title	Device Type	Date Opened
<b>Networking1 - Last Refreshed - 11/01/2016 07:59 AM</b>						
<input type="checkbox"/>	Networking1	907354354	Submitted	WCG: ENTPIRISE  PS  FA  PowerEdge  Windows  Thermal shutdown protection has been initiated.	Networking	10/28/2016
<input type="checkbox"/>	Networking1	907336850	Open	Hardware (Other)	Networking	10/21/2016
<input type="checkbox"/>	Networking1	907132901	Open	Hardware (Other)	Networking	09/21/2016
<input type="checkbox"/>	Networking1	906904890	Open	Dell PC Diagnostics : 123	Networking	08/30/2016
<input type="checkbox"/>	Networking1	906900423	Open	Dell PC Diagnostics : 123	Networking	08/26/2016
<input type="checkbox"/>	Networking1	906898747	Open	Dell PC Diagnostics : 123	Networking	08/25/2016
<input type="checkbox"/>	Networking1	906894408	Open	Dell PC Diagnostics : 123	Networking	08/22/2016
<input type="checkbox"/>	Networking1	906854768	Open	Dell PC Diagnostics : 123	Networking	08/18/2016
<input type="checkbox"/>	Networking1	906834523	Open	Dell PC Diagnostics : 123	Networking	08/16/2016
<input type="checkbox"/>	Networking1	906754336	Open	Dell PC Diagnostics : 123	Networking	08/12/2016

Figure 10. Cases page

**NOTE: By default, the case list is grouped by the device name or device IP address. The last refreshed date and time that is displayed in the group header indicates when the case information was last retrieved from Dell.**

Support case information is automatically available, for supported devices that have valid Service Tags when SupportAssist Enterprise connects to the Dell support case and service contract databases over the internet. Support case information is refreshed only in the following situations:

- When you open the **Cases** page.
- When you click the **Refresh** link on the **Cases** page.
- When the **Cases** page is open and you refresh the web browser window.

After SupportAssist Enterprise has completed its open support cases update, the **Cases** page displays the current support cases. For information on the fields and details displayed on the **Cases** page, see [Case page](#).

## Case management options

The **Cases** page provides options that you can use to manage the support cases that were opened automatically by SupportAssist Enterprise. You can request Dell Technical Support to perform the following activities by using the available case management options:

- Suspend activities related to a support case
- Resume activities related to a support case
- Close a support case

 **NOTE: The case management options are applicable only for support cases that were opened automatically by SupportAssist Enterprise.**

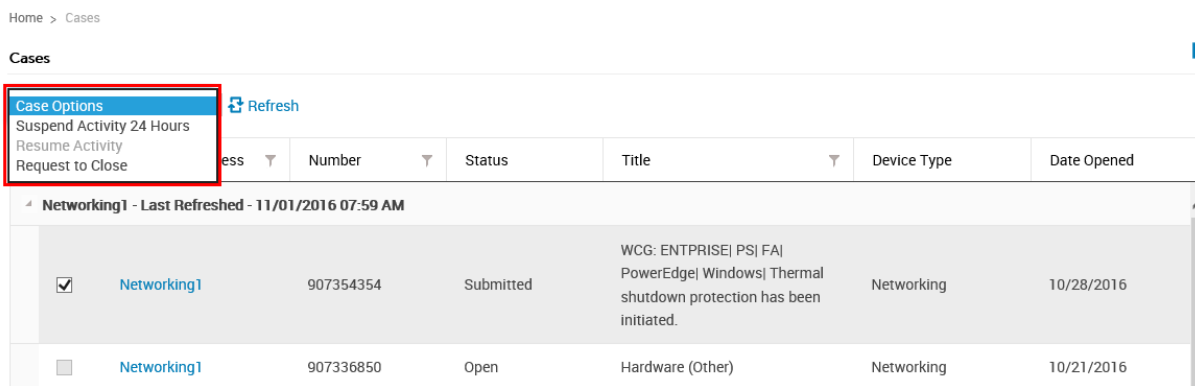


Figure 11. Case options

## Requesting to suspend case activities for 24 hours

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

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

- If you want to resolve the issue without any assistance from Dell Technical Support
- If you do not want to receive any notifications related to the support case from Dell during a planned maintenance activity

 **NOTE: You can request Dell Technical Support to stop activities related to a support case only if the support case was opened by SupportAssist.**


### Steps

1. Click **Cases**.  
The **Cases** page is displayed.
2. In the **Refine by** pane, from the **Source Type** list, select **SupportAssist**.  
The list of all cases that were opened by SupportAssist are displayed.
3. Select the support case that you want to suspend.

 **NOTE: The Case Options list is enabled only if the support case that you have selected was opened by SupportAssist.**

 **NOTE: The Suspend Activity 24 hours option is disabled if you have already requested to suspend notifications for the selected support case.**

4. From the **Case Options** list, select **Suspend Activity 24 hours**.  
The **Suspend case activities for 24 hours** window is displayed.
5. (Optional) Type your reason for requesting to suspend activities for the support case.
6. Click **OK**.  
The **Updating Case** message is displayed. After the case is updated successfully, the **Case Status** message is displayed.
7. Click **OK**.  
The support case displays a **Suspended** status.

 **NOTE: If SupportAssist Enterprise is unable to process your request, an appropriate error message is displayed. In such a scenario, you can run the case creation test to verify connectivity to Dell, and then retry the operation.**

#### Related links

[Testing the case creation capability](#)

## Requesting to resume support activities



### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

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

### Steps

1. Click **Cases**.  
The **Cases** page is displayed.
2. In the **Refine by** pane, from the **Source Type** list, select **SupportAssist**.  
The list of all cases that were opened by SupportAssist are displayed.
3. Select the support case that you want to resume.  
 **NOTE: The Case Options list is enabled only if the support case that you have selected was opened by SupportAssist.**  
 **NOTE: The Resume Activity option is enabled only if you had previously requested to suspend notifications for the selected support case.**
4. From the **Case Options** list, select **Resume Activity**.  
The **Resume Activity** window is displayed.
5. (Optional) Type your reason for requesting to resume activities for the support case.
6. Click **OK**.  
The **Updating Case** message is displayed. After the case is updated successfully, the **Case Status** message is displayed.
7. Click **OK**.  
The support case displays the appropriate status.

 **NOTE: If SupportAssist Enterprise is unable to process your request, an appropriate error message is displayed. In such a scenario, you can run the case creation test to verify connectivity to Dell, and then retry the operation.**

#### Related links

[Testing the case creation capability](#)

## Requesting to close a support case

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

If you have resolved a problem with a device, you can request Dell Technical Support to close the corresponding support case.

 **NOTE: You can request Dell Technical Support to close a support case only if the support case was opened by SupportAssist.**

 **NOTE: You can request Dell Technical Support to close a support case that is in any status, except the Closed and Closure Requested status.**

### Steps

1. Click **Cases**.

The **Cases** page is displayed.

2. In the **Refine by** pane, from the **Source Type** list, select **SupportAssist**.

The list of all cases that were opened by SupportAssist are displayed.

3. Select the support case that you want to close.

 **NOTE: The Case Options list is enabled only if the support case that you have selected was opened by SupportAssist.**

4. From the **Case Options** list, select **Request to Close**.

The **Request to close the case** window is displayed.

5. (Optional) Type your reason for requesting to close the support case.

6. Click **OK**.

The **Updating Case** message is displayed. After the case is updated successfully, the **Case Status** message is displayed.

7. Click **OK**.

The support case displays a **Closure requested** status.

 **NOTE: After you request to close a support case, Dell Technical Support may contact you to get more details before closing the support case.**

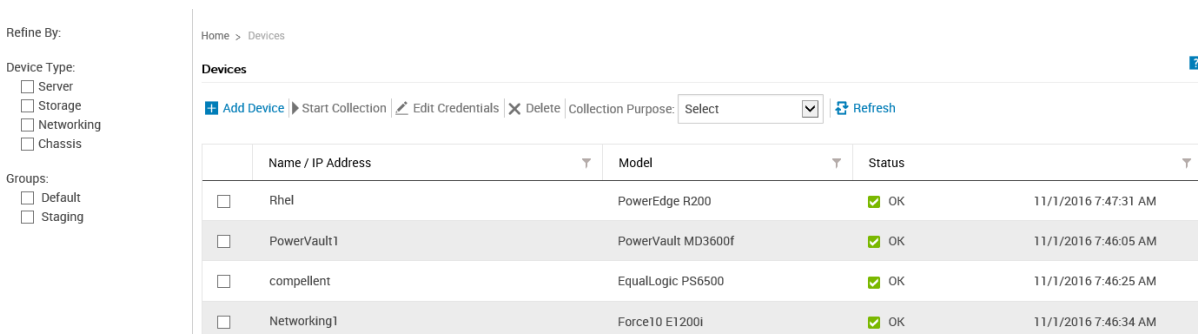
 **NOTE: If SupportAssist Enterprise is unable to process your request, an appropriate error message is displayed. In such a scenario, you can run the case creation test to verify connectivity to Dell, and then retry the operation.**

### Related links

[Testing the case creation capability](#)

## Viewing the device inventory

To view the device inventory, click **Devices**.



The screenshot shows the 'Devices' page in a web application. On the left, there are filters for 'Device Type' (Server, Storage, Networking, Chassis) and 'Groups' (Default, Staging). The main area displays a table of devices with the following data:

	Name / IP Address	Model	Status	
<input type="checkbox"/>	Rhel	PowerEdge R200	OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	OK	11/1/2016 7:46:25 AM
<input type="checkbox"/>	Networking1	Force10 E1200i	OK	11/1/2016 7:46:34 AM

Figure 12. Device Inventory page

 **NOTE: The Devices page is refreshed automatically every 3 minutes.**

For information on the fields and details displayed on the **Devices** page, see [Device inventory](#).

# Viewing the device overview pane

## About this task

You can view details of a device such as the IP address, device type, model number, Service Tag, collection status, collection history, and so on in the device overview pane. From the device overview pane, you can also perform the following tasks:

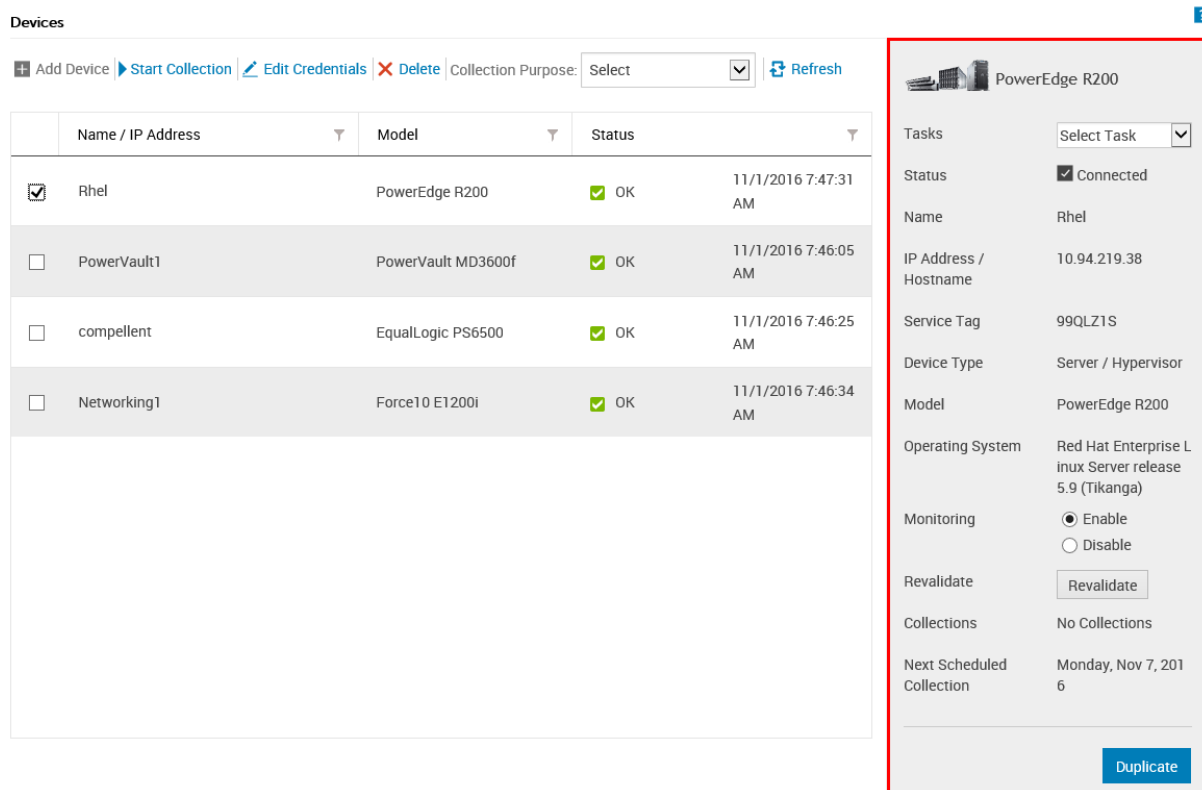
- Clear the System Event Log of a server
- Check for support cases of a specific device
- Enable or disable maintenance mode for a device
- Install or upgrade OMSA on a server
- Configure the SNMP settings of a device
- Enable or disable monitoring of a device
- Revalidate a device that is present in the **Staging** group.
- Access the configuration viewer that allows you to view the data collected from a device
- Add a device by duplication

## Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select a device.

 **NOTE: The device overview pane is displayed if only one device is selected in the Devices page.**


 **NOTE: If a SupportAssist Enterprise-initiated task is already running on a device, you may not be able to select that device.**



Devices ?

[+ Add Device](#) [▶ Start Collection](#) [✎ Edit Credentials](#) [✖ Delete](#) | Collection Purpose: Select [Refresh](#)

	Name / IP Address	Model	Status	
<input checked="" type="checkbox"/>	Rhel	PowerEdge R200	<input checked="" type="checkbox"/> OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:25 AM
<input type="checkbox"/>	Networking1	Force10 E1200i	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:34 AM

 PowerEdge R200

Tasks Select Task

Status  Connected

Name Rhel

IP Address / Hostname 10.94.219.38

Service Tag 99QLZ1S

Device Type Server / Hypervisor

Model PowerEdge R200

Operating System Red Hat Enterprise Linux Server release 5.9 (Tikanga)

Monitoring  Enable  Disable

Revalidate Revalidate

Collections No Collections

Next Scheduled Collection Monday, Nov 7, 2016

Duplicate

Figure 13. Device overview pane

The device overview pane is displayed.

## Refining the displayed data

By default, SupportAssist Enterprise displays all devices that you have added and the support cases that are open for those devices. You can refine the data displayed on the **Devices** or **Cases** page based on the available options. The **Devices** page can be refined based on the device type and device group. The **Cases** page can be refined based on the device type, case status, service contract, and case source.

1. Click **Devices** or **Cases**.  
The **Device** or **Cases** page is displayed.
2. In the **Refine by** pane, select one or more options of the available options.  
The displayed data is refined based on the selected options.

## Filtering the displayed data


You can filter the data displayed on the **Devices** and **Cases** pages based on your preference.

1. Click the filter icon  displayed in the column header.  
The **Filter Option** panel is displayed.
2. In the **Contains** field, type the filtering criteria.
3. Click **Filter**.

The displayed data is filtered depending on the criteria and the column header displays the filtered icon .

## Clearing the data filter

You can clear the data filter you applied on the **Cases** and **Devices** pages to view all the available data.

1. Click the filtered icon  displayed in the column header.  
The filtering options are displayed.
2. Click **Clear**.  
The user interface displays all the available data.

## Sorting the displayed data

To sort the data displayed on the **Cases** and **Devices** pages, click a column header. The displayed data is sorted and an arrow that indicates the sorting type (ascending or descending) is displayed next to the column title. To reset the sorting, click the column header again.

## Checking support cases for a specific device

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

You can view the open support cases for a specific monitored device by using the **Check for cases** option available in the device overview pane.

### Steps

1. Click **Devices**.

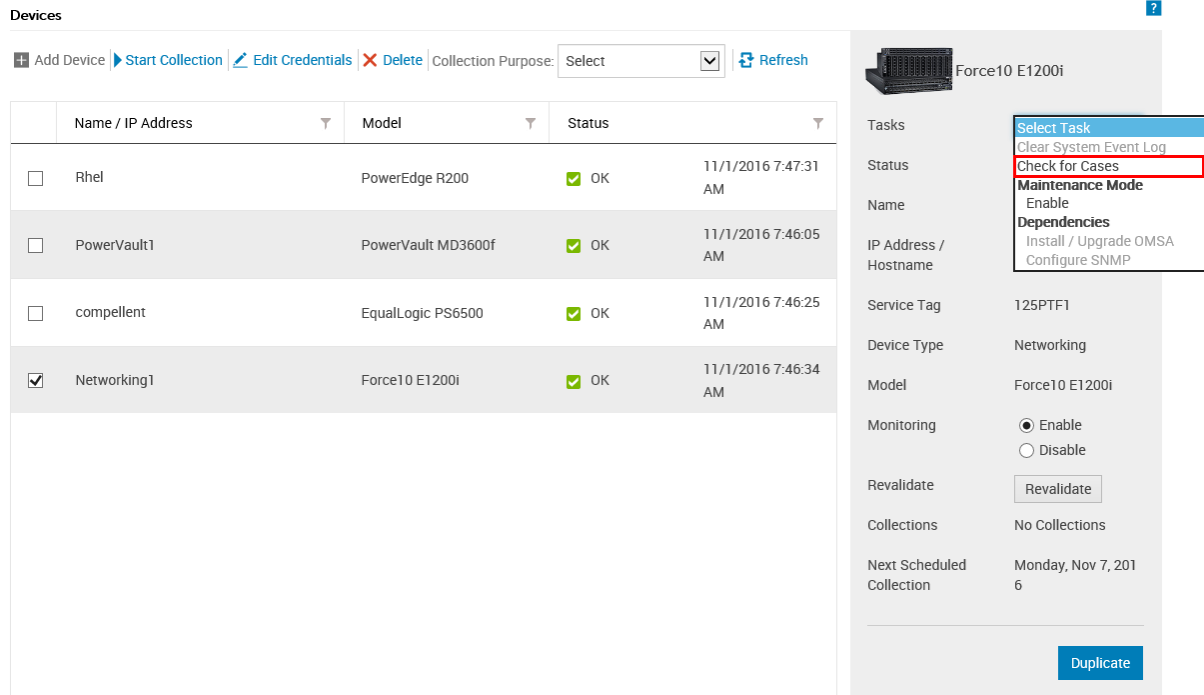
The **Devices** page is displayed.

2. Select the device for which you want to check for support cases.

The device overview pane is displayed.

 **NOTE: The device overview pane is displayed only if a single device is selected in the Devices page.**

3. From the **More Tasks** list, select **Check for cases**.



The screenshot shows the 'Devices' page with a table of devices and a detailed view for a Force10 E1200i device. The table lists four devices: Rhel, PowerVault1, compellent, and Networking1. The 'Networking1' device is selected. The detailed view for 'Force10 E1200i' shows various settings and a 'More Tasks' dropdown menu. The 'Check for Cases' option is highlighted in the dropdown menu.

	Name / IP Address	Model	Status	
<input type="checkbox"/>	Rhel	PowerEdge R200	OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	OK	11/1/2016 7:46:25 AM
<input checked="" type="checkbox"/>	Networking1	Force10 E1200i	OK	11/1/2016 7:46:34 AM

Force10 E1200i

Tasks

- Select Task
- Clear System Event Log
- Check for Cases
- Maintenance Mode
- Enable
- Dependencies
- Install / Upgrade OMSA
- Configure SNMP

Name

IP Address / Hostname

Service Tag: 125PTF1

Device Type: Networking

Model: Force10 E1200i

Monitoring:  Enable  Disable

Revalidate:

Collections: No Collections

Next Scheduled Collection: Monday, Nov 7, 2016

**Figure 14. Check for cases option**

- If support cases are present for the device, you are navigated to the **Cases** page. Support cases that are present for the device are displayed at the top of the **Cases** page with a blue border along the rows.
- If no support cases are present for the device, an appropriate message is displayed.

Cases



Case Options

	Name / IP Address	Number	Status	Title	Device Type	Date Opened
Networking1 - Last Refreshed - 11/01/2016 11:51 AM						
<input type="checkbox"/>	Networking1	907354354	Submitted	WCG: ENTPRISE PS  FA  PowerEdge  Windows  Thermal shutdown protection has been initiated.	Networking	10/28/2016
<input type="checkbox"/>	Networking1	907336850	Open	Hardware (Other)	Networking	10/21/2016
<input type="checkbox"/>	Networking1	907132901	Open	Hardware (Other)	Networking	09/21/2016
<input type="checkbox"/>	Networking1	906904890	Open	Dell PC Diagnostics : 123	Networking	08/30/2016
<input type="checkbox"/>	Networking1	906900423	Open	Dell PC Diagnostics : 123	Networking	08/26/2016
<input type="checkbox"/>	Networking1	906898747	Open	Dell PC Diagnostics : 123	Networking	08/25/2016
<input type="checkbox"/>	Networking1	906894408	Open	Dell PC Diagnostics : 123	Networking	08/22/2016
<input type="checkbox"/>	Networking1	906854768	Open	Dell PC Diagnostics : 123	Networking	08/18/2016
<input type="checkbox"/>	Networking1	906834523	Open	Dell PC Diagnostics : 123	Networking	08/16/2016

Figure 15. Cases for the device



**NOTE:** When you check for support cases, the latest support cases information is retrieved from Dell for the selected device. If support case information cannot be retrieved because of an issue, an appropriate message is displayed.




# Device grouping

Dell EMC SupportAssist Enterprise has two predefined device groups (**Default** 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, storage, or switch)
- 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 credentials for each device type included in 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 Enterprise.**
-  **NOTE: You can create and manage device groups only if you are logged in to SupportAssist Enterprise with elevated or administrative privileges. For information on the SupportAssist Enterprise user groups, see [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).**
-  **NOTE: The credentials, contact information, and parts dispatch information configured for a device group override the default credentials, contact information, and parts dispatch information configured through the Settings pages. For example, if you have created a device group and configured the primary contact for the device group, all SupportAssist Enterprise notifications for issues with any device included in the device group are sent to the primary contact assigned to that device group.**

## Related links

- [Viewing device groups](#)
- [Creating a device group](#)
- [Managing devices in a device group](#)
- [Managing the credentials of a device group](#)
- [Viewing and updating the contact information of a device group](#)
- [Editing device group details](#)
- [Deleting a device group](#)

## Predefined device groups

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

- **Default** group — Contains devices that you have assigned to the **Default** group. By default, all devices that are discovered successfully are assigned to this group, unless you assign the device to any other group.
- **Staging** group — Contains devices that were only discovered partially while you tried to import them because certain requirements were not met. Devices in this group will be automatically moved to the **Default** group when you revalidate them after the requirement is met. SupportAssist Enterprise capabilities are not available for devices that are present in this group. Typically, a device is added to the staging group in the following scenarios:

- The iDRAC does not have an Enterprise license installed
- SupportAssist is not enabled in the Dell Compellent Enterprise Manager application
- Certain prerequisites for adding the device are not met

## Viewing device groups

You can view the devices groups that you have created in the **Device Groups** page.

To view the device groups, point to **Devices** and click **Groups**.

The **Device Groups** page is displayed.

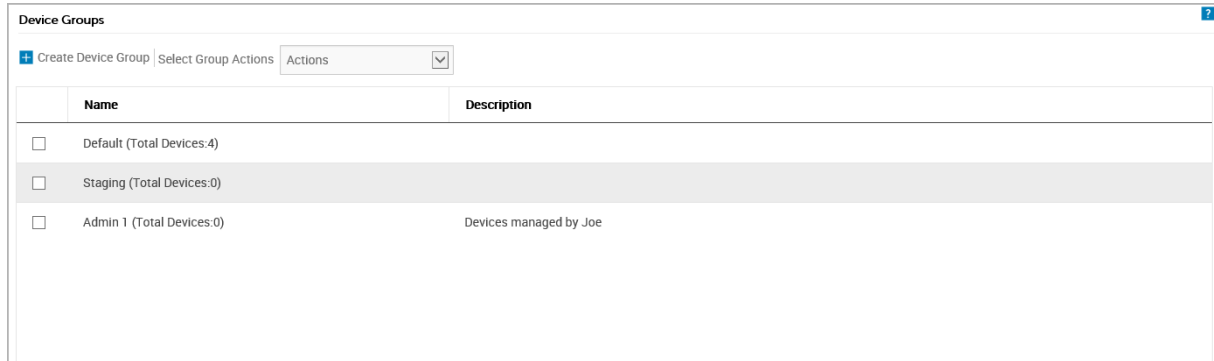


Figure 16. Device Groups page

## Creating a device group

You can create a device group based on your requirement. For example, you can create device groups based on the device types.

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### Steps

1. Point to **Devices** and click **Groups**.  
The **Device Groups** page is displayed.
2. Click **Create Device Group**.  
The **Create Group** window is displayed.
3. Type a unique name and description for the device group and click **Save**.  
The device group that you created is displayed in the **Device Groups** page.

## Managing devices in a device group

After creating a device group, you can select the devices you want to add or remove from the device group.

### Prerequisites

- Ensure that you have already created a device group. See [Creating a device group](#).
- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

You can use the **Manage Devices** action available in the **Device Groups** page to add or remove devices from the device group.

 **NOTE: A device can be included in only one device group.**

 **NOTE: You add up to 100 devices to a device group in a single operation.**

## Steps

1. Point to **Devices** and click **Groups**.  
The **Device Groups** page is displayed.
2. Select a device group.
3. In the **Select group actions** list, select **Manage Devices**.  
The **Manage Devices** window is displayed.

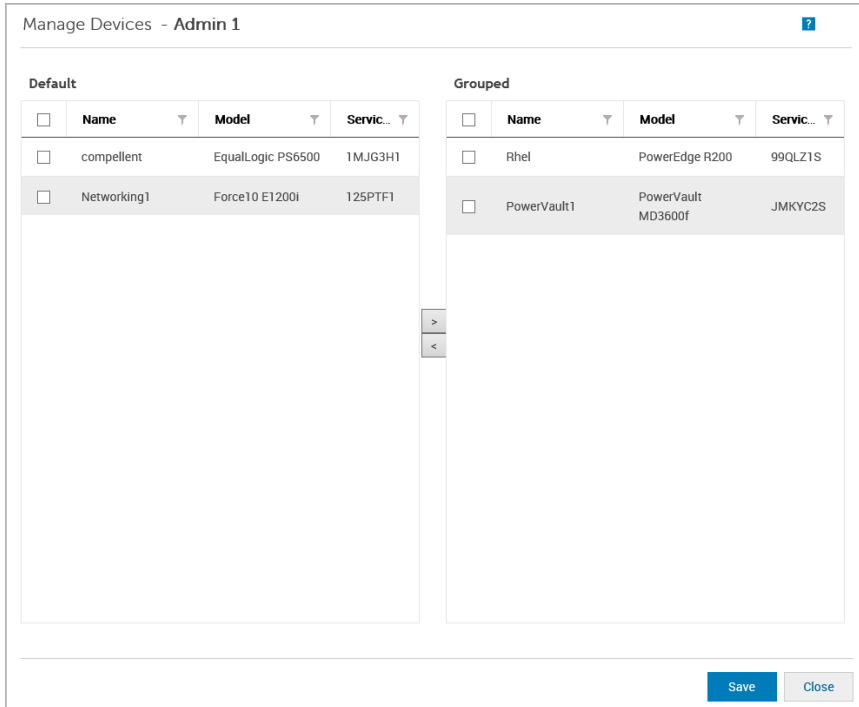




Figure 17. Manage Devices window

4. To add devices to the device group, select the devices in the **Default** pane, and click  .  
The selected devices are moved to the **Grouped** pane.
5. To remove devices from the device group, select the devices in the **Grouped** pane, and click  .  
The selected devices are moved to the **Default** pane.
6. Click **Save**.

 **NOTE:** Including or excluding one listing of a correlated device from a device group results in the automatic inclusion or exclusion of the other associated listing. For more information about device correlation, see [Device correlation](#).

## Managing the credentials of a device group

If device types within the device group have the same credentials, you can configure common credentials for each device type within the device group.

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

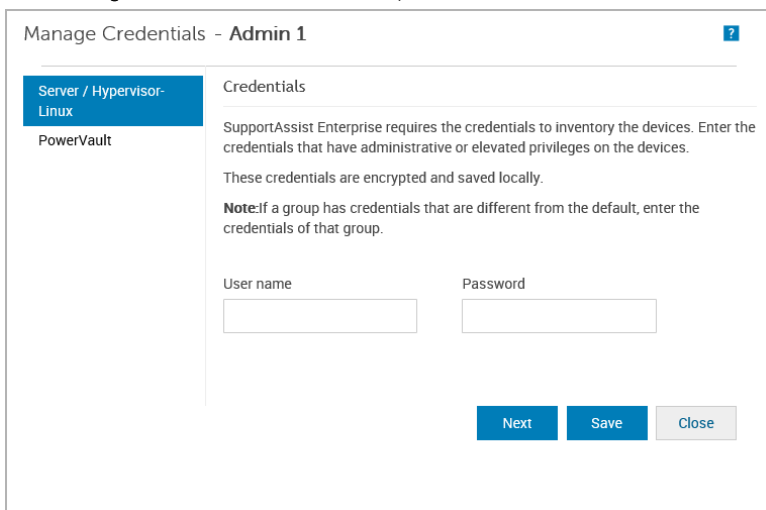
You can use the **Manage Credentials** option available in the **Device Groups** page to configure the credentials for the different device types within a device group.

**NOTE:** The device group credentials override the default credentials that you provided for adding a device in SupportAssist Enterprise. When the device group credentials are configured:

- SupportAssist Enterprise uses the device group credentials (not the default credentials) to collect system information from the device type.
- If SupportAssist Enterprise is unable to connect to the device using the device group credentials, SupportAssist Enterprise uses the default credentials.

### Steps

1. Point to **Devices** and click **Groups**.  
The **Device Groups** page is displayed.
2. Select a device group.
3. In the **Select group actions** list, select **Manage Credentials**.  
The **Manage Credentials** window is displayed.



**Figure 18. Manage Credentials window**

4. Type the user name and password for the device type highlighted in the left pane.
5. Click **Save**.
6. If more than one device type is included in the device group, click **Next**.  
The next device type is highlighted in the left pane.
7. Repeat steps 4, 5, and step 6 until you have provided the user name and password for all device types included in the device group.
8. Click **Close**.

## Viewing and updating the contact information of a device group

You can view or update the contact information, preferred contact method and time, and the parts dispatch information of a device group.

### Prerequisites



You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

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

**NOTE:** The device group contact information overrides the default contact information configured through the **Settings** → **Contact Information** page. If an issue is detected on devices included in a group, SupportAssist Enterprise sends notifications to the device group contact (not the default contact).

## Steps

1. Point to **Devices** and click **Groups**.  
The **Device Groups** page is displayed.
2. Select a device group.
3. From the **Select group actions** list, select **Manage Contacts**.  
The **Manage Contacts** window is displayed.
4. If you want to use the contact information provided in the **Settings** → **Contact Information** page, select **Use Default**.
5. Select the type of contact:
  - **Primary**
  - **Secondary**
6. Type the first name, last name, phone number, alternate phone number (optional), and email address in the appropriate fields.
7. Select the preferred contact method, preferred contact hours, and time zone.
8. In the **Parts Dispatch (Optional)** section:
  -  **NOTE: The parts dispatch information is optional. If the Dell Technical Support agent 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.**
  -  **NOTE: The device group parts dispatch information overrides the default parts dispatch information that you configured through 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).**
  - a. Type the address and city/town in the appropriate fields.
  - b. Select the country.
  - c. Type the state/province/region and zip/postal code in the appropriate fields.
9. Click **Save**.

## Editing device group details

You can edit the name and description of a device group based on your preference.

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### Steps

1. Point to **Devices** and click **Groups**.  
The **Device Groups** page is displayed.
2. Select a device group.
3. From the **Select group actions** list, select **Edit / Delete Device Group**.  
The **Edit / Delete Group** window is displayed.
4. Edit the name and description based on your preference and click **Update**.

## Deleting a device group

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

You can delete device groups based on your preference.

-  **NOTE: Deleting a device group only removes the device group, device group credentials, and contact information. It does not delete any devices from the Devices page.**

## Steps

1. Point to **Devices** and click **Groups**.  
The **Device Groups** page is displayed.
2. Select a device group.
3. From the **Select group actions** list, select **Edit / Delete Device Group**.  
The **Edit / Delete Group** window is displayed.
4. Click **Delete**.

# Understanding maintenance mode

The maintenance mode functionality suspends the alert processing and automatic case creation capability of Dell EMC SupportAssist Enterprise, thereby preventing the creation of unnecessary support cases during an alert storm or a planned maintenance activity. If an alert storm is received from a monitored device, SupportAssist Enterprise automatically places the device in maintenance mode. You can also manually 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.


## Global-level maintenance mode


Global-level 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 Enterprise 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 [Enabling or disabling global-level maintenance mode](#).


## Device-level maintenance mode

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

- **Automated device-level maintenance mode** — By default, if SupportAssist Enterprise receives 10 or more valid hardware alerts within 60 minutes from a specific device, SupportAssist Enterprise automatically places that device in maintenance mode. The device remains in maintenance mode for 30 minutes, allowing 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  on the **Devices** page. After 30 minutes, the device is automatically removed from maintenance mode, enabling SupportAssist Enterprise 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 [Enabling or disabling device-level maintenance mode](#).

 **NOTE: When a device is placed automatically in maintenance mode, an email notification is sent to your primary or secondary contact. However, you can receive the email notification for automated device-level maintenance mode only if the SMTP server (email server) settings are configured in SupportAssist Enterprise. For instructions to configure the SMTP server settings, see [Configuring SMTP server settings](#).**

- **Manual device-level maintenance mode** — If you have a planned maintenance activity for a device, and do not want SupportAssist Enterprise to automatically create support cases, you can place that device in maintenance mode. While in maintenance mode, the device displays the maintenance mode icon  on the **Devices** page. After the maintenance activity is completed, you can remove the device from maintenance mode, enabling SupportAssist Enterprise to resume processing alerts from the device normally. For instructions to enable device-level maintenance mode, see [Enabling or disabling device-level maintenance mode](#).

The global-level and device-level maintenance mode functionalities 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.

# Enabling or disabling global-level maintenance mode

Enabling global-level maintenance mode suspends the automatic case creation capability for all devices.

## Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

## Steps

1. Point to **Settings** and click **Preferences**.  
The **Preferences** page is displayed.
2. In **Maintenance Mode**, depending on your requirement, select or clear the **Temporarily suspend case generation activity (for example, for purposes of downtime, external troubleshooting, etc.)** option.
3. Click **Apply**.  
The **Saving Preferences Data** window is displayed. If you enabled maintenance mode, a **Maintenance Mode** banner is displayed at the top of the SupportAssist Enterprise user interface. After global-level maintenance mode is enabled, SupportAssist Enterprise remains in that state unless you clear the option as in step 2.

## Related links

[Preferences](#)

# Enabling or disabling device-level maintenance mode

If you have a planned maintenance activity for a specific device and do not want SupportAssist Enterprise to process alerts from that device, you can place that device in maintenance mode. After the maintenance activity is completed, you can remove the device from maintenance mode, enabling SupportAssist Enterprise to process alerts from the device normally.

## Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

## Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select a device on the **Devices** page.  
The device overview pane is displayed at the right side of the **Devices** page.
3. From the **Tasks** list, under **Maintenance Mode**, select **Enable** or **Disable** depending on your requirement.

**Devices** ?

+ Add Device | 
 [▶ Start Collection](#) | 
 [✎ Edit Credentials](#) | 
 [✖ Delete](#) | 
 Collection Purpose: Select ▼ | 
 [🔄 Refresh](#)

	Name / IP Address	Model	Status	
<input type="checkbox"/>	Rhel	PowerEdge R200	<input checked="" type="checkbox"/> OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:25 AM
<input checked="" type="checkbox"/>	Networking1	Force10 E1200i	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:34 AM

**Force10 E1200i**

Tasks

Status

Name

IP Address / Hostname

Service Tag: 125PTF1

Device Type: Networking

Model: Force10 E1200i

Monitoring:  Enable  Disable

Revalidate:

Collections: No Collections

Next Scheduled Collection: Monday, Nov 7, 2016

Select Task

Clear System Event Log

Check for Cases

**Maintenance Mode**


Enable

Dependencies

Install / Upgrade OMSA

Configure SNMP

**Figure 19. Maintenance mode options**

If maintenance mode is enabled for a specific device, the maintenance mode icon  is displayed with the name of the device on the **Devices** page. If you disable maintenance mode for a device, the maintenance mode icon is removed from the device name.

# Maintaining SupportAssist Enterprise capability

The changes that occur in your company's IT setup over a period of time may require configuration or updates in Dell EMC SupportAssist Enterprise. To maintain SupportAssist Enterprise capability over a period of time for all your devices, you may be required to:

- Enable monitoring of devices. See [Enabling or disabling monitoring of a device](#).
- Edit the credentials (user name and password) of a device, if the device credentials were changed because of your company's security policy or for other reasons. See [Editing device credentials](#).
- Install or upgrade dependent components such as Dell OpenManage Server Administrator (OMSA). See [Installing or upgrading OMSA by using SupportAssist Enterprise](#).
- Configure the SNMP settings of a device. See [Configuring SNMP settings by using SupportAssist Enterprise](#).
- Update the primary and secondary contact information, if there is a change in the contact details. See [Viewing and updating the contact information](#).
- Update the proxy server settings in SupportAssist Enterprise, if applicable. See [Configuring proxy server settings](#).
- Update the SMTP server (email server) settings in SupportAssist Enterprise, if applicable. See [Configuring the SMTP server settings](#).
- Perform the connectivity test to ensure that SupportAssist Enterprise is able to connect to all dependent network resources. See [Connectivity test](#).
- Perform the case creation test to verify the automatic case creation capability of SupportAssist Enterprise. See [Testing the case creation capability](#).
- Clear the System Event Log of a server. See [Clearing the System Event Log \(SEL\)](#).
- Upgrade or update SupportAssist Enterprise. See [Automatic update](#).

You may also want to delete a device, if you do not want SupportAssist Enterprise to monitor a device or for other reasons. See [Deleting a device](#).

## Enabling or disabling monitoring of a device

### Prerequisites

Ensure that you have completed the registration of SupportAssist Enterprise. See [Registering SupportAssist Enterprise](#).

### About this task

For devices that SupportAssist Enterprise can monitor, you can enable monitoring while adding the device. Depending on your requirement, you can also enable or disable monitoring of a device at any time from the **Devices** page. For SupportAssist Enterprise to automatically create a support case when a hardware issue occurs on a device, monitoring must be enabled for that device.

### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select the device for which you want to enable or disable monitoring.  
The device overview pane is displayed at the right side of the **Devices** page.
3. In **Monitoring**, select **Enable** or **Disable** depending on your requirement.

Devices ?

+ Add Device | [▶ Start Collection](#) | [✎ Edit Credentials](#) | [✖ Delete](#) | Collection Purpose: Select ▼ | [🔄 Refresh](#)

	Name / IP Address	Model	Status	
<input type="checkbox"/>	Rhel	PowerEdge R200	<input checked="" type="checkbox"/> OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:25 AM
<input checked="" type="checkbox"/>	Networking1	Force10 E1200i	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:34 AM

**Force10 E1200i**

Tasks

Status

Name

IP Address / Hostname

Service Tag: 125PTF1

Device Type: Networking

Model: Force10 E1200i

Monitoring:  Enable  Disable

Revalidate: [Revalidate](#)

Collections: No Collections

Next Scheduled Collection: Monday, Nov 7, 2016

[Duplicate](#)

Figure 20. Enable or disable monitoring option

- NOTE:** If the registration of SupportAssist Enterprise is not completed, the Enable monitoring option is disabled.
- NOTE:** To allow SupportAssist Enterprise to monitor a device, in addition to enabling monitoring, the SNMP settings of the device must also be configured. For instructions to configure the SNMP settings of a device, see [Configuring SNMP settings by using SupportAssist Enterprise](#) and [Manually configuring SNMP settings](#).

## Editing device credentials

SupportAssist Enterprise utilizes the credentials (user name and password) that you provided for adding the device—to log in to the device, collect system information, and send it securely to Dell. If the credentials of a device are changed because of your company's security policy or for other reasons, you must ensure that the credentials of the devices are updated in SupportAssist Enterprise.

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select the device for which you want to edit the credentials.  
The **Edit Credentials** link is enabled.

Devices ?

+ Add Device ▶ Start Collection ✎ Edit Credentials ✗ Delete | Collection Purpose: Select ↕ Refresh

	Name / IP Address	Model	Status	
<input checked="" type="checkbox"/>	Rhel	PowerEdge R200	<input checked="" type="checkbox"/> OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:25 AM
<input type="checkbox"/>	Networking1	Force10 E1200i	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:34 AM

**PowerEdge R200**

Tasks Select Task

Status  Connected

Name Rhel

IP Address / Hostname 10.94.219.38

Service Tag 99QLZ1S

Device Type Server / Hypervisor

Model PowerEdge R200

Operating System Red Hat Enterprise Linux Server release 5.9 (Tikanga)

Monitoring  Enable  Disable

Revalidate Revalidate

Collections No Collections

Next Scheduled Collection Monday, Nov 7, 2016

Duplicate

Figure 21. Edit Credentials option

3. Click **Edit Credentials**.

The **Edit Credentials** window is displayed with the existing device credentials. The device credentials displayed in the **Edit Credentials** window may vary depending on the selected device type.

**NOTE: SupportAssist Enterprise does not require you to edit or provide the credentials of the local system (server where SupportAssist Enterprise is installed). For the local system, the Edit Credentials window does not display the user name or password.**

4. Edit the credentials of the device as required.

5. Click **Save**.

**NOTE: The edited credentials are saved only if SupportAssist Enterprise is able to connect to the device by using the provided credentials.**

## Installing or upgrading OMSA by using SupportAssist Enterprise

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

For monitoring hardware issues that may occur on a server, the Dell OpenManage Server Administrator (OMSA) agent must be installed and running on the server. If OMSA is either not installed or requires an upgrade on a device, the **Status** column on the **Devices** page displays an appropriate message. You can use the **Install / Upgrade OMSA** option to automatically download and install the recommended version of OMSA on a device.

**NOTE: The SupportAssist Enterprise recommended version of OMSA may vary depending on the generation of the PowerEdge server and the operating system running on the server. For information on the recommended versions of OMSA, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).**

**NOTE:** Installation or upgrade of OMSA by using SupportAssist Enterprise is not supported on servers running the following operating systems and hypervisors:

- Oracle Enterprise Linux
- CentOS
- Citrix XenServer
- VMware ESX or ESXi
- Oracle Virtual Machine

**Steps**

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select the server where you want to install or upgrade OMSA.  
The device overview pane is displayed at the right side of the **Devices** page.
3. From the **Tasks** list, select **Install / Upgrade OMSA**.

**NOTE:** If SupportAssist Enterprise does not support the installation or upgrade of OMSA on the server that you have selected, the **Install / Upgrade OMSA** option is disabled.

The screenshot shows the 'Devices' page in SupportAssist Enterprise. At the top, there are buttons for 'Add Device', 'Start Collection', 'Edit Credentials', and 'Delete', along with a 'Collection Purpose' dropdown and a 'Refresh' button. Below this is a table with columns for 'Name / IP Address', 'Model', and 'Status'. The table lists four devices: 'Rhel' (PowerEdge R200), 'PowerVault1' (PowerVault MD3600f), 'compellent' (EqualLogic PS6500), and 'Networking1' (Force10 E1200i). The 'Rhel' device is selected with a checkmark. To the right of the table is a detailed view for the 'PowerEdge R200' device. This view includes fields for 'Tasks', 'Status', 'Name', 'IP Address / Hostname', 'Service Tag', 'Device Type', 'Model', 'Operating System', 'Monitoring', 'Revalidate', 'Collections', and 'Next Scheduled Collection'. A 'Select Task' dropdown menu is open, showing options: 'Clear System Event Log', 'Check for Cases', 'Maintenance Mode', 'Enable', 'Dependencies', 'Install / Upgrade OMSA' (highlighted with a red box), and 'Configure SNMP'. A 'Duplicate' button is located at the bottom right of the detailed view.

**Figure 22. Install / Upgrade OMSA option**

The **Status** column on the **Devices** page displays the status of the OMSA installation or upgrade.

**Related links**

[Support for automatically installing or upgrading OMSA](#)

## Configuring SNMP settings by using SupportAssist Enterprise

**Prerequisites**

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

Configuring SNMP settings sets the alert destination of a device, and ensures that alerts from the device are forwarded to the server where SupportAssist Enterprise is installed. If the SNMP settings of a device are not configured, the status column on the **Devices** page displays an appropriate message. You can use the **Configure SNMP** option to automatically configure the SNMP settings of a device.

**NOTE: Configuring SNMP by using SupportAssist Enterprise is not supported on devices running the following operating system and hypervisors:**

- Oracle Enterprise Linux
- VMware ESXi
- Oracle Virtual Machine

### Steps

1. Click **Devices**.

The **Devices** page is displayed.

2. Select the device where you want to configure the SNMP settings.

**NOTE: If SupportAssist Enterprise does not support the configuration of SNMP on the device that you have selected, the Configure SNMP option is disabled.**

The device overview pane is displayed at the right side of the **Devices** page.

3. From the **Tasks** list, select **Configure SNMP**.

The screenshot shows the 'Devices' page with a table of devices and a detailed view of a PowerEdge R200 server. The table lists four devices: RHEL, PowerVault1, compellent, and Networking1, all with a status of 'OK'. The detailed view for the PowerEdge R200 shows various settings like IP address, hostname, service tag, and monitoring options. A dropdown menu is open over the 'Tasks' section, with 'Configure SNMP' highlighted in red.

	Name / IP Address	Model	Status	
<input checked="" type="checkbox"/>	Rhel	PowerEdge R200	OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	OK	11/1/2016 7:46:25 AM
<input type="checkbox"/>	Networking1	Force10 E1200i	OK	11/1/2016 7:46:34 AM

PowerEdge R200

Tasks

- Select Task
- Clear System Event Log
- Check for Cases
- Maintenance Mode
- Enable
- Dependencies
- Install / Upgrade OMSA
- Configure SNMP

Service Tag: 99QLZ1S

Device Type: Server / Hypervisor

Model: PowerEdge R200

Operating System: Red Hat Enterprise Linux Server release 5.9 (Tikanga)

Monitoring:  Enable  Disable

Revalidate:

Collections: No Collections

Next Scheduled Collection: Monday, Nov 7, 2016

Figure 23. Configure SNMP option

The **Status** column on the **Devices** page displays the status of the SNMP configuration.

### Related links

[Support for automatically configuring SNMP settings](#)

## Viewing and updating the contact information

You can update the primary contact details and also provide secondary contact information. If the primary contact is unavailable, Dell will contact your company through the secondary contact. If both the primary and secondary contacts are configured with valid email addresses, both receive SupportAssist Enterprise emails.

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### Steps

1. Point to **Settings** and click **Contact Information**.  
The **Contact Information** page is displayed.
2. Select the type of contact:
  - **Primary**
  - **Secondary**
3. In the contact details section:
  - a. Type or edit the first name, last name, phone number, alternate phone number, and email address.
  - b. Select the preferred contact method.
  - c. Select the preferred contact hours.
  - d. Select the time zone.
4. In the **Parts Dispatch (Optional)** section:
  - a. Type or edit the shipping address and city.
  - b. Select the country.
  - c. Type or edit the state/province/region and zip/postal code.
  - d. For Brazil only: Type the CNPJ and IE numbers.
5. Click **Apply**.



## Configuring proxy server settings

If the server where SupportAssist Enterprise is installed connects to the Internet through a proxy server, you must ensure that the proxy settings are configured in SupportAssist Enterprise. You must also ensure that the proxy server settings are updated in SupportAssist Enterprise, whenever the settings of the proxy server are changed.

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### Steps

1. Point to **Settings** and click **Proxy Settings**.  
The **Proxy Settings** page is displayed.
2. Select **Use Proxy Settings**.  
 **NOTE: SupportAssist Enterprise supports Windows NT LAN Manager (NTLM) and basic proxy authentication protocols.**
3. Type the proxy server IP address or name and port number in the appropriate fields.  
 **NOTE: If the user name and password required to connect to the proxy server are not provided, SupportAssist Enterprise connects to the proxy server as an anonymous user.**
4. If a user name and password are required to connect to the proxy server, select **Proxy requires authentication** and then type the user name and password in the corresponding fields:
  - **User Name** — The user name must contain one or more printable characters, and not exceed 104 characters.
  - **Password** — The password must contain one or more printable characters, and not exceed 127 characters.
5. Click **Apply**.

SupportAssist Enterprise verifies the connection to the proxy server by using the provided proxy server details, and displays a message indicating the connectivity status.

 **NOTE: The proxy settings are saved only if SupportAssist Enterprise is able to connect to the proxy server by using the provided details.**

 **NOTE: If the proxy server is configured to allow anonymous authentication, the credentials you provide for the proxy server are saved, but the credentials are not validated.**

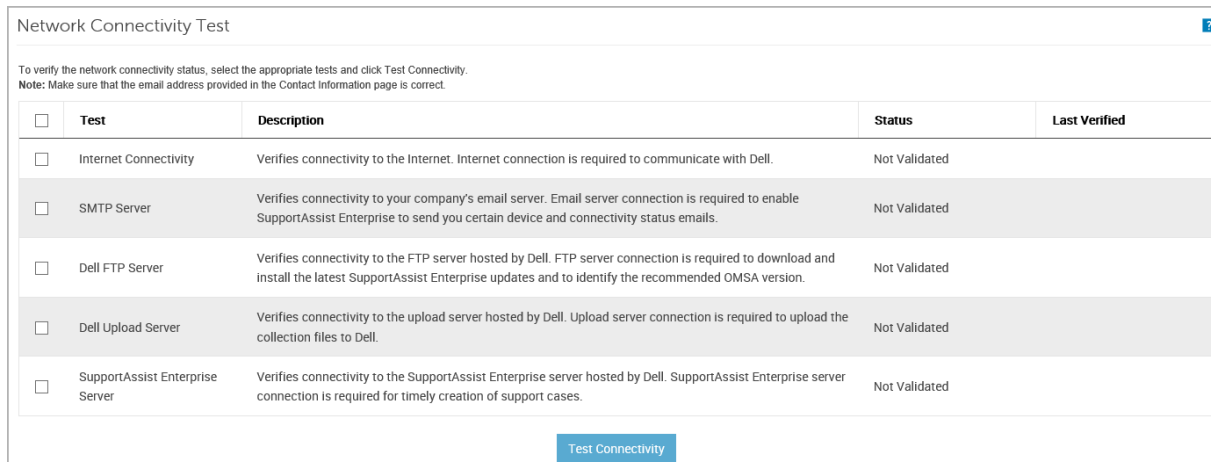
### Related links

[Proxy Settings](#)

## Connectivity test

The **Network Connectivity Test** page enables you to verify and test connectivity status to resources that affect the functionality of SupportAssist Enterprise. You can use the connectivity tests to verify if SupportAssist Enterprise is able to connect successfully to the following resources:

- Internet (including the proxy server, if the server where SupportAssist Enterprise is installed connects to the internet through a proxy server)
- The SMTP server (email server) utilized by your company
- Dell FTP server
- File upload server hosted by Dell
- SupportAssist server hosted by Dell



<input type="checkbox"/>	Test	Description	Status	Last Verified
<input type="checkbox"/>	Internet Connectivity	Verifies connectivity to the Internet. Internet connection is required to communicate with Dell.	Not Validated	
<input type="checkbox"/>	SMTP Server	Verifies connectivity to your company's email server. Email server connection is required to enable SupportAssist Enterprise to send you certain device and connectivity status emails.	Not Validated	
<input type="checkbox"/>	Dell FTP Server	Verifies connectivity to the FTP server hosted by Dell. FTP server connection is required to download and install the latest SupportAssist Enterprise updates and to identify the recommended OMSA version.	Not Validated	
<input type="checkbox"/>	Dell Upload Server	Verifies connectivity to the upload server hosted by Dell. Upload server connection is required to upload the collection files to Dell.	Not Validated	
<input type="checkbox"/>	SupportAssist Enterprise Server	Verifies connectivity to the SupportAssist Enterprise server hosted by Dell. SupportAssist Enterprise server connection is required for timely creation of support cases.	Not Validated	

**Figure 24. Network Connectivity Test page**


By default, SupportAssist Enterprise automatically tests connectivity to the dependent resources every day at 11 p.m. (time as on the server where SupportAssist Enterprise is installed), and displays the result in the **Status** column. If there is an issue with connectivity to a dependent resource, a status email is sent to your primary and secondary SupportAssist Enterprise contacts.

 **NOTE: You can receive the connectivity status email only if you have configured the details of the SMTP server (email server) utilized by your company in SupportAssist Enterprise. See [Configuring the SMTP server settings](#).**

You can also test SupportAssist Enterprise connectivity to the dependent resources at any time. The result of the test is displayed in the **Status** column.


## Viewing the connectivity status

In the SupportAssist Enterprise header area, point to the **user name** link, and then click **Connectivity Test**.

The **Status** column displays the connectivity status to the dependent resources. If an  **Error** status is displayed, click the **Error** link to view a description of the problem and the possible resolution steps.

## Performing the connectivity test

1. In the SupportAssist Enterprise header area, point to the *user name* link, and then click **Connectivity Test**.  
The **Network Connectivity Test** page is displayed.
2. Select the tests that you want to perform.
3. Click **Test Connectivity**.

The **Status** column displays the result of the connectivity test. If an  **Error** status is displayed, click the **Error** link to view a description of the problem and the possible resolution steps.


### Related links

[Network Connectivity Test](#)

## Testing the case creation capability

### About this task

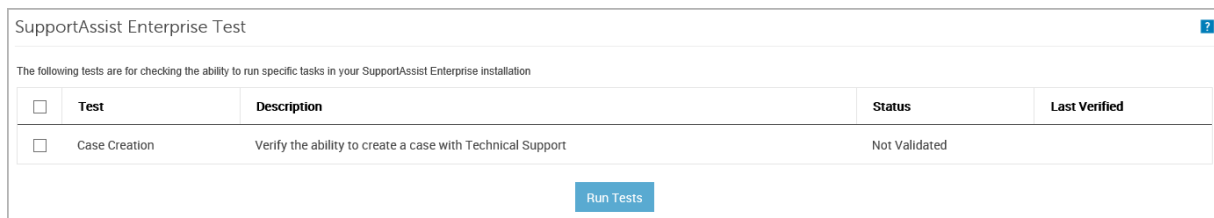
By default, SupportAssist Enterprise automatically verifies the case creation capability every day between 11 p.m. and 4 a.m. (time as on the server where SupportAssist Enterprise is installed). If an issue is identified during the automatic verification of the case creation flow, an alert notification email is sent to your primary and secondary contact.

 **NOTE: The case creation alert notification email is sent only if the SMTP server (email server) settings are configured in SupportAssist Enterprise. See [Configuring SMTP server settings](#).**

You can also use the **Case Creation** test to ensure that support case creation is working prior to an actual alert that would automatically create a support case.

### Steps


1. In the SupportAssist Enterprise header area, point to the *user name* link, and then click **Test SupportAssist Enterprise**.  
The **SupportAssist Enterprise Test** page is displayed.
2. Select the check box for the **Case Creation** test.




<input type="checkbox"/>	Test	Description	Status	Last Verified
<input type="checkbox"/>	Case Creation	Verify the ability to create a case with Technical Support	Not Validated	

Figure 25. Testing case creation

3. Click **Run Tests**.

The **Status** column displays the result of the test. If the test is successful, the  **Ready to Create Cases** status is displayed.

 **NOTE: The case creation alert notification email is sent only on issue detection during the automatic verification of the case creation capability. No alert email notification is sent even if an issue is detected when you run the case creation test manually.**

### Related links

[Test SupportAssist Enterprise](#)

# Clearing the System Event Log (SEL)

## Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

## About this task


The System Event Log (SEL) or hardware log, also known as the Embedded System Management (ESM) log, reports potential hardware problems in Dell PowerEdge servers. You can use the **Clear System Event Log** option available in SupportAssist Enterprise to clear the SEL in the following scenarios:

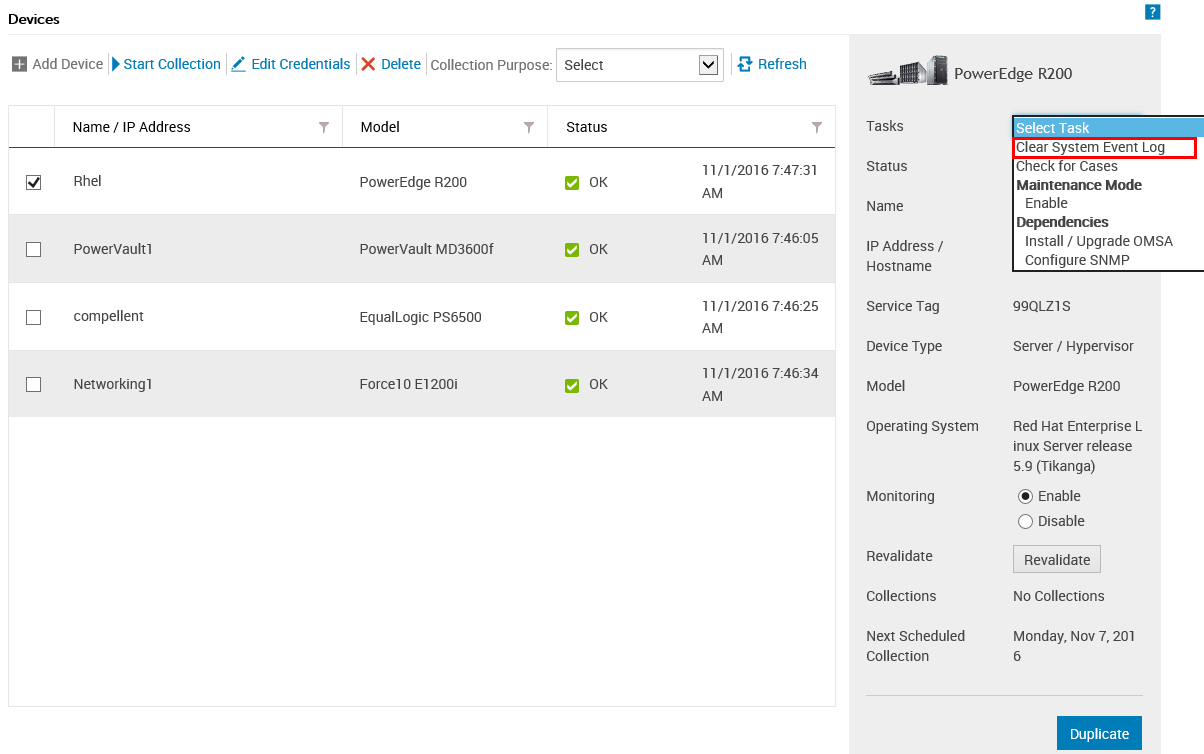
- An error message is displayed on a server even after the problem is resolved.
- An SEL full error message is displayed.

 **CAUTION: Clearing the SEL removes the event history of the server.**

## Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select the server where you want to clear the System Event Log.

 **NOTE: If OMSA is not installed on a device that you have added in SupportAssist Enterprise with the Device Type as Server, the Clear System Event Log option is disabled.**



The screenshot shows the 'Devices' page in SupportAssist Enterprise. At the top, there are buttons for 'Add Device', 'Start Collection', 'Edit Credentials', and 'Delete', along with a 'Collection Purpose' dropdown and a 'Refresh' button. Below this is a table with the following data:


	Name / IP Address	Model	Status	
<input checked="" type="checkbox"/>	Rhel	PowerEdge R200	OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	OK	11/1/2016 7:46:25 AM
<input type="checkbox"/>	Networking1	Force10 E1200i	OK	11/1/2016 7:46:34 AM

On the right side, the 'PowerEdge R200' device overview pane is displayed. It includes a 'Tasks' section with a 'Select Task' dropdown menu. The dropdown menu is open, showing options: 'Clear System Event Log' (highlighted with a red box), 'Check for Cases', 'Maintenance Mode', and 'Enable'. Below this, various device details are shown, including 'Service Tag', 'Device Type', 'Model', 'Operating System', 'Monitoring' (with 'Enable' selected), 'Revalidate' button, 'Collections', and 'Next Scheduled Collection'.

**Figure 26. Clear System Event Log option**

The device overview pane is displayed at the right side of the **Devices** page.

3. From the **Tasks** list, select **Clear System Event Log**.

While the SEL is cleared from a device, the device displays a  **Clearing System Event Log** status in SupportAssist

Enterprise. After the SEL is cleared successfully, the device displays a  **System Event Log cleared** status.

# Automatic update

The types of SupportAssist Enterprise updates that are available is as follows:

- **SupportAssist Enterprise application** update — Upgrades the SupportAssist Enterprise application with additional capability, protocol support, usability enhancements, and patches to fix existing issues.
- **Policy files** update — Defines SupportAssist Enterprise alert handling and case creation. By updating this file, SupportAssist Enterprise will have optimized case management as per the latest Dell definitions.
- **Product support files** update — Defines the Dell devices and operating systems that are compatible with SupportAssist Enterprise. By updating this file, SupportAssist Enterprise will be able to connect to, and collect data from more device models.

By default, automatic update is enabled for the SupportAssist Enterprise application, policy files, and product support files. This ensures that SupportAssist Enterprise is automatically updated whenever an update is available. You can choose to enable or disable the automatic update of a specific component based on your preference. For instructions to enable or disable automatic updates, see [Enabling or disabling automatic updates](#).

 **NOTE: Dell recommends that you enable automatic update to ensure that SupportAssist Enterprise is up-to-date with the latest features and enhancements.**

The SupportAssist Enterprise application checks if any updates are available, every Monday at 11 a.m. (date and time as on the server where SupportAssist Enterprise is installed):

- If updates are available and automatic updates are enabled, the updates are downloaded and automatically installed in the background.
- If updates are available, but automatic update is disabled, the **update available** banner is displayed at the top of the page. You can click **Update now** to allow SupportAssist Enterprise to download and install the latest updates.

 **NOTE: After the updates are downloaded and installed, an update successful message is displayed. To view and use the latest updates and enhancements, you must refresh the SupportAssist Enterprise user interface.**

Information about the SupportAssist Enterprise update is logged in the log file available at the following location based on the operating system where SupportAssist Enterprise is installed:

- On Windows — C:\Program Files\Dell\SupportAssist\logs
- On Linux — /opt/dell/supportassist/logs

## Enabling or disabling automatic updates

Enabling automatic updates ensures that SupportAssist Enterprise is automatically updated whenever updates are available.

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### Steps

1. Point to **Settings** and click **Preferences**.  
The **Preferences** page is displayed.
2. In **Automatically update the following features in SupportAssist Enterprise**, select or clear the options that you want to enable or disable.
3. Click **Apply**.

### Related links

[Preferences](#)

## Deleting a device

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

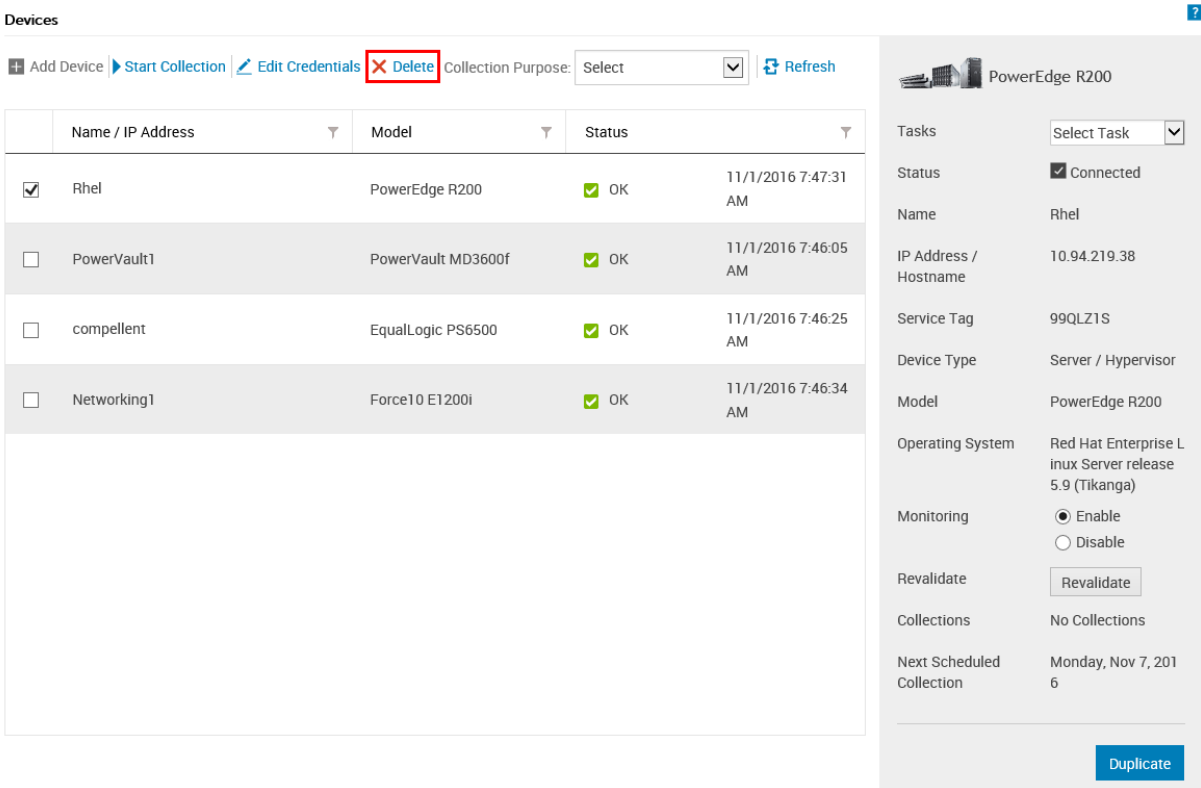
## About this task

You can delete a device from SupportAssist Enterprise, if you do not want to monitor a device or for other reasons.

 **NOTE: Deleting a device only removes the device from the SupportAssist Enterprise user interface; it does not affect the functionality of the device.**

## Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select the device that you want to delete.
3. Click **Delete**.



The screenshot shows the 'Devices' management interface. At the top, there are navigation links: 'Add Device', 'Start Collection', 'Edit Credentials', and 'Delete' (highlighted with a red box). A 'Collection Purpose' dropdown menu is set to 'Select', and a 'Refresh' button is present. Below this is a table of devices:


	Name / IP Address	Model	Status	
<input checked="" type="checkbox"/>	Rhel	PowerEdge R200	<input checked="" type="checkbox"/> OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:25 AM
<input type="checkbox"/>	Networking1	Force10 E1200i	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:34 AM

On the right, a detailed view for a 'PowerEdge R200' device is shown. It includes a 'Tasks' dropdown (set to 'Select Task'), a 'Status' indicator (Connected), and various system details: Name (Rhel), IP Address / Hostname (10.94.219.38), Service Tag (99QLZ1S), Device Type (Server / Hypervisor), Model (PowerEdge R200), Operating System (Red Hat Enterprise Linux Server release 5.9 (Tikanga)), Monitoring (Enable selected), Revalidate button, Collections (No Collections), and Next Scheduled Collection (Monday, Nov 7, 2016). A 'Duplicate' button is located at the bottom right of this panel.

**Figure 27. Delete option**

The **Confirm Device Deletion** window is displayed.

4. Click **Yes**.  
The device is deleted from the **Devices** page.

 **NOTE: When a device is deleted, the credentials of the device are deleted immediately from SupportAssist Enterprise. However, the system information collected from the device is not deleted until the purge collections task deletes the collected system information. The purge collection task only deletes system information collections that are 30 days or older and collections that are older than the last 5 collections over the last 30 days.**

## Opting in or opting out from ProSupport Plus server recommendation report emails

### Prerequisites


- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).
- Ensure that you have completed the registration of SupportAssist.

- The local system must have internet connectivity for uploading the collected system information to Dell.

### About this task

The ProSupport Plus server recommendation reports provide an overall health assessment of your Dell servers by comparing the BIOS, firmware, and selected device drivers with the Dell recommended versions. SupportAssist Enterprise provides you an option to either opt in or opt out from receiving Dell ProSupport Plus recommendation reports through email. When you opt in to receive the ProSupport Plus server recommendation reports through email, you will receive the report once every month.

 **NOTE: The ProSupport Plus server recommendation reports are applicable only for devices with an active ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract.**

 **NOTE: The server recommendation reports are dependent on the system information that is collected and sent to Dell periodically. Therefore, you must ensure that the periodic collection of system information is enabled in SupportAssist Enterprise. For information on enabling the periodic collection of system information, see [Enabling or disabling the periodic collection of system information from all devices](#).**

### Steps

1. Point to **Settings** and click **Preferences**.

The **Preferences** page is displayed.

2. In **Recommendation Report Settings**, select or clear the **Automatically receive recommendation reports via email** option to opt in or opt out from receiving ProSupport Plus server recommendation reports through email.

 **NOTE: By default, the Automatically receive recommendation reports via email option is selected.**

3. Click **Apply**.

# Configuring email notifications

By default, Dell EMC SupportAssist Enterprise is configured to send an email notification when a support case is created automatically. SupportAssist Enterprise can also send email notifications about maintenance mode, device status, and network connectivity status, if the SMTP server (email server) settings are configured. You can configure the email notification settings based on your preference. For example, you can:

- Disable the case creation email notification and/or select the preferred language for email notifications. See [Configuring email notification settings](#).
- Configure SupportAssist Enterprise to send email notifications through the SMTP server (email server) utilized by your company. See [Configuring SMTP server settings](#).

 **NOTE:** For information about the different types of SupportAssist Enterprise email notifications, see [Types of email notifications](#).

## Configuring email notification settings

You can enable or disable automatic email notifications from SupportAssist Enterprise and also select the preferred language for email notifications.

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### Steps

1. Point to **Settings** and click **Preferences**.  
The **Preferences** page is displayed.
2. To receive email notifications when a new support case is opened, in **Email Settings**, select **Receive email notification when a new support case is opened**.

 **NOTE:** Disabling support case email notifications also disables the automatic email notifications that are sent if an issue occurs while:

- Creating a support case
- Collecting the system information from a device
- Sending the system information from a device to Dell

3. To set the language in which you want to receive email notifications, from the **Preferred Email Language** list, select a language.

 **NOTE:** The Preferred Email Language is enabled only when the Receive email notification when a new support case is opened option is selected.

4. Click **Apply**.

### Related links

[Preferences](#)

## Configuring SMTP server settings

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

If your company utilizes an SMTP server (email server), Dell recommends that you configure the SMTP server settings in SupportAssist Enterprise. Configuring the SMTP server settings enables SupportAssist Enterprise to send maintenance mode, device status, and network connectivity status email notifications through the SMTP server.

 **NOTE: You will not receive certain device status and connectivity status email notifications in the following situations:**

- The SMTP server settings are not configured in SupportAssist Enterprise.
- The SMTP server credentials (user name and password) you have provided in SupportAssist Enterprise are incorrect.
- If you have configured SupportAssist Enterprise to send email notifications over Secure Socket Layer (SSL), but the SSL certificate of the SMTP server has expired.
- The SMTP server port configured in SupportAssist Enterprise is blocked by any other application.

### Steps

1. Point to **Settings** and click **SMTP Settings**.  
The **SMTP Settings** page is displayed.
2. Select **Enable Email Notification**.
3. Provide the following information in the corresponding fields:
  - **Host Name/IP address** — the host name or the IP address of the SMTP server
  - **Port** — the port number of the email server
4. If the SMTP server requires authentication for sending emails, select **Requires authentication**.
5. Type the user name and password in the corresponding fields.
6. To send email notifications securely, select **Use SSL**.
7. Click **Apply**.

### Related links




[SMTP Settings](#)

## Types of email notifications

The following table provides a summary of the different types of email notifications that are sent by SupportAssist Enterprise.

**Table 7. Types of email notifications**

Email notification type	When the email notification is sent	Origin of the email notification
Registration confirmation and welcome email	After the <b>Registration</b> step of the <b>SupportAssist Enterprise Registration Wizard</b> is completed successfully.	SupportAssist server hosted by Dell
Case created	After a hardware issue is detected and a support case is created.	SupportAssist server hosted by Dell
Unable to create a case	After a hardware issue is detected, but a support case could not be created because of technical difficulties.	SupportAssist server hosted by Dell
Unable to collect system information	After a support case is created automatically for a device, but SupportAssist Enterprise is unable to collect system information from the device.	SupportAssist server hosted by Dell
Unable to send the collected system information to Dell	After a support case is created automatically for a device, but SupportAssist Enterprise is unable to send the collected system information from the device to Dell.	SupportAssist server hosted by Dell

Email notification type	When the email notification is sent	Origin of the email notification
Inactive notification	If SupportAssist Enterprise is not monitoring any device and no device has been added in the past 30 days.	SupportAssist server hosted by Dell
Connectivity test alert	<p>At 11 p.m. each day (date and time as on the server where SupportAssist Enterprise is installed).</p> <p> <b>NOTE: The connectivity test alert notification is sent only if an issue is detected with connectivity to dependent resources.</b></p>	SupportAssist Enterprise application
Automatic maintenance mode	If an alert storm received from a device has resulted in SupportAssist Enterprise placing the device automatically in maintenance mode.	SupportAssist Enterprise application
Device status alert	<p>At 5 p.m. each day (date and time as on the server where SupportAssist Enterprise is installed). If less than 10 devices have issues, the email includes details about the issues and the possible resolution steps. If more than 10 devices have issues, the email only includes a summary of the issues.</p> <p> <b>NOTE: The device alert notification is sent only if an issue exists (warning or error status) with the setup or configuration of the devices.</b></p>	SupportAssist Enterprise application
Case creation connectivity alert	<p>Between 11 p.m. and 4 a.m. each day (date and time as on the server where SupportAssist Enterprise is installed).</p> <p> <b>NOTE: The case creation connectivity alert notification is sent only if an issue is detected with connectivity to dependent resources.</b></p>	SupportAssist Enterprise application

 **NOTE:** Email notifications originating from the SupportAssist server hosted by Dell can be received only if the Receive email notification when a new support case is opened option is selected. See [Configuring email notification settings](#).

 **NOTE:** Email notifications originating from the SupportAssist Enterprise application can be received only if the SMTP server (email server) settings are configured in SupportAssist Enterprise. See [Configuring SMTP server settings](#).

# Configuring data collection settings

By default, when registration is complete, Dell EMC SupportAssist Enterprise automatically collects system information from all devices at periodic intervals. SupportAssist Enterprise also collects system information automatically from a device when a support case is created for an issue with the device. If required, you can configure the data collection options based on your preference. For example, you can:

- Disable the automatic collection of system information from devices when a support case is created or updated. See [Enabling or disabling the automatic collection of system information on case creation](#).
- Disable the periodic collection of system information from all devices. See [Enabling or disabling the periodic collection of system information from all devices](#).
- Customize the schedule for periodic collection of system information. See [Customizing the schedule for periodic collection of system information](#).
- Disable the periodic collection of system information from specific devices. See [Disabling the periodic collection of system information from specific devices](#).
- Disable the collection of identity information from all devices. See [Enabling or disabling the collection of identity information](#).
- Disable the collection of software information and the system log from all devices. See [Enabling or disabling the collection of software information and the system log](#).

## Prerequisites for collecting system information

The following are the SupportAssist Enterprise prerequisites for collecting system information:

- The local system (server where SupportAssist Enterprise is installed) must have sufficient hard drive space to save the collected system information. For information on the hard-drive space requirements, see [Hardware requirements](#).
- For collecting system information from a remote devices, the remote devices must be reachable from the local system.
- The local system and remote devices (devices you have added in SupportAssist Enterprise) must meet the network port requirements. For information on the network port requirements, see [Network requirements](#).
- If you have added a server in SupportAssist Enterprise by using the operating system IP address or host name (agent-based monitoring):
  - The server must preferably have Dell OpenManage Server Administrator (OMSA) installed.
  - If the server is running a Windows operating system:
    - \* The device credentials you have entered in SupportAssist Enterprise must have administrative privileges.
    - \* The device credentials must have privileges required for Windows Management Instrumentation (WMI) communication. For information on ensuring WMI communication, see the “Securing a Remote WMI Connection” technical documentation at [msdn.microsoft.com](http://msdn.microsoft.com).
  - If the server is running a Linux operating system:
    - \* The device credentials you have entered in SupportAssist Enterprise must have administrative privileges.
    - \* If you have entered the credentials of a sudo user, the sudo user must be configured for SupportAssist Enterprise. For information on configuring the sudo user, see [Configuring sudo access for SupportAssist Enterprise \(Linux\)](#).
    - \* No resource (network share, drive, or ISO image) 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 on OpenSSL, see the resolution for *OpenSSL CCS injection vulnerability (CVE-2014-0224)* available in the support website of the operating system.

 **NOTE: If the server you have added for agent-based monitoring does not have OMSA installed, periodic collections from the device will not include storage and system details.**

- If you have added a server in SupportAssist Enterprise by using the iDRAC IP address (agentless monitoring), the iDRAC credentials that you entered must have administrator privileges.
- The local system must have internet connectivity for uploading the collected system information to Dell.

## Enabling or disabling the automatic collection of system information on case creation

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

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

 **NOTE: To receive the full benefits of the support, reporting, and maintenance offering of the ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract for a device, automatic collection of system information must be enabled.**

### Steps

1. Point to **Settings** and click **Preferences**.  
The **Preferences** page is displayed.
2. In **Automatically collect system state information**, depending on your requirement, select or clear the **When a new support case is created** option.

 **NOTE: By default, the When a new support case is created option is selected.**

3. Click **Apply**.

### Related links

[Preferences](#)

## Enabling or disabling the periodic collection of system information from all devices


### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

By default, SupportAssist Enterprise collects system information from all monitored devices at periodic intervals and sends it securely to Dell. If required, you can enable or disable the periodic collection of system information from all monitored devices based on your preference.

 **NOTE: To receive the ProSupport Plus server recommendation report by email, periodic collection of system information must be enabled.**

 **NOTE: If you do not want SupportAssist Enterprise to collect system information from a specific device type, you can disable scheduling for that specific device type through the Collection Schedules page. For more information, see [Disabling the periodic collection of system information from specific devices](#).**

### Steps

1. Point to **Settings** and click **Preferences**.  
The **Preferences** page is displayed.
2. In **Automatically collect system state information**, depending on your requirement, select or clear the **On a regular schedule as specified in Collection Schedules** option.

 **NOTE:** By default, the **On a regular schedule as specified in Collection Schedules** option is selected.

3. Click **Apply**.

#### Related links

[Preferences](#)

## Customizing the schedule for periodic collection of system information

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).
- Ensure that the **On a regular schedule as specified in Collection Schedules** option is selected in the **Preferences** page.

### About this task

By default, SupportAssist Enterprise is scheduled to collect system information from all monitored devices at periodic intervals and send it securely to Dell. For information about the default frequency for collection of system information, see [Default schedule for collection of system information](#). If required, you can customize the schedule for periodic collection of system information from devices based on your preference.

 **NOTE:** The performance of the server where SupportAssist Enterprise is installed may be affected when running periodic collections on a large number of devices. Therefore, Dell recommends that you schedule the periodic collection during off-peak hours.

### Steps

1. Point to **Settings** and click **Collection Schedules**.  
The **Collection Schedules** page is displayed.
2. From the **Device Type** list, select a device type for which you want to configure the periodic collection schedule.
3. From the **Recurs Every** list, select the frequency of collection.

 **NOTE:** If you want to disable the periodic collection for the selected device type, from the **Recurs Every** list, select **None**.

4. In the **Specify day and time** fields, select an appropriate schedule.
5. Repeat steps 2 to step 4 until you have scheduled the periodic collection of system information for all device types.
6. Click **Apply**.

#### Related links

[Collection Schedules](#)

## Default schedule for collection of system information

By default, SupportAssist Enterprise automatically collects and sends system information from your devices to Dell at periodic intervals and also when a support case is created. The following table provides the default schedule for the collection of system information from various device types.

**Table 8. Default collection schedule**

Device type	Default collection schedule
Chassis	Monthly; First Monday of the month at 12:00 AM
Fluid File System (FluidFS)	Monthly; First Monday of the month at 12:00 AM
iDRAC	Monthly; First Monday of the month at 12:00 AM
Networking	Monthly; First Monday of the month at 12:00 AM
Peer Storage (PS) / EqualLogic	Monthly; First Monday of the month at 12:00 AM
PowerVault	Monthly; First Monday of the month at 12:00 AM

Device type	Default collection schedule
Server / Hypervisor	Monthly; First Monday of the month at 12:00 AM
Storage Center (SC) / Compellent	Monthly; First Monday of the month at 12:00 AM

## Disabling the periodic collection of system information from specific devices

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

By default, SupportAssist Enterprise collects system information from all your devices at periodic intervals and sends it securely to Dell. If required, you can disable the periodic collection of system information from devices of a specific type. For example, you can disable the periodic collection of system information from all your Dell servers.

 **NOTE: Disabling the collection schedule for a specific device type only disables the periodic collection of system information from those devices. It does not disable SupportAssist Enterprise from collecting and sending the system information to Dell, if a support case is opened for those devices.**

### Steps

1. Point to **Settings** and click **Collection Schedules**.

The **Collection Schedules** page is displayed.

2. From the **Device Type** list, select a device type for which you want to disable the periodic collection schedule.
3. From the **Recurs Every** list, select **None**.
4. Click **Apply**.

The following message is displayed `Collection scheduling is turned off for the current Device Type.`

## Enabling or disabling the collection of identity information

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task


The system information that is collected by SupportAssist Enterprise includes identity information (PII) such as the complete configuration snapshot of systems, hosts, and network devices that can contain host identification and network configuration data. In most cases, part or all of this data is required to properly diagnose issues. If the security policy of your company restricts sending identity data outside of the company network, you can configure SupportAssist Enterprise to filter such data from being collected and sent to Dell.

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 — host World Wide Name (WWN) and port WWN

 **NOTE:** When the **Include identification information in collections** option is cleared, some of the data about your company network (including the system log) is not transmitted to Dell. This may impede Dell Technical Support from resolving issues that may occur on your devices.

 **NOTE:** If your devices have an active ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract, when the **Include identification information in data sent to Dell** option is disabled, you will not receive some reporting information about your devices.


### Steps


1. Point to **Settings** and click **Preferences**.

The **Preferences** page is displayed.

2. In **Identification Information Settings**, depending on your requirement, select or clear the **Include identification information in data sent to Dell** option.

 **NOTE:** By default, the **Include identification information in data sent to Dell** option is selected.

 **NOTE:** If you clear the **Include identification information in data sent to Dell** option, the settings for collection of logs, diagnostic data, and support data are also cleared automatically. Therefore, logs and diagnostic data are not sent to Dell when you disable sending the identity information.

 **NOTE:** If you have disabled the collection of identity information from devices, the identity information is replaced by tokenized values in the collected data. The tokenized values are represented as TOKEN*n*—for example, TOKEN0, TOKEN1, or TOKEN2.

3. Click **Apply**.

### Related links

[Preferences](#)

## Enabling or disabling the collection of software information and the system log

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

By default, the data that is collected and sent to Dell by SupportAssist Enterprise includes software information and system logs. If required, you can configure SupportAssist Enterprise to exclude the collection of software information and system logs from all devices.

### Steps

1. Point to **Settings** and click **Preferences**.

The **Preferences** page is displayed.

2. In **Collection Data Settings**, select or clear the available options for each device type.

 **NOTE:** By default, all **Collection Data Settings** options are selected.

 **NOTE:** For information on the logs that are collected by SupportAssist Enterprise, see the *Dell SupportAssist Enterprise Version 1.0 Reportable Items* document at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

3. Click **Apply**.

# Viewing collections


Dell EMC SupportAssist Enterprise collects system information from each device you have added and sends the information securely to Dell. Typically, the system information is collected as follows:

- Periodically — At regular intervals, depending on the configured collection schedule. For information on the default collection schedule, see [Default schedule for collection of system information](#).
- On case creation — When a support case is created for an issue that has been identified by SupportAssist Enterprise.
- Manual (on demand) — If requested by Dell Technical Support, you can initiate the collection of system information from one or more devices at any time.

 **NOTE: By default, SupportAssist Enterprise collects data periodically and on case creation only when the registration is completed. For more information on registration, see [Registering SupportAssist Enterprise](#).**

You can also use SupportAssist Enterprise to collect and send system information from multiple devices to Dell. For more information on collecting system information from multiple devices, see [Starting a multiple device collection](#).

The collected system information is saved in a secured database on the server where SupportAssist Enterprise is installed. You can access the collected system information from the **Devices** or **Collections** page. The data available in a collection is displayed in the **Configuration Viewer** that is available in SupportAssist Enterprise.

 **NOTE: You can only view the last 5 system information collections through the Configuration Viewer. 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. The purge collections task runs automatically every day at 10 p.m. (time as on the server where SupportAssist Enterprise is installed).**

 **NOTE: The Configuration Viewer does not support viewing the data collected from storage devices with Fluid File System (FluidFS).**

## Viewing a collection from the Devices page

### About this task

The device overview pane lists the collections that have been performed on a specific device. To view a collection from a specific device, select the device and then select a collection from the device overview pane.

### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select the device for which you want to view collections.  
The device overview pane is displayed at the right side of the **Devices** page.
3. From the **Collections** list, select a collection date and time.

Devices ?

+ Add Device | [▶ Start Collection](#) | [✎ Edit Credentials](#) | [✖ Delete](#) | Collection Purpose: Select | [↻ Refresh](#)

	Name / IP Address	Model	Status	
<input checked="" type="checkbox"/>	Rhel	PowerEdge R200	<input checked="" type="checkbox"/> OK	11/1/2016 7:47:31 AM
<input type="checkbox"/>	PowerVault1	PowerVault MD3600f	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:05 AM
<input type="checkbox"/>	compellent	EqualLogic PS6500	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:25 AM
<input type="checkbox"/>	Networking1	Force10 E1200i	<input checked="" type="checkbox"/> OK	11/1/2016 7:46:34 AM

**PowerEdge R200**

Tasks: Select Task

Status:  Connected

Name: Rhel

IP Address / Hostname: 10.94.219.38

Service Tag: 99QLZ1S

Device Type: Server / Hypervisor

Model: PowerEdge R200

Operating System: Red Hat Enterprise Linux (Tikanga) 5.9

Monitoring:  Enable /  Disable

Revalidate: Revalidate

Collections: Select collection

Next Scheduled Collection: 6

Duplicate

**Figure 28. Selecting a collection**

If the device is a server, the **Configuration Viewer** is displayed in a new web browser window. For storage, networking, or chassis, you are prompted to save the collection as a **.zip** file. To view the collection, you can extract the **.zip** file and click the **index.html** file.

## Viewing a collection from the Collections page

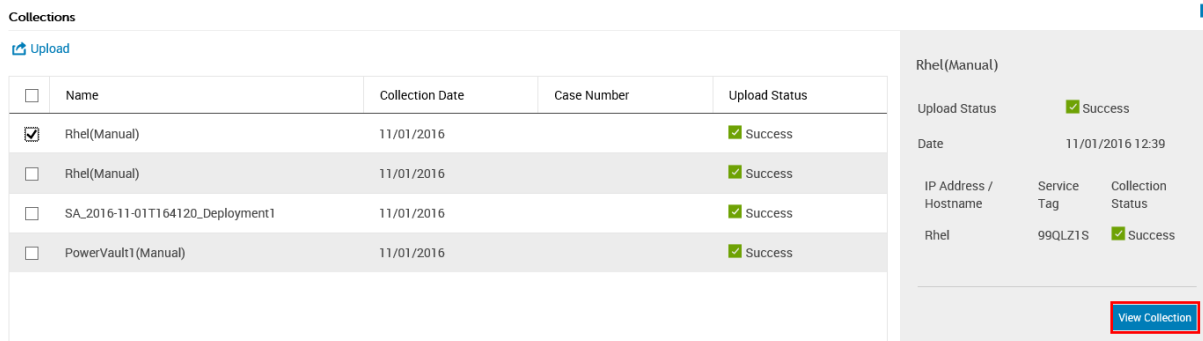
### About this task

The **Collections** page lists all the collections that have been performed successfully. From the list of collections, you can select any available collection that you want to view. You can identify whether the collection is either a single or multiple device collection based on the collection name.

- Collections from a single device are named in the following format: `device name (collection type)`. If the device name is not available, the collection name contains the IP address or hostname of the device.
- Multiple device collections are named in the following format: `SA_yyyy-mm-dd_unique identifier_collection name`

### Steps

1. Click **Collections**.  
The **Collections** page is displayed.
2. Select a collection that you want to view.



**Figure 29. View Collection option**

The collection overview pane is displayed.

3. Click **View Collection** (server only) or **Download Collection** (storage, networking, chassis, and multiple device).

If the collection is from a server, the **Configuration Viewer** is displayed in a new web browser window. For collections from storage, networking, chassis, and multiple devices, you can download and save the collection as a **.zip** file. To view the collection, you can extract the **.zip** file and click the **index.html** file.

## Configuration Viewer

The **Configuration Viewer** enables you to view the data collected by SupportAssist Enterprise from your devices. The title bar of the **Configuration Viewer** displays the date of the collection and the Service Tag of the device. The collected data is displayed in the **Configuration Viewer** under various categories and sub categories. In addition, the **Configuration Viewer** displays a **Summary** category. You can select the **Summary** category to view the following:

- The data collection settings in SupportAssist Enterprise at the time of the collection
- Summary of errors that were detected in the collected data
- Brief information about the device

The layout of the **Configuration Viewer** is as follows:

User interface	Description
<b>Left pane</b>	Displays the various categories and sub categories of data in an expanded tree format. A category may display a warning or critical icon to indicate the health status roll-up of its subcategories. When you can click a category, the category is expanded, enabling you to view its sub categories. You can click <b>Expand All</b> or <b>Collapse All</b> to quickly expand or collapse all categories.
<b>Divider</b>	Is displayed between the left and right panes. You can click and drag the divider to the left or right to increase or decrease the viewable area of the right pane. You can also hide the left pane if necessary. To hide the left pane, click the <b>&lt;</b> icon that is displayed at the top of the divider. To view the left pane again, click the <b>&gt;</b> icon that is displayed at the top of the divider.
<b>Right pane</b>	Displays the data available for the category or subcategory that is selected in the left pane. This pane includes a navigation trail, which you can click to navigate backward on the current trail.




The screenshot shows the Configuration Viewer interface for a PowerEdge R520 server. The left sidebar contains a tree view of system components, including Main Chassis, BIOS, Battery, Processor(s), Fans, Fan Redundancy, Firmware, Front Panel, FRU, Intrusion, Memory Array, Network(s), and Power Supplies. The main area displays a 'Summary' page for the server IP 10.94.100.203. The page includes a 'Collection Settings' table, an 'Error Summary' table, and a 'Main Chassis' table. The 'Collection Settings' table has columns for Options, Identification Shared With Dell, Mode, and Source. The 'Error Summary' table has columns for Status, Name, and Location. The 'Main Chassis' table has columns for Server Model, Server Service Tag, Express Service Code, Chassis Lock, and Server Asset Tag.

Options	Identification Shared With Dell	Mode	Source
Hardware, Software, Logs	Yes	On Demand	SupportAssist

Status	Name	Location
⊘	HardwareLog [2 critical]	<a href="#">HardwareLog</a>
⊘	PowerSupply	<a href="#">PS2_Status</a>

Server Model	Server Service Tag	Express Service Code	Chassis Lock	Server Asset Tag
PowerEdge R520	HFB2X02	37930904210	Present	Unknown

Figure 30. Configuration Viewer

-  **NOTE:** If you have disabled the collection of identity information from devices, the identity information is replaced by tokenized values in the collected data. The tokenized values are represented as TOKEN $n$ —for example, TOKEN0, TOKEN1, or TOKEN2.
-  **NOTE:** For a list of items that may be reported in the collected data, see [Items reported in periodic collections from servers](#).
-  **NOTE:** The Configuration Viewer does not support viewing the data collected from storage devices with Fluid File System (FluidFS).

## Data views

By default, the data for a selected category or sub category is displayed in a grid format. For some categories, a grid may present several columns or rows of data. When the data is presented either in more than 4 columns or less than 50 rows, the **Grid View** and **List View** toggle options are displayed at the top-right of the data display area. The **Grid View** and **List View** toggle options enable you to view the data efficiently by transposing the displayed data as follows:

- **Grid View** (default) — When the data is displayed in **List View**, selecting this option transposes the displayed data from rows to columns
- **List View** — When the data is displayed in **Grid View**, selecting this option transposes the displayed data from columns to rows


-  **NOTE:** If multiple grids are displayed for a selected category, the **Grid View** and **List View** selections are applied only on those grids that present data in either more than 4 columns or less than 50 rows.

To toggle the views, click at the appropriate side of the slider.

## Log types

You can use the configuration viewer to access two types of logs from the system information that is collected by SupportAssist Enterprise:

Log types	Description
Structured logs	Contain application logs, Embedded Server Management (ESM) logs, and event logs. When you click the <b>Structured Logs</b> category, the configuration viewer displays the list of available structured logs. You can click any of the listed structured logs to view the details of the log in a new web browser window.

Log types	Description
Unstructured logs	Contain a snapshot of the system files such as the Remote Access Controller (RAC) logs, Windows event logs, and other logs. When you click the <b>Unstructured Logs</b> category, the configuration viewer displays the list of available unstructured logs.
	 <b>NOTE: Unstructured logs cannot be viewed within the configuration viewer. You can only save the unstructured logs and view the log details using an appropriate application.</b>


## Items reported in periodic collections from servers

The items reported in the data collected from servers vary depending on the following:

- **Device Type** used to add the device in SupportAssist Enterprise
- Type of collection (manual, periodic, or support case)

The following table provides a summary of the items reported in the collected data for a periodic collection from servers.

 **NOTE: Data in a collection that is performed due a support case creation and a manually-initiated collection is more detailed in comparison with the data collected in a periodic collection. For the complete list of items that are collected by SupportAssist Enterprise, see the *Dell SupportAssist Enterprise Version 1.0 Reportable Items* document at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).**

 **NOTE: Data from periodic collections enables Dell to provide you an insight into your company's as-maintained environment configuration with proactive firmware recommendations and other reports.**

**Table 9. Items reported in periodic collections from servers**

Items reported	Device added in SupportAssist Enterprise with Device Type as Server / Hypervisor		Device added in SupportAssist Enterprise with the Device Type as iDRAC
	OMSA is installed on the device	OMSA is not installed on the device	
Memory	✓	✗	✓
Memory Array	✓	✗	✓
Memory Operating Mode	✓	✗	✗
Memory Redundancy	✓	✗	✗
Slot	✓	✗	✓
Controller	✓	✗	✓
Connector	✓	✗	✗
PCIe-SSD-Extender	✓	✗	✓
Enclosure	✓	✗	✓
Array Disk	✓	✗	✓

Items reported	Device added in SupportAssist Enterprise with Device Type as Server / Hypervisor		Device added in SupportAssist Enterprise with the Device Type as iDRAC
	OMSA is installed on the device	OMSA is not installed on the device	
Intrusion Switch	✓	✗	✓
Hardware Log	✓	✗	✓
Main Chassis	✓	✗	✓
Additional Information	✓	✗	✓
Modular Enclosure Information	✓	✗	✓
Firmware	✓	✗	✓
Processor	✓	✗	✓
Fan	✓	✗	✓
Fan Redundancy	✓	✗	✓
Temperature	✓	✗	✓
Voltage	✓	✗	✓
Power Supply	✓	✗	✓
Power Supply Redundancy	✓	✗	✓
Network	✓	✗	✓
IPv4 Address	✓	✗	✗
IPv6 Address	✓	✗	✗
Network Team Interface	✓	✗	✗
Interface Member	✓	✗	✗
Remote Access Device	✓	✗	✓
DRAC Information	✓	✗	✗
Serial Over LAN Configuration	✓	✗	✓

Items reported	Device added in SupportAssist Enterprise with Device Type as Server / Hypervisor		Device added in SupportAssist Enterprise with the Device Type as iDRAC
	OMSA is installed on the device	OMSA is not installed on the device	
IPv6 Detail	✓	✗	✗
User Setting	✓	✗	✓
User Information	✓	✗	✓
iDRAC User Privilege	✓	✗	✓
DRAC User Privilege	✓	✗	✗
Serial Port Configuration	✓	✗	✓
NIC Configuration	✓	✗	✓
Component Detail	✓	✗	✓
Controller TTY Log	✓	✗	✓
Operating System	✓	✓	✗

 **NOTE:** In a collection from an iDRAC, Controller TTY Log is available only if iDRAC firmware version 2.00.00.00 or later installed on the server.

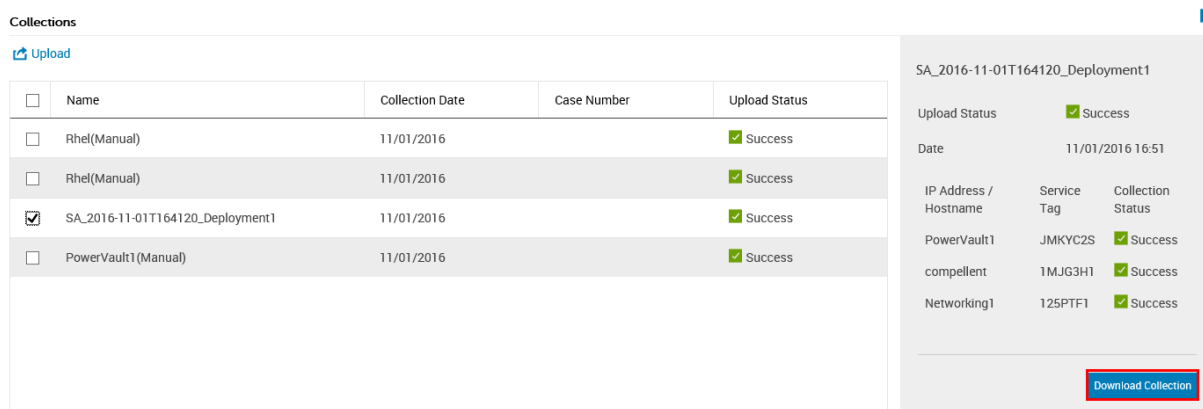
## Downloading and viewing a multiple device collection

### About this task

You can also view data available in the multiple device collections that you have performed. To view a multiple device collection, you must download the multiple device collection and open the collection by using a web browser.

### Steps

1. Click **Collections**.  
The **Collections** page is displayed.
2. Select a multiple device collection that you want to view.



**Figure 31. Download Collection option**

The collection overview pane is displayed.

**3. Click **Download Collection**.**

You are prompted to open or save the collection file.

**4. Save the collection file.**

**5. Extract the multiple device collection .zip file.**

**6. Open the folder where you extracted the collection file.**

**7. Double-click the **index.html** file.**

The multiple device configuration viewer opens in a new web browser window. You can view data collected from each device by accessing the device type menu.

## Multiple device configuration viewer

The multiple device configuration viewer displays information in a tabbed format. The **Contacts** tab is the default tab of the multiple device configuration viewer. The **Contacts** tab displays the case details, customer information, and collection details.

Depending on the device types from which the collection was performed, the multiple device configuration viewer may display the following tabs:

- **Server** — If the collection includes data from a server
- **Storage** — If the collection includes data from a storage device
- **Networking** — If the collection includes data from a network device
- **Chassis** — If the collection includes data from a chassis

To access the data collected from a specific device, point to the device type tab and click the device from the menu that is displayed. The data collected from a device is displayed as categories and subcategories. Click a category to expand or collapse the category. The data available in a category can be viewed when the category is expanded. You can click **Expand All** or **Collapse All** to quickly expand or collapse all categories.

Contacts Server

Collection Category Hardware, Software, Logs Expand All Collapse All

PowerEdge R200 10G

Model	PowerEdge R200	Service Tag	99QLZ15
OS Name	Red Hat Enterprise Linux Server release 5.9 (Tikanga)		

System

Storage

Software

Operating System

OS Name	Red Hat Enterprise Linux Server release 5.9 (Tikanga)	Version	2.6.18-348.el5
System Name	localhost.localdomain	Install Date	Wed 21 May 2014 06:50:49 PM IST

Resources

IO Ranges

IRQ

Environment

Component

OpenManage

**Figure 32. Multiple device configuration viewer**

 **NOTE:** The Configuration Viewer does not support viewing the data collected from storage devices with Fluid File System (FluidFS).

# Using SupportAssist Enterprise to collect and send system information


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

 **NOTE:** For information on the devices from which SupportAssist Enterprise can collect and send system information to Dell, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).

## Setting up SupportAssist Enterprise for collecting and sending system information


### About this task

Installing SupportAssist Enterprise enables you to use SupportAssist Enterprise to collect and send system information to Dell from the local system. To use SupportAssist Enterprise to collect and send system information to Dell from remote devices, you must add each remote device in SupportAssist Enterprise.

 **NOTE:** The following steps are only required if you have not installed SupportAssist Enterprise. If you have already installed SupportAssist Enterprise, follow the instructions in [Starting the collection of system information from a single device](#) to manually start the collection and upload of system information to Dell.

### Steps

1. Install SupportAssist Enterprise. See [Installing SupportAssist Enterprise](#).
2. (Optional) Register SupportAssist Enterprise. See [Registering SupportAssist Enterprise](#).  
SupportAssist Enterprise is now ready to collect system information from the local system.
3. Add each remote device in SupportAssist Enterprise. See [Adding devices](#).

 **NOTE:** System information collected from servers running OMSA contains additional troubleshooting information that may not be available in the data collected from servers that are not running OMSA. Therefore, Dell recommends that you install OMSA on the servers that you have added in SupportAssist Enterprise.

SupportAssist Enterprise is now ready to collect system information from remote devices.

## Starting the collection of system information from a single device

### Prerequisites

- Ensure that you have completed setting up SupportAssist Enterprise. See [Setting up SupportAssist Enterprise for collecting and sending system information](#).
- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task

When a support case is opened or updated for a device, SupportAssist Enterprise automatically collects system information from that device, and uploads the information to Dell. If necessary, you can also manually start the collection of system information from a device. For example, if an error occurs during the automatic collection and upload of system information, you must resolve the underlying issue, and then manually start the collection and upload of system information. You may also be required to manually start the collection and upload of system information, if requested by Dell Technical Support.

## Steps

### 1. Click **Devices**.

The **Devices** page is displayed.

### 2. Select the local system or a remote device from which you want to collect system information.

The **Start Collection** link is enabled.

The screenshot shows the 'Devices' page with a table of devices and a detailed view for a PowerEdge R200 device. The table has columns for Name / IP Address, Model, and Status. The 'Start Collection' link is highlighted in red. The detailed view shows the device's name, IP address, service tag, device type, model, operating system, monitoring status, and next scheduled collection.

Name / IP Address	Model	Status
<input checked="" type="checkbox"/> Rhel	PowerEdge R200	OK
<input type="checkbox"/> PowerVault1	PowerVault MD3600f	OK
<input type="checkbox"/> compellent	EqualLogic PS6500	OK
<input type="checkbox"/> Networking1	Force10 E1200i	OK

PowerEdge R200

Tasks: Select Task

Status:  Connected

Name: Rhel

IP Address / Hostname: 10.94.219.38

Service Tag: 99QLZ1S

Device Type: Server / Hypervisor

Model: PowerEdge R200

Operating System: Red Hat Enterprise Linux Server release 5.9 (Tikanga)

Monitoring:  Enable  Disable

Revalidate: Revalidate

Collections: No Collections

Next Scheduled Collection: Monday, Nov 7, 2016

Duplicate

Figure 33. Starting a collection from a single device

### 3. Click **Start collection**.

The screenshot shows the 'Devices' page with a table of devices. The 'Start Collection' link is highlighted in red. The 'Rhel' device row is highlighted with a red box, showing a progress bar and a red 'x' icon, indicating that the collection is in progress.


Name / IP Address	Model	Status
<input type="checkbox"/> Rhel Collection in progress	PowerEdge R200	OK
<input type="checkbox"/> PowerVault1	PowerVault MD3600f	OK
<input type="checkbox"/> compellent	EqualLogic PS6500	OK
<input type="checkbox"/> Networking1	Force10 E1200i	OK

Figure 34. Collection status

The **Name/IP Address** column on the **Devices** page displays a progress bar and a message that indicate the status of the collection and upload of system information to Dell.



**NOTE:** If you want to cancel the collection of system information, click the **X** icon that is displayed next to the progress bar.

 **NOTE:** Until the collection is complete, the check box that is used to select the device is disabled. Therefore, you cannot initiate any other tasks on the device until the collection is complete.

## Starting the collection of system information from multiple devices

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

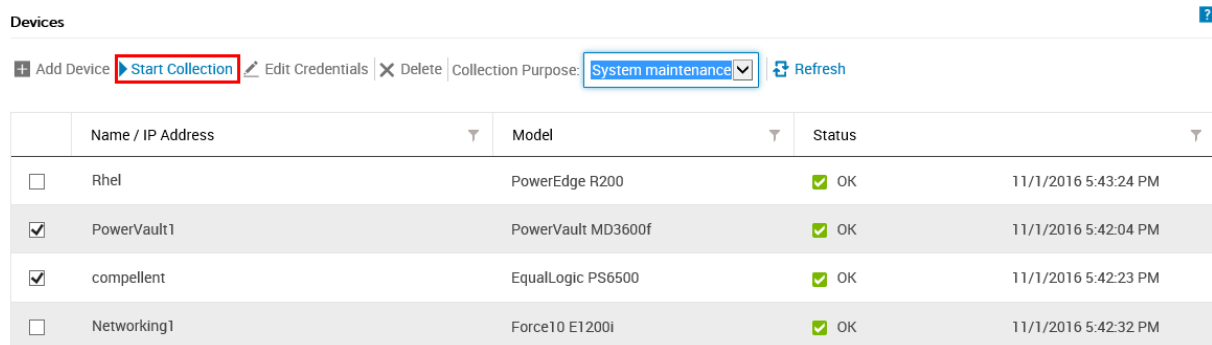
### About this task

You can use SupportAssist Enterprise to create and upload a collection bundle that contains the collected system information from multiple devices.





 **NOTE:** You can select up to 30 devices per multiple device collection.





### Steps

1. Click **Devices**.  
The **Devices** page is displayed.
2. Select the devices from which you want to collect system information.  
The **Start Collection** link is disabled when you select more than one device.
3. From the **Collection Purpose** list, select a reason for the collection.  
The **Start Collection** link is enabled.
4. Click **Start Collection**.



Devices ?


 Add Device ▶ Start Collection  Edit Credentials  Delete | Collection Purpose: System maintenance  Refresh

	Name / IP Address	Model	Status	
<input type="checkbox"/>	Rhel	PowerEdge R200	 OK	11/1/2016 5:43:24 PM
<input checked="" type="checkbox"/>	PowerVault1	PowerVault MD3600f	 OK	11/1/2016 5:42:04 PM
<input checked="" type="checkbox"/>	compellent	EqualLogic PS6500	 OK	11/1/2016 5:42:23 PM
<input type="checkbox"/>	Networking1	Force10 E1200i	 OK	11/1/2016 5:42:32 PM

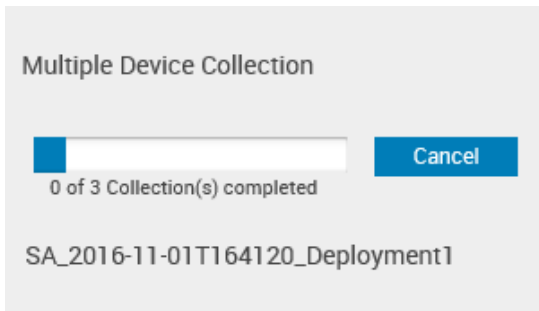
**Figure 35. Starting a multiple device collection**

The **Multiple Device Collection** window is displayed.

5. (Optional) Type a name for the collection bundle, support case number, and the name or email address of the Dell Technical Support contact.
6. If you want SupportAssist Enterprise to upload the collection bundle to Dell, ensure that the **Upload Collection** option is selected.



 **NOTE:** If you clear the **Upload Collection** option, the collection bundle is saved on the local system (server where SupportAssist Enterprise is installed). You can upload the collection bundle at a later time through the **Collections** page.

7. Click **OK**.



**Figure 36. Multiple Device Collection pane**

The collection progress status is displayed in the **Multiple Device Collection** pane on the **Devices** page. If the collection is completed successfully, the **Collections** page displays the details of the collection. You can also download the multiple device collection from the **Collections** page. For information on viewing a multiple device collection, see [Downloading and viewing a multiple device collection](#).

-  **NOTE:** To cancel the multiple device collection, click **Cancel** on the **Multiple Device Collection** pane.
-  **NOTE:** Until the multiple device collection is complete, the check box that is used to select the devices is disabled. Therefore, you cannot initiate any other tasks on the devices until the multiple device collection is complete.

## Uploading a collection

### Prerequisites

You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).

### About this task


You can use the **Upload** option available in the **Collections** page to upload collections to Dell. You may choose to upload a collection in the following scenarios:





- Collection of system information was successful, but upload of the collection was unsuccessful.
- While starting a multiple device collection, you had chosen not to upload the multiple device collection to Dell. Such collections display a **Never Uploaded** status in the **Collections** page.
- You want to upload a collection to Dell once again.

### Steps

1. Click **Collections**.  
The **Collections** page is displayed.
2. Select a collection that you want to upload and click **Upload**.

**Collections**

 **Upload**

<input type="checkbox"/>	Name	Collection Date	Case Number	Upload Status
<input type="checkbox"/>	Rhel(Manual)	11/01/2016		 Success
<input type="checkbox"/>	Rhel(Manual)	11/01/2016		 Success
<input type="checkbox"/>	SA_2016-11-01T164120_Deployment1	11/01/2016		 Success
<input type="checkbox"/>	PowerVault1(Manual)	11/01/2016		 Success
<input checked="" type="checkbox"/>	SA_2016-11-01T170251_Maint	11/01/2016		Never Uploaded

**Figure 37. Upload collection option**


The **Upload Status** column displays the status of the upload.

## Uploading a collection from a disconnected site

### About this task

When internet connectivity is available, SupportAssist Enterprise automatically collects and sends system information from your devices to Dell. If the server where SupportAssist Enterprise is installed does not have internet connectivity, you can choose to manually upload collections to Dell.

### Steps

1. Perform a collection from the device. See [Starting the collection of system information from a single device](#).
2. Access the collection file by using one of the following methods:
  - For collections from a storage, networking, chassis, or multiple device only — In the **Collections** page, select the collection and in the collection overview pane, click **Download File**.
  - If SupportAssist Enterprise is installed on a Windows operating system — Navigate to C:\Program Files\Dell\SupportAssist\reports and locate the collection .zip file.
  - If SupportAssist Enterprise is installed on a Linux operating system — Navigate to /opt/dell/supportassist/scripts/reports and locate the collection .zip file.
3. Copy and paste the collection .zip file to another system that has internet connectivity.
4. Visit <https://techdirect.dell.com/fileUpload/>  
The **Dell Technical Support File Upload** page is displayed.
5. Type the Service Tag of the device.
6. Type your company name, contact name, Service Request #, email address, Dell contact email, and address in the appropriate fields.  
 **NOTE: If you do not have a Service Request number, contact Dell Technical Support to open a service request.**
7. Click **Choose File** and browse to select the collection .zip file.
8. Click **Submit**.

## SupportAssist Enterprise user groups

Dell EMC SupportAssist Enterprise maintains security and privileges through the following user groups that are created during the installation of SupportAssist Enterprise:

- **SupportAssistAdmins** — Users who are members of this group have elevated or administrative privileges required for performing both basic and advanced functions in SupportAssist Enterprise.
- **SupportAssistUsers** — Users who are members of this group have normal privileges required for performing only basic functions in SupportAssist Enterprise.

After the installation of SupportAssist Enterprise, by default, the operating system user groups specified in the following table are automatically added to the SupportAssist Enterprise user groups.

**Table 10. Operating system user groups that are added to the SupportAssist Enterprise user groups**

Operating system where SupportAssist Enterprise is installed	SupportAssistAdmins	SupportAssistUsers
Microsoft Windows	Local Administrators	Users
Windows domain controller	Domain Admins	Domain Users
Linux	root user	—

If you have Administrator privileges (Windows) or root privileges (Linux) on the system, you can add user accounts to the appropriate SupportAssist Enterprise user groups based on your requirement. Users who are members of the operating system user groups on the system where SupportAssist Enterprise is installed have the following privileges in SupportAssist Enterprise:

- If SupportAssist Enterprise is installed on Windows:
  - Users who are members of the **Administrators** user group have elevated or administrative privileges in SupportAssist Enterprise.
  - Users who are members of the **Users** user group have normal privileges in SupportAssist Enterprise.
- If SupportAssist Enterprise is installed on Linux:
  - Users who are members of the **root** group have elevated or administrative privileges in SupportAssist Enterprise.
  - Users who are members of the **users** group have normal privileges in SupportAssist Enterprise.

## SupportAssist Enterprise functions and user privileges

The following table provides a list of functions that can be performed by the SupportAssist Enterprise users depending on their privileges.

**Table 11. SupportAssist Enterprise functions and user privileges**

SupportAssist Enterprise functions	SupportAssistAdmins and users with elevated or administrative privileges	SupportAssistUsers and users with normal privileges
View cases and check for cases	✓	✓
View the device inventory and device groups	✓	✓

SupportAssist Enterprise functions	SupportAssistAdmins and users with elevated or administrative privileges	SupportAssistUsers and users with normal privileges
View the collections page	✓	✓
View the collected system information	✓	✓
Perform network connectivity tests	✓	✓
Perform the case creation test	✓	✓
Perform case management actions	✓	✗
Create, manage, edit, or delete device groups	✓	✗
Complete the registration of SupportAssist Enterprise	✓	✗
Add devices	✓	✗
Edit device credentials	✓	✗
Delete devices	✓	✗
Install/upgrade OMSA by using SupportAssist Enterprise	✓	✗
Configure SNMP by using SupportAssist Enterprise	✓	✗
Enable or disable global-level maintenance mode	✓	✗
Enable or disable device-level maintenance mode	✓	✗
Manually start the collection and upload of system information from a single device or multiple devices	✓	✗
View and configure SupportAssist Enterprise settings	✓	✗
Perform automatic update	✓	✗
Clear System Event Log	✓	✗
Uninstall SupportAssist Enterprise	✓	✗

## Granting elevated or administrative privileges to users

You can grant elevated or administrative privileges to users by adding them to specific user groups on the system where SupportAssist Enterprise is installed. The user groups to which a user must be added to grant elevated or administrative privileges vary depending on the operating system where SupportAssist Enterprise is installed.

- If SupportAssist Enterprise is installed on Windows, you can grant elevated or administrative privileges through one of the following methods:
  - Add the user to the **SupportAssistAdmins** user group. See [Adding users to the SupportAssist Enterprise user groups \(Windows\)](#).
  - Add the user to the Windows **Administrators** user group.
- If SupportAssist Enterprise is installed on Linux, you can grant elevated or administrative privileges through one of the following methods:
  - Add the user to the **SupportAssistAdmins** user group. See [Adding users to the SupportAssist Enterprise user groups \(Linux\)](#).
  - Add the user to the Linux **root** group.

## Adding users to the SupportAssist Enterprise user groups (Windows)

### Prerequisites

Ensure that you are logged in to the server where SupportAssist Enterprise is installed with administrator privileges.

### Steps

1. Open the command prompt window.
2. To add an existing user account to a SupportAssist Enterprise user group, use the following syntax: `net localgroup SupportAssist_Enterprise_user_group_name user_name`.

For example:

- To add an existing user account (for example, User1) to the **SupportAssistAdmins** user group, type `net localgroup SupportAssistAdmins User1` and press Enter.
- To add an existing user account (for example, User2) to the **SupportAssistUsers** user group, type `net localgroup SupportAssistUsers User2` and press Enter.

## Adding users to the SupportAssist Enterprise user groups (Linux)

### Prerequisites

Ensure that you are logged in to the server where SupportAssist Enterprise is installed with root privileges.

### Steps

1. Open the terminal window.
2. To create a new user account and add the user account to a SupportAssist Enterprise user group, use the following syntax: `useradd -G SupportAssist_Enterprise_user_group_name User_name`

For example:

- To create a new user account (for example, User1) and add it to the **SupportAssistAdmins** user group, type `useradd -G Supportassistadmins User1` and press Enter.
  - To create a new user account (for example, User2) and add it to the **SupportAssistUsers** user group, type `useradd -G Supportassistusers User2` and press Enter.
3. To add an existing user account to a SupportAssist Enterprise user group, use the following syntax: `usermod -G SupportAssist_Enterprise_user_group_name User_name`
- For example:
- To add an existing user account (for example, User1) to the **SupportAssistAdmins** user group, type `usermod -G SupportAssistAdmins User1` and press Enter.
  - To add an existing user account (for example, User2) to the **SupportAssistUsers** user group, type `usermod -G SupportAssistUsers User2` and press Enter.

# Manually configuring SNMP settings

Configuring the SNMP settings (alert destination) of a device ensures that Dell EMC SupportAssist Enterprise receives alerts from the device. SupportAssist Enterprise can automatically configure the SNMP settings of Dell servers. For Dell chassis and networking devices, you must manually configure the SNMP settings.

## Manually configuring the alert destination of a server

By default, when you add a server you can allow SupportAssist Enterprise to automatically configure the alert destination of the server. If the automatic SNMP configuration is unsuccessful, you can configure the SNMP settings of a device by using the following methods:

- Running a script file — The SupportAssist Enterprise installation folder includes two script files (one for Microsoft Windows and another for Linux) that you can use to configure the alert destination of a server.
- Manually configure the SNMP settings — You can configure settings by accessing the SNMP trap service.


 **NOTE: You can retry the automatic configuration of the alert destination at any time using the Configure SNMP option available in SupportAssist Enterprise. For information on using the Configure SNMP option, see [Configuring SNMP settings by using SupportAssist Enterprise](#).**

### Related links

- [Manually configuring the alert destination of a server by using the script file \(Windows\)](#)
- [Manually configuring the alert destination of a server \(Windows\)](#)
- [Manually configuring the alert destination of a server by using the script file \(Linux\)](#)
- [Manually configuring the alert destination of a server \(Linux\)](#)

## Manually configuring the alert destination of a server by using the script file (Windows)

### Prerequisites

- Microsoft Windows PowerShell version 1.0 or later must be installed on the device.
-  **NOTE: The script file is supported only on Windows PowerShell. It is not supported on Windows PowerShell (x86), Windows PowerShell ISE, or Windows PowerShell ISE (x86).**
- Ensure that you have administrator rights on the device to run the PowerShell script file.
- Ensure that you have write permissions on the C:\ drive of the device.
- If the device is running Windows 2003, ensure that the SNMP service is installed. On all other supported operating systems, the script file installs the SNMP service if it is not installed already.

The script file is supported only on devices running the following operating systems:

- Windows Server 2003
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2008 SP2 (64-bit)
- Windows Server 2008 SP2 (32-bit)
- Windows Small Business Server 2008
- Windows Small Business Server 2011
- Windows Server 2012

- Windows Server 2012 R2
- Windows Server 2016
- Server Core for Windows Server 2012

### Steps

1. On the server where SupportAssist Enterprise is installed, browse to the `C:\Program Files\Dell\SupportAssist\scripts` folder.
2. Copy the script file (`WindowsSNMPConfig.ps1`) located in the folder and paste the file at a desired location (for example, `C:\temp`) on the device.
3. Perform one of the following, depending on the operating system running on the device:
  - In Windows Server 2012, on the **Start** screen, right-click the **Windows PowerShell** tile, and in the app bar, click **Run as administrator**.
  - In Windows Server 2003, 2008, or Windows Small Business Server 2011, click **Start**, type `PowerShell`, right-click **Windows PowerShell**, and then click **Run as administrator**.
4. Set the PowerShell execution policy as appropriate on the device. For example, type the following command: `Set-ExecutionPolicy RemoteSigned` or `Set-ExecutionPolicy AllSigned`.
5. Run the script file on the device using the following syntax: `<script file path> -hosts <IP address of server where SupportAssist Enterprise is installed>`. For example, `./WindowsSNMPConfig.ps1 -hosts 10.55.101.20`.
6. If Verisign is not included as a trusted publisher on the device, you are prompted to confirm if you want to run the software from an untrusted publisher. Press `<R>` to run the script.

### Related links

[Manually configuring the alert destination of a server](#)

## Manually configuring the alert destination of a server (Windows)

Perform the following steps to manually configure the alert destination of a server running Microsoft Windows:

1. Open a command prompt, type `services.msc`, and press Enter.  
The **Services** window is displayed.
2. Browse the list of services, and ensure that the status of the **SNMP Service** is displayed as **Started**.
3. Right-click **SNMP Service** and select **Properties**.  
The **SNMP Service Properties** window is displayed.
4. Click the **Traps** tab, and perform the following:
  - a. In the **Community name** box, type the community name, and click **Add to list**.
  - b. In **Trap destinations**, click **Add**.  
The **SNMP Service Configuration** window is displayed.
  - c. In the **Host name, IP or IPX address** field, type the host name or IP address of the server where SupportAssist Enterprise is installed, and click **Add**.
5. Click **Apply**.
6. In the **Services** window, right-click **SNMP Service** and click **Restart**.

### Related links

[Manually configuring the alert destination of a server](#)

## Manually configuring the alert destination of a server by using the script file (Linux)

### Prerequisites

- Net-SNMP must be installed on the system. For information on installing Net-SNMP, see [Installing Net-SNMP \(Linux only\)](#)
- Ensure that you have root privileges on the device.

The script file is supported only on devices running the following operating systems:

- Red Hat Enterprise Linux 5.5 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.7 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.8 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.9 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.10 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.11 (32-bit and 64-bit)
- Red Hat Enterprise Linux 6.1 (64-bit)
- Red Hat Enterprise Linux 6.2 (64-bit)
- Red Hat Enterprise Linux 6.3 (64-bit)
- Red Hat Enterprise Linux 6.4 (64-bit)
- Red Hat Enterprise Linux 6.5 (64-bit)
- Red Hat Enterprise Linux 6.7 (64-bit)
- Red Hat Enterprise Linux 6.8 (64-bit)
- Red Hat Enterprise Linux 7.0 (64-bit)
- Red Hat Enterprise Linux 7.1 (64-bit)
- Red Hat Enterprise Linux 7.2 (64-bit)
- SUSE Linux Enterprise Server 10 SP3 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 11 (64-bit)
- SUSE Linux Enterprise Server 11 SP1 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 11 SP2 (64-bit)
- SUSE Linux Enterprise Server 11 SP3 (64-bit)
- SUSE Linux Enterprise Server 11 SP4 (64-bit)
- SUSE Linux Enterprise Server 12 (64-bit)
- SUSE Linux Enterprise Server 12 SP1 (64-bit)
- CentOS 7.0
- CentOS 6.0
- Oracle Linux 7.1
- Oracle Linux 6.7
- VMware ESX 4.1

### Steps

1. On the server where SupportAssist Enterprise is installed, browse to the `C:\Program Files\Dell\SupportAssist\scripts` folder.
2. Copy the script file (`LinuxSNMPConfig.sh`) located in the folder and paste the file at a desired location (for example, `\root`) on the device.
3. Open the terminal window and log in as a user with root privileges.
4. Run the script file on the device using the following syntax: `sh LinuxSNMPConfig.sh -d <IP address of the server where SupportAssist Enterprise is installed>`. For example, `sh LinuxSNMPConfig.sh -d 10.10.10.10`.

### Related links

[Manually configuring the alert destination of a server](#)

## Manually configuring the alert destination of a server (Linux)

Perform the following steps to manually configure the alert destination of a server running Linux:

1. Run the command `rpm -qa | grep snmp`, and ensure that the **net-snmp** package is installed.
2. Run `cd /etc/snmp` to navigate to the snmp directory.
3. Open **snmpd.conf** in the VI editor (**vi snmpd.conf**).

4. Search `snmpd.conf` for `# group context sec.model sec.level prefix read write notif` and ensure that the values for fields `read`, `write`, and `notif` are set to `all`.
5. At the end of the `snmpd.conf` file, just before **Further Information**, add an entry in the following format: `Trapsink <IP address of the server where SupportAssist Enterprise is installed> <community string>` For example, `trapsink 10.94.174.190 public`.
6. Restart the SNMP services (`service snmpd restart`).

#### Related links

[Manually configuring the alert destination of a server](#)

## Manually configuring the alert destination of iDRAC by using the web interface

Perform the following steps to manually configure the alert destination of an iDRAC:

1. Log in to the iDRAC web interface.
2. Go to **Overview** → **Server** → **Alerts**.
3. In the **Alerts** section, make sure that the **Enabled** option is selected.
4. In the **Alerts Filter** section, make sure that the following options are selected:
  - **System Health**
  - **Storage**
  - **Configuration**
  - **Audit**
  - **Updates**
  - **Warning**
  - **Critical**
5. In the **Alerts and Remote System Log Configuration** section, make sure that all fields in the **SNMP Trap** column are selected.
6. Click **SNMP and Email Settings**.
7. In the **IP Destination List** section, select the **State** option to enable the alert destination field.  
You can specify up to eight destination addresses. For more information about the options, see the *iDRAC Online Help*.
8. In the **Destination Address** field, type the IP address of the server where SupportAssist Enterprise is installed.
9. Type the iDRAC SNMP community string (for example, public) and the SNMP alert port number (for example, 162) in the appropriate fields.  
For more information about the options, see *iDRAC Online Help*.



**NOTE:** The community string value indicates the community string to be used in a Simple Network Management Protocol (SNMP) alert trap sent from iDRAC. Ensure that the destination community string is the same as the iDRAC community string. The default community string is Public.

10. Click **Apply**.  
The alert destination is configured.
11. In the **SNMP Trap Format** section, make sure that either **SNMP v1** or **SNMP v2** is selected, and click **Apply**.  
iDRAC is now configured to forward alerts to the server where SupportAssist Enterprise is installed.




**NOTE:** For information on configuring the alert destination of an iDRAC using other methods, see the “Configuring IP Alert Destinations” section in the *iDRAC User's Guide* at [Dell.com/idracmanuals](http://Dell.com/idracmanuals).

## Manually configuring the alert destination of a chassis by using the web interface

#### Prerequisites

You must be logged in to the CMC web interface with administrator privileges.

## Steps

1. In the system tree, go to **Chassis Overview**, and then click **Alerts** → **Chassis Events**.  
The **Chassis Events** page is displayed.
2. Under **Chassis Event Filters Configuration** section, select **Enable Chassis Event Alerts** option to enable alert generation.
3. Under the **Chassis Event List** section, select the **Enable Alert** option on the column header to generate alerts for all events.
4. In the system tree, go to **Chassis Overview**, and then click **Alerts** → **Trap Settings**.  
The **Chassis Event Alert Destinations** page is displayed.
5. Perform the following:
  - In the **Destination** field, enter the IP address of the server where SupportAssist Enterprise is installed.
  - In the **Community String** field, enter a valid community string to which the server where SupportAssist Enterprise is installed belongs.  
 **NOTE: CMC uses a default SNMP community string as public. To ensure higher security, it is recommended to change the default community string and set a value which is not blank.**
  - Under **Enabled**, select the check box corresponding to the IP address of the server where SupportAssist Enterprise is installed.
6. Click **Apply** to save the settings.
7. To test whether the destination IP address is receiving the SNMP traps, click **Send** in the **Test SNMP Trap** column.  
The IP alert destinations are configured.

## Manually configuring the alert destination of a networking device

### About this task

 **NOTE: The steps to configure the alert destination of networking devices may vary based on the networking device type and model. For information on configuring the alert of a specific networking device model, see the networking device documentation.**

### Steps





1. Log in to the networking device by using a terminal emulator such as PuTTY.  
The terminal window is displayed.
2. Type **configure** and press Enter.
3. Type **snmp-server host <IP address of the server where SupportAssist Enterprise is installed> traps version 1**.
4. To verify if the alert destination is configured successfully, type **show running-config snmp** and press Enter.  
The list of alert destinations that are configured on the device is displayed.

## Other useful information

This chapter provides additional information that you may require while using Dell EMC SupportAssist Enterprise.

### Monitoring servers for hardware issues

SupportAssist Enterprise can monitor Dell servers through the following methods:

- Agent-based monitoring** — This method is used to monitor devices that are added with the **Device Type** as **Server / Hypervisor**. In this method, an agent acts as an interface between the device and SupportAssist Enterprise. The agent generates an alert (SNMP trap) whenever a hardware event occurs on the device. For monitoring a device using the agent-based method, SupportAssist Enterprise depends on the Dell OpenManage Server Administrator (OMSA) agent. The OMSA agent is an application that monitors the health of various components of the device where it is installed. Whenever a hardware event occurs on the device, the OMSA agent generates an alert. SupportAssist Enterprise processes the alert to determine if the alert qualifies for creating a support case. For instructions to add a device for agent-based monitoring, see [Adding a server or hypervisor](#).
  -  **NOTE: Without OMSA, SupportAssist Enterprise will not be able to monitor a device through the agent-based monitoring method.**
  -  **NOTE: Installation of OMSA may not be supported on certain operating systems. SupportAssist Enterprise may be able to monitor devices running such operating systems only through the agentless monitoring method. For information on the operating system requirements for agent-based monitoring, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).**
- Agentless monitoring** — This method is used to monitor devices that are added with the **Device Type** as **iDRAC**. In this method, the Integrated Dell Remote Access Controller (iDRAC) available on the device acts as an interface between the device and SupportAssist Enterprise. Whenever a hardware event occurs on the device, the iDRAC generates an alert. SupportAssist Enterprise processes the alert to determine if the alert qualifies for creating a support case. For instructions to add a device for agentless monitoring, see [Adding an iDRAC](#).
  -  **NOTE: Agentless monitoring is supported only for Dell's 12th and 13th generation of PowerEdge servers (iDRAC 7 and iDRAC 8).**
  -  **NOTE: The iDRAC can be configured to send alerts through SNMP and IPMI. However, SupportAssist Enterprise can only receive alerts sent through SNMP. To ensure that SupportAssist Enterprise receives alerts sent from an iDRAC, you must ensure that all SNMP Trap options are selected in the Alerts and Remote System Log Configuration section of the iDRAC web console.**

### Benefits of agent-based monitoring

Even though Dell's 12th and 13th generation of PowerEdge servers can be monitored through the agentless (iDRAC) method, agent-based (OMSA) method has the following benefits:

- Alert generation capabilities of OMSA and iDRAC are not the same. In Dell's 13th generation of PowerEdge servers, the alert generation capabilities of OMSA and iDRAC are almost similar. However, alerts from chipset and software RAID are available only through OMSA.
- For devices with a ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract Dell's recommendations for operating system and software component versions are available only if the device is monitored through OMSA.
- OMSA is the only option available for monitoring Dell's 9th to 11th generation of PowerEdge servers.

### Support for automatically installing or upgrading OMSA


To monitor a device through the agent-based method, SupportAssist Enterprise requires the Dell OpenManage Server Administrator (OMSA) agent to be installed and running on the device. The OMSA agent is an application that monitors the health of various

components of the device where it is installed. When OMSA is installed and running on a device, the OMSA agent generates an alert whenever a hardware event occurs on the device. SupportAssist Enterprise receives the alert from the device and processes the alert to identify if the alert indicates a hardware issue. For more information on OMSA, visit [Delltechcenter.com/OMSA](http://Delltechcenter.com/OMSA).


 **NOTE: The SupportAssist Enterprise recommended version of OMSA may vary depending on the generation of the PowerEdge server and the operating system running on the server. For information on the recommended versions of OMSA, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).**


SupportAssist Enterprise has the capability to automatically download and install the recommended version of OMSA on a device. By default, when a server is added for agent-based monitoring, SupportAssist Enterprise verifies if the recommended version of OMSA is installed on the device.


- If OMSA is not installed on the device, SupportAssist Enterprise prompts for your confirmation to download and install the recommended version of OMSA on the device. On confirmation, SupportAssist Enterprise downloads and installs OMSA in the background. The OMSA installation status is displayed in the **Status** column on the **Devices** page. If you choose not to install

OMSA, the status of the device is displayed as  **OMSA not installed**. To install OMSA at a later time, you can use the **Tasks** → **Install / Upgrade OMSA** option on the device overview pane.


- If OMSA is already installed on the device, SupportAssist Enterprise verifies if the version of OMSA matches with the recommended OMSA version for SupportAssist Enterprise. If the existing version of OMSA is not the recommended version, but supports direct upgrade to the recommended version of OMSA, SupportAssist Enterprise prompts for your confirmation to download and upgrade OMSA on the device. The OMSA upgrade status is displayed in the **Status** column on the **Devices** page.

If you choose not to upgrade OMSA, the status of the device is displayed as  **New version of OMSA available**. To upgrade OMSA at a later time, use the **Tasks** → **Install / Upgrade OMSA** option on the device overview pane.

 **NOTE: Direct upgrade to OMSA version  $n$  is supported only from the two previous versions ( $n-2$ ) of OMSA. If direct upgrade is not supported, you must manually download and upgrade OMSA on the device. For example, if OMSA version 7.0 is already installed on the device, but the recommended version of OMSA is 7.4, you must manually upgrade from OMSA version 7.0 to 7.2. After upgrading to OMSA version 7.2, you can upgrade to OMSA version 7.4 using the **More Tasks** → **Install/Upgrade OMSA** option on the device overview pane or you can manually download and upgrade to OMSA version 7.4.**

 **NOTE: When you allow or use SupportAssist Enterprise to install or upgrade OMSA, the downloaded packages of OMSA are retained in the SupportAssist Enterprise installation folder. If a compatible version of OMSA was already downloaded during an earlier operation, SupportAssist Enterprise does not download OMSA again. In this scenario, SupportAssist Enterprise only installs or upgrades OMSA on the device using the already downloaded version of OMSA.**

 **NOTE: The time taken to download OMSA is dependent on the internet download speed and network bandwidth.**

If the recommended version of OMSA is installed and running on the device, the status of the device is displayed as  **OK**.


 **NOTE: Automatic installation of OMSA through SupportAssist Enterprise is not supported on devices running Citrix XenServer, VMware ESXi, or ESX. To allow SupportAssist Enterprise to detect hardware issues on these devices, you must manually download and install OMSA.**


#### Related links

[Installing or upgrading OMSA by using SupportAssist Enterprise](#)

## Support for automatically configuring SNMP settings

To enable SupportAssist Enterprise to monitor a device, the device must be configured to forward alerts (SNMP traps) to the server where SupportAssist Enterprise is installed. Configuring the SNMP settings sets the alert destination of a device, and ensures that alerts from the device are forwarded to the server where SupportAssist Enterprise is installed. SupportAssist Enterprise has the capability to automatically configure the SNMP settings of a device, such that the device forwards alerts to the server where SupportAssist Enterprise is installed. You can allow SupportAssist Enterprise to configure the SNMP settings of the device while adding the device or at a later time. The status of the SNMP configuration is displayed in the **Status** column on the **Devices** page.

While SupportAssist Enterprise configures the SNMP settings of a device, the device displays a  **Configuring SNMP** status. You can also use the **Tasks** → **Configure SNMP** option on the device overview pane to automatically configure the SNMP settings of a device at any time.

 **NOTE: When you allow or use SupportAssist Enterprise to automatically configure the SNMP settings of a device, the alert destination of the device is set to the IP address of the server where SupportAssist Enterprise is installed.**

#### Related links

[Configuring SNMP settings by using SupportAssist Enterprise](#)

## Device correlation

You can add (discover) a server in SupportAssist Enterprise by using both the host operating system IP address and iDRAC IP address of the device. In such a scenario, the **Devices** page displays two separate listings for the same device. SupportAssist Enterprise receives alerts from the device through both the operating system and the iDRAC. However, for operational purposes, SupportAssist Enterprise correlates the operating system IP address and iDRAC IP address of the device and considers the device as a single device. The following are the expected behaviors when a device is correlated:

- Alerts originating from the operating system and the iDRAC are correlated and a support case is created for the Service Tag of the device.
- When system information is collected, the **Devices** page display the same status for both the listings.
- For a manually-initiated collection of system information — System information is gathered through the selected device listing in the **Devices** page. For example, if the operating system listing is selected, system information is gathered through the operating system. However, if SupportAssist Enterprise is unable to connect to the device by using the operating system IP address, system information is gathered through the iDRAC.
- For periodic collections and on case creation — System information is typically gathered through the operating system. However, if SupportAssist Enterprise is unable to connect to the device by using the operating system IP address, system information is gathered through the iDRAC.

## Detection of hardware issues in attached storage devices

In addition to monitoring PowerEdge servers, SupportAssist Enterprise can also process alerts received from Dell PowerVault MD series storage arrays that may be attached to a server. Alert generation from an attached storage device occurs through the Dell OpenManage Storage Services (OMSS) application installed on the server. When you allow SupportAssist Enterprise to automatically install OMSA on the server, by default, OMSS is also installed. If you manually download and install OMSA on the server, ensure that you also install OMSS. Otherwise, SupportAssist Enterprise will not be able to detect hardware issues that may occur on the attached storage device. When a hardware issue is detected on an attached storage device, SupportAssist Enterprise automatically creates a support case for the associated server.

## Support for Dell OEM servers

Dell OEM-ready devices (either re-branded or de-branded Dell hardware), when added, are classified under the re-branded name and not the original Dell hardware name. All of the functionality available for Dell standard devices, such as alerts handling, automatic case creation (when the support level has been validated at the time of the support incident as ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center) and ProSupport Plus reports are available for OEM-ready devices. On ProSupport Plus reports, OEM-ready devices are listed with the re-branded name.

Automatic case creation is supported through Dell Enterprise Technical Support and not available for other support case service request management systems.

As with any system that is modified for custom solutions, Dell recommends that you verify all SupportAssist Enterprise features to ensure proper operation with those modifications.

## Installing Net-SNMP (Linux only)

### Prerequisites

Ensure that you are logged in to the device with a user account that has root privileges.

### About this task

SupportAssist Enterprise receives alerts that are forwarded from remote devices through an SNMP agent. Net-SNMP consists of a suite of SNMP tools, including an SNMP agent. On devices running Linux operating systems, Net-SNMP must be installed to allow SupportAssist Enterprise to receive alerts.

## Steps

1. Open the terminal window on the device running the Linux operating system.
2. Type the following commands based on the operating system:
  - Red Hat Enterprise Linux, CentOS, and VMware ESX: **yum install net-snmp**
  - Oracle Linux: **rpm -ivh net-snmp-x.x-xx.x.x.xxx.x86\_64.rpm**, where x.x-xx.x.x.xxx.x represents the version number included in the rpm file name.
  - SUSE Linux Enterprise Server:
    1. **zypper addrepo http://download.opensuse.org/repositories/net-snmp:factory/SLE\_12/net-snmp:factory.repo**
    2. **zypper refresh**
    3. **zypper install net-snmp**

## Configuring sudo access for SupportAssist Enterprise (Linux)

In Linux operating systems, users with sudo access may be granted administrative privileges to run certain commands. If you have added a remote device in SupportAssist Enterprise using the credentials of a sudo user, you must perform the following steps to allow SupportAssist Enterprise to monitor and collect system information from the device.

### Prerequisites

Ensure that you are logged in to the remote device as a user with root privileges.

### Steps

1. Open the terminal window.
2. Set the home directory path for the user — Type `useradd user_name -d /home` and press Enter.
3. Open the `/etc/sudoers` file.
4. Insert an exclamation mark [!] on the requiretty line. For example, `!requiretty`
5. Add one of the following based on your preference:
  - `%root ALL=(ALL) NOPASSWD: ALL` — To grant permission to all users in the root group.
  - `user_name ALL=(ALL) NOPASSWD: ALL` — To grant permission to only a specific user.
6. Save the `/etc/sudoers` file.

## Ensuring successful communication between the SupportAssist Enterprise application and the SupportAssist server

The server where SupportAssist Enterprise is installed must be able to communicate with the SupportAssist server hosted by Dell to:

- Automatically create a support case if there is a problem with a device in your environment.
- Upload the collected system information to Dell.

To ensure that the SupportAssist Enterprise application is able to successfully communicate with the SupportAssist server:

- The server where the SupportAssist Enterprise application is installed must be able to connect to the following destinations:
  - **https://apidp.dell.com** and **https://api.dell.com** — end point for the SupportAssist server. On the server where SupportAssist Enterprise is installed, verify if you can access the following locations using the web browser: **https://apidp.dell.com** and **https://api.dell.com**.
  - **https://is.us.dell.com/FUS/api/2.0/uploadfile** — the file upload server where the collected system information is uploaded.
  - **https://is.us.dell.com/FUSCHUNK/api/1.0/file/uploadChunk** — the file upload server where the collection files greater than 10 MB in size are uploaded.
  - **https://downloads.dell.com/** — for downloading Dell OpenManage Server Administrator (OMSA) and also for getting new SupportAssist Enterprise release information, policy files, and product support files. On the server where SupportAssist Enterprise is installed, verify if you can access the following location using the web browser: **https://downloads.dell.com/**
  - On the server where SupportAssist Enterprise is installed, verify if port 443 is open for **is.us.dell.com**, **downloads.dell.com**, **apidp.dell.com**, and **api.dell.com**. You can use a telnet client to test the connection. For example, use the following command: `o downloads.dell.com 443`

- On the server where SupportAssist Enterprise is installed, verify if the network settings are correct.
- If the server where SupportAssist Enterprise is installed connects the Internet through a proxy server, configure the proxy settings in SupportAssist Enterprise. See [Configuring proxy server settings](#).

If the communication problem persists, contact your network administrator for further assistance.

## Accessing the SupportAssist Enterprise application logs

SupportAssist Enterprise saves system events and log messages in the following locations:

- On Windows:
  - Windows Event Log
  - The installation logs folder (C:\Program Files\Dell\SupportAssist\logs)
- On Linux:
  - var logs
  - The installation logs folder (/opt/dell/supportassist/logs)

A new log file is created daily at 11:59 p.m. based on the time zone configured on the system, and the log is stored in the logs folder. The log file contains log information for the current day. At the end of each day, the log file is renamed as **application.log <date format in yyyyymmdd>**. If the log file is older than two days, the log file is zipped automatically. This enables you to identify the exact log file stored for a given date when alerts occur. For example, log files similar to the following can be seen:

- **application.log**
- **application.log.20161101**
- **application.log.20161102.zip**
- **application.log.20161103.zip**

The log files are purged from storage after 30 days.


The log file contains log messages that correspond to the following values (or higher) in the **log4j.xml** file: FATAL, ERROR, WARN, INFO, and DEBUG, with special values of OFF and ALL. The **log4j.xml** file is available at C:\Program Files\Dell\SupportAssist\config (on Windows) and /opt/dell/supportassist/config (on Linux). A value of ERROR in the **log4j.xml** file results in log messages of FATAL, and ERROR, since FATAL is a higher level than ERROR.

## Event storm handling

SupportAssist Enterprise intelligently handles event storm conditions, allowing up to nine separate alerts from a device within a 60-minute timespan. However, if 10 or more separate alerts are received from a device, SupportAssist Enterprise automatically places the device in maintenance mode. Maintenance mode prevents any further processing of alerts from the device, enabling you to make infrastructure changes without creating unnecessary support cases. After 30 minutes in maintenance mode, SupportAssist Enterprise automatically removes the device from maintenance mode and resumes normal alert processing for the device. For more information about maintenance mode, see [Understanding maintenance mode](#).

## Accessing the context-sensitive help

Context-sensitive help provides information about features and tasks that are applicable to the current view on the user interface. Once you invoke the context-sensitive help, you can navigate or search through the entire SupportAssist Enterprise help system.

To access context-sensitive help, click the  icon that appears in the user interface. Context-sensitive help is displayed in a new browser window.

## Viewing SupportAssist Enterprise product information

Click **About** in the SupportAssist Enterprise header area.

The **About** page is displayed, where you can view the SupportAssist Enterprise product version and the registration ID.

## Uninstalling SupportAssist Enterprise

You can uninstall SupportAssist Enterprise based on your preference. During the uninstallation, you can choose to provide a reason for the uninstallation and also provide feedback to Dell. Your feedback will remain confidential and will allow Dell to make product improvements. The following sections provide information about uninstalling SupportAssist Enterprise on Windows and Linux operating systems.

### Uninstalling SupportAssist Enterprise (Windows)

#### Prerequisites

Log in to the server where SupportAssist Enterprise is installed with administrator privileges.

#### Steps

1. Perform one of the following based on the operating system:
  - On Windows Server 2012 or 2016, point to the bottom-left corner of the screen, and then click the **Start** icon. On the **Start** screen, click the **Control Panel** tile. On the **Control Panel**, click **Uninstall a program**.
  - On Windows Server 2008 or Windows Small Business Server 2011, click **Start** → **Control Panel** → **Programs and Features**.

The **Uninstall or change a program** window is displayed.

2. Select **Dell SupportAssist Enterprise** and click **Change**.

The **Welcome to Dell SupportAssist Enterprise Installer** window is displayed.

3. Click **Next**.

The **Dell SupportAssist Enterprise Maintenance** window is displayed.

4. Select **Remove**, and click **Next**.

The **Feedback** window is displayed.

5. Select an appropriate reason from the **Select an option** drop-down list, provide your comments, and click **Remove**.

The **Remove the Program** window is displayed.

6. Click **Remove**.



**NOTE:** In Windows Server 2016, the User Account Control dialog box may be displayed more than once while the uninstallation is in progress.

The **Uninstallation Completed** window is displayed.

7. Click **Finish**.

SupportAssist Enterprise is now uninstalled.

### Uninstalling SupportAssist Enterprise (Linux)

#### Prerequisites

Ensure that you are logged in to the server where SupportAssist Enterprise is installed with root privileges.

#### Steps

1. Open the terminal window.
2. Browse to the `/opt/dell/supportassist/bin` folder.
3. Type `./uninstall` and press Enter.
4. To continue the uninstallation, type `c`.
5. When prompted for your feedback, perform one of the following:
  - To skip the feedback and start the uninstallation, type `n`.
  - To provide feedback, type `y`.
6. If you selected to provide feedback, press a number that matches your reason for uninstalling SupportAssist Enterprise.

The **Dell SupportAssist Enterprise uninstallation is complete** message is displayed.

## Uninstalling SupportAssist Enterprise in silent mode (Linux)

### Prerequisites

Ensure that you are logged in to the server where SupportAssist Enterprise is installed with root privileges.

### Steps


1. Open the terminal window on the system where SupportAssist Enterprise is installed.
2. Browse to the `/opt/dell/supportassist/bin` folder.
3. Type `./uninstall silent` and press Enter.

## Identifying the generation of a Dell PowerEdge server

You can quickly identify the generation of a PowerEdge server by observing the representation of the server model. The following table provides information about the various generations of PowerEdge servers and their model representation.

**Table 12. PowerEdge server examples**

PowerEdge server generation	Representation of the server model	Examples of server models
9th	PowerEdge x9xx	PowerEdge 2900 Power Edge 6950
10th	PowerEdge yx0x	PowerEdge M600 PowerEdge R300 Power Edge T105
11th	PowerEdge yx1x	PowerEdge M610 PowerEdge R310 PowerEdge T110
12th	PowerEdge yx2x	PowerEdge M620 PowerEdge R620 PowerEdge T620
13th	PowerEdge yx3x	PowerEdge M630 PowerEdge R630 PowerEdge R730

 **NOTE:** In the representation of the server models, *x* denotes numbers (0 to 9) and *y* denotes alphabets such as M, R, and T. The alphabets denote the type of server as follows: M = Modular; R = Rack; T = Tower.

# Troubleshooting

The following sections provide the information required to troubleshoot issues that may occur while installing and using SupportAssist Enterprise.

## Installing SupportAssist Enterprise

If you experience any issues while installing SupportAssist Enterprise:

- Ensure that the server is running a 64-bit operating system.
- Ensure that the server where you are installing SupportAssist Enterprise does not have any other SupportAssist application installed already.
- On Windows operating systems, ensure that you right-click the installer package and select **Run as administrator** to start the installation.
- On Linux operating systems, ensure that the permission of the installer file is updated.
- Ensure that you agree to allow Dell to save your Personally Identifiable Information (PII) on the **License Agreement** page of the installation wizard.
- Ensure that the server where you are installing SupportAssist Enterprise has internet connectivity. If the server connects to the internet through a proxy server, enter the proxy server details in the installation wizard.

## SupportAssist Enterprise registration

If you experience any issues with the registration of SupportAssist Enterprise:

- Verify if the server where SupportAssist Enterprise is installed can connect to the internet.
- If the server where SupportAssist Enterprise is installed connects to the internet through a proxy server, enter the proxy server details in the SupportAssist Enterprise **Settings** → **Proxy Settings** page.
- Verify if the network settings of the server where SupportAssist Enterprise is installed are correct.
- Ensure that the registration details, such as first name, last name, email address, and phone number you have provided are valid.
- Ensure that you use an English keyboard layout to type data in the **Phone Number**, **Alternate Phone Number**, and **Email Address** fields.
- Verify if port 443 is open on the firewall to access <https://apidp.dell.com> and <https://api.dell.com>.
- Perform the **Network Connectivity Test** and ensure that connectivity to the SupportAssist server is successful. For instructions to perform the connectivity test, see [Performing the connectivity test](#). If the test is successful, close the web browser, open the SupportAssist Enterprise user interface again, and retry the registration.
- Retry the registration after some time.

## Opening the SupportAssist Enterprise user interface

If a `Problem starting the SupportAssist Service` error is displayed when you open the SupportAssist Enterprise user interface:

- Ensure that you are logged in to the server with a user account that has the required privileges to start system services.
- Try to restart the **Dell SupportAssist Service**. For instructions to restart the SupportAssist Service, see [SupportAssist service](#).
- Check the log file, `application.log`, available at `C:\Program Files\Dell\SupportAssist\logs` (on Windows) or `/opt/dell/supportassist/logs` (on Linux) to identify the component that failed to load.

# Logging in to SupportAssist Enterprise

If you experience any issues while logging in to SupportAssist Enterprise:

- Verify if the user account you are using to log in is a member of the **SupportAssistAdmins** or **SupportAssistUsers** user groups:
  - Open a command prompt as an administrator and type the following commands: `net localgroup SupportAssistAdmins` and `net localgroup SupportAssistUsers`. If the user account is not listed in the **SupportAssistAdmins** or **SupportAssistUsers** group, add the user account to one of the SupportAssist Enterprise user groups.
  - If you want to add users to the SupportAssist Enterprise users groups, open a command prompt as an administrator, and type the following commands:
    - \* `net localgroup SupportAssistAdmins <User1> /add` — To add User1 to the **SupportAssistAdmins** user group.
    - \* `net localgroup SupportAssistUsers <User2> /add` — To add User2 to the **SupportAssistUsers** user group.
- If you manually deleted the **SupportAssistAdmins** or **SupportAssistUsers** user groups, create the SupportAssist Enterprise user groups, and then add users to the groups:
  - To create the SupportAssist Enterprise user groups, open a command prompt as an administrator, and type the following commands:
    - \* `net localgroup SupportAssistAdmins /add` — To create the **SupportAssistAdmins** user group.
    - \* `net localgroup SupportAssistUsers /add` — To create the **SupportAssistUsers** user group.
  - To add users to the SupportAssist Enterprise users groups, open a command prompt as an administrator, and type the following commands:
    - \* `net localgroup SupportAssistAdmins <User1> /add` — To add User1 to the **SupportAssistAdmins** user group.
    - \* `net localgroup SupportAssistUsers <User2> /add` — To add User2 to the **SupportAssistUsers** user group.
- Verify if the **Dell SupportAssist Service** is running. For instructions to verify the status of the SupportAssist Service, see [SupportAssist service](#).

## Unable to add device

If a device displays an  **Unable to add device** status:

- If the device is an iDRAC, ensure that the iDRAC has an Enterprise or Express license installed. For information on purchasing and installing an Enterprise or Express license, see "Managing Licenses" section in the *iDRAC User's Guide* at [Dell.com/idracmanuals](#).
- If the device is a Compellent storage array, ensure that SupportAssist is enabled in Enterprise Manager. For information on enabling SupportAssist in Enterprise Manager, see the *Dell Enterprise Manager Administrator's Guide* at [Dell.com/storagemanuals](#).
- Revalidate the device. See [Revalidating a device](#).

If an error message is displayed stating that SupportAssist Enterprise is unable to add the device:

- Ensure that the device model is supported. For a complete list of supported device models, see the *Dell SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](#).
- Ensure that the prerequisites for adding the device are met. For information on the prerequisites for adding a device, see [Adding devices](#).

- Verify if the device is reachable from the server where SupportAssist Enterprise is installed.
- Verify if the device credentials (user name and password) you provided are correct.
- If the error message states that the device could not be added within the predefined time limit, retry adding the device.

## Servers

- If you are adding a server by providing the operating system details (agent-based monitoring) and the device is running a Windows operating system:
  - Verify if the credentials you provided have administrator rights on the device.
  - Verify if the Windows Management Instrumentation (WMI) service is running on the device.
  - If the issue persists, review the instructions in “Securing a Remote WMI Connection” technical documentation at [msdn.microsoft.com](https://msdn.microsoft.com).
- If you are adding a server by providing the operating system details (agent-based monitoring) and the device is running a Linux operating system:
  - Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist Enterprise. See [Configuring sudo access for SupportAssist Enterprise \(Linux\)](#).
  - Verify if the Secure Shell (SSH) service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).
- If you are adding a server by providing the iDRAC details (agentless monitoring), ensure that the iDRAC has an Enterprise or Express license installed. For information on purchasing and installing an Enterprise or Express license, see the “Managing Licenses” section in the *iDRAC User’s Guide* at [Dell.com/idracmanuals](https://Dell.com/idracmanuals).
- If the error message states that SupportAssist Enterprise is unable to add the device because the SSL encryption level of the device is set to 256 bit or higher:
  - a. Download the [Zulu Cryptographic Extension Kit](#) available at the Azul Systems website.
  - b. Extract the downloaded file.
  - c. Copy the **local\_policy.jar** and **US\_export\_policy.jar** files and paste them at the following location on the system where SupportAssist Enterprise is installed:
    - On Windows: **C:\Program Files\Dell\SupportAssist\jre\lib\security**
    - On Linux: **/opt/dell/supportassist/jre/lib/security**
  - d. Restart the SupportAssist service and retry the operation.

## Storage

If the device is an EqualLogic PS storage array:

- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- Ensure that you provide the management group IP address of the device in the add device wizard.

If the device is a Compellent SC series storage array:

- Ensure that the REST service is running on the device.
- Ensure that SupportAssist is enabled in Enterprise Manager. For information on enabling SupportAssist in Enterprise Manager, see the *Dell Enterprise Manager Administrator’s Guide* at [Dell.com/storagemanuals](https://Dell.com/storagemanuals).

If the device is a FluidFS NAS device, ensure that SSH service is running on the device.

## Networking

- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- If the enable password is configured on the device, ensure that you provide the enable password in the add device wizard.

## Chassis

Ensure that Secure Shell (SSH) service is running on the device.

## Importing multiple devices

If you have problems importing multiple devices by using a .csv file:

- Ensure that the .csv file is valid. If necessary, download the .csv template and use it for importing devices.
- Ensure that the .csv file is not corrupted.
- Ensure that you have not edited the header in the .csv file.
- If some devices are not imported, download the list of failed devices as a .csv file. Then, open the file to see the reason why the devices were not imported.
- Ensure that you have followed the instructions in [Importing multiple devices](#).
- If devices are added to the **Staging** group:
  - a. Ensure that all prerequisites for adding the device are met. For information on the prerequisites for adding a device, see the "Prerequisites" section in the instructions for adding each device type. See [Adding a single device](#).
  - b. Revalidate each device. See [Revalidating a device](#).

## OMSA not installed

If a device displays an  **OMSA not installed** status:

- Install OMSA on the device by using the **Install / Upgrade OMSA** option. See [Installing or upgrading OMSA by using SupportAssist Enterprise](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log in to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](#).

## SNMP not configured

If a device displays an  **SNMP not configured** status:

- Configure the SNMP settings on the device by using the **Configure SNMP** option. See [Configuring SNMP settings by using SupportAssist Enterprise](#).
- If the SNMP configuration cannot be completed successfully even after repeated attempts, log in to the device and manually configure SNMP settings. For instructions to manually configure the SNMP settings:
  - For a server or hypervisor that you have added in SupportAssist Enterprise by using the operating system IP address: [Manually configuring the alert destination of a server](#).
  - For a server that you added in SupportAssist Enterprise by using the iDRAC IP address: [Manually configuring the alert destination of an iDRAC by using the web interface](#).

## New version of OMSA available

If a device displays a  **New version of OMSA available** status:

- Install OMSA on the device by using the **Install / Upgrade OMSA** option. See [Installing or upgrading OMSA by using SupportAssist Enterprise](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log in to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](#).

## Unable to configure SNMP

If a device displays an  **Unable to configure SNMP** status:

- Ensure that the network settings are correct.
- Ensure that the SNMP port (162) is open.
- Ensure that the firewall settings are correct.
- Configure the SNMP settings of the device by using the **Configure SNMP** option. See [Configuring SNMP settings by using SupportAssist Enterprise](#).

If the SNMP configuration is still unsuccessful, you can manually configure the SNMP. For instructions to manually configure the SNMP settings:

- For a server or hypervisor that you have added in SupportAssist Enterprise by using the operating system IP address: [Manually configuring the alert destination of a server](#).
- For a server that you added in SupportAssist Enterprise by using the iDRAC IP address: [Manually configuring the alert destination of an iDRAC by using the web interface](#).

## Unable to verify SNMP configuration


If the device displays an  **Unable to verify SNMP configuration** status:

- Ensure that the DNS is configured correctly.
- Ensure that the SNMP port (162) is open.
- Ensure that the firewall settings are correct.
- Configure the SNMP settings of the device by using the **Configure SNMP** option. See [Configuring SNMP settings by using SupportAssist Enterprise](#).

## Unable to install OMSA

If a device displays an  **Unable to install OMSA** status:

- Verify if the device is reachable from the server where SupportAssist Enterprise is installed.
- Verify if the device credentials (user name and password) you provided are correct.
- If the device is running a Windows operating system:
  - Verify if the credentials you provided have administrator rights on the device.
  - Restart the Windows Management Instrumentation (WMI) service on both the server where SupportAssist Enterprise is installed and the remote device.
  - Delete any files available in the **C:\Windows\temp** folder on the server where SupportAssist Enterprise is installed.
- If the device is running a Linux operating system:
  - Verify if the Secure Shell (SSH) service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).
  - Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist Enterprise. See [Configuring sudo access for SupportAssist Enterprise \(Linux\)](#).
  - Ensure that the device has all the required OMSA dependencies installed. For more information about OMSA dependencies, see the “Remote Enablement Requirements” section in the *Dell OpenManage Server Administrator Installation Guide* at [DellTechCenter.com/OMSA](#).
- Retry the installation of OMSA. See [Installing or upgrading OMSA by using SupportAssist Enterprise](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log in to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](#).

 **NOTE:** Upgrade from a 32-bit version of OMSA to a 64-bit version of OMSA is not supported. In this scenario, you must uninstall the existing version of OMSA, and install OMSA by using SupportAssist Enterprise. For instructions to install OMSA by using SupportAssist Enterprise, see [Installing or upgrading OMSA by using SupportAssist Enterprise](#).

## Unable to verify OMSA version

If an error message is displayed stating that SupportAssist Enterprise is unable to verify the OMSA version installed on the device:

- Click the error status link in the **Status** column on the **Devices** page to view the possible resolution steps.
- Perform the connectivity test and ensure that connectivity to the Dell FTP server is successful. See [Performing the connectivity test](#).
- Ensure that the OMSA services are running on the device.
- Retry the installation of OMSA. See [Installing or upgrading OMSA by using SupportAssist Enterprise](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log in to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix* at [Dell.com/ServiceabilityTools](#).

## OMSA not supported

If a device displays the  **OMSA not supported** status:

- Log in to the device and uninstall the existing version of OMSA.
- Install OMSA on the device by using the **Install / Upgrade OMSA** option. See [Installing or upgrading OMSA by using SupportAssist Enterprise](#).

## Unable to reach device

If a device displays an  **Unable to reach device** status:

- Click the error status link in the **Status** column on the **Devices** page to view the possible resolution steps.
- Verify if the device is turned on and connected to the network.
- Verify if ports 22, 23, 80, 135, 443, 1311, 2463, and 5989 are open on the device.
- If you added the device in SupportAssist Enterprise by providing the device IP address, verify if the IP address of the device has changed. The IP address may change each time the device is restarted, if the device is configured to obtain a dynamic IP address.
- If the IP address of the device has changed:
  - Delete the device from SupportAssist Enterprise. See [Deleting a device](#).
  - Add the device again. See [Adding devices](#).

 **NOTE:** To avoid deleting and adding a device each time the IP address of the device changes, Dell recommends that you provide the host name of the device (instead of the IP address) while adding the device.

## Unable to gather system information

If a device displays an  **Unable to gather system information** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Verify if the device is reachable from the server where SupportAssist Enterprise is installed.
- Verify if the device credentials (user name and password) you provided are correct.
- If the password of the device is lengthy (10 or more characters), try assigning a shorter password (about 5 to 7 characters), that does not include spaces and quotes, and then update the password in SupportAssist Enterprise.

## Servers

- If you are adding a device by providing the operating system details (agent-based monitoring) and the device is running a Windows operating system:
  - Verify if the credentials you provided have administrator rights on the device.
  - Verify if the Windows Management Instrumentation (WMI) service is running on the device.
  - If the issue persists, review the instructions in “Securing a Remote WMI Connection” technical documentation at [msdn.microsoft.com](https://msdn.microsoft.com).
- If you are adding a device by providing the operating system details (agent-based monitoring) and the device is running a Linux operating system:
  - Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist Enterprise. See [Configuring sudo access for SupportAssist Enterprise](#).
  - Verify if the Secure Shell (SSH) service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).
  - Ensure that OpenSSL is updated. For more information, see the resolution for *OpenSSL CCS injection vulnerability (CVE-2014-0224)* available in the support website of the operating system.
- If you are adding a device by providing the iDRAC details (agentless monitoring), ensure that the iDRAC has an Enterprise or Express license installed. For information on purchasing and installing an Enterprise or Express license, see the “Managing Licenses” section in the *iDRAC User’s Guide* at [Dell.com/idracmanuals](https://Dell.com/idracmanuals).
- If the error message states that SupportAssist Enterprise is unable to gather system information from the device because the SSL encryption level of the device is set to 256 bit or higher:
  - a. Download the [Zulu Cryptographic Extension Kit](#) available at the Azul Systems website.
  - b. Extract the downloaded file.
  - c. Copy the `local_policy.jar` and `US_export_policy.jar` files and paste them at the following location on the system where SupportAssist Enterprise is installed:
    - On Windows: `C:\Program Files\Dell\SupportAssist\jre\lib\security`
    - On Linux: `/opt/dell/supportassist/jre/lib/security`
  - d. Restart the SupportAssist service and retry the operation.

After resolving the underlying issue, manually initiate the collection and upload of system information. See [Starting the collection of system information from a single device](#).

## Storage

If the device is an EqualLogic PS storage array:

- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- Ensure that you provide the management group IP address of the device in the add device wizard.

If the device is a Compellent SC series storage array:

- Ensure that the REST service is running on the device.
- Ensure that SupportAssist is enabled in Enterprise Manager. For information on enabling SupportAssist in Enterprise Manager, see the *Dell Enterprise Manager Administrator’s Guide* at [Dell.com/storagemanuals](https://Dell.com/storagemanuals).

If the device is a FluidFS NAS device, ensure that SSH service is running on the device.

## Networking

- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- If the enable password is configured on the device, ensure that you provide the enable password in SupportAssist Enterprise.

## Chassis

Ensure that Secure Shell (SSH) service is running on the device.

## Insufficient storage space to gather system information

If a device displays an  **Insufficient storage space to gather system information** status, ensure that the server where SupportAssist Enterprise is installed has sufficient free space on the C:\drive.

## Unable to export collection

If a device displays an  **Unable to export collection** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Manually initiate the collection and upload of system information. See [Starting the collection of system information from a single device](#).

If the problem persists, contact Dell Technical Support for assistance.

## Unable to send system information

If a device displays an  **Unable to send system information** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Verify if the server where SupportAssist Enterprise is installed is able to connect to the internet.
- If the server where SupportAssist Enterprise is installed connects to the internet through a proxy server, ensure that the proxy settings are configured in SupportAssist Enterprise. See [Configuring proxy server settings](#).
- Perform the network connectivity test and ensure that connectivity to the Dell upload server is successful. See [Performing the connectivity test](#).

After resolving the underlying issue, manually initiate the collection and upload of system information. See [Starting the collection of system information from a single device](#).

## Authentication failed

If a device displays an  **Authentication failed** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Verify if the device credentials (user name and password) you provided are correct. If the credentials have changed, update the credentials of the device. See [Editing device credentials](#).

## Server

- If you added the device by providing the operating system details (agent-based monitoring) and the device is running a Windows operating system:
  - Verify if the credentials you provided have administrator rights on the device.
  - Verify if the WMI service is running on the device.
  - If the issue persists, review the instructions in “Securing a Remote WMI Connection” technical documentation at [msdn.microsoft.com](https://msdn.microsoft.com).
- If you added the device by providing the operating system details (agent-based monitoring) and the device is running a Linux operating system:

- Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist Enterprise. See [Configuring sudo access for SupportAssist Enterprise \(Linux\)](#).
- Verify if the SSH service is running on the device.
- Verify if SSH password authentication is enabled (enabled by default).

## Storage

If the device is an EqualLogic PS storage array:

- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- Ensure that you provide the management group IP address of the device in the add device wizard.

If the device is a Compellent SC series storage array:

- Ensure that the REST service is running on the device.
- Ensure that SupportAssist is enabled in Enterprise Manager. For information on enabling SupportAssist in Enterprise Manager, see the *Dell Enterprise Manager Administrator's Guide* at [Dell.com/storagemanuals](http://Dell.com/storagemanuals).

If the device is a FluidFS NAS device, ensure that SSH service is running on the device.


## Networking

- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- If the enable password is configured on the device, ensure that you provide the enable password in the add device wizard.

## Chassis

Ensure that Secure Shell (SSH) service is running on the device.

## Clearing System Event Log failed

If the device displays a  **Clearing System Event Log failed** status, ensure that the following requirements are met and then retry clearing the System Event Log:

- The device is reachable from the server where SupportAssist Enterprise is installed.
- If the device is a member of a domain, the host name of the device is added in the DNS server.
- The credentials you have provided for the device in SupportAssist Enterprise are correct.
- The credentials you have provided for the device in SupportAssist Enterprise have administrative privileges.
- If you have added the device in SupportAssist Enterprise with the operating system IP address, ensure that the following requirements are met depending on the operating system running on the device:
  - For Windows, the WMI service is running on the device and the firewall allows WMI communication.
  - For Linux, the SSH service is running on the device and the firewall allows SSH communication.
- If you have added the device in SupportAssist Enterprise with the iDRAC IP address, the WS-MAN service is running on the device.

If the problem persists, try clearing the System Event Log by using one of the following methods:

- [Clearing the System Event Log by using iDRAC](#)
- [Clearing the System Event Log by using OMSA](#)


## Clearing the System Event Log by using iDRAC

### Prerequisites

Ensure that you are logged in to the iDRAC web console with administrative privileges.

### About this task

You can perform the following steps to clear the System Event Log by using the iDRAC web console.

 **NOTE: If you want to clear the System Event Log using the command line interface (CLI), connect to the iDRAC over SSH protocol using any telnet client and run the following command: `racadm clrsl`**

### Steps

1. In the iDRAC web console, click **Overview** → **Server** → **Logs Page**.
2. Click **Clear Log**.

## Clearing the System Event Log by using OMSA

### Prerequisites

Ensure that you are logged in to OMSA with administrative privileges.

### About this task

If OMSA is installed on the device, you can perform the following steps to clear the System Event Log.

 **NOTE: If you want to clear the System Event Log using the CLI, log in to the device and run the following command from a command prompt (Windows) or terminal (Linux): `omconfig system esmlog action=clear`**

 **NOTE: If the device is running VMware ESX, log in to OMSA from another remote device using the Server Administrator Managed System Login option, and then perform the following steps.**

### Steps

1. In OMSA, perform one of the following, depending on the type of server:
  - If the device is a modular server, click **Modular Enclosure** → **Server Module**.
  - If the device is not a modular server, click **System** → **Main System Chassis**.
2. Click the **Logs** tab.
3. Click **Clear Log**.

## Maintenance mode

If a device displays the  **Maintenance Mode** status:

- Ensure that the issue with the device is resolved.
- If more time is required to resolve the issue, you may place the device in manual maintenance mode. See [Enabling or disabling device-level maintenance mode](#).
- If required, you may place SupportAssist Enterprise in maintenance mode. See [Enabling or disabling global-level maintenance mode](#).

## Auto update

If the auto update is unsuccessful:

1. Perform the network connectivity test and ensure that connectivity to the Dell FTP server is successful. See [Performing the connectivity test](#).
2. Click the **Update Available** banner and try installing the update again.

## Unable to edit device credentials

If an error message is displayed stating that SupportAssist Enterprise is unable to edit the credentials of a device:

- Verify if the device is reachable from the server where SupportAssist Enterprise is installed.
- Verify if the device credentials (user name and password) you provided are correct.

## Servers

- If you are editing the credentials of a device running a Windows operating system:
  - Verify if the credentials you provided have administrator rights on the device.
  - Verify if the Windows Management Instrumentation (WMI) service is running on the device.
  - If the issue persists, review the instructions in “Securing a Remote WMI Connection” technical documentation at [msdn.microsoft.com](https://msdn.microsoft.com).
- If you are editing the credentials of a device running a Linux operating system:
  - Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist Enterprise. See [Configuring sudo access for SupportAssist Enterprise \(Linux\)](#).
  - Verify if the Secure Shell (SSH) service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).
- If the error message states that SupportAssist Enterprise is unable to edit the credentials of the device because the SSL encryption level of the device is set to 256 bit or higher:
  - a. Download the [Zulu Cryptographic Extension Kit](#) available at the Azul Systems website.
  - b. Extract the downloaded file.
  - c. Copy the `local_policy.jar` and `US_export_policy.jar` files and paste them at the following location on the system where SupportAssist Enterprise is installed:
    - On Windows: `C:\Program Files\Dell\SupportAssist\jre\lib\security`
    - On Linux: `/opt/dell/supportassist/jre/lib/security`
  - d. Restart the SupportAssist service and retry the operation.

## Storage

If the device is an EqualLogic PS storage array:

- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- Ensure that you provide the management group IP address of the device in the add device wizard.

If the device is a Compellent SC series storage array:

- Ensure that the REST service is running on the device.
- Ensure that SupportAssist is enabled in Enterprise Manager. For information on enabling SupportAssist in Enterprise Manager, see the *Dell Enterprise Manager Administrator's Guide* at [Dell.com/storagemanuals](https://Dell.com/storagemanuals).

If the device is a FluidFS NAS device, ensure that SSH service is running on the device.

## Networking


- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- If the enable password is configured on the device, ensure that you provide the enable password in the add device wizard.

## Chassis

Ensure that Secure Shell (SSH) service is running on the device.

## Automatic case creation

If an issue occurs on a device, but a support case is not created automatically:

 **NOTE: SupportAssist Enterprise does not create a support case for every alert received from a monitored device. A support case is created only if the alert type and number of alerts received from a device match with the criteria defined by Dell for support case creation.**

- Ensure that the device is a server, networking switch, or chassis.
- Ensure that monitoring is enabled for the device in SupportAssist Enterprise. See [Enabling or disabling monitoring of a device](#).
- Ensure that the device is configured to forward alerts to the server where SupportAssist Enterprise is installed.
- Perform the network connectivity test and ensure that the connectivity to the SupportAssist server is successful. See [Performing the connectivity test](#).
- Perform the case creation test and ensure that the **Ready to Create Cases** status is displayed. See [Testing the case creation capability](#).
- Check the **application.log** file available at `C:\Program Files\Dell\SupportAssist\logs` (on Windows) or `/opt/dell/supportassist/logs` (on Linux) to identify if the alert was received successfully by SupportAssist Enterprise.

## Scheduled tasks

If the time or time zone of the system on which SupportAssist Enterprise is installed is changed, all built-in and user-defined schedule tasks do not work as expected. Examples of scheduled tasks include the following:

- Periodic collection of system information from monitored devices
- Upload of device inventory information to Dell
- Connectivity test email notifications

To resolve this issue, restart the **Dell SupportAssist Service**.

## SupportAssist service

If the SupportAssist Enterprise application does not respond appropriately, ensure that the SupportAssist service is running:

1. On the server where SupportAssist Enterprise is installed, verify if the SupportAssist service is running. For information on verifying the status of the SupportAssist service, see [Verifying the SupportAssist service status \(Windows\)](#) or [Verifying the SupportAssist service status \(Linux\)](#).
2. If the service cannot or does not start, open the most recent SupportAssist Enterprise application log file (**application.log**), and then search for text with a timestamp of when you tried to start the service. The log file may contain a message indicating any user interface startup errors and a possible problem diagnosis.

 **NOTE: You can access the SupportAssist Enterprise application log file (application.log) at the following location depending on the operating system:**

- On Windows — `C:\Program Files\Dell\SupportAssist\logs`
  - On Linux — `/opt/dell/supportassist/logs`
3. To verify if the SupportAssist Enterprise application can connect to the SupportAssist Enterprise server hosted by Dell, perform the connectivity test. See [Performing the connectivity test](#).
    - If the server is responding, a success message is displayed in the user interface. If not, the server may be unreachable. If this is the scenario, check the **application.log** file to find details. If there are no discernible details in the log file, and the server is not reachable, contact Dell Technical Support for assistance.
    - If communication is successful, but no data updates occur, the SupportAssist Enterprise application may be identifying itself with an ID that is unknown to the server. If this is the scenario, check the **application.log** file to find details. The log file may contain a message stating that the SupportAssist Enterprise application was not recognized. If the SupportAssist Enterprise application is not recognized by the SupportAssist server, uninstall and reinstall the SupportAssist Enterprise application.

## Verifying the SupportAssist service status (Windows)

To verify the status of the SupportAssist service on Windows operating systems:

1. On the server where SupportAssist Enterprise is installed, click **Start** → **Run**.  
The **Run** dialog box is displayed.
2. Type `services.msc`, and then click **OK**.  
The **Services** Microsoft Management Console (MMC) is displayed.
3. Verify if the **Dell SupportAssist Service** displays the status as **Running**.
4. If the service is not running, right-click the service and select **Start**.

## Verifying the SupportAssist service status (Linux)

To verify the status of the SupportAssist service on Linux operating system:

1. Open the terminal window on the system where SupportAssist Enterprise is installed.
2. Type `service supportassist status` and press Enter.  
The status of the SupportAssist service is displayed.
3. If the service is not running, type `service supportassist start` and press Enter.  
The SupportAssist service is restarted.

## Other services

To add a device and perform other operations on the device, SupportAssist Enterprise requires the following services to be installed and running on the device:

- WMI service (on devices running a Windows operating system)
- SSH service (on devices running a Linux operating system)

If the services are either not installed or not running, an error message is displayed in SupportAssist Enterprise. The following sections provide information about verifying the status of the service and restarting the service (if required).

### WMI service

To verify the status of the WMI service and to start the service (if required):

1. Click **Start** → **Run**. The **Run** dialog box is displayed.
2. Type `services.msc`, and then click **OK**. The **Services** Microsoft Management Console (MMC) is displayed.
3. In the list of services, verify the status of the **Windows Management Instrumentation** service. If the service is running, the status is displayed as **Running**.
4. If the service does not display a **Running** status, right-click **Windows Management Instrumentation** and click **Start**.

### SSH service

You can use the following commands to verify the status of the SSH service and to start the service (if required):

- `service sshd status` — Displays the status of the SSH service.
- `service sshd start` — Starts the SSH service.

## Security

If the **Edit Credentials** or **Start Collection** links remain disabled even after selecting a device in the **Devices** page, ensure that you are logged in to SupportAssist Enterprise with elevated or administrative privileges. See [SupportAssist Enterprise user groups](#) and [Granting elevated or administrative privileges to users](#).


# SupportAssist Enterprise user interface

The Dell EMC SupportAssist Enterprise user interface contains the following tabs:

- **Cases** — Displays the support cases that are present for the devices that you have added in SupportAssist Enterprise.
- **Devices** — Displays the devices that you have added in SupportAssist Enterprise and their status. You can point to the **Devices** tab and click **Groups** to access the **Device Groups** page.
- **Settings** — Enables you to configure the options available in SupportAssist Enterprise. You can point to the **Settings** tab and click the available options to access following pages:
  - **Collection Schedules** — Enables you to select a custom schedule for collecting system information from your devices.
  - **Proxy Settings** — Enables you to configure the proxy server settings in SupportAssist Enterprise.
  - **Preferences** — Enables you to configure your preferences for tasks, collections, email notification, reports, and maintenance mode.
  - **Contact Information** — Enables you to update the details of your primary and secondary contacts.
  - **SMTP Settings** — Enables you to configure the details of the SMTP server utilized by your company.
- **Collections** — Displays the list of collections that have been performed.

At the top-right of the SupportAssist Enterprise header area, you can access links that allow you to navigate to resources or perform certain tasks. The following table describes the use of the available links.


**Table 13. Links in the SupportAssist Enterprise header area**

Link	Description
<b>SupportAssist Enterprise Community</b>	Opens the SupportAssist Enterprise community website in a new browser window.
<b>About</b>	Provides information about the SupportAssist Enterprise version, registration ID, policy file version, device configuration version, and the update history.
<b>User name</b>	<p>Displays the user name of the currently logged in user. Point to the <b>user name</b> link to view a drop-down list that contains the following links:</p> <ul style="list-style-type: none"> <li>• <b>Connectivity Test</b> — Opens the <b>Network Connectivity Test</b> page.</li> <li>• <b>SupportAssist Enterprise Test</b> — Opens the <b>SupportAssist Enterprise Test</b> page.</li> <li>• <b>Logout</b> — Allows you to log out of SupportAssist Enterprise.</li> </ul> <p> <b>NOTE: The Connectivity Test and SupportAssist Enterprise Test links are enabled only if you are logged in to SupportAssist Enterprise with administrative or elevated privileges.</b></p>
<b>Help icon</b>	Opens the context-sensitive help.

In some scenarios, a yellow banner may be displayed at the top of the SupportAssist Enterprise user interface. The following table describes the banners that may be displayed.

**Table 14. Banners in the SupportAssist Enterprise header area**

Banner	Description
Not registered	<p>This banner is displayed if you have not completed the registration of SupportAssist Enterprise. The not registered banner displays the following options:</p> <ul style="list-style-type: none"> <li>• <b>Register now</b> — To register SupportAssist Enterprise.</li> </ul>

Banner	Description
	<ul style="list-style-type: none"> <li>· <b>Remind me later</b> — To close the 'not registered' banner. The 'not registered' banner is not displayed until you log in to SupportAssist Enterprise again.</li> <li>· <b>Why register</b> — To learn about the importance of registering SupportAssist Enterprise.</li> </ul>
Update available	<p>This banner is displayed in the following scenarios:</p> <ul style="list-style-type: none"> <li>· If an update is available, but you have disabled the automatic update of the SupportAssist Enterprise application, policy files, and product support files.</li> <li>· If an error occurred during the update of SupportAssist Enterprise.</li> </ul> <p>The update available banner displays the following options:</p> <ul style="list-style-type: none"> <li>· <b>Update now</b> — To allow SupportAssist Enterprise to download and install the update.</li> <li>· <b>Skip this version</b> — To skip the update. The update available banner is not displayed again until the next version of the update is available.</li> <li>· <b>Remind me later</b> — To close the 'update available' banner. The 'update available' banner is not displayed until you log in to SupportAssist Enterprise again.</li> </ul> <p> <b>NOTE: The update available banner is displayed only if you are logged in to SupportAssist Enterprise with administrative or elevated privileges.</b></p>
<b>Maintenance Mode</b>	<p>This banner is displayed when you place SupportAssist Enterprise in maintenance mode. For more information on maintenance mode, see <a href="#">Understanding maintenance mode</a>.</p>

**Related links**

- [SupportAssist Enterprise Registration Wizard](#)
- [Login page](#)
- [Cases page](#)
- [Devices page](#)
- [Settings](#)
- [Collections page](#)
- [Network Connectivity Test](#)
- [Test SupportAssist Enterprise](#)

## SupportAssist Enterprise Registration Wizard

The **SupportAssist Enterprise Registration Wizard** guides you through the setup and registration of SupportAssist Enterprise. The fields displayed in the pages of the **SupportAssist Enterprise Registration Wizard** are described in the following sections.

**Related links**

- [Welcome](#)
- [Proxy Settings](#)
- [Registration](#)
- [Summary](#)
- [Registering SupportAssist Enterprise](#)

### Welcome

The **Welcome** page enables you to start the registration of SupportAssist Enterprise. Click **Next** to start the registration of SupportAssist Enterprise.

## Proxy Settings

The **Proxy Settings** page allows you to configure the proxy server settings.

 **NOTE:** The **Proxy Settings** page is displayed only if you confirm that the system connects to the Internet through a proxy server.

The following table provides information about the fields displayed in the **Proxy Settings** page.

**Table 15. Proxy Settings**

Field	Description
<b>Use proxy settings</b>	Select this option to enable configuring the proxy server settings.
<b>Proxy Server Address or Name</b>	The proxy server address or name.
<b>Proxy Port Number</b>	The proxy server port number.
<b>Proxy requires authentication</b>	Select this option if the proxy server requires authentication.
<b>Username</b>	The user name required to connect to the proxy server.
<b>Password</b>	The password required to connect to the proxy server.

## Registration

The **Registration** page enables you to provide your contact information and register SupportAssist Enterprise.

The fields displayed in the **Registration** page are described in the following table.

**Table 16. Registration**

Field	Description
<b>Company Information</b>	
<b>Company Name</b>	The name of the company.
<b>Country/Territory</b>	The location of the company.
<b>Primary Contact Information</b>	
<b>First Name</b>	The first name of the primary contact.
<b>Last Name</b>	The last name of the primary contact.
<b>Phone Number</b>	The phone number of the primary contact.
<b>Alternate Phone Number</b>	The alternate phone number of the primary contact.
<b>Email Address</b>	The email address of the primary contact. SupportAssist Enterprise email notifications will be sent to this email address.

## Summary

The **Summary** page allows you to complete the setup. Click **Finish** to open the SupportAssist Enterprise **Devices** page.

## Login page

The following table describes the fields displayed in the SupportAssist Enterprise login page.

Table 17. Login page

Field	Description
Username	User name required to log in to SupportAssist Enterprise.
Password	Password required to log in to SupportAssist Enterprise.
Login	Click to log in to SupportAssist Enterprise.

**Related links**


[Logging in to SupportAssist Enterprise](#)

## Cases page

The **Cases** page displays the support cases that are present for your devices that you have added in SupportAssist Enterprise. For devices with a ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract, the **Cases** page displays the case status irrespective of the case creation method. By default, the displayed support cases are grouped under their respective device name or device IP address. The last refreshed date and time that is displayed in the group header indicates when the case information was last retrieved from Dell.

The **Case Options** list, available at the top of the cases information, enables you to manage support cases that were opened by SupportAssist Enterprise based on your requirement. The following are the available options:

- **Suspend Activity 24 hours** — To request Dell Technical Support to suspend activities related to a support case for 24 hours. After 24 hours, Dell Technical Support automatically resumes activities related to the support case.
- **Resume Activity** — To request Dell Technical Support to resume activities related to a support case.

 **NOTE: The Resume Activity option is enabled only if you had previously requested to suspend activities related to a support case.**


- **Request to Close** — To request Dell Technical Support to close a support case.

 **NOTE: Only support cases that were opened by SupportAssist Enterprise can be managed by using the Case Options list.**

The **Refresh** link enables you to refresh the displayed cases.

The following table describes the support case information for your Dell devices that are monitored by SupportAssist Enterprise, as displayed in the **Cases** page.

Table 18. Cases page

Column name	Description
Check box	Use to select a support case for performing case management actions.   <b>NOTE: The check box is displayed only for cases that were automatically created by SupportAssist Enterprise.</b>
Name/IP Address	Displays the display name, host name, or IP address depending on the information you have provided for the device. The device name is displayed as a link that you can click to open the <b>Devices</b> page.
Number	The numeric identifier assigned to the support case.
Status	The current state of the support case. The status of a support case may be: <ul style="list-style-type: none"> <li>• <b>Submitted</b> — SupportAssist Enterprise has submitted the support case.</li> <li>• <b>Open</b> — Dell Technical Support has opened the submitted support case.</li> <li>• <b>In Progress</b> — Dell Technical Support is working on the support case.</li> <li>• <b>Customer Deferred</b> — Dell Technical Support has deferred the support case at the customer's request.</li> <li>• <b>Reopened</b> — The support case was previously closed, and has been reopened.</li> <li>• <b>Suspended</b> — Dell Technical Support has suspended activities related to the support case for 24 hours based on your request.</li> </ul>

Column name	Description
	<ul style="list-style-type: none"> <li>• <b>Closure Requested</b> — You have requested Dell Technical Support to close the support case.</li> <li>• <b>Closed</b> — The support case is closed.</li> <li>• <b>Not Applicable</b> — An issue was detected by SupportAssist Enterprise, but a support case was not created because the device has either an expired warranty or Basic Hardware warranty.</li> <li>• <b>Unavailable</b> — The support case status could not be retrieved from Dell.</li> <li>• <b>Unknown</b> — SupportAssist Enterprise is unable to determine the status of the support case.</li> </ul>
<b>Title</b>	<p>The support case name, which identifies:</p> <ul style="list-style-type: none"> <li>• Support case generation method</li> <li>• Device model</li> <li>• Device operating system</li> <li>• Alert ID, if available</li> <li>• Alert description, if available</li> <li>• Warranty status</li> <li>• Resolution description</li> </ul>
<b>Device Type</b>	Indicates the type of device.
<b>Date Opened</b>	The date and time when the support case was opened.
<b>Source</b>	<p>The method by which the support case was created. The <b>Source</b> column may display:</p> <ul style="list-style-type: none"> <li>• <b>SupportAssist</b> — The support case was created automatically by SupportAssist Enterprise.</li> <li>• <b>Phone</b> — The support case was created by contacting Dell Technical Support over phone.</li> <li>• <b>Email</b> — The support case was created by contacting Dell Technical Support through email.</li> <li>• <b>Chat</b> — The support case was created by contacting Dell Technical Support over chat.</li> <li>• <b>Help Desk</b> — The support case was created through the help desk.</li> <li>• <b>TechDirect</b> — The support case was created through Dell TechDirect.</li> <li>• <b>Others</b> — The support case was created by contacting Dell Technical Support through any other method.</li> </ul>
<b>Service Contract</b>	<p>The Dell service contract level under which the device is covered. The <b>Service Contract</b> column may display:</p> <ul style="list-style-type: none"> <li>• <b>Unknown</b> — SupportAssist Enterprise cannot determine the service contract.</li> <li>• <b>Invalid Service Tag</b> — The Service Tag of the device is invalid.</li> <li>• <b>No Service Contract</b> — This device is not covered under a Dell service contract.</li> <li>• <b>Expired Service Contract</b> — The service contract of the device has expired.</li> <li>• <b>Basic Support</b> — The device is covered under a Dell Basic Hardware service contract.</li> <li>• <b>ProSupport</b> — The device is covered under a Dell ProSupport service contract.</li> <li>• <b>ProSupport Plus</b> — The device is covered under a Dell ProSupport Plus service contract.</li> <li>• <b>ProSupport Flex for Data Center</b> — The device is covered under a ProSupport Flex for Data Center service contract.</li> <li>• <b>ProSupport One for Data Center Or ProSupport Flex for Data Center</b> — The device is covered under a ProSupport One for Data Center Or ProSupport Flex for Data Center service contract.</li> </ul>
<b>Service Tag</b>	A unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.

 **NOTE:** When you check for support cases of a specific device, the support cases of that device are displayed at the top of the Cases page with a blue border for the appropriate rows. See [Checking for support cases](#).

You can choose to refine the displayed devices based on the device type, case status, service contract type, case source, or other criteria. The following are the available options for refining the displayed data:

- **Device Type**
  - **Server**
  - **Storage**
  - **Networking**
  - **Chassis**
- **Case Status**
  - **Open**
  - **Submitted**
  - **In Progress**
  - **Suspended**
  - **Requested for Closure**
- **Service Contract**
  - **Basic**
  - **ProSupport**
  - **ProSupport Plus**
  - **ProSupport Flex for Data Center**
  - **ProSupport One for Data Center Or ProSupport Flex for Data Center**
- **Source Type**
  - **Email**
  - **Phone**
  - **Chat**
  - **SupportAssist**
  - **Help Desk**
  - **TechDirect**
  - **Others**



**NOTE:** You can also use the filter icon  available in the column headers to refine the displayed data based on a specific keyword.

#### Related links

- [Case management options](#)
- [Filtering the displayed data](#)
- [Clearing the data filter](#)
- [Sorting the displayed data](#)

## Devices page

The **Devices** page displays the devices that you have added and status of SupportAssist Enterprise functionality for each device. In the default view, the **Devices** page displays all the devices that you have added.

At the top of the **Devices** page, the navigation trail is displayed.







The following options available at the top of the device list enable you to perform certain tasks:

















- **Add Device** — To add a single device or to import multiple devices.
- **Start Collection** — To initiate a single device or multiple device collection.
- **Edit Credentials** — To edit the user name and password required to log in to a device and collect system information.
- **Delete** — To delete a device from SupportAssist Enterprise.
- **Collection Purpose** — To select a reason for performing a multiple device collection.












- **Refresh** — To refresh the device inventory view.

The following table describes the automatically generated inventory information for your supported Dell devices, as displayed in the **Devices** page.

**Table 19. Devices page**

Column name	Description
Check box	<p>Use to select a device for viewing the device overview pane, or for performing certain tasks on the device.</p> <p> <b>NOTE: The check box is disabled while the following SupportAssist Enterprise initiated tasks are in progress:</b></p> <ul style="list-style-type: none"> <li>• SNMP configuration</li> <li>• Installation or upgrade of OMSA</li> <li>• Clear System Event Log</li> <li>• Collection of system information immediately after an automatic support case creation and also during a manually initiated collection</li> </ul>
<b>Name/IP Address</b>	<p>Displays the following information:</p> <ul style="list-style-type: none"> <li>• Device name — Displays the display name, host name, or IP address depending on the information you have provided for the device.</li> <li>• Collection status — When a collection occurs, a progress bar and a corresponding message are displayed to indicate the status of the collection. The possible collection status messages are as follows: <ul style="list-style-type: none"> <li>– For a collection that you manually initiate: <p> <b>NOTE: When a manually initiated collection is in progress, a  icon is displayed next to the progress bar. Click the  icon to cancel the collection, if necessary.</b></p> <p> <b>NOTE: You can cancel a collection only when SupportAssist Enterprise is collecting data from the device. You cannot cancel a collection while the collected data is being sent to Dell.</b></p> <ul style="list-style-type: none"> <li>* Starting collection</li> <li>* Collection in progress</li> <li>* Sending collection</li> <li>* Canceling collection</li> </ul> </li> <li>– For an automated collection that is initiated because a support case was created for a detected hardware issue: <ul style="list-style-type: none"> <li>* Starting collection for support case</li> <li>* Collection for support case in progress</li> <li>* Sending collection for support case</li> </ul> <p> <b>NOTE: If a hardware issue is detected on a device with a Dell Basic Service contract, the automated collection is initiated. However, a support case is not created for that device.</b></p> </li> <li>– For an automated periodic collection based on the default or configured collection schedule: <ul style="list-style-type: none"> <li>* Starting periodic collection</li> <li>* Periodic collection in progress</li> <li>* Sending periodic collection</li> </ul> </li> </ul> </li> </ul>

Column name	Description
	<p> <b>NOTE: In some instances, when a collection is in progress (manual) on a device another collection (periodic) may be initiated. In such scenarios, the collection status is displayed in the following order of priority:</b></p> <ul style="list-style-type: none"> <li>- Manual collection</li> <li>- Support case collection</li> <li>- Periodic collection</li> </ul> <p>· Maintenance mode — If the device is placed in maintenance mode, the maintenance mode icon  is displayed.</p>
<b>Model</b>	Model of the device. For example, PowerEdge M820.
<b>Status</b>	<p>Displays the status of the SupportAssist Enterprise functionality on the device, and the date and time the status was generated. The status can be categorized as follows:</p> <p><b>Informational status</b></p> <ul style="list-style-type: none"> <li>·  <b>OK</b> — The device is configured correctly for SupportAssist Enterprise functionality.</li> <li>·  <b>Installing OMSA</b> — Installation or upgrade of Dell OpenManage Server Administrator (OMSA) is in progress.</li> <li>·  <b>Configuring SNMP</b> — Configuring the SNMP settings of the device is in progress.</li> <li>·  <b>Clearing System Event Log</b> — Clearing of the System Event Log is in progress.</li> <li>·  <b>System Event Log cleared</b> — System Event Log has been cleared successfully.</li> </ul> <p><b>Warning status</b></p> <ul style="list-style-type: none"> <li>·  <b>OMSA not installed</b> — OMSA is not installed on the device.</li> <li>·  <b>SNMP not configured; OMSA not latest</b> — SNMP settings of the device is not configured and the OMSA version installed on the device is prior to the recommended version of OMSA for SupportAssist Enterprise.</li> <li>·  <b>SNMP not configured</b> — SNMP settings of the device is not configured.</li> <li>·  <b>New version of OMSA available</b> — A newer version of OMSA is available for installation on the device.</li> <li>·  <b>OMSA installed, reboot the added device</b> — Installation of OMSA is complete on the device. Restart the device for the changes to take effect.</li> </ul> <p><b>Error status</b></p> <ul style="list-style-type: none"> <li>·  <b>Unable to add device</b> — SupportAssist Enterprise has placed the device in the <b>Staging</b> group because the device did not meet certain prerequisites. For more information on the <b>Staging</b> group, see <a href="#">Predefined device groups</a>.</li> <li>·  <b>Unable to configure SNMP</b> — SupportAssist Enterprise is unable to configure the SNMP trap destination of the device.</li> <li>·  <b>Unable to verify SNMP configuration</b> — SupportAssist Enterprise is unable to verify the SNMP configuration of the iDRAC.</li> <li>·  <b>Unable to install OMSA</b> — Installation of OMSA could not be completed.</li> </ul>

Column name	Description
	<ul style="list-style-type: none"> <li>·  <b>OMSA not supported</b> — Installation of OMSA is not supported.</li> <li>·  <b>Unable to reach device</b> — SupportAssist Enterprise is unable to communicate with the device.</li> <li>·  <b>Authentication failed</b> — SupportAssist Enterprise cannot log in to the device.</li> <li>·  <b>Unable to gather system information</b> — SupportAssist Enterprise is unable to collect system information from the device.</li> <li>·  <b>Insufficient storage space to gather system information</b> — The server where SupportAssist Enterprise is installed does not have sufficient space to gather system information from the device.</li> <li>·  <b>Unable to export collection</b> — SupportAssist Enterprise is unable to process the collected system information.</li> <li>·  <b>Unable to send system information</b> — SupportAssist Enterprise is unable to send the collected system information to Dell.</li> <li>·  <b>Clearing System Event Log failed</b> — SupportAssist Enterprise is unable to clear the System Event Log or Embedded System Management logs on the device.</li> <li>·  <b>Maintenance Mode</b> — SupportAssist Enterprise has placed the device in automatic maintenance mode because of an alert storm. No new support cases are created while the device is in maintenance. For more information, see <a href="#">Understanding maintenance mode</a>.</li> </ul> <p> <b>NOTE: The  error status may be displayed as a link that you can click to view a description of the issue and the possible resolution steps.</b></p>

You can choose to refine the displayed devices based on the device type, device group, or other criteria. The following are the available options for refining the displayed data:

- **Device Type**
  - **Server**
  - **Storage**
  - **Networking**
  - **Chassis**
- **Groups**
  - **Default**
  - **Staging**
  - Custom groups

 **NOTE: You can also use the filter icon  available in the column headers to refine the displayed data based on a specific keyword.**

The **Devices** page also display the following panes based on your actions:

- Device overview pane — When only a single device is selected. See [Device overview pane](#).
- **Device Import** pane — When you import multiple devices by using a .csv file. See [Device Import pane](#).
- **Multiple Device Collection** pane — When a multiple device collection is in progress. See [Multiple Device Collection pane](#).

## Related links

- [Adding devices](#)
- [Editing device credentials](#)
- [Deleting a device](#)
- [Enabling or disabling device-level maintenance mode](#)
- [Installing or upgrading OMSA by using SupportAssist Enterprise](#)
- [Checking support cases for a specific device](#)
- [Filtering the displayed data](#)
- [Clearing the data filter](#)
- [Sorting the displayed data](#)

## Add Single Device or Import Multiple Devices window

The **Add Single Device or Import Multiple Devices** window allows you to add devices.

You can choose from one of the following options to add devices:



- **Single device** (default) — To add a single device.
- **Multiple devices** — To import multiple devices by using a .csv file.



### Add Single Device

The **Add Single Device** page enables you to select the device type and provide details of the device you want to add.

The following table provides information about the items displayed in **Add Single Device** page

**Table 20. Add Single Device**

Field	Description
<b>Device Type</b>	Displays a list of device types that you can add. The available device types are: <ul style="list-style-type: none"><li>• <b>Chassis</b></li><li>• <b>Fluid File System (FluidFS)</b></li><li>• <b>iDRAC</b></li><li>• <b>Networking</b></li><li>• <b>Peer Storage (PS) / EqualLogic</b></li><li>• <b>PowerVault</b></li><li>• <b>Server / Hypervisor</b></li><li>• <b>Storage Center (SC) / Compellent</b></li></ul>
<b>IP Address / Host Name</b>	IP address or host name of the device that you want to add.  <b>NOTE: For adding an EqualLogic storage array, enter the management IP address.</b>
<b>Name</b> (Optional)	An optional name you want to use for identifying the device. If provided, this name is used to identify the device in SupportAssist Enterprise.
<b>Enable monitoring</b>	To allow SupportAssist Enterprise to monitor the device for hardware issues.  <b>NOTE: The Enable monitoring option is displayed only for the following Device Types: Server / Hypervisor, iDRAC, Chassis, and Networking.</b>
<b>Configure SNMP settings</b>	To allow SupportAssist Enterprise to configure the SNMP settings of the device. Configuring the SNMP settings of the device is a prerequisite to monitor the device for hardware

Field	Description
	<p>issues. By configuring the SNMP settings, alerts (SNMP traps) from device are forwarded to the server where SupportAssist Enterprise is installed.</p> <p> <b>NOTE: The Configure SNMP settings option is displayed only for the following Device Types: Server, iDRAC, and Hypervisor.</b></p>
<b>Install or upgrade OMSA</b>	<p>To allow SupportAssist Enterprise to install or upgrade the recommended version of Dell OpenManage Server Administrator (OMSA) on the device. Installing or upgrading OMSA is required for generating alerts and collecting system information from the device.</p> <p> <b>NOTE: The Install, or upgrade OMSA option is displayed only for the following Device Types: Server and Hypervisor.</b></p>

 **NOTE: If the registration of SupportAssist Enterprise is not complete, when you select the Enable monitoring option, a message is displayed requesting you to complete the registration.**

#### Related links

- [Adding a server or hypervisor](#)
- [Adding an iDRAC](#)
- [Adding a chassis](#)
- [Adding a Dell Networking device](#)
- [Adding a PowerVault MD Series storage array](#)
- [Adding a Dell EqualLogic PS Series storage array](#)
- [Adding a Dell Compellent SC Series storage solution](#)
- [Adding a Dell Fluid File System \(FluidFS\) NAS device](#)

#### **Device Credentials**

The **Device Credentials** page enables you to provide the credentials required to connect and identify the device.

The following table describes the fields displayed in the **Device Credentials** page.

**Table 21. Device Credentials**

Field	Description
<b>Username</b>	The username of a user account that has administrative or elevated privileges on the device.
<b>Password</b>	The password of a user account that has administrative or elevated privileges on the device.
<b>Enable Password</b>	The enable password configured on the device.
<b>Community String</b>	The community string configured on the device.

 **NOTE: The Enable Password and Community String are applicable only for Dell Networking devices.**

 **NOTE: The Community String is also applicable for Dell EqualLogic storage arrays.**

 **NOTE: Device credentials are not required for adding Dell PowerVault devices. Therefore, the Device Credentials page is not displayed when you add a PowerVault device.**

### ***Assign Device Group (Optional)***

The **Assign Device Group (Optional)** page enables you to assign the device to a custom device group.

The following table describes the fields display in the **Assign Device Group (Optional)** page.

**Table 22. Assign Device Group (Optional)**

Field	Description
<b>Name</b>	The name you have provided for the device.
<b>Current Group</b>	The device group the device is assigned to.
<b>Assign Other Group</b>	The available device groups to which you can assign the device.

### ***Summary page***

The **Summary** page displays the status and details of the device addition.

**Table 23. Summary page**

Field	Description
<b>Name</b>	The name that you have provided for the device.
<b>IP Address / Host name</b>	The IP address or host name that you have provided for the device.
<b>Service Tag</b>	A unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.
<b>Device Type</b>	The type of the device.
<b>Model</b>	The model of the device.
<b>OS Type</b>	The operating system installed on the device.
<b>Group</b>	The device group to which the device is assigned.

### **Import Multiple Devices**

The **Import Multiple Devices** page enables you to add multiple devices by using a .csv file.

The following are the items that are displayed on the **Import Multiple Devices** page:

- **Browse** — To select a .csv file that contains details of the devices that you want to import.
- **Download the .csv template** — To download a .csv template that you can use to import multiple devices.
- **Enable monitoring** — To allow SupportAssist Enterprise to monitor the devices for hardware issues. Additional configuration or installation may be required to allow SupportAssist Enterprise to monitor hardware issue that may occur on the devices.

 **NOTE: Monitoring of hardware issues is supported only for Dell server and Dell networking devices.**

#### **Related links**

[Importing multiple devices](#)

### ***Importing Devices***

The **Importing Devices** page displays the status and result of the device import.

The **Importing Devices** page displays the following:

- Progress bar that indicates the status of the device import
- Result of the device import
- Total number of devices that are processed

The result of the device import is displayed in both text and graphical format. The result of the device import is classified as follows:

- **Devices added to the inventory** — Number of devices that were discovered successfully and added to the device inventory.

- **Dependency devices are added to the staging group** — Number of devices that were discovered, but did not meet certain prerequisites. To add a device in the staging group to the device inventory, revalidate the device after the prerequisites are met.

 **NOTE: SupportAssist Enterprise capabilities are not available for devices that are in the Staging group.**

- **Failed devices** — Number of devices could not be discovered.
- **Save failed devices list** — To export details of the devices that were not discovered. The exported .csv file will contain the reason and resolution for the import issue.

 **NOTE: The Save failed devices list option is displayed only if devices could not be discovered.**

While importing devices that are members of one or more domains by using a .csv file, if SupportAssist Enterprise detects that the credentials of two of those devices of a certain domain are incorrect, the import operation is paused for other devices in that domain. The import operation is paused to prevent automatic lockout of the domain account due to repetitive authentication failures. For devices of other domains included in the .csv file, the import process continues normally. If the import process is paused for devices of a certain domain, the **Resume** option is displayed. You can click **Resume** to continue the import process for the other devices in that domain.

You can also use the following options that are available on the **Importing Devices** page:

- **Close** — To close the **Importing Devices** page. You can view progress status in the **Devices** pane.
- **Cancel** — To cancel the device import process.

## Device Import pane

The **Device Import** pane displays the status and result of the device import. This pane is displayed in the **Devices** page when you import multiple devices by using a .csv file.

The **Device Import** pane displays the following:

- Date and time when the device import was started
- Progress bar that indicates the status of the device import
- Result of the device import
- Total number of devices that are processed

The result of the device import is displayed in both text and graphical format. The result of the device import is classified as follows:

- **Devices added to the inventory** — Number of devices that were discovered successfully and added to the device inventory.
- **Dependency devices are added to the staging group** — Number of devices that were discovered, but did not meet certain prerequisites. To add a device in the staging group to the device inventory, revalidate the device after the prerequisites are met.

 **NOTE: SupportAssist Enterprise capabilities are not available for devices that are in the Staging group.**

- **Failed devices** — Number of devices could not be discovered.
- **Save failed devices list** — To export details of the devices that were not discovered. The exported .csv file will contain the reason and resolution for the import issue.

 **NOTE: The Save failed devices list option is displayed only if devices could not be discovered.**

While the device import is in progress, you can click **Cancel** to stop the device import process.

While importing devices that are members of one or more domains by using a .csv file, if SupportAssist Enterprise detects that the credentials of two of those devices of a certain domain are incorrect, the import operation is paused for other devices in that domain. The import operation is paused to prevent automatic lockout of the domain account due to repetitive authentication failures. For devices of other domains included in the .csv file, the import process continues normally. If the import process is paused for devices of a certain domain, the **Resume** option is displayed. You can click **Resume** to continue the import process for the other devices in that domain.

By default, the **Device Import** pane is displayed in an expanded format. You can collapse or expand the display of the **Device Import** pane by using the following options:

- **Hide Details** — Collapses the **Device Import** pane. In the collapsed view, only the progress status of the device import is displayed.


- **Show Details** — Expands the **Device Import** pane.

After the devices are imported, you can click **x** to close the **Device Import** pane.

## Device overview pane

The device overview pane displays the details of a device and allows you to perform certain operations on that device. This pane is displayed when you select only a single device in the **Devices** page.

**Table 24. Device overview pane**

Field	Description
<b>Tasks</b>	<ul style="list-style-type: none"> <li>· <b>Clear System Event Log</b> — To clear the System Event Log (SEL) or Embedded System Management (ESM) log.</li> <li>· <b>Check for Cases</b> — To check for support cases that are present for a device.</li> <li>· <b>Maintenance Mode</b> <ul style="list-style-type: none"> <li>– <b>Enable</b> — To place the device in maintenance mode.</li> <li>– <b>Disable</b> — To place the device in normal mode.</li> </ul> </li> <li>· <b>Dependencies</b> <ul style="list-style-type: none"> <li>– <b>Install / Upgrade OMSA</b> — To install or upgrade OMSA on the device.</li> <li>– <b>Configure SNMP</b> — To configure the SNMP settings of the device.</li> </ul> </li> </ul>
<b>Status</b>	Displays if the device is reachable from the local system (server where SupportAssist Enterprise is installed).
<b>Name</b>	Displays the display name that you have provided for the device.
<b>IP Address / Hostname</b>	Displays the IP address or host name of the device.
<b>Service Tag</b>	Displays a unique, alphanumeric identifier that allows Dell to individually recognize the device.
<b>Device Type</b>	Displays the type of the device. For example, Server.
<b>Model</b>	Displays the model information of the device. For example, PowerEdge M820.
<b>Operating System</b>	Displays the operating system installed on the device.
<b>Monitoring</b>	<ul style="list-style-type: none"> <li>· <b>Enable</b> — To enable monitoring hardware issues that may occur the device.</li> <li>· <b>Disable</b> — To disable monitoring hardware issues that may occur the device.</li> </ul>
<b>Revalidate</b>	To verify if a device present in the <b>Staging</b> group meets the prerequisites for enabling SupportAssist Enterprise capabilities.
<b>Collections</b>	<p>Displays a drop-down list that contains the data collection history. You can select a date and time from the list to view the data that was collected.</p> <p> <b>NOTE: The drop-down list is only displayed if data has been collected from the device.</b></p>
<b>Next Scheduled Collection</b>	Displays the date and time of the next scheduled data collection.

## Multiple Device Collection window

The **Multiple Device Collection** window prompts you to provide details about the multiple device collection that you want to start.

The following table describes the items displayed in the **Multiple Device Collection** window.

**Table 25. Multiple Device Collection window**

Field	Description
<b>Collection Name</b> (Optional)	The name that you want to assign to the collection.
<b>Dell Support Request/case number</b> (Optional)	The case identifier that you want to associate with the collection.
<b>Email</b> (Optional)	The email address or name of the Dell Technical Support contact.
<b>Upload collection</b>	<ul style="list-style-type: none"><li>• Select this option to upload the collection to Dell after the collection is completed.</li><li>• Clear this option to only save the collection on the local system (server where SupportAssist Enterprise is installed).</li></ul>

## Multiple Device Collection pane

The **Multiple Device Collection** pane displays the status of the collection from multiple devices. This **Multiple Device Collection** pane is displayed in the **Devices** page while the collection of data from multiple devices is in progress.

The **Multiple Device Collection** pane displays the following:

- Progress bar that indicates the collection status
- Collections status message
- Number of completed collections and the total number of collections
- Name assigned to the collection

The **Cancel** button enables you to cancel the collection at any time.

 **NOTE: After the collection of data is completed, the Multiple Device Collection pane closes automatically, and the collection details are displayed in the Collections page.**

## Device Groups page

The **Device Groups** page allows you to create and manage devices groups.

The **Create Device Group** option available at the top of the **Device Groups** page enables you to create a new device group.

At the top of the **Device Groups** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.

The **Select group actions** list enables you to select an action that you want to perform on the group. The following are the available actions:

- **Manage Devices** — To add or remove devices from a device group.
- **Manage Credentials** — To provide the credentials for the devices types included in a device group.
- **Manage Contacts** — To provide the contact information and parts dispatch information for each device type included in a device group.
- **Edit/Delete Group** — To edit the group details or delete a device group.

The following table describes the information displayed in the **Device Groups** page.

**Table 26. Device Groups**

Column name	Description
Check box	Use to select a device group for performing an action.
<b>Name</b>	Displays the name of the device group and the total number of devices in the device group.
<b>Description</b>	Displays the description provided for the device group.

**Related links**

- [Manage Devices](#)
- [Manage Credentials](#)
- [Manage Contacts](#)
- [Edit/Delete Device Group](#)

## Manage Devices

The **Manage Devices** window allows you to add or remove devices from a device group.

On the **Manage Devices** window:

- The **Default** pane displays all devices that are not included in the **Default** group.
- The **Grouped** pane displays devices that are included in the current device group.

The following table provides information about the fields displayed in the **Manage Devices** window.

**Table 27. Manage Devices**

Field	Description
<b>Name</b>	Displays the display name, host name, or IP address provided when adding the device.
<b>Model</b>	Model of the device. For example, PowerEdge M820.
<b>Service Tag</b>	Displays a unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.
<b>Save</b>	Click to save the changes you have made.
<b>Cancel</b>	Click to discard the changes you have made.



**NOTE:** You can use the filter icon  displayed in the column titles to filter the displayed data.

**Related links**

- [Device Groups page](#)
- [Managing devices in a device group](#)

## Manage Credentials

The **Manage Credentials** window allows you to provide the credentials for the device types included in a device group.

The left pane on the **Manage Credentials** window displays the device types, and the right pane allows you to provide the credentials. The following table provides information about the fields displayed in the **Credentials** section.

**Table 28. Manage Credentials**

Field	Description
<b>Username</b>	Allows you to view or edit the user name of a device type.
<b>Password</b>	Allows you to edit the password of a device type in a masked format.
<b>Save</b>	Click to save the credentials.

Field	Description
<b>Next</b>	Click to navigate to the next device type displayed in the left pane.
<b>Close</b>	Click to close the <b>Manage Credentials</b> window.

#### Related links

[Device Groups page](#)

[Managing the credentials of a device group](#)

## Manage Contacts

The **Manage Contacts** window allows you to provide the contact information and parts dispatch information for a device group.

The following table provides information about the fields displayed in the **Manage Contacts** window.

**Table 29. Manage Contacts**

Field	Description
<b>Use default</b>	Select to use the contact information already available in the <b>Settings</b> → <b>Contact Information</b> page.
<b>Primary</b>	Select to provide the primary contact details.
<b>Secondary</b>	Select to provide the secondary contact details.
<b>First Name</b>	Allows you to view or edit the first name of the primary or secondary contact.
<b>Last Name</b>	Allows you to view or edit the last name of the primary or secondary contact.
<b>Phone</b>	Allows you to view or edit the phone number of the primary or secondary contact.
<b>Alternate Phone</b>	Allows you to view or edit the alternate phone number of the primary or secondary contact.
<b>Email Address</b>	Allows you to view or edit the email address of the primary or secondary contact.
<b>Preferred Contact Method</b>	Allows you to select the preferred contact method. The available options are: <ul style="list-style-type: none"> <li>· <b>Phone</b></li> <li>· <b>Email</b></li> </ul>
<b>Preferred Contact Hours</b>	Allows you to view or edit the preferred hours at which Dell Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.
<b>Time Zone</b>	Allows you to select the time zone of the primary or secondary contact.
<b>Parts Dispatch (Optional)</b>	
<b>Address</b> <b>City/Town</b> <b>Country</b> <b>State/Province/Region</b> <b>Postal Code</b>	Allows you to view or edit the address to which a replacement part must be dispatched.

#### Related links

[Device Groups page](#)

[Viewing and updating the contact information of a device group](#)

## Edit/Delete Device Group

The **Edit/Delete Device Group** window allows you to edit the device group details or delete a device group.

The following table provides information about the fields displayed on the **Edit/Delete Device Group** window.

**Table 30. Edit/Delete Device Group**

Field	Description
<b>Name</b>	Allows you to view or edit the name of the device group.
<b>Description</b>	Allows you to view or edit the description of the device group.
<b>Update</b>	Click to save the edited device group information.
<b>Delete</b>	Click to delete the device group.
<b>Cancel</b>	Click to discard the changes you have made.

**Related links**

[Device Groups page](#)

[Editing device group details](#)

[Deleting a device group](#)

## Collections page

The **Collections** page displays the collections that have been performed successfully. From the **Collections** page, you can view the collected data, download multi-device collections, and also upload collections to Dell.

At the top of the **Collections** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.

The **Upload** option displayed at the top of the collections list enables you to upload a collection to Dell. The following table describes the information displayed in the **Collections** page.

**Table 31. Collections page**

Column name	Description
Check box	Use to select a collection for viewing the collection overview pane and to upload a collection.
<b>Name</b>	The name of the device or collection. For single device collections, the name of the device is followed by the type of collection. For example, manual, periodic, and so on.
<b>Collection Date</b>	The date and time when the collection was started.
<b>Case</b>	The numeric support case identifier.
<b>Upload Status</b>	The upload status of the collection.

## Collection overview pane

The collection overview pane displays the details of a collection and enables you to view or download the collected data. This pane is displayed when you select a collection that is listed in the **Collections** page.

The following table describes the information displayed in the collection overview pane.

**Table 32. Collection overview pane**

Field	Description
Name	The name assigned of the collection.
<b>Upload status</b>	The status of the collection upload.
<b>Date</b>	The date and time when the collection was started.
<b>IP Address / Host name</b>	The IP address of host name of the device.

Field	Description
<b>Service Tag</b>	A unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.
<b>Collection status</b>	The status of the collection from the device.
<b>View Collection</b> (for server collections only)	Click to open a collection from a server in the <b>Configuration Viewer</b> .
<b>Download Collection</b> (for storage, networking, chassis, and multiple-device collections only)	Click to download the collection as a .zip file.

## Settings

The **Settings** tab enables you to configure the options available in SupportAssist Enterprise. You can point to the **Settings** tab and click the available options to access the following pages:

- **Collection Schedules** — To configure the schedule for the periodic collection of system information for each device type.
- **Proxy Settings** — To configure the settings of the proxy server available in your environment. This setting is required only if the server where SupportAssist Enterprise is installed connects to the internet through a proxy server.
- **Preferences** — To configure your preferences for the following: automatic update, data collection, email notification, recommendation report, and maintenance mode.
- **Contact Information** — To view and update your company's primary and secondary SupportAssist Enterprise contacts.
- **SMTP Settings** — To configure the details of the SMTP server utilized by your company. This setting is applicable only if your company utilizes an SMTP server. If your company does not utilize an SMTP server, you may not receive certain email notifications from SupportAssist Enterprise.

### Related links

- [Collection Schedules](#)
- [Proxy Settings](#)
- [Preferences](#)
- [Contact Information](#)
- [SMTP Settings](#)

## Collection Schedules

The **Collection Schedules** page enables you to schedule the collection of system information from your devices.

At the top of the **Collection Schedules** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.

The following table provides information about the fields displayed in the **Collection Schedules** page.



-  **NOTE:** The options in the **Collection Schedules** page are only enabled if the **On a regular schedule as specified in Collection Schedules** option is selected in the **Preferences** page.
-  **NOTE:** If your devices are covered under the **ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center** service contract, when the **On a regular schedule as specified in Collection Schedules** option is not selected, you will not receive some reporting information about your devices.

Table 33. Collection Schedules

Field	Description
<b>Device Type</b>	The available device type are: <ul style="list-style-type: none"> <li>• <b>Chassis</b></li> <li>• <b>Fluid File System (FluidFS)</b></li> <li>• <b>iDRAC</b></li> <li>• <b>Networking</b></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <b>Peer Storage (PS) / EqualLogic</b></li> <li>• <b>PowerVault</b></li> <li>• <b>Server / Hypervisor</b></li> <li>• <b>Storage Center (SC) / Compellent</b></li> </ul>
<b>Rekurs every</b>	<p>Allows you to select the frequency of at which system information will be collected. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Week</b></li> <li>• <b>Month</b></li> </ul>
<b>Specify day and time</b>	<p>Allows you to select the day and time when the system information will be collected.</p> <ul style="list-style-type: none"> <li>• If you select <b>None</b>, the periodic collection of system information is disabled for the selected <b>Device Type</b>.</li> <li>• If you select <b>Weekly</b>, the available options are: <ul style="list-style-type: none"> <li>– Weeks (<b>1</b> or <b>2</b>)</li> <li>– Day of the week (<b>Sunday, Monday, Tuesday, Wednesday, Thursday, Friday</b>, and <b>Saturday</b>)</li> <li>– Hour (in hh:mm format)</li> </ul> </li> <li>• If you select <b>Monthly</b>, the available options are: <ul style="list-style-type: none"> <li>– Week of the month (<b>First, Second, Third, Fourth</b>, and <b>Last</b>)</li> <li>– Day of the week (<b>Sunday, Monday, Tuesday, Wednesday, Thursday, Friday</b>, and <b>Saturday</b>)</li> <li>– Hour (in hh:mm format)</li> <li>– Months (<b>1</b> or <b>3</b>)</li> </ul> </li> </ul>
<b>Next collection date</b>	Displays the date and time at which the system information will be collected next.

#### Related links

[Customizing the schedule for periodic collection of system information](#)

## Proxy Settings

The **Proxy Settings** page enables you to configure the settings of the proxy server available in your environment.

At the top of the **Proxy Settings** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.

 **NOTE: Configuring the proxy settings is required only if the server where SupportAssist Enterprise is installed connects to the internet through a proxy server.**

The following table provides information about the items displayed in the **Proxy Settings** page.

**Table 34. Proxy Settings**

Field	Description
<b>Use Proxy Settings</b>	Select this option to enable configuring the proxy server settings.
<b>Host Name / IP Address</b>	View or edit the proxy server address or name.
<b>Port</b>	View or edit the proxy server port number.

Field	Description
<b>Proxy requires authentication</b>	Select this option if a user name and password are required to login to the proxy server.
<b>User Name</b>	View or edit the user name required to connect to the proxy server.
<b>Password</b>	Edit the password required to login to the proxy server.

#### Related links

[Configuring proxy server settings](#)


## Preferences



The **Preferences** page enables you to configure data collection settings, automatic updates, recommendation report settings, and maintenance mode.

At the top of the **Preferences** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.

The following table provides information about the options displayed in the **Preferences** page.

**Table 35. Preferences**

Field	Description
<b>Automated Tasks</b>	
<b>Automatically update the following:</b>	Displays options to automatically download and install the latest updates, when they are available. The download and installation of the updates occur in the background. If a problem occurs during the update, an appropriate error message will be displayed.   <b>NOTE: Dell recommends that you select automatic updates to ensure that SupportAssist Enterprise is up-to-date with the latest features and enhancements.</b>
<b>SupportAssist Enterprise application</b>	Select this option to automatically download and install the SupportAssist Enterprise application update whenever it is available.
<b>Policy files</b>	Select this option to automatically download and install the policy files update whenever it is available.
<b>Product support files</b>	Select this option to automatically download and install the device support update whenever it is available.
<b>Automatically collect system state information:</b>	
<b>On a regular schedule as specified in Collection Schedule</b>	Select this option to enable scheduling the periodic collection of system information from each device type.
<b>When a new support case is created</b>	Select this option to automatically start a system log collection when a new support case is generated.
<b>Email Settings</b>	
<b>Receive email notification when a new support case is opened</b>	Select this option to receive an email notification when a new support case is opened.
<b>Preferred email Language</b>	Select the preferred language for email notifications.

Field	Description
<b>Recommendation Report Settings</b>	
<b>Automatically receive recommendation reports via email</b>	Select this option to automatically receive ProSupport Plus server recommendation reports through email.
<b>Collection Data Settings</b>	
<b>Storage Center with Fluid File System</b>	Select <b>Logs</b> to collect logs from the device.
<b>Server</b>	<ul style="list-style-type: none"> <li>Select <b>Software</b> to collect software-related information from the device.</li> <li>Select <b>Logs</b> to collect logs from the device.</li> </ul> <p> <b>NOTE: For information on the logs that are collected by SupportAssist Enterprise, see the <i>Dell SupportAssist Enterprise Version 1.0 Reportable Items</i> document at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</b></p>
<b>Storage: Fluid File System (FluidFS)</b>	Select <b>Logs</b> to collect logs from the device.
<b>Storage: Peer Storage (PS) / EqualLogic</b>	<ul style="list-style-type: none"> <li>Select <b>Diagnostic Data (Diags collection)</b> to collect diagnostic information from the device.</li> <li>Select <b>Inter Array Connectivity Test (Ping Test)</b> to collect the ping test result from the device.</li> </ul>
<b>Storage: PowerVault</b>	Select <b>Support Data</b> to collect support data from the device.
<b>Storage: Storage Center (SC) / Compellent</b>	Select <b>Logs</b> to collect logs from the device.
<b>Identification Information Settings</b>	
<b>Include identification information in data sent to Dell</b>	<p>Select this option to allow sending identity information to Dell.</p> <p> <b>NOTE: If you clear this option, settings for the collection of logs and diagnostic data under Collection Data Settings are automatically disabled.</b></p>
<b>Maintenance Mode</b>	
<b>Temporarily suspend case generation activity (e.g., for purposes of downtime, external troubleshooting, etc.)</b>	Select this option to set all devices to maintenance mode. While in maintenance mode, no new support cases are opened.

#### Related links

- [Enabling or disabling automatic updates](#)
- [Configuring email notification settings](#)
- [Enabling or disabling the automatic collection of system information on case creation](#)
- [Enabling or disabling the periodic collection of system information from all devices](#)
- [Enabling or disabling the collection of identity information](#)
- [Enabling or disabling global-level maintenance mode](#)

## Contact Information

The **Contact Information** page enables you to view and edit the primary and secondary contact information. The following table provides information about the items displayed in the **Contact Information** page.

At the top of the **Contact Information** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.

 **NOTE:** It is mandatory to provide information for all fields, except the alternate phone number.

**Table 36. Contact Information**

Field	Description
<b>Company</b>	View or edit the company name.
<b>Primary</b>	Select this option to view the primary contact information.
<b>Secondary</b>	Select this option to view the secondary contact information.
<b>First Name</b>	View or edit the first name of the primary or secondary contact.
<b>Last Name</b>	View or edit the last name of the primary or secondary contact.
<b>Phone</b>	View or edit the phone number of the primary or secondary contact.
<b>Alternate Phone</b>	View or edit the alternate phone number of the primary or secondary contact.
<b>Email</b>	View or edit the email address of the primary or secondary contact.
<b>Country</b>	View or select the country.
<b>Preferred Contact Method</b>	Select the preferred contact method. The available options are: <ul style="list-style-type: none"> <li>· <b>Phone</b></li> <li>· <b>Email</b></li> </ul>
<b>Preferred Contact Hours</b>	View or edit the preferred hours at which Dell Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.
<b>Time Zone</b>	Select the time zone of the primary or secondary contact.
<b>Parts Dispatch (Optional)</b>	
<b>Address</b> <b>City/Town</b> <b>Country</b> <b>State/Province/Region</b> <b>Postal Code</b>	View or edit the address to which a replacement part must be dispatched.
<b>CNPJ</b> <b>IE</b>	For Brazil only: View or edit the CNPJ and IE number of your company.

**Related links**

[Viewing and updating the contact information](#)

## SMTP Settings

The **SMTP Settings** page enables you to configure the SMTP server (email server) settings. If your company utilizes an SMTP server, Dell recommends that you configure the SMTP server settings.

At the top of the **SMTP Settings** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.



**NOTE:** SupportAssist Enterprise utilizes the SMTP server to send you device status and connectivity status email notifications. You will not receive those email notifications if:

- Your company does not utilize an SMTP server
- Your company utilizes an SMTP server, but the SMTP server settings are either not configured or configured incorrectly.

The following table provides information about the items displayed in the **SMTP Settings** page.

**Table 37. SMTP Settings**

Field	Description
<b>Enable Email Notification</b>	Select this option to enable configuring the email server settings.
<b>Host Name / IP Address</b>	View or edit the email server address or name.
<b>Port</b>	View or edit the email server port number.
<b>Requires Authentication</b>	Select this option if the email server requires authentication.
<b>User Name</b>	View or edit the user name required to connect to the email server.
<b>Password</b>	Edit the password required to connect to the email server.
<b>Use SSL</b>	Select this option to use secure communication for sending emails.

**Related links**

[Configuring SMTP server settings](#)


## Network Connectivity Test





The **Network Connectivity Test** page allows you to test SupportAssist Enterprise connectivity to the dependent network resources.

At the top of the **Network Connectivity Test** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.

The following table describes the fields displayed on the **Network Connectivity Test** page.

**Table 38. Connectivity Test**

Field	Description
Check box	Select the appropriate check boxes to test the connectivity status you want to verify.
<b>Test</b>	Displays the dependent network resources that you can test. The available options are: <ul style="list-style-type: none"> <li>· <b>Internet Connectivity</b></li> <li>· <b>SMTP Server</b></li> <li>· <b>Dell FTP Server</b></li> <li>· <b>Dell Upload Server</b></li> <li>· <b>SupportAssist Server</b></li> </ul>
<b>Description</b>	Describes the purpose of each test.
<b>Connectivity Status</b>	Displays an icon and a message that indicates the connectivity status. The possible statuses are: <ul style="list-style-type: none"> <li>·  <b>Not Configured</b> (applicable only for the SMTP Server test) — The SMTP server settings are not configured in SupportAssist Enterprise. If your company utilizes an SMTP server (email server), Dell recommends that you configure <b>SMTP Settings</b> in SupportAssist Enterprise.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li> <b>In Progress</b> — The connectivity test is in progress.</li> <li> <b>Connected</b> — The connectivity test is successful.</li> <li> <b>Error</b> — The connectivity test is unsuccessful.</li> </ul> <p> <b>NOTE: The Error status is displayed as a link that you can click to view a description of the issue and the possible resolution steps.</b></p>
<b>Last Verified</b>	Displays the date and time the connectivity status was last verified.
<b>Test Connectivity</b>	Click to perform the selected connectivity tests.

#### Related links

[Performing the connectivity test](#)




## Test SupportAssist Enterprise

The **Test SupportAssist Enterprise** page enables you to verify the ability of SupportAssist Enterprise to run specific tasks.

At the top of the **Test SupportAssist Enterprise** page, the navigation trail is displayed. You can click **Home** on the navigation trail to go to the **Devices** page.

The following table describes the fields that are displayed in the **Test SupportAssist Enterprise** page.

**Table 39. Test SupportAssist Enterprise**

Field	Description
Check box	Select the appropriate check box to test the task that you want to verify.
<b>Test</b>	Displays the task that you can test. The available option is <b>Case Creation</b> , which enables you to verify the ability of SupportAssist Enterprise to create a support case with Dell Technical Support.
<b>Description</b>	Describes the purpose of the test.
<b>Status</b>	Displays an icon and a message that indicates the test status. The possible statuses are: <ul style="list-style-type: none"> <li><b>Not validated</b> — The support case creation task has not been tested.</li> <li> <b>In Progress</b> — The support case creation test is in progress.</li> <li> <b>Ready to Create Cases</b> — SupportAssist Enterprise can create cases successfully.</li> <li> <b>Unable to Create Case</b> — SupportAssist Enterprise cannot create support cases because of a possible issue with the support case creation workflow.</li> </ul>
<b>Last Verified</b>	Displays the date and time the status was last verified.
<b>Test</b>	Click to perform the selected test.

#### Related links

[Testing the case creation capability](#)

## Error code appendix

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

**Table 40. Error code appendix**

Error code	Error message	Possible resolution
3000_1 3000_2 3000_3 3000_4 3000_5	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <i>device name</i> .	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Select the device in the <b>Devices</b> page, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list.</li> <li>Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_6 3000_9 3000_11	A component required for installing Dell OpenManage Server Administrator (OMSA) could not be downloaded.	<ol style="list-style-type: none"> <li>Make sure that the system has internet connectivity.</li> <li>Perform the Connectivity Test and ensure that the system has connectivity to the dependent resources.</li> <li>Select the device in the <b>Devices</b> page, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list.</li> </ol> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_7	Installation of Dell OpenManage Server Administrator (OMSA) is not supported on the operating system running on <i>device name</i> .	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Select the device in the <b>Devices</b> page, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list.</li> <li>Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell EMC SupportAssist Enterprise version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_8	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <i>device name</i> .	<p>Try to repair the SupportAssist Enterprise installation:</p> <ol style="list-style-type: none"> <li>Open <b>Control Panel</b>.</li> <li>In <b>Programs</b>, click <b>Uninstall a Program</b>.</li> <li>In the <b>Programs and Features</b> window, select <b>Dell SupportAssist</b> and click <b>Change</b>.</li> <li>In the <b>Welcome to Dell SupportAssist Enterprise Installer</b> window, click <b>Next</b>.</li> <li>Click <b>Repair</b> and then click <b>Install</b>.</li> </ol>

Error code	Error message	Possible resolution
		If the problem persists, contact Dell Technical Support for further assistance.
3000_10 3000_12 3000_13 3000_14	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <i>device name</i> .	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Select the device in the <b>Devices</b> page, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list.</li> <li>Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell EMC SupportAssist Enterprise version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_15 3000_16 3000_17 3000_22 3000_23 3000_29 3000_47 3000_48 3000_50 3000_56 3000_61	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <i>device name</i> .	<p>Make sure that the device is reachable and the configured device credentials have Administrator rights, and then do one of the following:</p> <ul style="list-style-type: none"> <li>Select the device in the <b>Devices</b> page, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list.</li> <li>Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell EMC SupportAssist Enterprise version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_18	A service required for the installation of Dell OpenManage Server Administrator (OMSA) is either not running or not enabled on <i>device name</i> .	<ul style="list-style-type: none"> <li>If the device is running Microsoft Windows, make sure that the WMI service is running.</li> <li>If the device is running Linux, make sure that SSH is enabled.</li> </ul> <p>For more information, see <a href="#">Other services</a>.</p>
3000_19	A service required for the installation of Dell OpenManage Server Administrator (OMSA) is not running on <i>device name</i> .	Make sure that the WMI service is running on the device. For more information, see <a href="#">Other services</a> .
3000_20 3000_21 3000_24 3000_25 3000_26 3000_27 3000_28 3000_30 3000_31 3000_32 3000_33 3000_34 3000_35 3000_36 3000_37 3000_38	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <i>device name</i> .	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Select the device in the <b>Devices</b> page, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list.</li> <li>Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell EMC SupportAssist Enterprise version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>

Error code	Error message	Possible resolution
3000_39 3000_40 3000_41 3000_42 3000_43 3000_44 3000_45 3000_46 3000_49 3000_51 3000_54 3000_55 3000_57 3000_58 3000_59		
3000_52 3000_53	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <i>device name</i> .	Make sure that port 22 is open and SSH is enabled on the system, and then do one of the following: <ul style="list-style-type: none"> <li>· Select the device in the <b>Devices</b> page, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list.</li> <li>· Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell EMC SupportAssist Enterprise version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> If the problem persists, contact Dell Technical Support for assistance.
3000_60	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <i>device name</i> .	<ul style="list-style-type: none"> <li>· Verify if the device is reachable.</li> <li>· Verify if the configured device credentials have Administrator rights.</li> <li>· Select the device in the <b>Devices</b> page, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list.</li> <li>· Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell EMC SupportAssist Enterprise version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> If the problem persists, contact Dell Technical Support for assistance.
3000_62	The time allowed for OMSA installation has expired.	Log on to the device and verify if OMSA is installed. If OMSA is not installed, select the device, and in the device overview pane, select <b>Install / Upgrade OMSA</b> from the <b>Tasks</b> list. If the problem persists, contact Dell Technical Support for assistance.
4000_500	This device has generated an unusual number of alerts exceeding the set threshold limit. SupportAssist Enterprise has temporarily placed it under maintenance mode. During this period, SupportAssist Enterprise will not process any alerts from this device.	Ensure that the health of this device is restored for optimal SupportAssist Enterprise operations.

Error code	Error message	Possible resolution
5000_1	SNMP settings of the device could not be configured because of an unexpected error.	You must either try to configure the SNMP settings through the <b>Tasks</b> → <b>Configure SNMP</b> option or manually configure the SNMP settings. For instructions to manually configure the SNMP settings, see <a href="#">Configuring the alert destination of an iDRAC by using the web interface</a> .
5000_2	SNMP settings of the device could not be configured because the integrated Dell Remote Access Controller (iDRAC) does not have the required license installed.	Make sure that iDRAC has an Enterprise or Express license installed, and then try to configure the SNMP settings through the <b>Tasks</b> → <b>Configure SNMP</b> option.
5000_3	SNMP settings of the device could not be configured because all configurable fields of the integrated Dell Remote Access Controller (iDRAC) are occupied.	You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see <a href="#">Configuring the alert destination of an iDRAC by using the web interface</a> .
5000_4	SNMP settings of the device could not be configured because the credentials you have entered do not have the required privileges.	Make sure that the credentials have either Administrator or Operator privileges on the integrated Dell Remote Access Controller (iDRAC), and then try to configure the SNMP settings through the <b>Tasks</b> → <b>Configure SNMP</b> option on the device overview pane.
5000_5	SNMP settings of the device could not be configured because an attempt to connect to the integrated Dell Remote Access Controller (iDRAC) was unsuccessful.	Make sure that iDRAC is reachable from the system on which SupportAssist Enterprise is installed, and then try to configure the SNMP settings through the <b>Tasks</b> → <b>Configure SNMP</b> option on the device overview pane.
5000_6	SNMP settings of the device could not be configured because the credentials you have entered are invalid.	Make sure that the credentials are valid, and then try to configure the SNMP settings through the <b>Tasks</b> → <b>Configure SNMP</b> option on the device overview pane. If the problem persists, contact your system administrator for assistance.
5000_7 5000_8	SNMP settings of the device could not be configured because of an unexpected error.	You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see <a href="#">Configuring the alert destination of an iDRAC using the web interface</a> .
5000_9	SNMP settings of the device could not be configured because the user account does not have the sufficient privileges on the device.	You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see <a href="#">Manually configuring the alert destination (Windows)</a> or <a href="#">Manually configuring the alert destination (Linux)</a> .
5000_10	SNMP settings of the device could not be configured because the hostname/IP address of the system on which SupportAssist Enterprise is installed was not provided.	If you ran the script file to configure the SNMP settings, make sure that you type the IP address of the system on which SupportAssist Enterprise is installed as an argument.
5000_11	SNMP settings of the device could not be configured because the SNMP service is not installed on the device.	Manually install the SNMP service on the device, and then try to configure the SNMP settings through the <b>Tasks</b> → <b>Configure SNMP</b> option on the device overview pane.
5000_12	SNMP settings of the device could not be configured because SupportAssist Enterprise does not support the operating system running on the device.	For information on the operating systems supported by SupportAssist Enterprise, see the <i>Dell EMC</i>

Error code	Error message	Possible resolution
		SupportAssist Enterprise Version 1.0 Support Matrix at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a> .
5000_13	SNMP settings of the device could not be configured because the SNMP service has not started.	Manually start the SNMP service on the device, and then try to configure the SNMP settings through the <b>Tasks</b> → <b>Configure SNMP</b> option.
5000_14	SNMP settings of the device could not be configured because the WMI service is disabled.	Manually start the WMI service on the device, and then try to configure the SNMP settings through the <b>Tasks</b> → <b>Configure SNMP</b> option on the device overview pane.
5000_15	SupportAssist Enterprise has configured the SNMP settings successfully, but the automated test to verify that the SNMP settings was unsuccessful.	To resolve the issue, verify the network settings and make sure that the SNMP port (162) is open.
6000_01 6000_11 6000_12 6000_13 6000_14 6000_24	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because of a technical error.	To resolve this issue, contact Dell Technical Support for assistance.
6000_02	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because the device is not reachable.	Make sure that the device is reachable from the server running SupportAssist Enterprise and then retry the operation.
6000_03	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because the host name of the device could not be resolved to an IP address.	If the device is a member of a domain, make sure that the host name of the device is added in the DNS server, and then retry the operation.
6000_4 6000_5	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because of an internal error.	To resolve this issue, contact Dell Technical Support for assistance.
6000_6 6000_8 6000_9	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because an attempt to connect to the device is unsuccessful.	Make sure that WMI service is running on the device and then retry the operation.
6000_7 6000_15 6000_19 6000_21 6000_23	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because the credentials of the device are either incorrect or do not have the required privileges.	<ul style="list-style-type: none"> <li>Make sure that SupportAssist Enterprise is updated with the correct user name and password of the device.</li> <li>Make sure that the user account has administrator or root privileges on the device.</li> </ul>
6000_10	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because the credentials of the device do not have the required privileges.	Make sure that the user account has administrator or root privileges on the device and then retry the operation.
6000_16	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because of an unknown error.	To resolve this issue, contact Dell Technical Support for assistance.
6000_17	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because the device does not support this operation.	Not applicable.

Error code	Error message	Possible resolution
6000_18 6000_20 6000_22	SupportAssist Enterprise is unable to clear System Event Log from <i>device name</i> because an attempt to connect to the device is unsuccessful.	Make sure that the SSH service is running on the device and then retry the operation.
SA-0001	SupportAssist Enterprise is unable to import devices because the device count is more than 300.	Make sure that the device count is below 300 and then retry the operation.
SA-0002	SupportAssist Enterprise is unable to import devices because the .csv file is empty.	Make sure that the .csv file is not empty and then retry the operation.
SA-0003	SupportAssist Enterprise is unable to import devices because the .csv file is corrupted.	Make sure that the .csv file is not corrupted and then retry the operation.
SA-0004	SupportAssist Enterprise is unable to import devices because the .csv file is not available at the specified location.	Make sure that the .csv file is available at the specified location and then retry the operation.
SA-0006	SupportAssist Enterprise is unable to import devices because the .csv file is not valid.	Make sure that the .csv file is valid and then retry the operation.
SA-0007	SupportAssist Enterprise is unable to import devices because the imported file does not contain a valid header.	Make sure that the system running SupportAssist Enterprise and the imported file contains a valid header.
SA-0008	The device import operation is canceled.	Not applicable.
SA-0009	SupportAssist Enterprise is unable to import one or more devices because the credentials of the devices were not included in the .csv file.	Make sure that the credentials of the devices are included in the .csv file and then retry the operation.
SA-0011	SupportAssist Enterprise is unable to import devices because the .csv file already exists.	Delete the .csv file available at the temporary location: <b>C:\Users\<user name="">\AppData\Local\temp</user></b> and then retry the operation.
SA-0012	SupportAssist Enterprise is unable to add the devices because the entered host name or IP address, and device type are incorrect.	Retry adding the device with the correct host name or IP address, and device type.
SA-0005	SupportAssist Enterprise is unable to add the <i>device name</i> because an attempt to connect to the device is unsuccessful.	Make sure that both the system running SupportAssist Enterprise and the device you are trying to add are connected to the network, and then retry adding the device.
SA-0010	SupportAssist Enterprise is unable to add the <i>device name</i> because the entered host name or IP address is incorrect.	Retry adding the device with the correct host name or IP address.
SA-0015	SupportAssist Enterprise is unable to add the <i>device name</i> because an unknown error occurred while discovering the device.	Verify the following and then retry adding the device: <ul style="list-style-type: none"> <li>Make sure that the device is supported by SupportAssist Enterprise. For the list of supported device models, see the <i>Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> <li>Make sure that the user account has administrator/ root privileges.</li> </ul>
SA-0020	SupportAssist Enterprise is unable to add the <i>device name</i> because the device is already added.	Not applicable.

<b>Error code</b>	<b>Error message</b>	<b>Possible resolution</b>
SA-0025	SupportAssist Enterprise is unable to add the <i>device name</i> because of an unknown error.	Verify if the device is supported by SupportAssist Enterprise. For the list of supported device models, see the <i>Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a> . If the problem persists, contact Dell Technical Support for assistance.
SA-0030	SupportAssist Enterprise is unable to add the <i>device name</i> because the User Name or Password is incorrect.	Verify the device information, ensure that the user account has administrator/root privileges, and then retry adding the device. If the problem persists, contact your network administrator for assistance.
SA-0035	SupportAssist Enterprise is unable to add the <i>device name</i> because the enable password is not provided.	Enter the enable password and then retry adding the device.
SA-0040	SupportAssist Enterprise is unable to add the <i>device name</i> because the Display Name is already in use by another device.	Retry adding the device with any other Display Name.
SA-0045	Identification or cancellation for this device is already in progress.	Not applicable.
SA-0050	SupportAssist Enterprise is unable to add the <i>device name</i> because of an unknown error.	Verify if the device is supported by SupportAssist Enterprise. For the list of supported device models, see the <i>Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a> .
SA-0055	SupportAssist Enterprise is unable to add the <i>device name</i> because the device is not supported.	For the list of supported device models, see the <i>Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a> .
SA-0060	SupportAssist Enterprise is unable to add the <i>device name</i> because a required file has either been deleted or moved.	Restart the Dell SupportAssist service on the system running SupportAssist Enterprise, and then retry adding the device.
SA-0065	SupportAssist Enterprise is unable to add the <i>device name</i> because the entered credentials do not have superuser privileges.	Enter the credentials that have superuser privileges, and then retry adding the device.
SA-0070	Installation of Dell OpenManage Server Administrator (OMSA) is not supported on this device.	Not applicable.
SA-0075	SupportAssist Enterprise has detected that Dell OpenManage Server Administrator (OMSA) is not installed on the device. Installing OMSA is required to generate alerts for hardware events that occur on the device.	Not applicable.
SA-0080	SupportAssist Enterprise has detected that the Dell OpenManage Server Administrator (OMSA) services are not running on the device.	For optimal SupportAssist Enterprise capability, you must restart the OMSA services.
SA-0085	SupportAssist Enterprise has detected that Dell OpenManage Server Administrator (OMSA) version x.x is installed on the device.	For optimal SupportAssist Enterprise capability, Dell recommends that you upgrade OMSA to version x.x.

Error code	Error message	Possible resolution
SA-0090	SupportAssist Enterprise has detected that Dell OpenManage Server Administrator (OMSA) version x.x is installed on the device.	It is recommended that you download and install OMSA version x.x on the device.
SA-0095	SupportAssist Enterprise is unable to verify the OMSA version installed on the device.	To resolve the issue, see <a href="#">Unable to verify OMSA version</a> .
SA-0100	The recommended version of Dell OpenManage Server Administrator (OMSA) is already installed on the device.	Not applicable.
SA-0105	SupportAssist Enterprise monitors the device through the integrated Dell Remote Access Controller (iDRAC). Therefore, installation or upgrade of Dell OpenManage Server Administrator (OMSA) is not required.	Not applicable.
SA-0110	SupportAssist Enterprise is unable to add the <i>device name</i> because it does not have a valid license.	Make sure that the iDRAC has a valid Enterprise or Express license, and then retry the operation.
SA-0115	SupportAssist Enterprise is unable to add the <i>device name</i> because the operating system is not supported.	Not applicable.
SA-0120	SupportAssist Enterprise is unable to add the device because a required service is disabled on the <i>device name</i> .	Make sure that the required service is running on the device, and then retry adding the device. For information on the required service, see <a href="#">Other services</a> .
SA-0125	SupportAssist Enterprise is unable to add the <i>device name</i> because a response was not received within the predefined time limit.	Try adding the device again. For additional troubleshooting information, see <a href="#">Unable to add the device</a> .
SA-0130	SupportAssist Enterprise is unable to add the <i>device name</i> because the SSL encryption level of the device is set to 256 bit or higher.	For troubleshooting steps, see <a href="#">Unable to add the device</a> .
SA-0135	SupportAssist Enterprise is unable to add the <i>device name</i> because the device type that you selected is incorrect.	Ensure that you select the correct device type and then try again.
SA-0140	SupportAssist Enterprise is unable to add the <i>device name</i> because a connection to the device was unsuccessful.	Perform the following: <ul style="list-style-type: none"> <li>• Ensure that the required ports are open on the device. For information on the required ports, see the <i>Dell EMC SupportAssist Enterprise Version 1.0 User's Guide</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> <li>• Ensure that you have selected the correct device type. Verify if the device is supported by SupportAssist Enterprise. For the list of supported device models, see the <i>Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul>
SA-0145	SupportAssist Enterprise is unable to add the <i>device name</i> because the device credentials were not provided.	Enter the device credentials and then try again.
SA-0150	SupportAssist Enterprise is unable to add the <i>device name</i> because the device credentials were either not provided or incorrectly provided.	<ol style="list-style-type: none"> <li>1. Enter the device credentials.</li> <li>2. Ensure that the device credentials are correct.</li> </ol>

Error code	Error message	Possible resolution
SA-0155	SupportAssist Enterprise is unable to add the <i>device name</i> because it is a Dell Peer Storage or EqualLogic member IP address.	Try adding the device again with the Dell Peer Storage or EqualLogic group IP address.
SA-0160	The IP address that you have entered is a Dell Peer Storage/EqualLogic member IP address.	Ensure that you add the device by using the group IP address.
SA-1005	SupportAssist Enterprise is unable to edit the credentials of the <i>device name</i> because an attempt to connect to the device is unsuccessful.	Make sure that both the system running SupportAssist Enterprise and the device are connected to the network, and then retry the operation.
SA-1010	SupportAssist Enterprise is unable to edit the credentials of the <i>device name</i> because of an unexpected error.	Verify the following and then retry editing the device credentials: <ul style="list-style-type: none"> <li>Make sure that the required services are running on the device. For information on the required services, see the Online Help.</li> <li>Make sure that the entered credentials have administrator or root privileges.</li> </ul>
SA-1015	SupportAssist Enterprise is unable to edit the credentials of the <i>device name</i> because the user name or password is incorrect.	Verify the user name and password, ensure that the user account has administrator/root privileges, and try again. If the problem persists, contact your network administrator for assistance.
SA-1025	SupportAssist Enterprise is unable to edit the credentials of the <i>device name</i> because the entered Display Name it is already in use by another device.	Enter any other Display Name, and then retry editing the device credentials.
SA-1030	SupportAssist Enterprise is unable to edit the device credentials because the entered credentials do not have superuser rights.	Enter the credentials that have superuser rights, and then retry saving the device credentials.
SA-1035	SupportAssist Enterprise is unable to update the device credentials because a required service is disabled on the device.	Make sure that the required services are running on the device, and then retry editing the device credentials. For information on the required services, see <a href="#">Other services</a> .
SA-1040	SupportAssist Enterprise is unable to edit the credentials of the <i>device name</i> because the SSL encryption level of the device is set to 256 bit or higher.	For troubleshooting steps, see <a href="#">Unable to edit device credentials</a> .
SA-0165 SA-1045	SupportAssist Enterprise is unable to edit the credentials of the device because an attempt to connect to the device is unsuccessful.	Perform the following: <ol style="list-style-type: none"> <li>Ensure that the FTP port is open.</li> <li>Enter the correct device credentials.</li> <li>If the problem persists, contact your network administrator for assistance.</li> </ol>
SA-2000	SupportAssist Enterprise is unable to establish connections required to auto create cases with Dell Technical Support.	Perform the connectivity test and ensure that the internet connectivity is successful.
SA-2001 SA-2002 SA-2003 SA-2004	SupportAssist Enterprise is unable to establish connections required to auto create cases with Dell Technical Support.	Not applicable.

Error code	Error message	Possible resolution
SA-4015 SA-4020 SA-4025 SA-4030 SA-4035 SA-4040 SA-4045 SA-4050 SA-4055 SA-4060 SA-4065 SA-4070 SA-4071 SA-4072	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because of an unknown error.	To retry collecting the system information, select the device and click <b>Start Collection</b> . If the problem persists, contact Dell Technical Support for assistance.
SA-4073 SA-4074	SupportAssist Enterprise is unable to package the system information collected from the <i>device name</i> because of an unknown error.	To retry collecting the system information, select the device and click <b>Start Collection</b> . If the problem persists, contact Dell Technical Support for assistance.
SA-4075 SA-4080	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because an attempt to connect to the device is unsuccessful.	<ul style="list-style-type: none"> <li>• Make sure that WMI service is running on the device.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-4085 SA-4090	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because an attempt to connect to the device is unsuccessful.	<ul style="list-style-type: none"> <li>• Make sure that WS-Man service is running on the device.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>. If the problem persists, contact Dell Technical Support for assistance.</li> </ul>
SA-4110 SA-4115 SA-4120	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because an attempt to connect to the device is unsuccessful.	<ul style="list-style-type: none"> <li>• Make sure that SNMP service is running on the device.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>. If the problem persists, contact Dell Technical Support for assistance.</li> </ul>
SA-4125 SA-4130	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because an attempt to connect to the device is unsuccessful.	<ul style="list-style-type: none"> <li>• Make sure that Symbol SDK service is running on the device.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>. If the problem persists, contact Dell Technical Support for assistance.</li> </ul>
SA-4135 SA-4140	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because an attempt to connect to the device is unsuccessful.	<ul style="list-style-type: none"> <li>• Make sure that vSphere SDK service is running on the device.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>. If the problem persists, contact Dell Technical Support for assistance.</li> </ul>
SA-4145 SA-4150	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because an attempt to connect to the device is unsuccessful.	<ul style="list-style-type: none"> <li>• Make sure that REST API service is running on the device.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>. If the problem persists, contact Dell Technical Support for assistance.</li> </ul>

Error code	Error message	Possible resolution
		persists, contact Dell Technical Support for assistance.
SA-4095 SA-4100 SA-4105	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because an attempt to connect to the device is unsuccessful.	<ul style="list-style-type: none"> <li>Make sure that the SSH service is running on the device.</li> <li>To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-4155	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because the device is not reachable.	<ul style="list-style-type: none"> <li>Make sure that the device is reachable from the server running SupportAssist Enterprise.</li> <li>To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-4160	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because the IP address of the device is invalid.	<ul style="list-style-type: none"> <li>Make sure that SupportAssist Enterprise is updated with the correct IP address of the device.</li> <li>To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-4165	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because the download of a certificate file could not be completed successfully.	<ul style="list-style-type: none"> <li>Verify the firewall and network settings to make sure that download of the certificate file is not blocked.</li> <li>To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-4170 SA-4175	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because the credentials of the device are either incorrect or do not have the required privileges.	<ul style="list-style-type: none"> <li>Make sure that SupportAssist Enterprise is updated with the correct user name and password of the device.</li> <li>Make sure that the user account has administrator or root privileges on the device.</li> <li>To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-4180	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because the device is not supported.	For the list of supported device models, see the <i>Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a> .
SA-4185	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because of an attempt to connect to the device is unsuccessful.	<ul style="list-style-type: none"> <li>Make sure SupportAssist Enterprise is updated with the credentials of a user account that has root privileges. See <a href="#">Configuring sudo access for SupportAssist Enterprise (Linux)</a>.</li> <li>To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-4190	SupportAssist Enterprise is unable to gather system information from the <i>device name</i> because the SSL encryption level of the device is set to 256 bit or higher.	For troubleshooting steps, see <a href="#">Unable to gather system information</a> .
SA-4500	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because the receiving server hosted by Dell is unreachable.	To retry collecting the system information, select the device and click <b>Start Collection</b> . If the problem persists, contact Dell Technical Support for assistance.
SA-4501 SA-4502	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because of an unknown error.	To retry collecting the system information, select the device and click <b>Start Collection</b> . If the problem persists, contact Dell Technical Support for assistance.

Error code	Error message	Possible resolution
SA-4511 SA-4512 SA-15000 SA-15001 SA-15002	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because of an unknown error.	<ul style="list-style-type: none"> <li>• Perform <b>Network Connectivity Test</b> and make sure that connectivity to the <b>Dell Upload Server</b> is successful.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-15011 SA-15012	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because of an unknown error.	<ul style="list-style-type: none"> <li>• Perform <b>Network Connectivity Test</b> and make sure that connectivity to the <b>Dell Upload Server</b> is successful.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul>
SA-4513 SA-15013	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because of an invalid file token.	<ul style="list-style-type: none"> <li>• Perform <b>Network Connectivity Test</b> and make sure that connectivity to the <b>Dell Upload Server</b> is successful.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
SA-4514 SA-15014	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because the collection file is corrupted.	<ul style="list-style-type: none"> <li>• Perform <b>Network Connectivity Test</b> and make sure that connectivity to the <b>Dell Upload Server</b> is successful.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
SA-4521 SA-15021	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because the proxy server is not reachable.	<ul style="list-style-type: none"> <li>• Verify the proxy server settings in SupportAssist Enterprise.</li> <li>• Make sure that the proxy server is reachable.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul> <p>If the problem persists, contact your network administrator for assistance.</p>
SA-4522 SA-15022	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because an attempt to connect to proxy server is unsuccessful.	<ul style="list-style-type: none"> <li>• Verify the proxy server settings in SupportAssist Enterprise.</li> <li>• Make sure that the proxy server is reachable.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul> <p>If the problem persists, contact your network administrator for assistance.</p>
SA-4523 SA-15023	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because the proxy server user name or password is incorrect.	<ul style="list-style-type: none"> <li>• Make sure that the proxy server user name and password you have entered in SupportAssist Enterprise are correct.</li> <li>• To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul> <p>If the problem persists, contact your network administrator for assistance.</p>

Error code	Error message	Possible resolution
SA-4524 SA-15024	SupportAssist Enterprise is unable to send the collected system information from the <i>device name</i> because of an unknown error with reaching the proxy server.	<ul style="list-style-type: none"> <li>· Verify the proxy server settings in SupportAssist Enterprise.</li> <li>· Make sure that the proxy server is reachable.</li> <li>· To retry collecting the system information, select the device and click <b>Start Collection</b>.</li> </ul> <p>If the problem persists, contact your network administrator for assistance.</p>
SA-4550	SupportAssist Enterprise is unable to collect system information from the <i>device name</i> because the hard-drive space available on the server where SupportAssist Enterprise is installed has become critically low.	For information about the hard-drive space requirements for a SupportAssist Enterprise environment, see <a href="#">Hardware requirements</a> .
SA-30130	SupportAssist Enterprise has placed the <i>device name</i> in the <b>Staging</b> group because a required verification could not be completed.	To add the device, try to revalidate the device later.
SA-30180	SupportAssist Enterprise has placed the <i>device name</i> in the <b>Staging</b> group because the device does not have required license.	To add the device, ensure that iDRAC Enterprise license is installed on the device, and then revalidate the device.
SA-30260	SupportAssist Enterprise has placed the <i>device name</i> in the <b>Staging</b> group because SupportAssist is not enabled in Enterprise Manager.	To add the device, ensure that SupportAssist Enterprise is enabled in Enterprise Manager, and then revalidate the device.

## Related documents and resources

In addition to this guide you can access the following guides available on the Dell Support website.

**Table 41. Related documents**

Document title	How to access the document
<i>Dell EMC SupportAssist Enterprise Version 1.0 Online Help</i>	Click the help icon on the user interface.
<i>Dell EMC SupportAssist Enterprise Version 1.0 Quick Setup Guide</i>	<ol style="list-style-type: none"> <li>1. Visit <a href="https://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> <li>2. Click <b>SupportAssist Enterprise</b>.</li> <li>3. Click <b>Manuals</b>.</li> </ol>
<i>Dell EMC SupportAssist Enterprise Version 1.0 Support Matrix</i>	
<i>Dell EMC SupportAssist Enterprise Version 1.0 Reportable Items</i>	
<i>Dell EMC SupportAssist Enterprise Version 1.0 Release Notes</i>	
<i>Dell OpenManage Server Administrator Installation Guide</i>	Visit <a href="https://Dell.com/OpenManageManuals">Dell.com/OpenManageManuals</a> and click <b>OpenManage Server Administrator</b> .
<i>Dell OpenManage Server Administrator User's Guide</i>	
<i>iDRAC User's Guide</i>	Visit <a href="https://Dell.com/idracmanuals">Dell.com/idracmanuals</a> .
<i>Dell SupportAssist: Alert Policy</i>	Visit <a href="https://Dell.com/SupportAssistGroup">Dell.com/SupportAssistGroup</a> .
<i>Managing Windows Device Credentials in SupportAssist Using Service Account</i>	

## Video tutorials

You can access the following video tutorials related to SupportAssist Enterprise.

**Table 42. Video tutorials**

Video title	How to access the videos
Installing SupportAssist Enterprise	Visit the <b>Dell TechCenter</b> channel on YouTube, and click <b>Playlist</b> . On the playlist, click <b>SupportAssist Enterprise</b> .
Adding devices	
Importing multiple devices	
Revalidating a device	
Managing device groups	
Viewing collections	
Checking for cases	
Managing cases	
Testing network connectivity	
Testing case creation	

## SupportAssist Enterprise community

You can also find video tutorials, peer-to-peer questions, user's guides, and other useful information on the Dell SupportAssist Enterprise community forum at [Dell.com/SupportAssistGroup](https://Dell.com/SupportAssistGroup).

## Dell Remote Consulting Service

You can use your existing Dell Remote Consulting Service contract or place an order and schedule time with a systems management deployment expert for SupportAssist Enterprise installation, set up, and configuration from start to finish.


## Accessing documents from Dell support site

You can access the required documents in one of the following ways:

- Using the following links:
  - For all Enterprise Systems Management documents — [Dell.com/SoftwareSecurityManuals](https://Dell.com/SoftwareSecurityManuals)
  - For OpenManage documents — [Dell.com/OpenManageManuals](https://Dell.com/OpenManageManuals)
  - For Remote Enterprise Systems Management documents — [Dell.com/esmmanuals](https://Dell.com/esmmanuals)
  - For iDRAC and Lifecycle Controller documents — [Dell.com/idracmanuals](https://Dell.com/idracmanuals)
  - For OpenManage Connections Enterprise Systems Management documents — [Dell.com/OMConnectionsEnterpriseSystemsManagement](https://Dell.com/OMConnectionsEnterpriseSystemsManagement)
  - For Serviceability Tools documents — [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools)
  - For Client Command Suite Systems Management documents — [Dell.com/DellClientCommandSuiteManuals](https://Dell.com/DellClientCommandSuiteManuals)
- From the Dell Support site:
  - a. Go to [Dell.com/Support/Home](https://Dell.com/Support/Home).
  - b. Under **Select a product** section, click **Software & Security**.
  - c. In the **Software & Security** group box, click the required link from the following:
    - **Enterprise Systems Management**
    - **Remote Enterprise Systems Management**
    - **Serviceability Tools**
    - **Dell Client Command Suite**
    - **Connections Client Systems Management**
  - d. To view a document, click the required product version.
- Using search engines:
  - Type the name and version of the document in the search box.

## Contacting Dell

### Prerequisites

 **NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.**

### About this task

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

## Steps

1. Go to **Dell.com/support**.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.