

# SupportAssist Enterprise

Version 1.1 User's Guide

## Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

**Copyright © 2017 Dell Inc. or its subsidiaries. All rights reserved.** Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

# Contents

<b>1 Overview</b>	<b>10</b>
What is new in this release	10
Overview of supported device types	11
How SupportAssist Enterprise works	12
SupportAssist Enterprise capabilities available with Dell service contracts	12
System information collected by SupportAssist Enterprise	13
<b>2 Getting started with SupportAssist Enterprise</b>	<b>15</b>
Setting up SupportAssist Enterprise for the local system	15
Setting up SupportAssist Enterprise for remote devices	16
Evaluating SupportAssist Enterprise	16
Evaluating the monitoring capability	16
Evaluating the system information collection capability	16
Downloading the SupportAssist Enterprise installation package	17
Installing, Upgrading, or Migrating to SupportAssist Enterprise	17
Minimum requirements for installing and using SupportAssist Enterprise	18
Hardware requirements	18
Software requirements	19
Network requirements	20
Installing SupportAssist Enterprise	22
Operating system considerations for installing SupportAssist Enterprise	23
Installing SupportAssist Enterprise by using the SupportAssist Enterprise installer package (Windows)	23
Installing SupportAssist Enterprise by using the SupportAssist Enterprise installer package (Linux)	25
Installing SupportAssist Enterprise in silent mode (Linux)	26
Installing SupportAssist Enterprise by using the OpenManage Essentials installation package	27
Upgrading SupportAssist Enterprise	28
Upgrading SupportAssist Enterprise by using the SupportAssist Enterprise installation package	28
Upgrading SupportAssist Enterprise by using the OpenManage Essentials installer package	29
Migrating to SupportAssist Enterprise	29
Migrating to SupportAssist Enterprise by using the SupportAssist Enterprise installer package (Windows)	29
Migrating to SupportAssist Enterprise by using the SupportAssist Enterprise installer package (Linux)	31
Migrating to SupportAssist Enterprise by using the OpenManage Essentials installer package	32
Using SupportAssist Enterprise without registration	32
Registering SupportAssist Enterprise	33
Setting up an SELinux enabled system to receive alerts	35
Opening the SupportAssist Enterprise user interface	36
Logging in to SupportAssist Enterprise	36
Logging out of SupportAssist Enterprise	36
<b>3 Adding devices</b>	<b>37</b>
Device types and applicable devices	37

Adding a single device.....	39
Adding a server or hypervisor.....	39
Adding an iDRAC.....	42
Adding a chassis.....	43
Adding a Networking device.....	45
Adding a PowerVault MD Series storage array.....	46
Adding an EqualLogic PS Series storage solution .....	47
Adding a Compellent SC Series storage solution.....	48
Adding a Fluid File System (FluidFS) NAS device.....	49
Adding a software.....	50
Adding a solution.....	51
Adding a device by duplication.....	52
Importing multiple devices.....	54
Exporting details of devices that were not imported.....	57
Revalidating a device.....	57
<b>4 Viewing cases and devices.....</b>	<b>59</b>
Viewing all support cases.....	59
Viewing support cases for a specific device.....	60
Case management options.....	62
Requesting to suspend case activities for 24 hours.....	63
Requesting to resume support activities.....	63
Requesting to close a support case.....	64
Viewing the device inventory.....	65
Viewing the device overview pane.....	65
Refining the displayed data.....	66
Filtering the displayed data.....	66
Clearing the data filter.....	67
Sorting the displayed data.....	67
<b>5 Device grouping.....</b>	<b>68</b>
Predefined device groups.....	69
Viewing device groups.....	69
Creating a device group.....	69
Managing devices in a device group.....	70
Managing the credentials of a device group.....	71
Viewing and updating the contact information of a device group.....	71
Editing device group details.....	72
Deleting a device group.....	72
<b>6 Using Extensions .....</b>	<b>73</b>
Types of extensions.....	73
Support for setting up adapter or Remote Collector .....	73
Getting started with inventorying devices managed by OpenManage Essentials or Microsoft System Center Operations Manager.....	74
Adapters.....	74

Setting up OpenManage Essentials adapter.....	74
Setting up the Microsoft System Center Operations Manager adapter.....	76
Management Packs for inventorying devices managed by Operations Manager.....	78
Viewing adapter overview pane .....	79
Viewing devices inventoried by the adapter.....	79
Synchronizing adapter .....	79
Editing adapter.....	80
Deleting adapter.....	80
Remote Collectors.....	81
Minimum requirements for setting up a Remote Collector.....	81
Setting up Remote Collector.....	83
Viewing collections for devices associated with a Remote Collector.....	85
Viewing the Remote Collector overview pane.....	86
Viewing devices associated with a Remote Collector.....	86
Editing Remote Collector.....	87
Deleting Remote Collector.....	87
<b>7 Managing device credentials.....</b>	<b>89</b>
Editing device credentials.....	89
Account Credentials.....	90
Adding Account Credentials.....	91
Editing Account Credentials.....	92
Deleting Account Credentials .....	93
Credential Profiles.....	94
Creating Credential Profile .....	94
Assigning Credential Profile.....	96
Editing Credential Profile.....	96
Deleting Credential Profile .....	97
<b>8 Maintaining SupportAssist Enterprise capability.....</b>	<b>98</b>
Enabling or disabling monitoring of a device.....	98
Installing or upgrading OMSA by using SupportAssist Enterprise.....	99
Configuring SNMP settings by using SupportAssist Enterprise.....	101
Viewing and updating the contact information.....	102
Configuring proxy server settings.....	103
Connectivity test.....	104
Viewing the connectivity status.....	104
Performing the connectivity test.....	105
Testing the case creation capability.....	105
Clearing the System Event Log (SEL).....	105
Automatic update.....	106
Enabling or disabling automatic updates.....	107
Deleting a device.....	107
Opting in or opting out from ProSupport Plus recommendation report emails.....	108
<b>9 Configuring email notifications.....</b>	<b>110</b>

Configuring email notification settings.....	110
Configuring SMTP server settings.....	111
Types of email notifications.....	111
<b>10 Configuring collection settings.....</b>	<b>113</b>
Prerequisites for collecting system information.....	113
Enabling or disabling the automatic collection of system information on case creation.....	114
Enabling or disabling the periodic collection of system information from all devices.....	114
Enabling or disabling the collection of identity information.....	115
Enabling or disabling the collection of software information and the system log.....	116
Enabling or disabling the automatic upload of collections.....	116
<b>11 Viewing collections.....</b>	<b>117</b>
Viewing a collection from the Devices page.....	117
Viewing a collection from the Collections page.....	118
Refining collections based on a date range.....	119
Configuration Viewer.....	119
Data views.....	120
Log types.....	121
Items reported in periodic collections from servers.....	121
Downloading and viewing a multiple device collection.....	123
Multiple device configuration viewer.....	124
<b>12 Using SupportAssist Enterprise to collect and send system information.....</b>	<b>126</b>
Setting up SupportAssist Enterprise for collecting and sending system information.....	126
Starting the collection of system information from a single device.....	127
Starting the collection of system information from multiple devices.....	128
Uploading a collection.....	130
Uploading a collection from a disconnected site.....	130
<b>13 Understanding maintenance mode.....</b>	<b>132</b>
Global-level maintenance mode.....	132
Device-level maintenance mode.....	132
Enabling or disabling global-level maintenance mode.....	133
Enabling or disabling device-level maintenance mode.....	133
<b>14 SupportAssist Enterprise user groups.....</b>	<b>135</b>
SupportAssist Enterprise functions and user privileges.....	135
Granting elevated or administrative privileges to users.....	137
Adding users to the SupportAssist Enterprise user groups (Windows).....	137
Adding users to the SupportAssist Enterprise user groups (Linux).....	137
<b>15 Manually configuring SNMP settings.....</b>	<b>139</b>
Manually configuring the alert destination of a server.....	139
Manually configuring the alert destination of a server by using the script file (Windows).....	139
Manually configuring the alert destination of a server (Windows).....	140

Manually configuring the alert destination of a server by using the script file (Linux).....	141
Manually configuring the alert destination of a server (Linux).....	142
Manually configuring the alert destination of iDRAC by using the web interface.....	142
Manually configuring the alert destination of a chassis by using the web interface.....	143
Manually configuring the alert destination of a networking device.....	143
<b>16 Other useful information.....</b>	<b>144</b>
Monitoring servers for hardware issues.....	144
Benefits of agent-based monitoring.....	145
Support for automatically installing or upgrading OMSA.....	145
Support for automatically configuring SNMP settings.....	146
Device correlation.....	146
Detection of hardware issues in attached storage devices.....	147
Support for Dell OEM servers.....	147
Installing Net-SNMP (Linux only).....	147
Configuring sudo access for SupportAssist Enterprise (Linux).....	148
Ensuring successful communication between the SupportAssist Enterprise application and the SupportAssist server.....	148
Accessing the SupportAssist Enterprise application logs.....	149
Event storm handling.....	149
Accessing the context-sensitive help.....	149
Viewing SupportAssist Enterprise product information.....	149
Uninstalling SupportAssist Enterprise.....	150
Uninstalling SupportAssist Enterprise (Windows).....	150
Uninstalling SupportAssist Enterprise (Linux).....	150
Uninstalling SupportAssist Enterprise in silent mode (Linux).....	151
Identifying the generation of a Dell PowerEdge server.....	151
<b>17 Troubleshooting.....</b>	<b>153</b>
Installing SupportAssist Enterprise .....	153
SupportAssist Enterprise registration.....	154
Opening the SupportAssist Enterprise user interface.....	154
Logging in to SupportAssist Enterprise .....	154
Unable to add device.....	155
Servers.....	155
Storage.....	156
Networking.....	156
Chassis.....	156
Software.....	156
Unable to add adapter.....	157
Unable to add Remote Collector.....	157
Disconnected.....	157
Importing multiple devices.....	157
OMSA not installed.....	158
SNMP not configured.....	158
New version of OMSA available.....	158

Unable to configure SNMP.....	158
Unable to verify SNMP configuration.....	159
Unable to install OMSA.....	159
Unable to verify OMSA version.....	159
OMSA not supported.....	160
Unable to reach device.....	160
Unable to gather system information.....	160
Servers.....	160
Hypervisors.....	161
Storage.....	161
Networking.....	162
Chassis.....	162
Software.....	162
Insufficient storage space to gather system information.....	162
Unable to export collection.....	162
Unable to send system information.....	163
Authentication failed.....	163
Server.....	163
Storage.....	163
Networking.....	164
Chassis.....	164
Software.....	164
Clearing System Event Log failed.....	164
Clearing the System Event Log by using iDRAC.....	165
Clearing the System Event Log by using OMSA.....	165
Maintenance mode.....	165
Auto update.....	165
Unable to edit device credentials.....	166
Servers.....	166
Storage.....	166
Networking.....	166
Chassis.....	167
Software.....	167
Automatic case creation.....	167
Scheduled tasks.....	167
SupportAssist Enterprise services.....	168
Verifying the status of SupportAssist Enterprise services (Windows).....	168
Verifying the status of SupportAssist Enterprise services (Linux).....	169
Other services.....	169
WMI service.....	169
SSH service.....	169
Security.....	169
<b>18 SupportAssist Enterprise user interface.....</b>	<b>170</b>
SupportAssist Enterprise Registration Wizard.....	172
Welcome.....	172

Proxy Settings.....	172
Registration.....	173
Summary.....	173
Login page.....	173
Cases page.....	173
Devices page.....	176
Add Single Device or Import Multiple Devices window.....	180
Device Import pane.....	183
Device overview pane.....	184
Multiple Device Collection window.....	185
Multiple Device Collection pane.....	186
Device Groups page.....	186
Manage Devices.....	187
Manage Contacts.....	187
Edit/Delete Device Group.....	188
Manage Account Credentials.....	189
Add Account Credentials.....	189
Edit Account Credentials.....	190
Manage Credential Profiles .....	192
Add Credential Profile.....	192
Edit Credential Profile.....	193
Collections page.....	193
Collection overview pane.....	194
Extensions.....	195
Adapters.....	195
Remote Collectors.....	199
Settings.....	202
Proxy Settings.....	202
Preferences.....	203
Contact Information.....	205
SMTP Settings.....	206
Network Connectivity Test.....	207
SupportAssist Enterprise test.....	207
<b>19 Error code appendix.....</b>	<b>209</b>
<b>20 Related documents and resources.....</b>	<b>227</b>
Video tutorials.....	227
SupportAssist community.....	228
Accessing documents from the Dell EMC support site.....	228
Contacting Dell.....	229

# Overview

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 Technical Support and sends you an email notification. The system information required for troubleshooting the issue is automatically collected by SupportAssist Enterprise and sent securely to Technical Support. The collected system information helps Technical Support to provide you an enhanced, personalized, and efficient support experience. SupportAssist Enterprise capability also includes a proactive response from Technical Support to help you resolve the issue.

Additionally, SupportAssist Enterprise can monitor hardware issues that may occur on devices that you are managing by using OpenManage Essentials or Microsoft System Center Operations Manager.

- ① **NOTE:** SupportAssist Enterprise can monitor hardware issues that occur in Dell server and Dell networking devices. For certain Dell storage devices, monitoring of hardware issues is supported when the devices are inventoried in SupportAssist Enterprise by using the OpenManage Essentials adapter. For more information on adapters, see [Using Extensions](#).
- ① **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

- ① **NOTE:** In this document, the term *local system* refers to the server where SupportAssist Enterprise is installed; *remote device* refers to any other device in your environment.

Topics:

- [What is new in this release](#)
- [Overview of supported device types](#)
- [How SupportAssist Enterprise works](#)
- [SupportAssist Enterprise capabilities available with Dell service contracts](#)
- [System information collected by SupportAssist Enterprise](#)

## Related links

[System information collected by SupportAssist Enterprise](#)

## What is new in this release

- Set up an adapter to inventory devices that are managed by OpenManage Essentials or Microsoft System Center Operations Manager
- Create Account Credentials for each device type
- Create and assign Credential Profiles to devices
- Set up Remote Collectors to collect and upload system information from devices within specific IP address ranges
- Support for up to 15,000 devices on a Windows installation by setting up Remote Collectors

- Support for up to 3,500 devices on a Linux installation
- Support for the 14th generation of PowerEdge servers
- Support for VxRail appliances
- Support for additional storage and networking device models
- Collect system information from management and monitoring software such as VMware vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Dell EqualLogic SAN Headquarters (SAN HQ), and Host Integration Toolkit for VMware / Virtual Storage Manager (HIT Kit / VSM)
- Periodic collection of system information from all devices on a specific day of each month
- Enable or disable the automatic upload of collections
- Search for devices, cases, or collections based on specific criteria
- Set the number of items listed per page on the **Devices**, **Cases**, and **Collections** pages
- Configure an IP address exclusion list for the proxy server
- Migrate from SupportAssist for OpenManage Essentials or SupportAssist for Microsoft System Center Operations Manager to SupportAssist Enterprise
- Ability to assign custom ports for SupportAssist Enterprise

## Overview of supported device types

SupportAssist Enterprise is compatible with Dell server, storage, and networking 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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](https://www.dell.com/support/compat).

- Servers
  - 9th and later generations of PowerEdge servers
  - PowerEdge C Series servers
  - Datacenter Scalable Solutions
  - PowerVault NX devices
  - PowerVault DL devices
  - OEM-ready servers
- Storage
  - EqualLogic storage arrays
  - PowerVault MD Series storage arrays
  - Compellent storage arrays
  - Fluid File System (FluidFS) Network attached storage (NAS) devices
  - OEM-ready storage devices
- Networking
  - PowerConnect switches
  - Force10 switches
  - Networking switches
  - Networking X-Series switches
  - Networking Wireless Controllers Mobility Series
  - OEM-ready Networking devices
- Chassis
  - PowerEdge FX2/FX2s
  - PowerEdge VRTX
  - PowerEdge M1000e

- Software
  - HIT Kit / VSM for VMware
  - SAN HQ
  - vCenter
  - SCVMM
- Solution
  - XC Series of Web-scale Hyper-converged appliances

**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 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.

- ① **NOTE:** To experience the automatic case creation and system information 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 system information 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](#).
- ① **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 service contract, and if the alert type and number of alerts received from the device match with the predefined criteria for support case creation.
- ① **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.

- ① **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 system information collected from a monitored device is used to predict hardware failures that may occur in future.	✗	✗	✓
Automated collection of system information	The system information required for troubleshooting an issue 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 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 Technical Support	A 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 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	The system information 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 batteries, hard drives, backplanes, and expanders of 12th and later generation of PowerEdge servers that have PowerEdge RAID Controller (PERC) Series 5 to 9. Predictive detection of hardware failures is available only when the automated periodic collection and upload of system information is enabled in SupportAssist Enterprise.

## System information collected by SupportAssist Enterprise

SupportAssist Enterprise continually monitors the configuration information 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 system information inadvertently collected or viewed will be treated in accordance with the Dell Privacy Policy available for review at [Dell.com/privacy](https://www.dell.com/privacy).

The information encrypted in the collected system information log that is 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 system information collected by SupportAssist Enterprise. For information on viewing the collected system information, see [Viewing the collected system information](#).

By default, SupportAssist Enterprise collects system information from all devices, irrespective of the service contract of the devices, and sends the system information securely to Dell. System information is collected from one device at a time based on the predefined collection start day and time specified in the **Preferences** page.

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

# Getting started with SupportAssist Enterprise

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.

Topics:

- [Setting up SupportAssist Enterprise for the local system](#)
- [Setting up SupportAssist Enterprise for remote devices](#)
- [Evaluating SupportAssist Enterprise](#)
- [Downloading the SupportAssist Enterprise installation package](#)
- [Installing, Upgrading, or Migrating to SupportAssist Enterprise](#)
- [Minimum requirements for installing and using SupportAssist Enterprise](#)
- [Installing SupportAssist Enterprise](#)
- [Upgrading SupportAssist Enterprise](#)
- [Migrating to SupportAssist Enterprise](#)
- [Using SupportAssist Enterprise without registration](#)
- [Registering SupportAssist Enterprise](#)
- [Setting up an SELinux enabled system to receive alerts](#)
- [Opening the SupportAssist Enterprise user interface](#)
- [Logging in to SupportAssist Enterprise](#)
- [Logging out of SupportAssist Enterprise](#)

## 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 Install SupportAssist Enterprise. See [Installing 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 of system information from your devices. 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 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 [Setting up SupportAssist Enterprise for the local system](#).
- 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 remote devices in SupportAssist Enterprise. See [Adding devices](#).
- 4 (Optional) Set up an adapter to inventory and add devices from OpenManage Essentials or Microsoft System Center Operations Manager. See [Adapters](#).
- 5 (Optional) If you have more than 3,500 devices, set up Remote Collectors. See [Remote Collectors](#).
- 6 (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 system information 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 system information 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 system information collected by SupportAssist Enterprise from devices, see [System information collected by SupportAssist Enterprise](#).

You can also view the system information 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 system information 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 certain 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 automatic collection of system information when a support case is created. See [Enabling or disabling the automatic collection of system information](#).
- You can also prevent the upload of collections. See [Disabling the automatic upload of collections](#).

**NOTE:** In most cases, part or all of the system information collected by SupportAssist Enterprise is required by Technical Support to properly diagnose issues and provide an appropriate resolution. To receive the full benefits of SupportAssist Enterprise, you must enable all the system information 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 virtual machine or a 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 enterprise** 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 **SupportAssist Enterprise Windows Management Server** link.
  - For the Linux installation package, click the **SupportAssist Enterprise 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.

## Installing, Upgrading, or Migrating to SupportAssist Enterprise

Installing SupportAssist Enterprise enables you to receive the automated support capabilities for your Dell server, storage, and networking devices.

- If you are installing SupportAssist Enterprise for the first time, perform one of the following:
  - Install SupportAssist Enterprise by using the SupportAssist Enterprise installation package. For more information, see [Installing SupportAssist Enterprise by using the SupportAssist Enterprise installation package](#).
  - Install SupportAssist Enterprise by using the OpenManage Essentials installation package. For more information, see [Installing SupportAssist Enterprise by using the OpenManage Essentials installation package](#).

The following table provides information about the supported upgrade or migration paths.

**Table 2. Upgrading and migrating to SupportAssist Enterprise**

If you have installed...	Do this...
SupportAssist Enterprise version 1.0	Upgrade to SupportAssist Enterprise version 1.1. For more information, see <a href="#">Upgrading SupportAssist Enterprise</a> .
SupportAssist for Servers version 1.2 or 1.3	Migrate to SupportAssist Enterprise version 1.1. For more information, see <a href="#">Migrating to SupportAssist Enterprise</a> .
SupportAssist for Dell OpenManage Essentials version 2.1 or 2.2	
SupportAssist for Microsoft System Center Operations Manager Version 1.0 or 1.1	

## 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 — collection of system information only or both monitoring and collection of system information

You can install SupportAssist Enterprise on a virtual machine or 9th or later generation PowerEdge server.

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

**Table 3. Hardware requirements**

Requirement	Processor	Installed memory (RAM)	Hard drive (free space)
For collection of system information from a single device	1 core	4 GB	1 GB
For monitoring and collection of system information from up to 20 devices	2 cores	4 GB	4 GB
For monitoring and collection of system information from up to 100 devices	4 cores	8 GB	12 GB
For monitoring and collection of system information from up to 300 devices	4 cores	8 GB	32 GB
For monitoring and collection of system information from up to 1000 devices	8 cores	8 GB	60 GB

Requirement	Processor	Installed memory (RAM)	Hard drive (free space)
For monitoring and collection of system information from up to 3500 devices	8 cores	16 GB	90 GB

- ① **NOTE:** When SupportAssist Enterprise is installed on a Windows operating system, you can extend the monitoring and collection capabilities for up to 15,000 devices by setting up multiple Remote Collectors.
- ① **NOTE:** When SupportAssist Enterprise is installed on Windows, you can extend SupportAssist Enterprise capability to monitor more than 3,500 devices by setting up adapters and Remote Collectors. For more information on setting up adapters and Remote Collectors, see [Using extensions](#).
- ① **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 supported 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

- ① **NOTE:** SupportAssist Enterprise can be installed only on 64-bit operating systems.
- Microsoft Windows Server 2008 R2 SP1 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
- ① **NOTE:** In Windows Server 2016, ensure that you select Internet Explorer as the default browser for opening SupportAssist Enterprise.
- ① **NOTE:** SupportAssist Enterprise can also be installed on a Microsoft Windows domain controller.
- ① **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.

**NOTE:** To open SupportAssist Enterprise by using Internet Explorer:

- In the **Security** tab, enable **Active Scripting**.
- In the **Advanced** tab, enable **Play animations in web pages**.

## 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 or faster.
- 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 hosted by Dell.
  - <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 network bandwidth requirements for monitoring and collecting system information from devices.

**Table 4. Network bandwidth requirements**

Requirement	LAN bandwidth*	WAN bandwidth**
For collection of system information from a single device	10 Mbps	5 Mbps
For monitoring and collection of system information from up to 20 devices	0.5 Gbps	10 Mbps

Requirement	LAN bandwidth*	WAN bandwidth**
For monitoring and collection of system information from up to 100 devices	0.5 Gpbs	10 Mbps
For monitoring and collection of system information from up to 300 devices	0.5 Gpbs	10 Mbps
For monitoring and collection of system information from up to 1000 devices	1 Gpbs	20 Mbps
For monitoring and collection of system information from up to 3500 devices	1 Gpbs	20 Mbps

\* Network bandwidth required for monitoring and collecting system information from devices within a single site.

\*\* Network bandwidth required for monitoring and collecting system information from devices that are distributed across multiple sites.

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

**Table 5. 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 adding the local system running Windows (WMI) and to collect system information
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 6. 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
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
Software	22	For adding a device running HIT Kit for VMware and to collect system information
	443	For adding a device running VMware vCenter and to collect system information
	135	For adding a device running SCVMM and to collect system information
	135	For adding a device running SAN HQ and to collect system information
Solution	443	For adding a Web-Scale Converged Appliance and to collect system information

## Installing SupportAssist Enterprise

You can install SupportAssist Enterprise by using either the SupportAssist Enterprise installer package or the OpenManage Essentials installer package. The following sections provide the instructions to install SupportAssist Enterprise on Windows or 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 a Windows 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](#).

# Operating system considerations for installing SupportAssist Enterprise

The features available in SupportAssist Enterprise vary based on the operating system where SupportAssist Enterprise is installed. The complete features of SupportAssist Enterprise are available only when SupportAssist Enterprise is installed on a Windows operating system. The following table provides a comparison of the available features when SupportAssist Enterprise is installed on a Windows or Linux operating system.

**Table 7. Features available based on the operating system where SupportAssist Enterprise is installed**

Feature	Windows	Linux
Maximum device support	Up to 15, 000 devices	Up to 3,500 devices
Adding devices	Adding of all device types is supported	Adding all device types is supported, except for: <ul style="list-style-type: none"> <li>• Servers running Windows</li> <li>• SCVMM</li> <li>• SAN HQ</li> </ul>
Installing or upgrading OMSA on a remote server through SupportAssist Enterprise	Supported on Windows and Linux operating systems	Supported on Linux operating systems only
Set up Remote Collectors to enable a remote device to collect and upload system information to Dell	Supported	Not supported
Set up adapters to inventory and add devices that are managed by OpenManage Essentials or Microsoft System Center Operations Manager	Supported	Not supported

**NOTE:** For more information about setting up adapters and Remote Collectors, see [Using Extensions](#).

## Installing SupportAssist Enterprise by using the SupportAssist Enterprise installer package (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**.

If the default SupportAssist Enterprise ports (9099 and 2424) are already in use, the **Port Settings** page is displayed. Else, 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 If the **Port Settings** page is displayed, perform one of the following:

- Ensure that no other application is configured to use ports 9099 and 2424.
- Enter custom port numbers.

**NOTE:** Ensure that you enter a valid port number which is not in use and within the range 1025 to 65535.

- 6 Click **Finish** to exit the SupportAssist Enterprise installer.

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

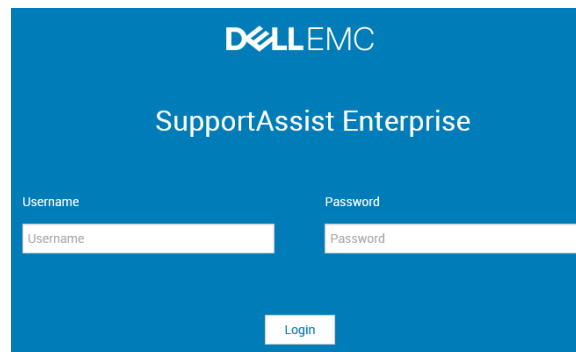


Figure 1. Login page

**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.

- 7 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 of system information from your devices. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.

# Installing SupportAssist Enterprise by using the SupportAssist Enterprise installer package (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](#).
- If you are using a Linux terminal emulator such as PuTTY to remotely install SupportAssist Enterprise, ensure that you are using PuTTY version 0.63 or later.

## 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 supportassistenterprise_1.1.0.bin` and press Enter.
  - Type `chmod +x supportassistenterprise_1.1.0.bin` and press Enter.
- 4 Type `./supportassistenterprise_1.1.0.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.

If the default SupportAssist Enterprise ports (9099 and 2424) are already in use, you are prompted to ensure that the ports are not in use or to enter custom port numbers. Else, the **SupportAssist Enterprise** login page opens in a web browser window.

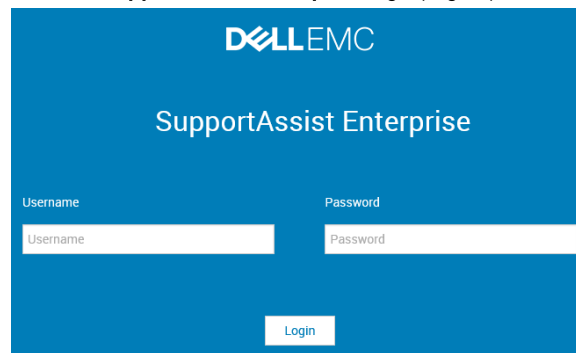


Figure 2. Login page

**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`
- NOTE:** If you entered a custom port number, you must replace 9099 with the custom port number in the web address.

**NOTE:** On certain Linux operating systems, the SupportAssist Enterprise services may not start automatically after the installation is complete. To resolve the issue, edit the `/etc/hosts` file to include the localhost entries. For example, `127.0.0.1 localhost`.

- 7 If you are prompted that the default SupportAssist Enterprise ports are in use, perform one of the following and then press `y`.
- Ensure that no other application is configured to use ports 9099 and 2424.
  - Enter custom port numbers.

**NOTE:** Ensure that you enter a valid port number which is not in use and within the range 1025 to 65535.

- 8 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 of system information from your devices. 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

- Open the terminal window on the system running the Linux operating system.
- Browse to the folder where the SupportAssist Enterprise installation package is available.
- Perform one of the following:
  - Type `chmod 744 supportassistenterprise_1.1.0.bin` and press Enter.

- Type `chmod +x supportassistenterprise_1.1.0.bin` and press Enter.
- 4 Type `./supportassistenterprise_1.1.0.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 of system information from your devices. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.

## Installing SupportAssist Enterprise by using the OpenManage Essentials installation package

### Prerequisites

- The system must have internet connectivity.
- You must have Administrator rights on the system.
- Port 443 must be open on the firewall to access:
  - <https://apidp.dell.com>
  - <https://api.dell.com/>
  - <https://is.us.dell.com/FUS/api/2.0/uploadfile>
  - <https://is.us.dell.com/FUSCHUNK/api/1.0/file/uploadChunk>
  - <https://downloads.dell.com/>
  - <ftp://ftp.dell.com/>

**① NOTE:** If the installation of SupportAssist Enterprise is unsuccessful, perform one of the following:

- Retry the installation. To retry the installation, right-click the SupportAssistSetup.exe file available at C:\Program Files\Dell\SysMgt\Essentials\SupportAssistSetup on the OpenManage Essentials custom installation folder, and select Run as administrator.
- Download the SupportAssist Enterprise installation package and install it on the server running OpenManage Essentials on any other server.

### Steps

- 1 Extract the OpenManage Essentials installation package to a folder on the system.
- 2 In the folder where you extracted the installation package, double-click the **Autorun.exe** file.  
The **Dell EMC OpenManage Install** window is displayed.
- 3 If OpenManage Essentials version 2.3 is not installed on the system, make sure that **Dell EMC OpenManage Essentials** is selected.
- 4 Select **Dell EMC SupportAssist Enterprise**, and then click **Install**.  
If you selected **Dell EMC OpenManage Essentials** and **Dell EMC SupportAssist Enterprise**, installation of OpenManage Essentials is completed and then SupportAssist Enterprise is installed. The system prerequisites for installing SupportAssist Enterprise are verified. If the system prerequisites are met, the **Welcome to Dell EMC SupportAssist Enterprise Installer** window is displayed.
- 5 Click **Next**.  
The **License Agreement** window is displayed.
- 6 Read the terms in the communication requirements and click **I Agree**.  
**① NOTE:** SupportAssist Enterprise installation requires that you allow Dell to save certain Personally Identifiable Information (PII) such as your contact information, administrator credentials of the devices to be monitored, and so on. SupportAssist Enterprise installation cannot proceed unless you allow Dell to save your PII.
- 7 Read the software license agreement, click **I Agree**, and then click **Next**.  
The **Installing SupportAssist Enterprise** window is displayed briefly, and then the **Installation Completed** window is displayed.
- 8 Click **Finish**.

## 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 of system information from your devices. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.

# Upgrading SupportAssist Enterprise

If you are using SupportAssist Enterprise version 1.0, you can upgrade to SupportAssist Enterprise version 1.1 by using one of the following installation packages:

- SupportAssist Enterprise version 1.1 installation package available at [Dell.com/SupportAssistGroup](https://Dell.com/SupportAssistGroup).
- OpenManage Essentials version 2.3 installation package available at [DellTechCenter.com/OME](https://DellTechCenter.com/OME).

**ⓘ NOTE:** Before you upgrade SupportAssist Enterprise, ensure that SupportAssist Enterprise is not open in any web browser window.

## Upgrading SupportAssist Enterprise by using the SupportAssist Enterprise installation package

- 1 On the Dell OpenManage Essentials management server, right-click the SupportAssist Enterprise installer package, and select **Run as administrator**.

**ⓘ NOTE:** UAC requires that the installation is performed with elevated privileges that are obtained only through the Run as administrator option. If you are logged on to the OpenManage Essentials server as an administrator, double-click the installer package to install SupportAssist Enterprise. However, ensure that you click Run on 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 Enterprise'. Do you want to continue?** prompt, click **Yes**.  
The **Preparing to Install** window is briefly displayed, and then the **Resuming the Install Wizard for SupportAssist Enterprise** window is displayed.
- 3 Click **Upgrade**.  
If the default SupportAssist Enterprise ports (9099 and 2424) are already in use, the **Port Settings** page is displayed. Else, the **Install Wizard Completed** window is displayed.
- 4 If the **Port Settings** page is displayed, perform one of the following:
  - Ensure that no other application is configured to use ports 9099 and 2424.
  - Enter custom port numbers.

**ⓘ NOTE:** Ensure that you enter a valid port number which is not in use and within the range 1025 to 65535.

- 5 Click **Finish**.

If you had created device groups and device group credentials prior to the upgrade, the following changes occur:

- Device group credentials are saved as Credential Accounts and Credential Profiles. However, if individual and device group credentials were configured for devices within the device group, only the individual device credentials are applied for those devices after the upgrade. If necessary, you can select those devices and apply the created credential profiles.
- Credential Accounts are not created for the existing individual device credentials. If devices within the device group were configured with individual credentials, the individual credentials are saved and applied on the devices.

- ① **NOTE:** After upgrading from an unregistered version of SupportAssist, collections that you manually initiate are not automatically uploaded. To ensure that these collections are automatically uploaded, enable the automatic collection upload settings in the Preferences page.

## Upgrading SupportAssist Enterprise by using the OpenManage Essentials installer package

- 1 Double-click the OpenManage Essentials executable file.  
The **Dell OpenManage Install** window is displayed.
- 2 Ensure that SupportAssist Enterprise is selected and then click **Install**.  
The **Welcome to Dell SupportAssist Enterprise Installer** window is displayed.
- 3 Click **Next**.  
The **Installing SupportAssist Enterprise** window is displayed briefly, and then the **Installation Completed** window is displayed.
- 4 Click **Finish**.

If you had created device groups and device group credentials prior to the upgrade, the following changes occur:

- Device group credentials are saved as Credential Accounts and Credential Profiles. However, if individual and device group credentials were configured for devices within the device group, only the individual device credentials are applied for those devices after the upgrade. If necessary, you can select those devices and apply the created credential profiles.
- Credential Accounts are not created for the existing individual device credentials. If devices within the device group were configured with individual credentials, the individual credentials are saved and applied on the devices.

- ① **NOTE:** If you have upgraded OpenManage Essentials, you must run discovery and inventory of all existing discovery ranges in OpenManage Essentials.

- ① **NOTE:** After upgrading from an unregistered version of SupportAssist, collections that you manually initiate are not automatically uploaded. To ensure that these collections are automatically uploaded, enable the automatic collection upload settings in the Preferences page.

## Migrating to SupportAssist Enterprise

If you are already using SupportAssist for Servers, SupportAssist for OpenManage Essentials, or SupportAssist for Microsoft System Center Operations Manager, you can migrate to SupportAssist Enterprise. When you migrate to SupportAssist Enterprise, the devices, cases, device credentials, user groups, and settings are migrated. Before you migrate, download the SupportAssist Enterprise Windows or Linux installer package depending on the operating system running on the server.

- ① **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 by using the SupportAssist Enterprise installer package (Windows)

### Prerequisites

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

### About this task

If you have SupportAssist for Servers version 1.2 or 1.3, SupportAssist for Dell OpenManage Essentials version 2.1 and 2.2, or SupportAssist for Microsoft System Center Operations Manager version 1.0 or 1.1 installed, you can migrate to SupportAssist Enterprise.

**NOTE:** Migration to SupportAssist Enterprise version 1.1 from SupportAssist for OpenManage Essentials is supported only if OpenManage Essentials version 2.3 is installed on the system.

## 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.

If you had created device groups and device group credentials prior to the upgrade, the following changes occur:

- Device group credentials are saved as Credential Accounts and Credential Profiles. However, if individual and device group credentials were configured for devices within the device group, only the individual device credentials are applied for those devices after the upgrade. If necessary, you can select those devices and apply the created credential profiles.
- Credential Accounts are not created for the existing individual device credentials. If devices within the device group were configured with individual credentials, the individual credentials are saved and applied on the devices.

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

## Next steps

For EqualLogic devices only: After migration from SupportAssist for OpenManage Essentials to SupportAssist Enterprise, members of an EqualLogic group that are discovered in OpenManage Essentials are replaced in SupportAssist Enterprise by only the EqualLogic group. The EqualLogic group is placed in the **Staging** group with an **Unable to add device** status because the credentials of the EqualLogic group are not available. To add the EqualLogic group in SupportAssist Enterprise, ensure that you edit the credentials or apply a Credential Profile to the EqualLogic group after migration.

For migration from SupportAssist for Microsoft System Center Operations Manager to SupportAssist Enterprise only: The servers that were discovered in SupportAssist for Microsoft System Center Operations Manager are placed in the **Staging** group with an **Unable to add device** status because the credentials of the servers are not available. To add the servers in SupportAssist Enterprise, ensure that you edit the credentials or apply a Credential Profile to the servers after migration.

**NOTE:** If the server running SupportAssist Enterprise connects to the internet through a proxy server, devices that were added with the iDRAC IP address are placed in the Staging group. To move the devices to the Default group, add the IP address of the iDRACs in the Proxy Exclusion List on the SupportAssist Enterprise Proxy Settings page and then revalidate each device.

After migration from an unregistered version of SupportAssist, collections that you manually initiate are not automatically uploaded. To ensure that these collections are automatically uploaded, enable the automatic collection upload settings in the **Preferences** page.

# Migrating to SupportAssist Enterprise by using the SupportAssist Enterprise installer package (Linux)

## Prerequisites

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

## About this task

If you have SupportAssist for Servers version 1.2 or 1.3 installed, you can migrate to 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 supportassistenterprise_1.1.0.bin` and press Enter.
  - Type `chmod +x supportassistenterprise_1.1.0.bin` and press Enter.
- 4 Type `./supportassistenterprise_1.1.0.bin` and press Enter.

**NOTE:** If you want to migrate SupportAssist Enterprise silently, type `./supportassistenterprise_1.1.0.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**.

If you had created device groups and device group credentials prior to migration, the following changes occur:

- Device group credentials are saved as Credential Accounts and Credential Profiles. However, if individual and device group credentials were configured for devices within the device group, only the individual device credentials are applied for those devices after the upgrade. If necessary, you can select those devices and apply the created credential profiles.
- Credential Accounts are not created for the existing individual device credentials. If devices within the device group were configured with individual credentials, the individual credentials are saved and applied on the devices.

The **Devices** page is displayed.

## Next steps

After migration from an unregistered version of SupportAssist, collections that you manually initiate are not automatically uploaded. To ensure that these collections are automatically uploaded, enable the automatic collection upload settings in the **Preferences** page.

# Migrating to SupportAssist Enterprise by using the OpenManage Essentials installer package

## About this task

If you have SupportAssist for OpenManage Essentials version 2.1 or 2.2 installed, you can migrate to SupportAssist Enterprise version 1.1 by using the OpenManage Essentials installer package.

**NOTE:** Migration to SupportAssist Enterprise version 1.1 from SupportAssist for OpenManage Essentials is supported only if OpenManage Essentials version 2.3 is installed on the system.

## Steps

- 1 Double-click the OpenManage Essentials executable file.  
The **Dell OpenManage Install** window is displayed.
- 2 Ensure that SupportAssist Enterprise is selected and then click **Install**.  
The **Welcome to Dell SupportAssist Enterprise Installer** window is displayed.
- 3 Click **Next**.  
The **Installing SupportAssist Enterprise** window is displayed briefly, and then the **Installation Completed** window is displayed.
- 4 Click **Finish**.

If you had created device groups and device group credentials prior to migration, the following changes occur:

- Device group credentials are saved as Credential Accounts and Credential Profiles. However, if individual and device group credentials were configured for devices within the device group, only the individual device credentials are applied for those devices after the upgrade. If necessary, you can select those devices and apply the created credential profiles.
- Credential Accounts are not created for the existing individual device credentials. If devices within the device group were configured with individual credentials, the individual credentials are saved and applied on the devices.

For devices that are not members of a device group:

- If only the default credentials were configured, the default credentials are saved as individual credentials and applied on all applicable devices.
- If both default and individual credentials were configured for the devices, only the individual credentials are saved and applied on those devices.

# 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 8. 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 from a single device or multiple devices</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 collection of system information</li><li>• View support cases that are open for your devices</li></ul>

Capabilities or features that are available	Capabilities or features that are not available
	<ul style="list-style-type: none"> <li>• Opt-in or opt-out from receiving ProSupport Plus Server Recommendation Report by email</li> <li>• Update contact details</li> <li>• Set up adapter</li> <li>• Set up Remote Collector</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 of system information from your devices. Until registration is completed, SupportAssist Enterprise can neither monitor your devices for hardware issues nor automatically collect system information.

The **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 **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.

**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 Red Hat Enterprise Linux 6 and 7, CentOS 6 and 7, and Oracle Enterprise Linux 6 and 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:
  - Double-click the Dell SupportAssist Enterprise desktop icon.
  - Open a web browser and type the address in the following format:  
`http://localhost:9099/SupportAssist`

**NOTE:** If you entered a custom port number during the installation of SupportAssist Enterprise, you must replace 9099 with the custom port number in the web address.

- 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 may be 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 may be 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 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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](https://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

**NOTE:** You can use the extensions available in SupportAssist Enterprise to inventory and add supported devices that are managed by OpenManage Essentials or Microsoft System Center Operations Manager. For more information about the available extensions, see [Using Extensions](#).

**NOTE:** By default, a SupportAssist option is available on all 14th generation of PowerEdge servers. By registering the SupportAssist option on a 14th generation server, you can receive the automated support capabilities of SupportAssist for that server. If such a server is added in SupportAssist Enterprise with the Device Type as iDRAC, the SupportAssist option on the server is disabled. However, the server receives the automated support capabilities through SupportAssist Enterprise.

**NOTE:** Only IPv4 addresses are supported for adding devices and collecting system information.

Topics:

- [Device types and applicable devices](#)
- [Adding a single device](#)
- [Importing multiple devices](#)
- [Exporting details of devices that were not imported](#)
- [Revalidating a device](#)

## 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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).

Table 9. Selecting a device type

Device Type	Devices that you can add
Chassis	<ul style="list-style-type: none"> <li>PowerEdge M1000e</li> <li>PowerEdge VRTX</li> <li>PowerEdge FX2/FX2s</li> </ul>
Fluid File System (FluidFS)	<ul style="list-style-type: none"> <li>EqualLogic with FluidFS</li> <li>PowerVault with FluidFS</li> <li>Compellent FS with FluidFS</li> </ul>
iDRAC	<p>12th and later generations of PowerEdge servers</p> <p><b>NOTE:</b> To add an iDRAC, you must provide the iDRAC IP address of the server.</p>
Networking	<ul style="list-style-type: none"> <li>PowerConnect</li> <li>Force10</li> <li>Networking</li> <li>Networking X-Series switches</li> <li>Networking Wireless Controllers Mobility Series</li> </ul>
Peer Storage (PS) / EqualLogic	EqualLogic PS Series storage arrays
PowerVault	PowerVault MD series storage arrays
Server / Hypervisor	<p>9th or later 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:</b> To add a Server / Hypervisor, you must provide the operating system IP address of the server.</p> <p><b>NOTE:</b> If SupportAssist Enterprise is installed on a Linux operating system, adding servers running Windows is not supported.</p>
Software	<ul style="list-style-type: none"> <li>HIT Kit / VSM for VMware</li> <li>SAN HQ</li> <li>vCenter</li> <li>SCVMM</li> </ul> <p><b>NOTE:</b> If SupportAssist Enterprise is installed on a Linux operating system, adding SCVMM and SAN HQ is not supported.</p>
Solution	XC Web-Scale Converged Appliance
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
- Software
- Solution
- 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.
  - Ports 22 and 443 must be open on the device.
  - For collecting system information from ESX and ESXi only, ensure that SFCBD and CIMOM are enabled.
- 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 Point to **Devices** and click **View Devices**.  
The **Devices** page is displayed.
- 2 Click **Add Devices**.

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

- 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**

- 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.

- 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.

- 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. 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.

- Click **Next**.

The **Device Credentials** page is displayed.

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

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 **Default** device group, 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 later generation Dell PowerEdge server (iDRAC7 or later). 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 or later 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.

**NOTE:** By default, a SupportAssist component is available on 14th generation of PowerEdge servers. You can register the SupportAssist component on the server to receive the automated support capabilities of SupportAssist. When an iDRAC is added in SupportAssist Enterprise, the SupportAssist component is automatically disabled, but the automatic support capabilities are available through SupportAssist Enterprise.

## Steps

- 1 Point to **Devices** and click **View 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. 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 **Default** device group, see [Predefined device groups](#).

10 Click **Finish**.


 **NOTE:** If you have selected the **Configure SNMP Settings** option, device addition may take some time.


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.
- Port 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 system information 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 Point to **Devices** and click **View 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. 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 **Default** device group, 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 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.
- Ports 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 system information 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 Point to **Devices** and click **View 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. 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](#).

- Click **Next**.  
The **Device Credentials** page is displayed.
- Type the user name, password, enable password, and community string of the device in the appropriate fields and click **Next**.

**NOTE:** Community string is required only for the following networking devices:

- PowerConnect family 28xx and X series
- Cisco
- Wireless controllers

**NOTE:** Enable password is required only when the networking device is configured with an enable password.

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.

- 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 **Default** device group, see [Predefined device groups](#).
- Click **Finish**.  
The device is added to the device inventory and the **Summary** page is displayed.
- 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:

- Ensure that all prerequisites for adding the device are met.
- 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 system information from the PowerVault MD Series storage arrays. By adding a PowerVault device, you will be able to collect system information on demand and after deployment.

### Steps

- Point to **Devices** and click **View Devices**.  
The **Devices** page is displayed.
- 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 **Default** device group, 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 an EqualLogic PS 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.
- 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 system information from the EqualLogic PS Series storage arrays. By adding a Dell EqualLogic device, you will be able to collect system information on demand and after deployment.

### Steps

- 1 Point to **Devices** and click **View 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 **Default** device group, 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 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 system information from the Dell Compellent SC Series storage solutions. By adding a Dell Compellent device, you will be able to collect system information on demand and after deployment.

### Steps

- 1 Point to **Devices** and click **View 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 **Default** device group, 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 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 system information from a Dell Fluid File System (FluidFS) network attached storage (NAS) device. By adding a FluidFS NAS device, you will be able to collect system information on demand and after deployment. The FluidFS NAS devices that you can add are:

- Dell Compellent
- Dell EqualLogic
- Dell PowerVault

### Steps

- 1 Point to **Devices** and click **View 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.

**① 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 **Default** device group, 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 software

### 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.

### About this task

SupportAssist Enterprise can only collect system information from the management and monitoring software such as VMware vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Dell EqualLogic SAN Headquarters (SAN HQ), and Host Integration Toolkit for VMware (HIT Kit / VSM).

### Steps

- 1 Point to **Devices** and click **View 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 **Software**.
- 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 From the **Select Software type** list, select the software type, and then type the user name and password in the appropriate fields.
- 8 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 **Default** device group, 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

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 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.
- Firmware version 4.x or later must be installed on the device for the collection of system information.

### About this task

SupportAssist Enterprise can monitor hardware issues and collect system information from a Web-Scale Hyper-converged appliance.

### Steps

- 1 Point to **Devices** and click **View 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 **Solution**.
- 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 From the **Select solution type** list, select the solution, and then type the user name and password of the solution in appropriate fields.
- 8 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 **Default** device group, 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

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 Point to **Devices** and click **View Devices**.

The **Devices** page is displayed.

2 Select a device which is of the same type as the device that you want to add.

**Devices** Search by  Search term

Collection purpose:

Assign Credential Profile:

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input checked="" type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

**PowerEdge T710**

Tasks:

Status:  Connected

Display Name: Server 1

Hostname / IP Address: 100.96.20.210

Service Tag: HKNK82S

Device Type: Server / Hypervisor

Model: PowerEdge T710

Operating System: VMware ESXi 5.5.0 build-2652839

Monitoring:  Enable  Disable

Revalidate:

Collections: No Collections

Next Scheduled Collection: Friday, Jun 9, 2017

**Figure 5. Duplicate option**

The device overview pane is displayed.

- 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 **Default** device group, 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

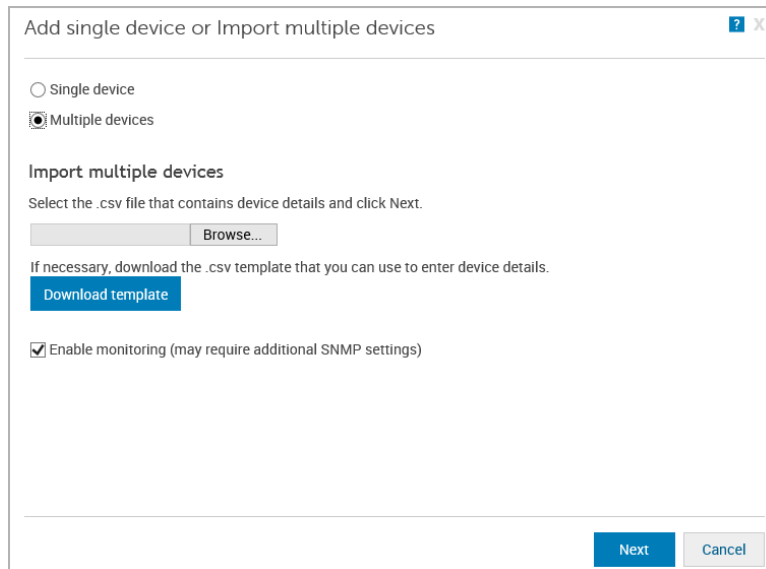
You can import multiple devices by using a .csv file that contains details of the devices in a specified format.

**NOTE:** The maximum number of devices that you can import by using a csv file is 3,500.

**NOTE:** The Import Multiple Devices option does not support the import of software.

## Steps

- 1 Point to **Devices** and click **View 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**.



Add single device or Import multiple devices

Single device  
 Multiple devices

**Import multiple devices**  
Select the .csv file that contains device details and click Next.

If necessary, download the .csv template that you can use to enter device details.

Enable monitoring (may require additional SNMP settings)

Figure 6. Import multiple devices window

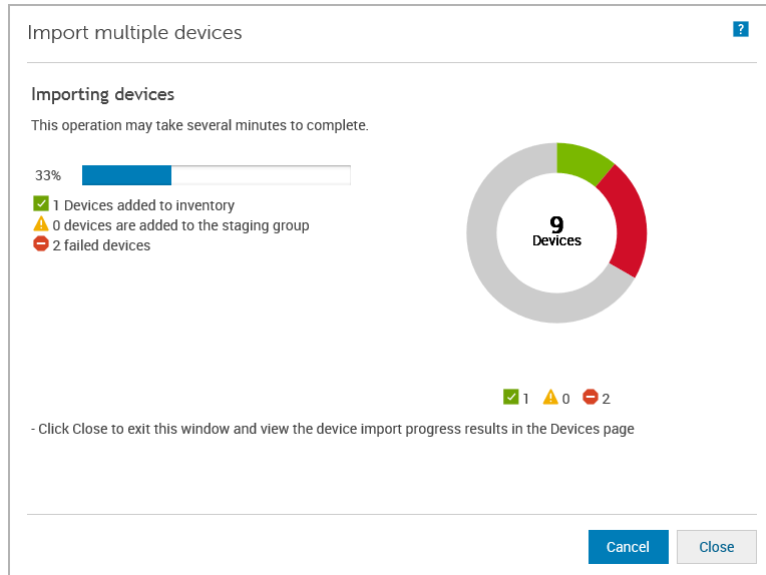
- 4 Click **Download .csv template** and save the .csv file.
- 5 Open the .csv template and update the details of the devices.

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:

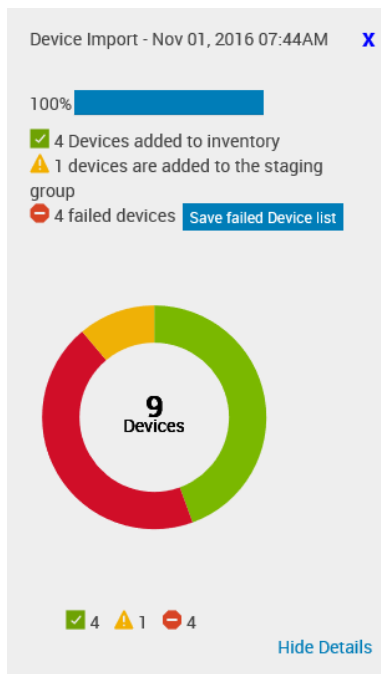
- The import operation is stopped after your confirmation.
- Devices that were already imported are retained in the **Default** or **Staging** group.
- The import operation continues for devices for which discovery has already started.
- Devices for which the initial identification is incomplete are 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. 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 enable 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 Point to **Devices** and click **View 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).
- 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](#).

## 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 Point to **Devices** and click **View 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** Search by  Search term

Collection purpose:

Assign Credential Profile:

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input checked="" type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

**PowerEdge T710**

Tasks:

Status:  Connected

Display Name: Server 1

Hostname / IP Address: 100.96.20.210

Service Tag: HKNK82S

Device Type: Server / Hypervisor

Model: PowerEdge T710

Operating System: VMware ESXi 5.5.0 build-2652839

Monitoring:  Enable  Disable

Revalidate:

Collections: No Collections

Next Scheduled Collection: Friday, Jun 9, 2017

**Figure 9. Revalidate option**

The device overview pane is displayed.

- 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 **Assign Device Group (Optional)** page is displayed.
- 5 If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.
- 6 Click **Finish**.  
The device is added to the device inventory and the **Summary** page is displayed.
- 7 Click **OK**.

# Viewing cases and devices

The 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.

Topics:

- [Viewing all support cases](#)
- [Viewing support cases for a specific device](#)
- [Case management options](#)
- [Viewing the device inventory](#)
- [Viewing the device overview pane](#)
- [Refining the displayed data](#)
- [Filtering the displayed data](#)
- [Clearing the data filter](#)
- [Sorting the displayed data](#)

## 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, point to **Cases** and click **View Cases**. A **Fetching Cases** progress indicator is displayed at the top of the **Cases** page when SupportAssist Enterprise is checking if cases are present for the devices that you have added.

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 D...
- ProSupport One for D...

Source Type :

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

Home > Cases

**Cases**

Search by Service Tag Search term

Case Options Refresh

	Name / IP Address	Number	Status	Title	Device Type	Date Opened
Networking1 - Last Refreshed 11/28/2016 07:55 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
<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](#).

## Viewing 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.

### Steps

- 1 Point to **Devices** and click **View 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 **Tasks** list, select **Check for cases**.

Devices Search by Name / IP Address  Search term

Collection purpose

Assign Credential Profile

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input checked="" type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

**PowerEdge T710**

Tasks

- 
- 
- 
- 
- 
- Dependencies**
- 
- 

Status

Display Name

Hostname / IP Address

Service Tag HKNK82S

Device Type Server / Hypervisor

Model PowerEdge T710

Operating System VMware ESXI 5.5.0 build-2652839

Monitoring  Enable  Disable

Revalidate

Collections No Collections

Next Scheduled Collection Friday, Jun 9, 2017

**Figure 11. 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

Search by Service Tag Search term

Case Options Refresh

	Name / IP Address	Number	Status	Title	Device Type	Date Opened
Networking1 - Last Refreshed - 10/28/2016 11:50 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

Figure 12. 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.

## 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 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.

Home > Cases

Cases

Search by Service Tag Search term

Case Options Refresh

	Name / IP Address	Number	Status	Title	Device Type	Date Opened
Networking1 - Last Refreshed - 10/28/2016 11:50 AM						
<input checked="" 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

Figure 13. 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 Technical Support to stop activities related to a support case for 24 hours, if necessary. For example, you may want Technical Support to suspend activities for a support case in the following scenarios:

- If you want to resolve the issue without any assistance from 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 Technical Support to stop activities related to a support case only if the support case was opened by SupportAssist.

## Steps

- 1 Point to **Cases** and click **View 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 Technical Support to resume activities for a support case, if you had previously requested to suspend activities for the support case.

## Steps

- 1 Point to **Cases** and click **View 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 for which you want to Technical Support to resume case activities.

**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 Technical Support to close the corresponding support case.

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

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

#### Steps

- 1 Point to **Cases** and click **View 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, 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, point to **Devices** and click **View Devices**.

Home > Devices

**Devices** Search by Name / IP Address Search term

[+ Add Device](#) [▶ Start Collection](#) [✎ Edit Credentials](#) [✕ Delete](#) Collection purpose [Select](#) Assign Credential Profile [Select](#) [Refresh](#)

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

Refine By:

Device Type:

- Server
- Storage
- Networking
- Chassis
- Software
- Solution

+ Groups:

Figure 14. 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 system information collected from a device
- Add a device by duplication

## Steps

- 1 Point to **Devices** and click **View Devices**.  
The **Devices** page is displayed.
- 2 Select a device.

① **NOTE:** The device overview pane is displayed if only one device is selected in the Devices page.

① **NOTE:** If a SupportAssist Enterprise-initiated task is already running on a device, you may not be able to select that device.

The device overview pane is displayed.

The screenshot shows the 'Devices' page with a search bar and a table of devices. The 'Server 1' device is selected, and its details are shown in the 'Device overview pane' on the right. The table lists the following devices:

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input checked="" type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

The 'Device overview pane' for 'PowerEdge T710' includes the following details:

- Tasks: Select Task
- Status:  Connected
- Display Name: Server 1
- Hostname / IP Address: 100.96.20.210
- Service Tag: HKNK82S
- Device Type: Server / Hypervisor
- Model: PowerEdge T710
- Operating System: VMware ESXi 5.5.0 build-2652839
- Monitoring:  Enable,  Disable
- Revalidate: Revalidate button
- Collections: No Collections
- Next Scheduled Collection: Friday, Jun 9, 2017
- Duplicate button

Figure 15. Device overview pane

## Refining the displayed data

### About this task

You can refine the data displayed on the **Devices**, **Cases** or **Collections** page based on the available options.

- The **Devices** page can be refined based on collection type, device type, adapter, and remote collectors.
- The **Cases** page can be refined by device type, case status, service contract of the device, and the source of the case.
- The **Collections** page can be refined by collection type, device type, and date range.

### Steps


- 1 Open the **Cases**, **Devices**, or **Collections** page.
- 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**, **Cases** or **Collections** page based on your preference.

- 1 Click the filter icon  displayed in the column header.

- The **Filter Option** panel is displayed.
- In the **Contains** field, type the filtering criteria.
- 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 **Devices**, **Cases** or **Collections** page to view all the available data.

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

## Sorting the displayed data

To sort the data displayed on the **Devices**, **Cases** or **Collections** page, 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.

# Device grouping

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 networking)
- 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.
- Assign a Credential Profile 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.

Topics:

- [Predefined device groups](#)
- [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](#)

## 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 add 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:
  - For servers, the iDRAC does not have an Enterprise license installed
  - For Compellent devices, 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 **Manage Device Groups**.

The **Device Groups** page is displayed.

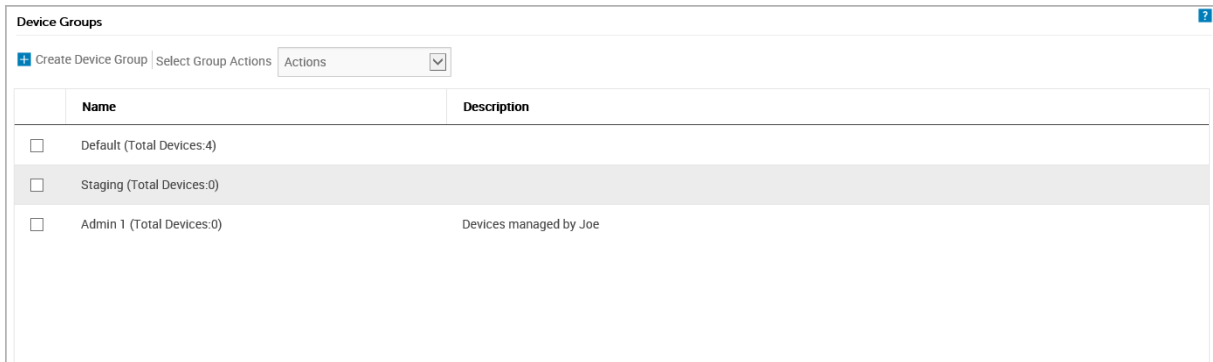


Figure 16. Device Groups page

# 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 **Manage Device 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.

### Steps

- 1 Point to **Devices** and click **Manage Device 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.

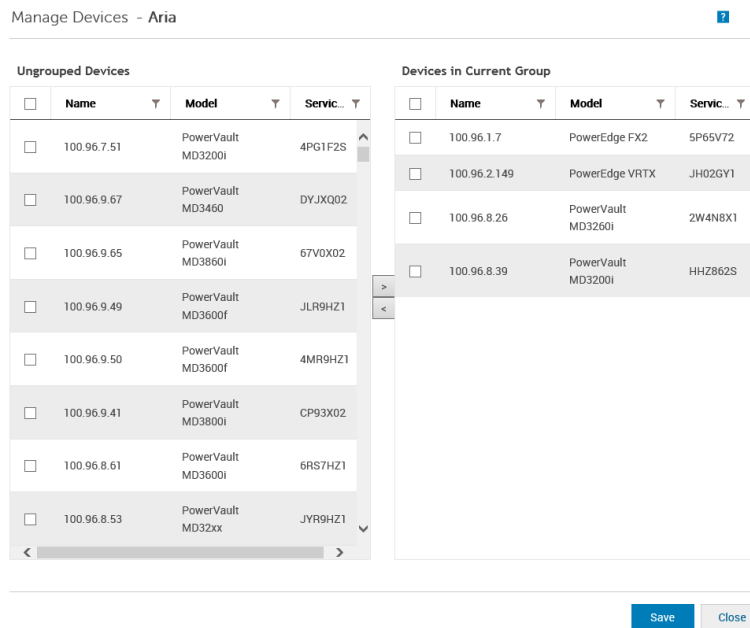


Figure 17. Manage Devices window

- 4 To add devices to the device group, select the devices in the **Ungrouped** pane, and click  .  
The selected devices are moved to the **Devices in current group** pane.

- 5 To remove devices from the device group, select the devices in the **Devices in current group** pane, and click  .

The selected devices are moved to the **Ungrouped** 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](#).
- You must have created a Credential Profile. See [Creating Credential Profile](#).

### About this task

You can use the **Assign Credential Profile** option to apply common credentials for the different device types within a device group.

The Credential Profile overrides the default credentials that you provided for adding a device in SupportAssist Enterprise. When a Credential Profile is applied:

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

### Steps

1 Point to **Devices** and click **View Devices**.

The **Devices** page is displayed.

2 From the **Refine by** pane, expand **Groups** and select a device group.

3 Select the devices for which you want to apply a Credential Profile.

4 From the **Assign Credential Profile** list, select a Credential Profile.

Credentials are assigned to the device group based on the credentials available in the selected Credential Profile.

## 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 **Manage Device 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 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

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

### Steps

- 1 Point to **Devices** and click **Manage Device 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 **Manage Device 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**.

# Using Extensions

The extensions available in SupportAssist Enterprise enable you to extend the SupportAssist Enterprise capability to many devices. You can use the extensions to inventory and add devices that are managed by a systems management console such as Dell OpenManage Essentials or Microsoft System Center Operations Manager. The extensions also enable you to optimize the performance of SupportAssist Enterprise by distributing the workload of collecting and uploading system information to remote systems.

Topics:

- [Types of extensions](#)
- [Support for setting up adapter or Remote Collector](#)
- [Getting started with inventorying devices managed by OpenManage Essentials or Microsoft System Center Operations Manager](#)
- [Adapters](#)
- [Remote Collectors](#)

## Types of extensions

Two types of extensions are available in SupportAssist Enterprise:

- **Adapter** — An application that acts as an interface between SupportAssist Enterprise and a systems management console. The adapter enables SupportAssist Enterprise to inventory and retrieve alerts from supported devices that are managed by a systems management console, instead of adding each device individually. After inventorying and adding the devices, SupportAssist Enterprise can monitor the devices for hardware issues and also collect and upload system information to Dell. Two types of adapters available in SupportAssist Enterprise:
  - OpenManage Essentials adapter — For inventorying devices managed by OpenManage Essentials
  - System Center Operations Manager adapter — For inventorying devices managed by System Center Operations Manager
- **Remote Collector** — A remote instance of SupportAssist Enterprise that collects and uploads system information from devices within a specific IP address range. The Remote Collector enables SupportAssist Enterprise to distribute the workload of collecting and uploading system information to a remote system. Typically, collection and upload of system information from all your devices is performed by the server where SupportAssist Enterprise is installed. When you set up a Remote Collector on a remote system, collection and upload of system information from devices within the specified IP address ranges is performed by the remote system. To ensure optimal performance of SupportAssist Enterprise, Dell recommends that you set up a separate Remote Collector for every 3,500 devices.

## Support for setting up adapter or Remote Collector

The capability to set up an adapter or Remote Collector is available only when SupportAssist Enterprise is installed on a Windows operating system. The following tables provide a summary of the capability to set up an adapter or Remote Collector depending on the operating system.

**Table 10. Support for setting up an adapter**

Operating system where SupportAssist Enterprise is installed	Support for setting up an adapter on a local or remote server running Windows	Support for setting up an adapter on a local or remote server running Linux
Windows	Yes	No
Linux	No	No

**NOTE:** For the devices that you can inventory in SupportAssist Enterprise by setting up an adapter, see the list of devices in the *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).

**Table 11. Support for setting up a Remote Collector**

Operating system where SupportAssist Enterprise is installed	Support for setting up Remote Collector on a remote server running Windows	Support for setting up Remote Collector on a remote server running Linux
Windows	Yes	No
Linux	No	No

**NOTE:** For the devices that you can assign to a Remote Collector, see the list of devices in the *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).

## Getting started with inventorying devices managed by OpenManage Essentials or Microsoft System Center Operations Manager

To get started with inventorying your devices that are managed by OpenManage Essentials or Operations Manager:

- 1 Add Account Credentials for your devices. See [Adding Account Credentials](#).
- 2 Create one or more Credential Profiles depending on the type of devices that you want to add. See [Creating Credential Profile](#).
- 3 Set up the adapter in SupportAssist Enterprise. See [Setting up OpenManage Essentials adapter](#) or [Setting up Microsoft System Center Operations Manager adapter](#).
- 4 If you have more than 3,500 devices, set up a Remote Collector. See [Setting up Remote Collector](#).

## Adapters

The adapter is an application that acts as an interface between SupportAssist Enterprise and a systems management console. Setting up an adapter enables SupportAssist Enterprise to inventory devices and retrieve alerts from devices that are managed by the systems management console. You can set up one or more of the following adapters depending on the systems management console that you are using:

- OpenManage Essentials adapter — To inventory devices that are managed by OpenManage Essentials
- System Center Operations Manager adapter — To inventory devices that are managed by Microsoft System Center Operations Manager

### Related links

[Extensions](#)

## Setting up OpenManage Essentials adapter

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The system where you want to set up the adapter must be running OpenManage Essentials version 2.3.
- You must have administrator privileges on the system running OpenManage Essentials.
- You must have created Account Credentials and a Credential Profile that contains the credentials of the devices that will be inventoried by the adapter. See [Creating Account Credentials](#) and [Creating Credential Profile](#).

### About this task

Setting up the OME adapter enables you to inventory devices that are managed by OpenManage Essentials. During the set up, SupportAssist Enterprise installs the adapter on the system running OpenManage Essentials, and then inventories the devices.

- ① **NOTE:** If you have installed SupportAssist Enterprise and OpenManage Essentials on the same server, you must also set up the adapter on the same server to add devices that are managed by OpenManage Essentials.
- ① **NOTE:** If you have upgraded from SupportAssist for OpenManage Essentials to SupportAssist Enterprise, the OpenManage Essentials adapter is automatically set up and your devices are inventoried in SupportAssist Enterprise.
- ① **NOTE:** The OpenManage Essentials adapter only inventories devices that are supported by SupportAssist Enterprise. For the list of supported devices, see the *SupportAssist Enterprise version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).

### Steps

- 1 Point to **Extensions** and click **Manage Adapters**.  
The **Adapters** page is displayed.
- 2 Click **Set Up Adapter**.  
The **Set Up Adapter** window is displayed.

Set Up Adapter

Adapter type: OpenManage Essentials

Enter details of the system where OpenManage Essentials is installed.

Hostname / IP address: Hostname / IP address

Name (optional): Name

User name: User name

Password: Password

Credential profile: Select

Update device inventory: Every 12 hours

Note: A credential profile is required for adding devices that will be inventoried by the adapter.

OK Cancel

Figure 18. Set Up Adapter window

- 3 From the **Adapter type** list, select **OpenManage Essentials**.
- 4 Perform the following:
  - a Type the hostname or IP address of the server where OpenManage Essentials is installed.
  - b If desired, type a name for the adapter in the appropriate field.  
The name you enter is used to represent the adapter in SupportAssist Enterprise. If you do not enter a name, the host name or IP address that you have entered is used to represent the adapter.
  - c Type the user name and password in the appropriate fields.
- 5 From the **Update device inventory** list, select the desired frequency for inventorying devices through the adapter.
- 6 From the **Credential profile** list, select a Credential Profile that contains the Account Credentials for the device types that will be inventoried by the adapter.
- 7 Click **OK**.  
Devices that are managed by OpenManage Essentials are inventoried in SupportAssist Enterprise.

Adapters		Remote Collectors			
<a href="#">+ Set Up Adapter</a>   <a href="#">Edit</a>   <a href="#">Delete</a>					
	Name	Type	Assigned Devices	Version	Status
<input type="checkbox"/>	AD1 100.96.20.124	OpenManage Essentials	5	1.0	Assigning Profiles 0 of 485 In Progress

Figure 19. Adapters page

**NOTE:** If the adapter is not added successfully, you may have to delete the adapter and set it up again.

### Next steps

If the Credential Profile that you selected contains the correct credentials for the inventoried devices, the devices are added to the **Default** group. Devices for which the credentials are either not correct or not available are moved to the **Staging** group.

**NOTE:** By default, monitoring is enabled for devices that are added successfully through the adapter.

**NOTE:** The automated support capabilities of SupportAssist Enterprise are not available for devices that are placed in the **Staging** group.

To add devices that are placed in the **Staging** group, you can either assign a Credential Profile that contains the correct credentials or enter the credentials for each device individually.

**NOTE:** For EqualLogic devices, only the EqualLogic group is added through the adapter. The EqualLogic members are not added through the adapter.

### Related links

[Adapters](#)

[Set Up Adapter \(OpenManage Essentials\)](#)

## Setting up the Microsoft System Center Operations Manager adapter

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The system or virtual machine where you want to set up the adapter must be running one of the following:
  - Microsoft System Center Operations Manager 2012 R2
  - Microsoft System Center Operations Manager 2012 SP1
  - Microsoft System Center Operations Manager 2016
- Dell Server Management Pack Suite Version 6.2 or 6.3 For Microsoft System Center Operations Manager and System Center Essentials must be installed on the system. For information on the required management packs, see [Management packs required by Operations Manager](#).
- You must have administrator privileges on the system or virtual machine running System Center Operations Manager.
- You must have created Account Credentials and a Credential Profile that contains the credentials of the devices that will be inventoried by the adapter. See [Creating Account Credentials](#) and [Creating Credential Profile](#).

### About this task

Setting up the System Center Operations Manager adapter enables you to inventory devices that are managed by System Center Operations Manager. During the set up, SupportAssist Enterprise installs the adapter on the system running Operations Manager, and then inventories the devices.

- ① **NOTE:** If you have upgraded from SupportAssist for Microsoft System Center Operations Manager to SupportAssist Enterprise, the System Center Operations Manager adapter is automatically set up and your devices are inventoried in SupportAssist Enterprise.
- ① **NOTE:** The System Center Operations Manager adapter only inventories Dell PowerEdge servers, iDRAC, and OEM devices that are supported by SupportAssist Enterprise. For the list of supported PowerEdge servers, see the *SupportAssist Enterprise version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

### Steps

- 1 Point to **Extensions** and click **Manage Adapters**.  
The **Adapters** page is displayed.
- 2 Click **Set Up Adapter**.  
The **Set Up Adapter** window is displayed.

**Figure 20. Set Up Adapter window**

- 3 From the **Adapter type** list, select **System Center Operations Manager**.
- 4 If desired, type a name for the adapter in the appropriate field.  
The name you enter is used to represent the adapter in SupportAssist Enterprise. If you do not enter a name, the host name or IP address that you have entered is used to represent the adapter.
- 5 If you are setting up the adapter on the management group:
  - a Type the hostname or IP address of the management group.
  - b Type the user name and password in the appropriate fields.
- 6 If you are setting up the adapter on a Remote Console (RC), select **Establish a remote connection with the management group**, and perform the following:
  - a Type the hostname or IP address of the management group.
  - b Type the user name and password in the appropriate fields.
  - c Type the hostname or IP address of the Remote Console.
  - d Type the user name and password in the appropriate fields.
- 7 From the **Credential profile** list, select a Credential Profile that contains the credentials of the devices that will be inventoried by the adapter.
- 8 From the **Update device inventory** list, select the desired frequency for inventorying devices through the adapter.
- 9 Click **OK**.  
Devices that are managed by System Center Operations Manager are inventoried in SupportAssist Enterprise.

**NOTE:** If the adapter is not added successfully, you may have to delete the adapter and set it up again.

### Next steps

If the Credential Profile that you selected contains the correct credentials for the inventoried devices, the devices are added to the **Default** group. Devices for which the credentials are either not correct or not available are moved to the **Staging** group.

**NOTE:** By default, monitoring is enabled for devices that are added successfully through the adapter.

**NOTE:** The automated support capabilities of SupportAssist Enterprise are not available for devices that are placed in the **Staging** group.

To add devices that are placed in the **Staging** group, you can either assign a Credential Profile that contains the correct credentials or enter the credentials for each device individually.

### Related links

[Adapters](#)

[Set Up Adapter \(Microsoft System Center Operations Manager\)](#)

## Management Packs for inventorying devices managed by Operations Manager

The following table lists the Dell Server Management Pack Suite Version 6.2 or 6.3 required for SupportAssist Enterprise to inventory devices managed by System Center Operations Manager.

**Table 12. Management Packs for inventorying devices managed by Operations Manager**

Devices to be monitored	Monitoring Feature	Required Management Packs
Dell's 9th or later generation of PowerEdge servers	Servers and Rack Workstations Agent-based Monitoring	<ul style="list-style-type: none"><li>• Dell Base Hardware Library</li><li>• Dell Server Model</li><li>• Dell Server Operations Library</li><li>• Dell Server View Library</li><li>• Dell Windows Server (Scalable Edition)</li><li>• Dell Operations Library Common</li></ul>
iDRAC	DRAC Monitoring	<ul style="list-style-type: none"><li>• Dell Feature Monitoring (optional)</li><li>• Dell Base Hardware Library</li><li>• Dell Operations Library Common</li><li>• Dell DRAC Model</li><li>• Dell DRAC View</li><li>• Dell DRAC Operations Library</li><li>• Dell DRAC (SC2012 OM)</li></ul>

**NOTE:** For information about importing the required management packs, see the *Dell Server Management Pack Suite For Microsoft System Center Operations Manager And System Center Essentials Installation Guide* at [Dell.com/OpenManageManuals](#), under Server Management Pack Versions for Microsoft System Center Operations Manager.

# Viewing adapter overview pane

## Prerequisites

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

## About this task

You can view details of an adapter such as the adapter type, operating system type, managed devices, staging devices, version, and the last inventory date and time in the adapter overview pane.

## Steps

- 1 Point to **Extensions** and click **Manage Adapters**.  
The **Adapters** page is displayed.
- 2 Select an adapter.  
The adapter overview pane is displayed.

## Related links

[Adapters](#)  
[Adapter overview pane](#)

# Viewing devices inventoried by the adapter

## Prerequisites

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

## Steps

- 1 Point to **Devices** and click **View Devices**.  
The **Devices** page is displayed.
- 2 In the **Refine By** pane, click + to expand the adapter list, and then select the adapter.  
The devices that are inventoried by the adapter are displayed.

## Related links

[Adapters](#)

# Synchronizing adapter

## Prerequisites

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

## About this task

By default, the adapter inventories devices from the systems management console at regular intervals, based on your selection. Depending on your requirement, you can also manually initiate the inventory of devices at any time.

## Steps

- 1 Point to **Extensions** and click **Manage Adapters**.  
The **Adapters** page is displayed.
- 2 Select an adapter.  
The adapter overview pane is displayed.
- 3 Click **Sync now**.

## Related links

[Adapters](#)

# Editing adapter

## Prerequisites

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

## About this task

You can edit the details of the adapter to update any of the following:

- Credentials of the server where the adapter is set up
- Inventory frequency
- Credential Profile
- Name

## Steps

- 1 Point to **Extensions** and click **Manage Adapters**.  
The **Adapters** page is displayed.
- 2 Select the adapter that you want to edit and click **Edit**.  
The **Edit Adapter** window is displayed.
- 3 Edit the name, user name, and password as required.
- 4 Change the update inventory frequency and Credential Profile as required.
- 5 Click **Update**.  
The details of the adapter are updated.

## Related links

[Adapters](#)

# Deleting adapter

## Prerequisites

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

## About this task

You can delete an adapter from SupportAssist Enterprise based on your preference.

## Steps

- 1 Point to **Extensions** and click **Manage Adapters**.  
The **Adapters** page is displayed.
- 2 Select the adapter you want to delete and click **Delete**.  
The **Delete Adapter** window is displayed.
- 3 Click **Yes**.  
Deleting an adapter results in the following:
  - Removes the adapter from SupportAssist Enterprise user interface
  - Removes the devices associated with the adapter
  - Uninstalls the adapter application from the server where it was set up

## Related links

[Adapters](#)

# Remote Collectors

The Remote Collector is a remote instance of SupportAssist Enterprise that collects and uploads system information from devices within a specified IP address range. The Remote Collector enables SupportAssist Enterprise to distribute the workload associated with collecting and uploading system information to a remote server. You can set up the Remote Collector on any remote server. Depending on the total number of devices, you can set up multiple Remote Collectors.

System information collected by a Remote Collector is saved on the remote server and directly uploaded to Dell from the remote server.

**NOTE:** A single Remote Collector can collect and upload system information to Dell from up to 3,500 devices.

**NOTE:** The Remote Collector (remote instance of SupportAssist Enterprise) can only collect and upload system information from devices. You cannot add devices to a Remote Collector.

## Related links

[Extensions](#)

# Minimum requirements for setting up a Remote Collector

The following sections describe the minimum hardware and networking requirements for setting up a Remote Collector in SupportAssist Enterprise.

## Hardware requirements

The following table provides a summary of the minimum hardware requirements on the server where the Remote Collector is set up.

**Table 13. Hardware requirements**

Requirement	Processor	Installed memory (RAM)	Hard drive (free space)
For collection of system information from a single device	1 core	4 GB	1 GB
For collection of system information from up to 20 devices	2 cores	4 GB	4 GB
For collection of system information from up to 100 devices	4 cores	8 GB	12 GB
For collection of system information from up to 300 devices	4 cores	8 GB	32 GB
For collection of system information from up to 1000 devices	8 cores	8 GB	60 GB
For collection of system information from up to 3500 devices	8 cores	16 GB	90 GB

## Network requirements

The following are the network requirements of the server where the Remote Collector is set up.

- Internet connection — standard 1 GbE network or faster.
- The server where the Remote Collector is set up must be able to communicate with the SupportAssist server hosted by Dell over HTTPS protocol.
- The Remote Collector must be able to connect to the following destinations:
  - <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.

The following table lists the network bandwidth requirements for collecting system information from devices.

**Table 14. Network bandwidth requirements**

Requirement	Minimum LAN bandwidth*	Minimum WAN bandwidth**
For collection of system information from a single device	10 Mbps	5 Mbps
For collection of system information from up to 20 devices	0.5 Gbps	10 Mbps
For collection of system information from up to 100 devices	0.5 Gbps	10 Mbps
For collection of system information from up to 300 devices	0.5 Gbps	10 Mbps
For collection of system information from up to 1000 devices	1 Gbps	20 Mbps
For collection of system information from up to 3500 devices	1 Gbps	20 Mbps

\* Network bandwidth required for collecting system information from devices within a single site.

\*\* Network bandwidth required for collecting system information from devices that are distributed across multiple sites.

The following table lists the ports that must be open on the server where the Remote Collector is set up.

**Table 15. Network port requirements on the server where the Remote Collector is set up**

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 adding the local system running Windows (WMI) and to collect system information
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

Port	Direction	Usage
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 16. Network port requirements on remote devices**

Device Type	Port	Usage
Server / Hypervisor	22	To collect system information from devices running a Linux operating system
	135	To collect system information from devices running a Linux Windows operating 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
EqualLogic	22	To collect system information
PowerVault	2463	To collect system information
Compellent	443	To collect system information
Fluid File System (FluidFS)	22 and 44421	To collect system information
Networking	22	To collect system information
Chassis	22	For adding the device and to collect system information
Software	22	For adding a device running HIT Kit for VMware and to collect system information
	443	For adding a device running VMware vCenter and to collect system information
	135	For adding a device running SCVMM and to collect system information
	135	For adding a device running SAN HQ and to collect system information
Solution	443	For adding a Web-Scale Converged Appliance and to collect system information

## Setting up Remote Collector

### Prerequisites

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The server where you want to set up the Remote Collector must be reachable from the server where SupportAssist Enterprise is installed.
- Port 5700 must be open on both the server running SupportAssist Enterprise and the server where you want to set up the Remote Collector.

- The remote system must have internet connectivity for uploading the collected system information to Dell.
- The remote system must meet the minimum requirements for setting up the Remote Collector. See [Minimum requirements for setting up a Remote Collector](#).

### About this task

Setting up a Remote Collector enables SupportAssist Enterprise to distribute the workload associated with collecting and uploading system information to a remote server. During the set up, SupportAssist Enterprise installs the Remote Collector on the remote server.

### Steps

- 1 Point to **Extensions** and click **Manage Remote Collectors**.

The **Remote Collectors** page is displayed.

- 2 Click **Set Up Remote Collector**.

The **Set Up Remote Collector** window is displayed.

Set Up Remote Collector

The Remote Collector distributes to a remote system, the task of collecting and uploading system information from devices within specific IP address ranges. During the setup, SupportAssist Enterprise will install the Remote Collector on the remote system.

Note: Set up of the Remote Collector may take several minutes to complete depending on your network bandwidth.

Enter details of the remote system.

Hostname / IP address      Name (optional)

Hostname / IP address      Name

User name      Password

User name      Password

Enter the IP address ranges to associate with the Remote Collector.

IP address / range ⓘ

· · · ·

+ Add IP address range

The remote system connects to the internet through a proxy server

OK Cancel

**Figure 21. Set Up Remote Collector window**

- 3 Type the hostname or IP address of the server where you want to set up the Remote Collector.
- 4 If desired, type a name for the Remote Collector in the appropriate field.
- 5 Type the user name and password in the appropriate fields.
- 6 Type the IP address or IP address ranges of the devices that you want to associate with the Remote Collector. To add multiple IP address ranges, click **Add address range**, and then type the IP address range of the devices.

You can add the IP address range by using one of the following formats:

**NOTE:** Ensure that the IP address ranges you have entered do not overlap with each other.

- 193.109.112.99
- 193.109.112.\*
- 193.104.20-40.\*
- 192.168.\*\*
- 192.168.2-51.3-91

- 193.109.112.45-99

**NOTE:** You can enter up to five different IP address ranges.

- 7 If the remote server connects to the internet through a proxy server, select the **Remote server connects to the internet through a proxy server** option and then do the following:
  - a Type the host name or IP address, and port number of the proxy server in the appropriate fields.
  - b 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 appropriate fields.
  - c In the **Proxy Exclusion List** box, type the IP address range or ranges of devices to which the Remote Collector must communicate directly and not through the proxy server. IP address of devices that communicate through https protocol must be included in the proxy exclusion list. Examples of devices that communicate through https protocol include iDRAC, Compellent storage arrays, VMware ESX and ESXi, and XC Series of Web-scale Hyper-converged appliances.

**NOTE:** You can enter one or more IP address ranges as semi-colon separated values. For example, 10.49.\*.\* ; 10.49.18.\* ; \*.\*.100.10

You can enter the IP address ranges in the following formats:

- 10.49.\*.\*
- 10.49.18.\*
- \*.\*.100.10
- \*\*\*.10
- \*.10.12.100
- 10.\*.\*.\*

The following IP address range formats are not supported:

- 10.\*.\*.49
- 10.\*.49.\*
- 10.49.\*.10

- 8 Click **OK**.

The Remote Collector (remote instance of SupportAssist Enterprise) is installed and set up on the remote server.

**NOTE:** If the Remote Collector is not added successfully, you may have to delete the Remote Collector and set it up again.

#### Related links

[Remote Collectors](#)

[Set Up Remote Collector](#)

## Viewing collections for devices associated with a Remote Collector

### About this task

Collections that are performed by Remote Collectors can only be viewed by manually accessing the collection file.

### Steps

- 1 Log in to the server where the Remote Collector is set up.
- 2 Browse to X:\bin\Collections\**<Appropriate Collection ID folder>**\Results\html folder, where X is the drive where Remote Collector is installed.
- 3 Extract the appropriate collection .zip file and then double click the **index.html** file.

**NOTE:** For collections from devices that are running a non-English operating system, the Configuration Viewer may not display certain attributes as expected.

The **Configuration Viewer** opens in a web browser window.

### Related links

[Remote Collectors](#)

## Viewing the Remote Collector overview pane

### Prerequisites

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

### About this task

You can view details of a Remote Collector such as the name of the Remote Collector, IP address, connectivity status, collection range, and the details of the connected devices in the Remote Collector overview pane.

### Steps

- 1 Point to **Extensions** and click **Manage Remote Collectors**.

The **Remote Collectors** page is displayed.

- 2 Select a Remote Collector.

The Remote Collector overview pane is displayed.

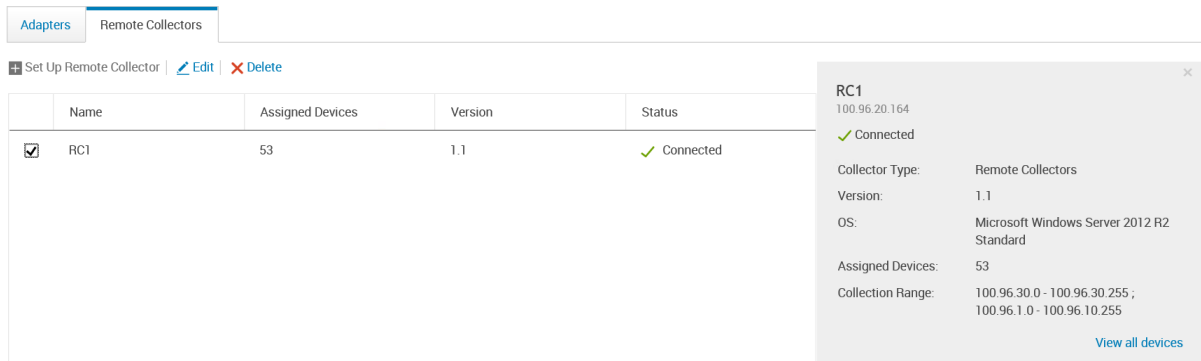


Figure 22. Remote Collector overview pane

### Related links

[Remote Collectors](#)

[Remote Collector overview pane](#)

## Viewing devices associated with a Remote Collector

### Prerequisites

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

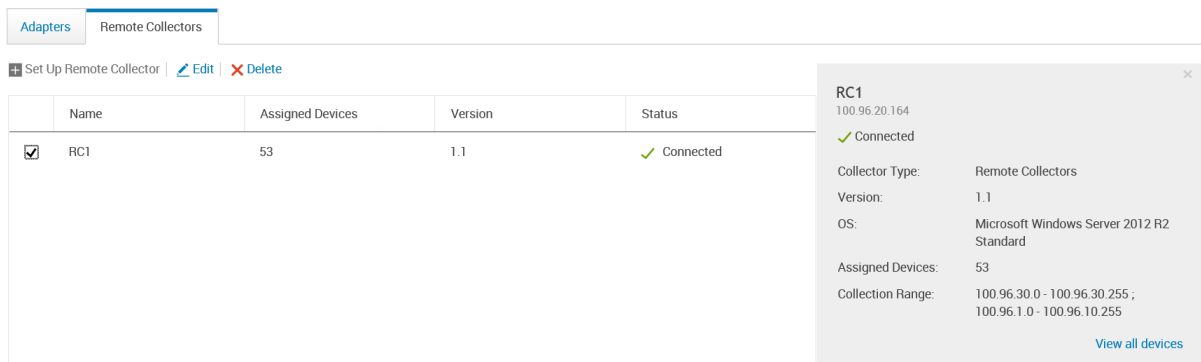
### Steps

- 1 Point to **Extensions** and click **Manage Remote Collectors**.

The **Remote Collectors** page is displayed.

- 2 Select a Remote Collector.

The Remote Collector overview pane is displayed.



**Figure 23. Remote Collector overview pane**

- 3 Click **View all devices**.

The devices associated with the Remote Collector are displayed on the **Devices** page.

#### Related links

[Remote Collectors](#)

## Editing Remote Collector

#### Prerequisites

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

#### About this task

You can edit the name, IP address range, user name, and password of a Remote Collector based on your preference.

#### Steps

- 1 Point to **Extensions** and click **Manage Remote Collectors**.  
The **Remote Collectors** page is displayed.
- 2 Select the Remote Collector you want to edit and click **Edit**.  
The **Edit Remote Collector** window is displayed.
- 3 Edit the name, IP address range, user name, password, proxy details, and the proxy exclusion list as required.
- 4 Click **Update**.

#### Related links

[Remote Collectors](#)

## Deleting Remote Collector

#### Prerequisites

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

#### About this task

You can delete a Remote Collector from SupportAssist Enterprise based on your preference.

**⚠ CAUTION:** Deleting the Remote Collector will also delete all collections that are saved on the remote system.

#### Steps

- 1 Point to **Extensions** and click **Manage Remote Collectors**.

The **Remote Collectors** page is displayed.

- 2 Select the Remote Collector you want to delete and click **Delete**.

The **Remove Remote Collector** window is displayed.

- 3 Click **Remove Remote Collector**.

The Remote Collector is removed from SupportAssist Enterprise and the Remote Collector application is uninstalled from the remote system. Collection and upload of system information from all devices that were associated with the Remote Collector are now associated with the server running SupportAssist Enterprise.

#### **Related links**

[Remote Collectors](#)

# Managing device credentials

SupportAssist Enterprise requires the device credentials to add devices and to collect system information.

You can enter or assign credentials to a device by using one of the following methods:

- While adding a single device or importing multiple devices
- By using the **Edit Device Credentials** option
- By assigning a Credential Profile

Topics:

- [Editing device credentials](#)
- [Account Credentials](#)
- [Credential Profiles](#)

## Editing device credentials

The **Edit Credentials** option enables you to update the credentials of a device. 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 Point to **Devices** and click **View 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** Search by  Search term

Collection purpose:

Assign Credential Profile:

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input checked="" type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

**PowerEdge T710**

Tasks:

Status:  Connected

Display Name: Server 1

Hostname / IP Address: 100.96.20.210

Service Tag: HKNK82S

Device Type: Server / Hypervisor

Model: PowerEdge T710

Operating System: VMware ESXi 5.5.0 build-2652839

Monitoring:  Enable  Disable

Revalidate:

Collections: No Collections

Next Scheduled Collection: Friday, Jun 9, 2017

**Figure 24. 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.

## Account Credentials

An Account Credential consists of the credentials of a specific device type. The Account Credentials is used by SupportAssist Enterprise connect to a device and to collect system information. Depending on the number of device types in your environment, you may have to create one or more Account Credentials.

### Related links

- [Manage Account Credentials](#)
- [Adding Account Credentials](#)
- [Editing Account Credentials](#)
- [Deleting Account Credentials](#)

# Adding Account Credentials

## Prerequisites

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

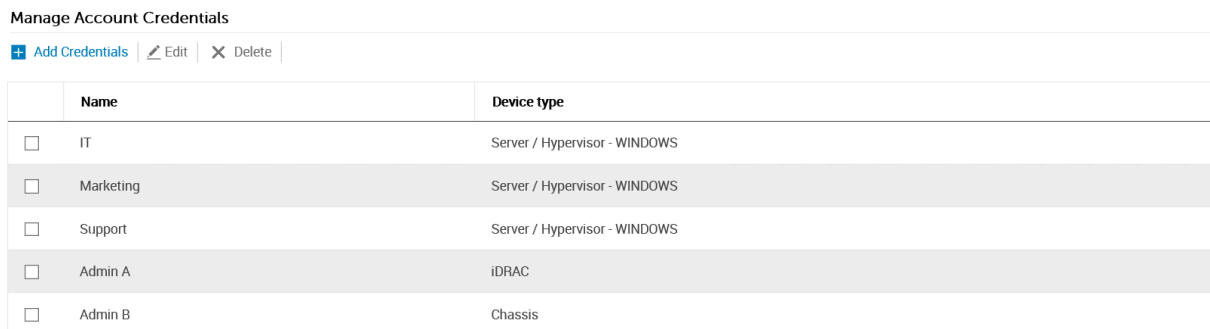
## About this task

Account Credentials are required to create a Credential Profile that you can apply to devices. Depending on your requirement, you can create an Account Credentials for each device type in your environment.

## Steps

- 1 Point to **Devices > Manage Credentials** and click **Account Credentials**.

The **Manage Account Credentials** page is displayed.

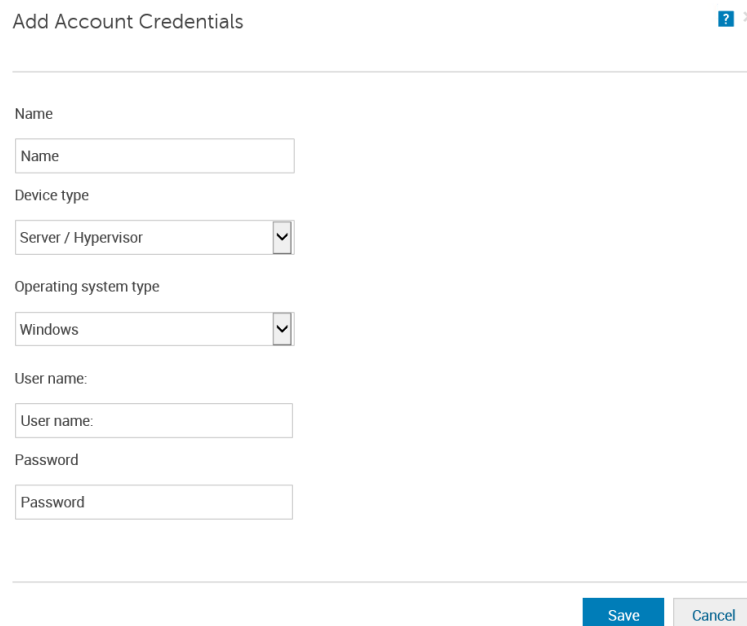


	Name	Device type
<input type="checkbox"/>	IT	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Marketing	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Support	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Admin A	iDRAC
<input type="checkbox"/>	Admin B	Chassis

Figure 25. Manage Account Credentials page

- 2 Click **Add Credentials**.

The **Add Account Credentials** window is displayed.



Add Account Credentials

Name

Name

Device type

Server / Hypervisor

Operating system type

Windows

User name:

User name:

Password

Password

Save Cancel

Figure 26. Add Account Credentials window

- 3 In the **Name** box, type a unique name for the Account Credentials.
- 4 From the **Device Type** list, select the type of device.

- 5 Type the credentials of the selected device type:
  - For **Server / Hypervisor** devices, from the **Operating System type** list, select the operating system, and then type the user name and password of the device in the appropriate fields.
  - For **Chassis, Fluid File System (FluidFS), iDRAC, and Storage Center (SC) / Compellent** devices, type the user name and password of the device in the appropriate fields.
  - For **Software**, from the **Software type** list, select the software type, and then type the user name and password in the appropriate fields.
  - For **Solution** devices, type the user name and password of the device in the appropriate fields.
  - For **Networking** devices, type the user name, password, community string, and enable password of the device in the appropriate fields.

**i** | **NOTE: Community string is required only for the following networking devices:**

- PowerConnect family 28xx and X series
- Cisco
- Wireless controllers

**i** | **NOTE: Enable password is required only when the networking device is configured with an enable password.**

- For **PeerStorage(PS) / EqualLogic** devices, type the user name, password, and community string of the device in the appropriate fields.

**i** | **NOTE: Credentials are not required for PowerVault devices.**

- 6 Click **Save**.

The Account Credentials is listed on the **Manage Accounts Credentials** page.

#### Related links

[Account Credentials](#)

[Manage Account Credentials](#)

[Add Account Credentials](#)

## Editing Account Credentials

#### Prerequisites

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

#### About this task

You can edit the Account Credentials based on your requirement. For example, you must edit the Account Credentials whenever there is a change in the credentials of the associated device type.

#### Steps

- 1 Point to **Devices > Manage Credentials** and click **Account Credentials**.

The **Manage Account Credentials** page is displayed.

**Manage Account Credentials**

[+ Add Credentials](#) | [Edit](#) | [Delete](#)

	Name	Device type
<input type="checkbox"/>	IT	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Marketing	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Support	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Admin A	iDRAC
<input type="checkbox"/>	Admin B	Chassis

**Figure 27. Manage Account Credentials page**

- 2 Select the Account Credentials that you want to edit and click **Edit**.

The **Edit Account Credentials** window is displayed.

- 3 Update the credentials as required.

**NOTE:** Editing the name of the Account Credentials is possible only if the Account Credentials is not assigned to any device.

- 4 Click **Update**.

The Account Credentials is updated. Devices to which the Account Credentials is assigned are re-validated.

#### Related links

[Account Credentials](#)

[Manage Account Credentials](#)

[Edit Account Credentials](#)

## Deleting Account Credentials

#### Prerequisites

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

#### About this task

You can delete the Account Credentials based on your preference.

**NOTE:** You cannot delete Account Credentials, if the Account Credentials is assigned to a device.

#### Steps

- 1 Point to **Devices > Manage Credentials** and click **Account Credentials**.

The **Manage Account Credentials** page is displayed.

**Manage Account Credentials**

[+ Add Credentials](#) | [Edit](#) | [Delete](#)

	Name	Device type
<input type="checkbox"/>	IT	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Marketing	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Support	Server / Hypervisor - WINDOWS
<input type="checkbox"/>	Admin A	iDRAC
<input type="checkbox"/>	Admin B	Chassis

**Figure 28. Manage Account Credentials page**

- 2 Select the Account Credentials that you want to delete and click **Delete**.  
The **Delete Account Credentials** window is displayed.
- 3 Click **Yes**.

**Related links**

- [Account Credentials](#)
- [Manage Account Credentials](#)

## Credential Profiles

A Credential Profile is a collection of Account Credentials of various device types. Credential Profiles enable you to assign a set of credentials to your devices, instead of entering the credentials for each device manually.

**Related links**

- [Manage Credential Profiles](#)
- [Creating Credential Profile](#)
- [Assigning Credential Profile](#)
- [Editing Credential Profile](#)
- [Deleting Credential Profile](#)

## Creating Credential Profile

**Prerequisites**

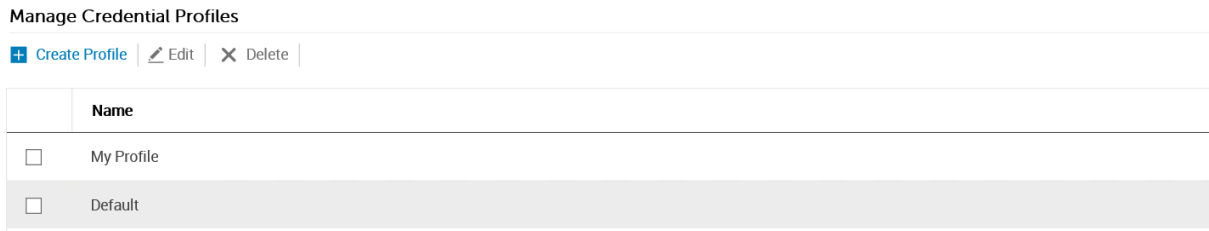
You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).

**About this task**

Creating a Credential Profile enables you to assign credentials to your devices.

**Steps**

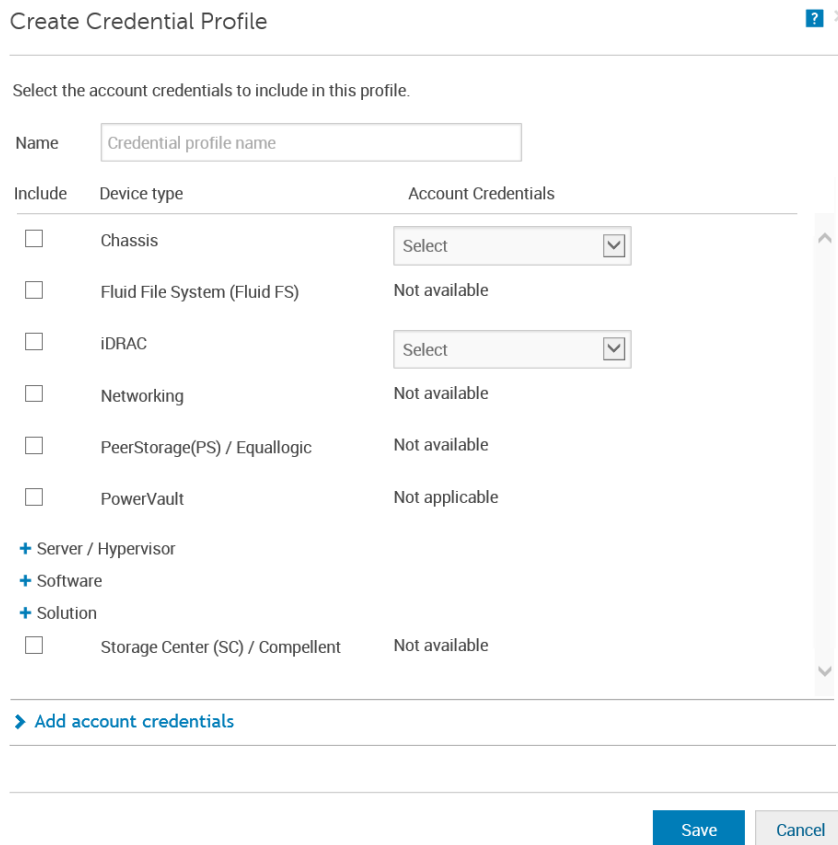
- 1 Point to **Devices > Manage Credentials** and click **Credential Profiles**.  
The **Manage Credential Profiles** page is displayed.



**Figure 29. Manage Credential Profiles window**

- 2 Click **Create Profile**.

The **Create Credential Profile** window is displayed.



**Figure 30. Create Credential Profile window**

- 3 In the **Name** box, type a unique name for the Credential Profile.
- 4 Select the device type you want to include in the profile.  
For **Server / Hypervisor**, **Software**, and **Solution**, click + to expand the list of device types.

The **Account Credentials** list is enabled for selection.

- 5 From the **Account Credentials** list, select the Account Credentials that you want to assign to the device type.

**NOTE:** The Account Credentials list displays Not available if you have not created an Account Credentials for the device type. To create a credential account, click Add New Account. For more information about creating Account Credentials, see Adding Account Credentials.

- 6 Repeat step 4 and 5 for each device type that you want to include in the Credential Profile.

- 7 Click **Save**.  
The Credential Profile is listed on the **Manage Credential Profiles** page.

#### Related links

- [Credential Profiles](#)
- [Manage Credential Profiles](#)
- [Add Credential Profile](#)

## Assigning Credential Profile

#### Prerequisites

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

#### Steps

- 1 Point to **Devices** and click **View Devices**.  
The **Devices** page is displayed.
- 2 Select one or more devices and from the **Assign Credential Profile** list, select a Credential Profile.  
The Credential Profile is assigned to the selected devices. Devices to which the Credential Profile is assigned are re-validated.

#### Related links

- [Credential Profiles](#)
- [Manage Credential Profiles](#)

## Editing Credential Profile

#### Prerequisites

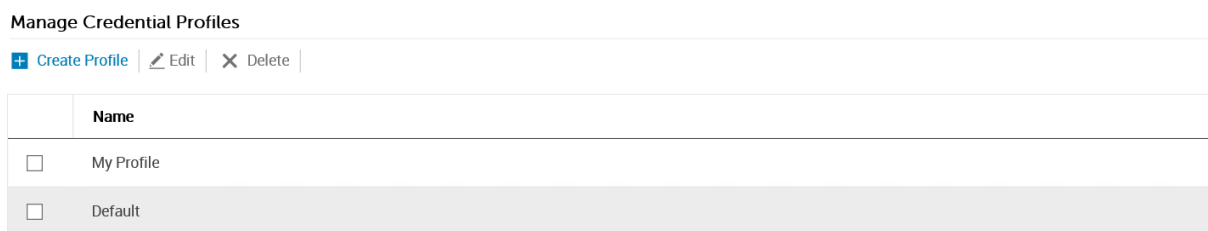
You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).

#### About this task

You can update the credentials of a profile based on your requirement. For example, you may edit the Credential Profile to add a new Account Credentials or change the Account Credentials for a device type.

#### Steps

- 1 Point to **Devices > Manage Credentials** and click **Credential Profiles**.  
The **Manage Credential Profiles** page is displayed.



**Figure 31. Manage Credential Profiles window**

- 2 Select the Credential Profile that you want to edit and click **Edit**.  
The **Edit Credential Profile** window is displayed.
- 3 Select the device type for which you want to edit Account Credentials.  
The **Account Credentials** list is enabled for selection.
- 4 From the **Account Credentials** list, select the Account Credentials that you want to assign to the device type.

- 5 Click **Update**.

The Credential Profile is updated. Devices to which the Credential Profile is assigned are re-validated.

#### Related links

- [Credential Profiles](#)
- [Manage Credential Profiles](#)
- [Edit Credential Profile](#)

## Deleting Credential Profile

#### Prerequisites

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

#### About this task

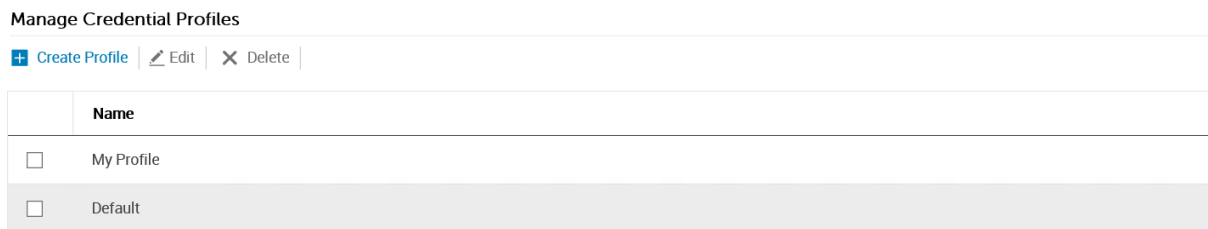
You can delete a Credential Profile based on your preference.

**NOTE:** You cannot delete a Credential Profile, if the Credential Profile is assigned to a device.

#### Steps

- 1 Point to **Devices > Manage Credentials** and click **Credential Profiles**.

The **Manage Credential Profiles** page is displayed.



**Figure 32. Manage Credential Profiles window**

- 2 Select the Credential Profile that you want to delete and click **Delete**.

The **Delete Credential Profile** window is displayed.

- 3 Click **Yes**.

#### Related links

- [Credential Profiles](#)
- [Manage Credential Profiles](#)

# 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 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](#) or [Editing Account 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](#).

Topics:

- [Enabling or disabling monitoring of a device](#)
- [Installing or upgrading OMSA by using SupportAssist Enterprise](#)
- [Configuring SNMP settings by using SupportAssist Enterprise](#)
- [Viewing and updating the contact information](#)
- [Configuring proxy server settings](#)
- [Connectivity test](#)
- [Testing the case creation capability](#)
- [Clearing the System Event Log \(SEL\)](#)
- [Automatic update](#)
- [Deleting a device](#)
- [Opting in or opting out from ProSupport Plus recommendation report emails](#)

## 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 Point to **Devices** and click **View 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.

The screenshot shows the 'Devices' page in SupportAssist Enterprise. At the top, there is a search bar and a 'Search term' input. Below that, there are action buttons: 'Add Device', 'Start Collection', 'Edit Credentials', and 'Delete'. A 'Collection purpose' dropdown is set to 'Select'. There is also an 'Assign Credential Profile' dropdown and a 'Refresh' button. The main table has columns for 'Name / IP Address', 'Model', and 'Status'. The 'Server 1' device is selected, and its details are shown on the right. In the 'Monitoring' section of the details, the 'Enable' radio button is selected, and the 'Disable' radio button is unselected. A red box highlights this section.

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input checked="" type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

PowerEdge T710

Tasks: Select Task

Status:  Connected

Display Name: Server 1

Hostname / IP Address: 100.96.20.210

Service Tag: HKNK82S

Device Type: Server / Hypervisor

Model: PowerEdge T710

Operating System: VMware ESXI 5.5.0 build-2652839

Monitoring:  Enable  Disable

Revalidate: Revalidate

Collections: No Collections

Next Scheduled Collection: Friday, Jun 9, 2017

Duplicate

Figure 33. Enable or disable monitoring option

- ① **NOTE:** If the registration of SupportAssist Enterprise is not completed, the Enable monitoring option is disabled.
- ① **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](#).

## 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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

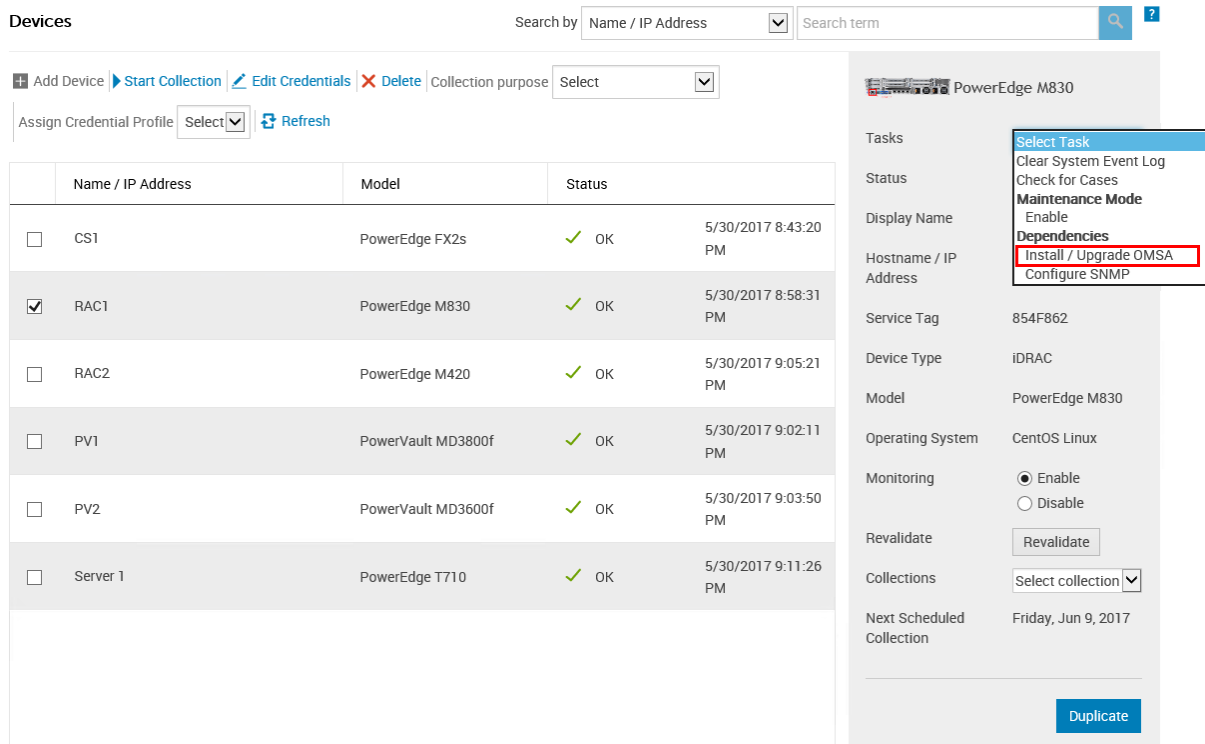
**NOTE:** Installation or upgrade of OMSA by using SupportAssist Enterprise is not supported on servers running the following operating systems or hypervisors:

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

**Steps**

- 1 Point to **Devices** and click **View 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.



**Figure 34. 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 or hypervisors:

- Oracle Enterprise Linux
- VMware ESXi
- Oracle Virtual Machine

## Steps

- 1 Point to **Devices** and click **View 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**.

**Devices** Search by Name / IP Address Search term

Collection purpose:

Assign Credential Profile:

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input checked="" type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

**PowerEdge M830**

Tasks

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

Status

Display Name

Hostname / IP Address

Service Tag: 854F862

Device Type: iDRAC

Model: PowerEdge M830

Operating System: CentOS Linux

Monitoring:  Enable  Disable

Revalidate:

Collections:

Next Scheduled Collection: Friday, Jun 9, 2017

**Figure 35. 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 server**.

**NOTE:** SupportAssist Enterprise supports Windows NT LAN Manager (NTLM) and basic proxy authentication protocols.

- 3 Type the host name or IP address, and port number of the proxy server 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 **Requires authentication** and then type the user name and password in the appropriate fields.

- 5 In the **Proxy exclusion list** box, type the IP address range or ranges of devices to which SupportAssist Enterprise must communicate directly and not through the proxy server. IP address of devices that communicate through https protocol must be included in the proxy exclusion list. Examples of devices that communicate through https protocol include iDRAC, Compellent storage arrays, VMware ESX and ESXi, and XC Series of Web-scale Hyper-converged appliances.

**NOTE:** You can enter one or more IP address ranges as semi-colon separated values. For example, 10.49.\*.\* ; 10.49.18.\* ; \*.\*.100.10

You can enter the IP address ranges in the following formats:

- 10.49.\*.\*
- 10.49.18.\*
- \*.\*.100.10
- \*.\*.\*.10
- \*.10.12.100
- 10.\*.\*.\*

The following IP address range formats are not supported:

- 10.\*.\*.49
- 10.\*.49.\*
- 10.49.\*.10

- 6 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 36. Network Connectivity Test page

**NOTE:** The network connectivity test does not verify the following:

- Ports used by SupportAssist Enterprise
- Internet connectivity of the server where the Remote Collector is set up


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 **Network 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 **Network 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

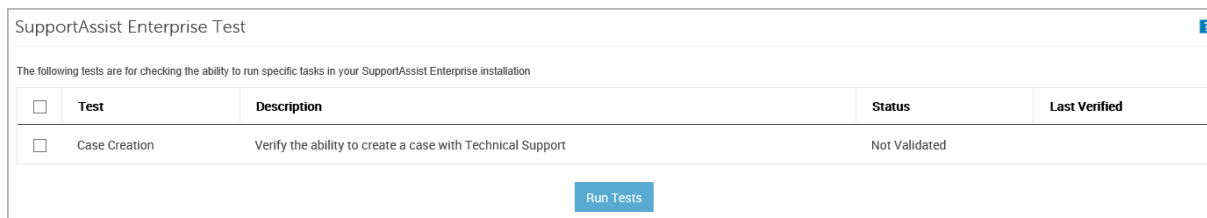
### About this task

You can 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.

 **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](#).

### Steps

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

[Run Tests](#)

Figure 37. 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.

### Related links

[SupportAssist Enterprise test](#)

## 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 Point to **Devices** and click **View 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 is a search bar and a 'Search by' dropdown set to 'Name / IP Address'. Below the search bar are buttons for 'Add Device', 'Start Collection', 'Edit Credentials', and 'Delete', along with a 'Collection purpose' dropdown. A table lists devices with columns for Name / IP Address, Model, Status, and a timestamp. The 'RAC1' device (PowerEdge M830) is selected. To the right of the table is a 'Device Overview' pane for 'PowerEdge M830', showing various settings like Service Tag, Device Type, Model, Operating System, and Monitoring. A 'Tasks' menu is open over the 'RAC1' row, listing tasks such as 'Clear System Event Log', 'Check for Cases', 'Maintenance Mode', and 'Dependencies'. The 'Clear System Event Log' option is highlighted with a red box.


	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	OK	5/30/2017 8:43:20 PM
<input checked="" type="checkbox"/>	RAC1	PowerEdge M830	OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	OK	5/30/2017 9:03:50 PM
<input type="checkbox"/>	Server 1	PowerEdge T710	OK	5/30/2017 9:11:26 PM

Figure 38. 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 installing this update, 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 installing this update, SupportAssist Enterprise will be able to connect to, and collect system information 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 one or more devices from SupportAssist Enterprise, if you do not want to monitor a device or for other reasons.

① **NOTE:** Deleting a device only removes the device from the SupportAssist Enterprise user interface; it does not affect the functionality of the device.

① **NOTE:** Devices that are inventoried and added in SupportAssist Enterprise through an adapter cannot be deleted. Those devices are deleted automatically from SupportAssist Enterprise when either the adapter is deleted or the devices are removed from the systems management console.

### Steps

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

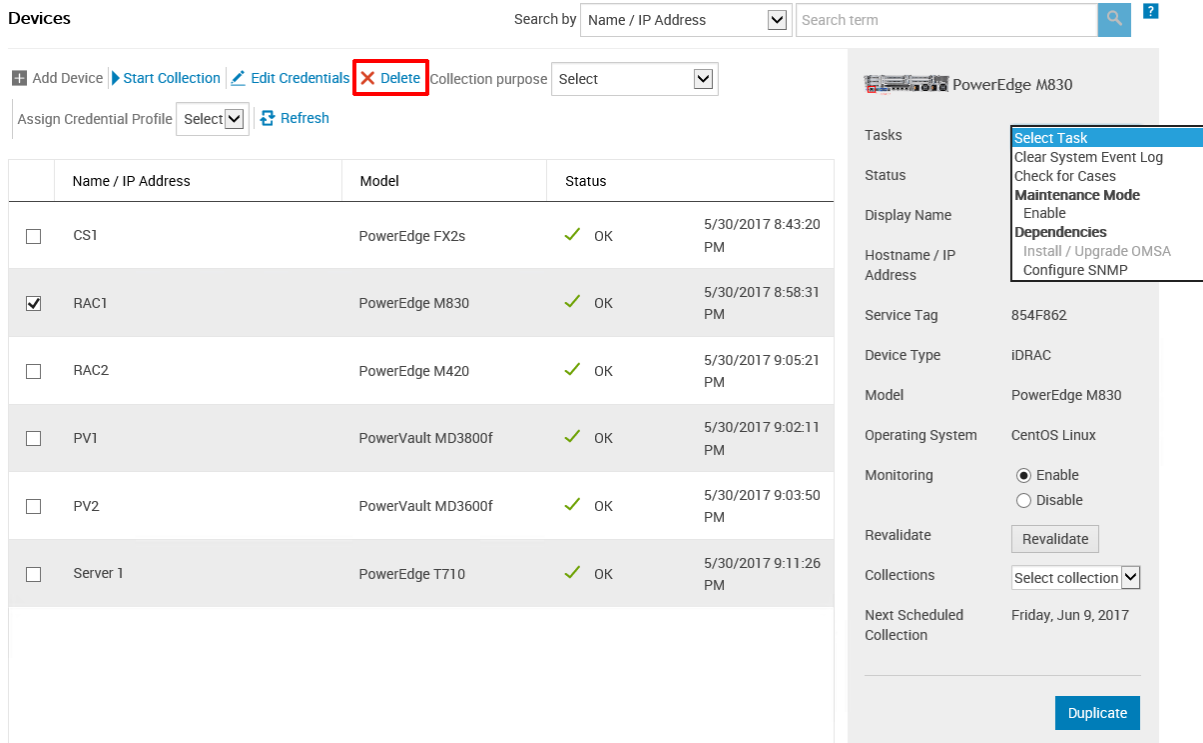


Figure 39. Delete option

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

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

① **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 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](#).

- You must 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 recommendation reports provide an overall health assessment of your devices 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 recommendation reports through email, you will receive the report once every month.

**① NOTE:** The ProSupport Plus 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.

**① NOTE:** The 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 recommendation reports through email.

**① NOTE:** By default, the **Automatically receive recommendation reports via email** option is selected.

- 3 Click **Apply**.

# Configuring email notifications

By default, 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. Depending on your preference, you can configure the following email notification settings:

- 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](#).

Topics:

- [Configuring email notification settings](#)
- [Configuring SMTP server settings](#)
- [Types of email notifications](#)

## Configuring email notification 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

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

### 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 scenarios:

- 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 in use by any other application.

## Steps

- 1 Point to **Settings** and click **SMTP Settings**.  
The **SMTP Settings** page is displayed.
- 2 Select **Use SMTP server**.
- 3 Type the host name or IP address, and the port number of the SMTP server in the appropriate fields.
- 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 17. 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 registration of SupportAssist Enterprise 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

Email notification type	When the email notification is sent	Origin of the email notification
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
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 11 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

**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 collection settings

By default, when registration is complete, 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. Depending on your preference, you can configure the following collection settings:

- 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](#).
- 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](#).
- Enable or disable the automatic upload of collections. See [Disabling the automatic upload of collections](#).

Topics:

- [Prerequisites for collecting system information](#)
- [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 the collection of software information and the system log](#)
- [Enabling or disabling the automatic upload of collections](#)

## 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. If the remote device is associated with a Remote Collector, the remote device must be reachable from the server where the Remote Collector is set up.
- 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](https://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.
- For collecting system information from ESX and ESXi only, ensure that SFCBD and CIMOM are enabled.

## 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 starts collecting system information from all monitored devices at periodic intervals and sends it securely to Dell. The collection start time is a randomly determined day of every month at 11 PM. 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 recommendation report by email, periodic 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 **Starting from day N of every month at 11 PM** option.
- 3 Click **Apply**.

#### Related links

[Preferences](#)

## 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 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 disabled automatically. Therefore, collections that are sent to Dell from your devices do not include certain categories of data.

**NOTE:** If you have disabled the collection of identity information from devices, the identity information such as host name, IP address, and so on are replaced by tokenized values in the collected system information. 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 system information 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 *SupportAssist Enterprise Version 1.1 Reportable Items* document at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).

3 Click **Apply**.

## Enabling or disabling the automatic upload of collections

### 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 system state information is collected from your devices by SupportAssist Enterprise and sent to Dell. If required, you can disable the automatic upload of collections.

**NOTE:** Auto upload setting is not applicable for multiple device collections.

### Steps

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

The **Preferences** page is displayed.

2 In **Automatically upload**, depending on your requirement, select or clear **System state information collected from devices to Dell** option.

3 Click **Apply**.

## Viewing collections

SupportAssist Enterprise collects system information from each device that 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 predefined collection start date specified in the **Preferences** page.
- 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 Technical Support, you can initiate the collection of system information from one or more devices at any time.

**NOTE:** By default, SupportAssist Enterprise collects system information periodically and on case creation only after 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 on the server that hosts the application that runs the collection task. Collections tasks that are run by SupportAssist Enterprise are saved on the server where SupportAssist Enterprise is installed. Collection tasks that are run by a Remote Collector are saved on the server where the Remote Collector is set up. You can access collections that are run by SupportAssist Enterprise from the **Devices** or **Collections** page. The system information available in a collection is displayed in the **Configuration Viewer** that is available in SupportAssist Enterprise.

**NOTE:** Collections that are performed by a Remote Collector cannot be viewed from SupportAssist Enterprise. For information on viewing such collections, see [Viewing collections for devices associated with a Remote Collector](#).

**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 system information collected from storage devices with Fluid File System (FluidFS).

**NOTE:** For collections from devices that are running a non-English operating system, the Configuration Viewer may not display certain attributes as expected.

Topics:

- [Viewing a collection from the Devices page](#)
- [Viewing a collection from the Collections page](#)
- [Refining collections based on a date range](#)
- [Configuration Viewer](#)
- [Items reported in periodic collections from servers](#)
- [Downloading and viewing a multiple device collection](#)
- [Multiple device configuration viewer](#)

## 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. You can select any collection that you want to view from the collections list.

## Steps

- 1 Point to **Devices** and click **View 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.  
The **Collections** field displays **No Collections** in the following scenarios:
  - No collections have been performed from the device
  - The device is associated with a Remote Collector
- 3 From the **Collections** list, select a collection date and time.

The screenshot shows the 'Devices' page in a web application. At the top, there is a search bar with 'Name / IP Address' selected and a search term field. Below the search bar, there are several action buttons: 'Add Device', 'Start Collection', 'Edit Credentials', and 'Delete'. A 'Collection purpose' dropdown menu is set to 'Select'. There is also an 'Assign Credential Profile' dropdown and a 'Refresh' button.

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input checked="" type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

On the right side, the 'PowerEdge M830' device overview pane is shown. It includes fields for 'Tasks', 'Status' (Connected), 'Display Name' (RAC1), 'Hostname / IP Address' (100.96.24.90), 'Service Tag' (854F862), 'Device Type' (iDRAC), 'Model' (PowerEdge M830), 'Operating System' (CentOS Linux), 'Monitoring' (Enable), and 'Revalidate' (Revalidate button). The 'Collections' section shows a 'Select collection' button highlighted with a red box, and a list of collection dates: 'Wed May 31 00:32:56 PDT 2017' and 'Tue May 30 21:44:45 PDT 2017'. A 'Duplicate' button is at the bottom.

Figure 40. Selecting a collection

If the device is a server, the **Configuration Viewer** is displayed in a new web browser window. For all other device types and multiple device collections, you are prompted to save the collection as a **.zip** file. To view the downloaded collection, 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. You can select any collection that you want to view from the collections list. You can also 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 Point to **Collections** and click **View Collections**.

The **Collections** page is displayed.

- 2 Select a collection that you want to view.

The screenshot shows the 'Collections' page with a table of collections and a detailed view for 'Server 1 (Manual)'. The table has columns for Name, Collection Date, Collection Purpose, Case Number, and Upload Status. The 'Server 1 (Manual)' row is selected. The detailed view shows the upload status as 'Success' and the date as '05/31/2017 00:28'. It also shows a table for IP Address / Hostname, Service Tag, and Collection Status, with 'Server 1' having a 'Success' status. A 'View Collection' button is highlighted in red.

<input type="checkbox"/>	Name	Collection Date	Collection Purpose	Case Number	Upload Status
<input type="checkbox"/>	PV1 (Manual)	05/30/2017			✓ Success
<input type="checkbox"/>	RAC1 (Manual)	05/30/2017			✓ Success
<input type="checkbox"/>	PV1 (Manual)	05/31/2017			✓ Success
<input checked="" type="checkbox"/>	Server 1 (Manual)	05/31/2017			✓ Success
<input type="checkbox"/>	RAC1 (Manual)	05/31/2017			✓ Success
<input type="checkbox"/>	SA_2017-05-31T002622210_Deployment1	05/31/2017	Deployment		✓ Success

**Server 1 (Manual)**

Upload Status:  Success

Date: 05/31/2017 00:28

IP Address / Hostname	Service Tag	Collection Status
Server 1	HKNK82S	<input checked="" type="checkbox"/> Success

[View Collection](#)

Figure 41. View Collection option

The collection overview pane is displayed.

**NOTE:** The **View Collection** or **Download Collection** option is disabled if the collection was performed by a Remote Collector.

- 3 Click **View Collection** (for server collections) or **Download Collection** (for all other device types and multiple device collections). If the collection is from a server, the **Configuration Viewer** is displayed in a new web browser window. For collections from all other device types and multiple device collections, download and save the collection as a **.zip** file. To view the downloaded collection, extract the **.zip** file and click the **index.html** file.

## Refining collections based on a date range

### Prerequisites

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

### Steps

- 1 Point to **Collections** and click **View Collections**. The **Collections** page is displayed.
- 2 From the **Date Range** filter, select the start and end dates, and then click **Apply**. Collections in the selected date range are displayed.

## Configuration Viewer

The **Configuration Viewer** enables you to view the system information 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 system information 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 system information collection settings in SupportAssist Enterprise at the time of the collection
- Summary of errors that were detected in the collected system information
- Brief information about the device

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

User interface	Description
Left pane	Displays the various categories and sub categories of system information 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.
Divider	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.
Right pane	Displays the system information 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.

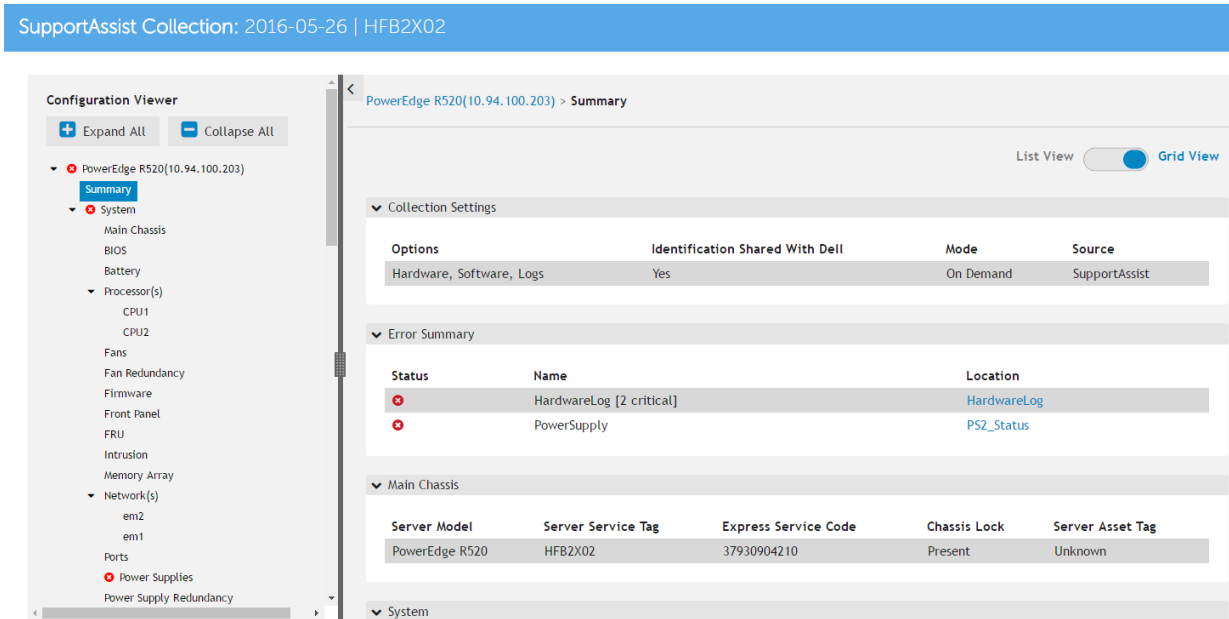


Figure 42. Configuration Viewer

- ① **NOTE:** If you have disabled the collection of identity information from devices, the identity information such as host name, IP address, and so on are replaced by tokenized values in the collected system information. The tokenized values are represented as **TOKEN<sub>n</sub>**—for example, **TOKEN0**, **TOKEN1**, or **TOKEN2**.
- ① **NOTE:** For a list of items that may be reported in collections from a server, see [Items reported in periodic collections from servers](#).
- ① **NOTE:** The Configuration Viewer does not support viewing the system information 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.
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.

**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.

## Items reported in periodic collections from servers

The items reported in the system information 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 system information for a periodic collection from servers.

- NOTE:** The system information in a collection that is performed for a support case creation and a manually-initiated collection is more detailed in comparison with the system information collected in a periodic collection. For the complete list of items that are collected by SupportAssist Enterprise, see the *SupportAssist Enterprise Version 1.1 Reportable Items* document at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).
- NOTE:** The system information 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 18. 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	✓	✗	✗

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	
Slot	✓	✗	✓
Controller	✓	✗	✓
Connector	✓	✗	✗
PCIe-SSD-Extender	✓	✗	✓
Enclosure	✓	✗	✓
Array Disk	✓	✗	✓
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	✓	✗	✗

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 Address	✓	✗	✗
Network Team Interface	✓	✗	✗
Interface Member	✓	✗	✗
Remote Access Device	✓	✗	✓
DRAC Information	✓	✗	✗
Serial Over LAN Configuration	✓	✗	✓
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 the system information 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 Point to **Collections** and click **View Collections**.  
The **Collections** page is displayed.
- 2 Select a multiple device collection that you want to view.

**Collections**      Date Range:        Search by: Service Tag       Search term:   

[Upload](#)

<input type="checkbox"/>	Name	Collection Date	Collection Purpose	Case Number	Upload Status
<input checked="" type="checkbox"/>	PV1 (Manual)	05/30/2017			✓ Success
<input type="checkbox"/>	RAC1 (Manual)	05/30/2017			✓ Success
<input type="checkbox"/>	PV1 (Manual)	05/31/2017			✓ Success
<input type="checkbox"/>	Server 1 (Manual)	05/31/2017			✓ Success
<input type="checkbox"/>	RAC1 (Manual)	05/31/2017			✓ Success
<input type="checkbox"/>	SA_2017-05-31T002622210_Deployment1	05/31/2017	Deployment		✓ Success

**PV1 (Manual)**

Upload Status: ✓ Success

Date: 05/30/2017 21:40

IP Address / Hostname	Service Tag	Collection Status
PV1	87V0X02	<span style="color: green;">✓</span> Success

[Download Collection](#)

**Figure 43. 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 the system information 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 the system information from a server
- **Storage** — If the collection includes the system information from a storage device
- **Networking** — If the collection includes the system information from a network device
- **Chassis** — If the collection includes the system information from a chassis

To access the system information collected from a specific device, point to the device type tab and click the device from the menu that is displayed. The system information collected from a device is displayed as categories and subcategories. Click a category to expand or collapse the category. The system information 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.

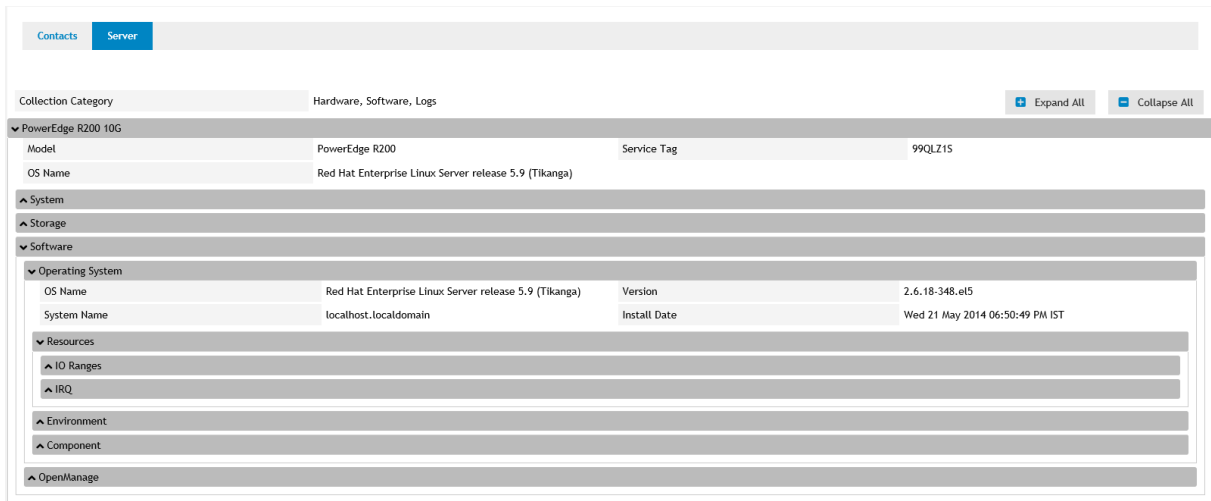


Figure 44. Multiple device configuration viewer

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

# Using SupportAssist Enterprise to collect and send system information

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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).

Topics:

- [Setting up SupportAssist Enterprise for collecting and sending system information](#)
- [Starting the collection of system information from a single device](#)
- [Starting the collection of system information from multiple devices](#)
- [Uploading a collection](#)
- [Uploading a collection from a disconnected site](#)

## 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 Technical Support.

## Steps

- 1 Point to **Devices** and click **View 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' management interface. At the top, there is a search bar and a 'Search by' dropdown set to 'Name / IP Address'. Below this, there are action buttons: 'Add Device', 'Start Collection' (highlighted with a red box), 'Edit Credentials', and 'Delete'. A 'Collection purpose' dropdown is set to 'Select'. There is also an 'Assign Credential Profile' dropdown and a 'Refresh' button.

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input checked="" type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

On the right, a detailed view for 'PowerEdge M420' is shown. It includes a 'Tasks' dropdown, a 'Status' indicator (Connected), 'Display Name' (RAC2), 'Hostname / IP Address' (100.96.25.45), 'Service Tag' (84NLNW1), 'Device Type' (iDRAC), 'Model' (PowerEdge M420), 'Operating System' (VMware ESXi 6.5.0 build-4564106), 'Monitoring' options (Enable/Disable), a 'Revalidate' button, 'Collections' (No Collections), and 'Next Scheduled Collection' (Friday, Jun 9, 2017). A 'Duplicate' button is at the bottom right.

Figure 45. Starting a collection from a single device

- 3 Click **Start collection**.

Devices Search by Name / IP Address  Search term

[+ Add Device](#) | [▶ Start Collection](#) | [✎ Edit Credentials](#) | [✕ Delete](#) | Collection purpose  | Assign Credential Profile  [Refresh](#)

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2 Collection in progress	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

**Figure 46. 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 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.
- NOTE:** If the registration is not complete, the collection is not automatically sent to Dell. However, you can go to the **Collections** page, and then manually initiate the upload.

## 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.
- NOTE:** System information is collected only from devices that are not present in the Staging group.

### Steps

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

Devices Search by Name / IP Address  Search term

Collection purpose: 
 Assign Credential Profile:

	Name / IP Address	Model	Status	
<input type="checkbox"/>	CS1	PowerEdge FX2s	✓ OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	✓ OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	✓ OK	5/30/2017 9:05:21 PM
<input checked="" type="checkbox"/>	PV1	PowerVault MD3800f	✓ OK	5/30/2017 9:02:11 PM
<input checked="" type="checkbox"/>	PV2	PowerVault MD3600f	✓ OK	5/30/2017 9:03:50 PM
<input checked="" type="checkbox"/>	Server 1	PowerEdge T710	✓ OK	5/30/2017 9:11:26 PM

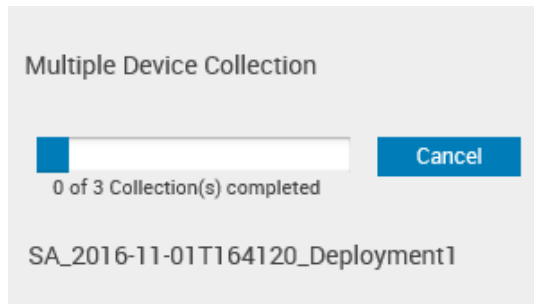
**Figure 47. Starting a multiple device collection**

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 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, but not uploaded to Dell. You can upload the collection bundle at a later time through the **Collections** page.

- 7 Click **OK**.



**Figure 48. 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.
- NOTE:** If the registration is not complete, the collection is not automatically sent to Dell. However, you can go to the **Collections** page, and then manually initiate the upload.
- NOTE:** When you are collecting system information from multiple devices, if the devices you have selected are associated with multiple Remote Collectors, then each Remote Collector generates a separate collection bundle.

# 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.

**NOTE:** Manual upload is not supported for collections that were performed by a Remote Collector.

## Steps

- 1 Point to **Collections** and click **View Collections**.  
The **Collections** page is displayed.
- 2 Select one or more collections that you want to upload and click **Upload**.

**NOTE:** The total file size of the all collections that you have selected must be lesser than 2 GB.

The screenshot shows the 'Collections' page in SupportAssist Enterprise. At the top, there are filters for 'Date Range' and 'Search by' (set to 'Service Tag'). A search bar is also present. Below the filters, there is a table of collections. The first row is highlighted, and the 'Upload' button is visible above it. The table has columns for Name, Collection Date, Collection Purpose, Case Number, and Upload Status. The first row is 'PV1 (Manual)' with a date of 05/30/2017 and a status of 'Success'. Other rows include 'RAC1 (Manual)', 'PV1 (Manual)', 'Server 1 (Manual)', 'RAC1 (Manual)', and 'SA\_2017-05-31T002622210\_Deployment1', all with 'Success' status. To the right of the table, there is a detailed view for the selected 'PV1 (Manual)' collection, showing its upload status as 'Success' and a date of 05/30/2017 21:40. Below this, there is a table with columns for IP Address / Hostname, Service Tag, and Collection Status, with one row for 'PV1' with status 'Success'. A 'Download Collection' button is at the bottom right.

<input type="checkbox"/>	Name	Collection Date	Collection Purpose	Case Number	Upload Status
<input checked="" type="checkbox"/>	PV1 (Manual)	05/30/2017			✓ Success
<input type="checkbox"/>	RAC1 (Manual)	05/30/2017			✓ Success
<input type="checkbox"/>	PV1 (Manual)	05/31/2017			✓ Success
<input type="checkbox"/>	Server 1 (Manual)	05/31/2017			✓ Success
<input type="checkbox"/>	RAC1 (Manual)	05/31/2017			✓ Success
<input type="checkbox"/>	SA_2017-05-31T002622210_Deployment1	05/31/2017	Deployment		✓ Success

Figure 49. 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 or the server where the Remote Collector is set up 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 — **Browse** to C:\Program Files\Dell\SupportAssist\reports and locate the collection **.zip** file.
  - If SupportAssist Enterprise is installed on a Linux operating system — **Browse** to /opt/dell/supportassist/scripts/reports and locate the collection **.zip** file.
  - If the collection was performed by a Remote Collector – Log in to the server where the Remote Collector is set up. Browse to X:\bin\Collections\\Results\html folder, where X is the drive where the Remote Collector is installed 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 EMC 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 Technical Support to open a service request.**
  - 7 Click **Choose File** and browse to select the collection **.zip** file.
  - 8 Click **Submit**.

# Understanding maintenance mode

The maintenance mode functionality suspends the alert processing and automatic case creation capability of 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.

Topics:

- [Enabling or disabling global-level maintenance mode](#)
- [Enabling or disabling device-level maintenance mode](#)

## 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 Search by Name / IP Address  Search term

Collection purpose:

Assign Credential Profile:

	Name / IP Address	Model	Status	
<input checked="" type="checkbox"/>	CS1	PowerEdge FX2s	OK	5/30/2017 8:43:20 PM
<input type="checkbox"/>	RAC1	PowerEdge M830	OK	5/30/2017 8:58:31 PM
<input type="checkbox"/>	RAC2	PowerEdge M420	OK	5/30/2017 9:05:21 PM
<input type="checkbox"/>	PV1	PowerVault MD3800f	OK	5/30/2017 9:02:11 PM
<input type="checkbox"/>	PV2	PowerVault MD3600f	OK	5/30/2017 9:03:50 PM
<input type="checkbox"/>	Server 1	PowerEdge T710	OK	5/30/2017 9:11:26 PM

**PowerEdge FX2s**

Tasks

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

Status

Display Name

Hostname / IP Address

Service Tag: 12D5082

Device Type: Chassis

Model: PowerEdge FX2s


Monitoring:  Enable  Disable

Revalidate:

Collections: No Collections

Next Scheduled Collection: Friday, Jun 9, 2017

**Figure 50. 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.

# SupportAssist Enterprise user groups

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 19. 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.

Topics:

- [SupportAssist Enterprise functions and user privileges](#)
- [Granting elevated or administrative privileges to users](#)
- [Adding users to the SupportAssist Enterprise user groups \(Windows\)](#)
- [Adding users to the SupportAssist Enterprise user groups \(Linux\)](#)

## 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 20. SupportAssist Enterprise functions and user privileges**

<b>SupportAssist Enterprise functions</b>	<b>SupportAssistAdmins and users with elevated or administrative privileges</b>	<b>SupportAssistUsers and users with normal privileges</b>
View cases and check for cases	✓	✓
View the device inventory and device groups	✓	✓
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	✓	✗
Set up, edit, or delete an adapter	✓	✗

SupportAssist Enterprise functions	SupportAssistAdmins and users with elevated or administrative privileges	SupportAssistUsers and users with normal privileges
Set up, edit, or delete a Remote Collector	✓	✗
Create, edit, or delete an Account Credentials	✓	✗
Create, edit, or delete a Credential Profile	✓	✗
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 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.

Topics:

- [Manually configuring the alert destination of a server](#)
- [Manually configuring the alert destination of iDRAC by using the web interface](#)
- [Manually configuring the alert destination of a chassis by using the web interface](#)
- [Manually configuring the alert destination of a networking device](#)

## 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 SupportAssist Enterprise.

Topics:

- [Monitoring servers for hardware issues](#)
- [Support for automatically installing or upgrading OMSA](#)
- [Support for automatically configuring SNMP settings](#)
- [Device correlation](#)
- [Detection of hardware issues in attached storage devices](#)
- [Support for Dell OEM servers](#)
- [Installing Net-SNMP \(Linux only\)](#)
- [Configuring sudo access for SupportAssist Enterprise \(Linux\)](#)
- [Ensuring successful communication between the SupportAssist Enterprise application and the SupportAssist server](#)
- [Accessing the SupportAssist Enterprise application logs](#)
- [Event storm handling](#)
- [Accessing the context-sensitive help](#)
- [Viewing SupportAssist Enterprise product information](#)
- [Uninstalling SupportAssist Enterprise](#)
- [Identifying the generation of a Dell PowerEdge server](#)

## 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 *SupportAssist Enterprise Version 1.1 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 later generation of PowerEdge servers (iDRAC 7 and later).

**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 later generations 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 or later 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 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 *SupportAssist Enterprise Version 1.1 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: `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 *yyyymmdd*>. 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 or on the log in page.

The **About** page is displayed, where you can view the following:

- SupportAssist Enterprise version

- Registration ID
- Policy file version
- Device configuration file version
- Update history

## 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**.

**NOTE:** If you have set up an adapter or a Remote Collector, you are prompted to delete the adapter or Remote Collector before you uninstall SupportAssist Enterprise.

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`.

**NOTE:** If you have set up an adapter or a Remote Collector, you are prompted to delete the adapter or Remote Collector before you uninstall SupportAssist Enterprise.

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 21. 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 server generation	Representation of the server model	Examples of server models
		PowerEdge R730
14th	PowerEdge yx4x	PowerEdge R740

**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.

## Topics:

- [Installing SupportAssist Enterprise](#)
- [SupportAssist Enterprise registration](#)
- [Opening the SupportAssist Enterprise user interface](#)
- [Logging in to SupportAssist Enterprise](#)
- [Unable to add device](#)
- [Unable to add adapter](#)
- [Unable to add Remote Collector](#)
- [Disconnected](#)
- [Importing multiple devices](#)
- [OMSA not installed](#)
- [SNMP not configured](#)
- [New version of OMSA available](#)
- [Unable to configure SNMP](#)
- [Unable to verify SNMP configuration](#)
- [Unable to install OMSA](#)
- [Unable to verify OMSA version](#)
- [OMSA not supported](#)
- [Unable to reach device](#)
- [Unable to gather system information](#)
- [Insufficient storage space to gather system information](#)
- [Unable to export collection](#)
- [Unable to send system information](#)
- [Authentication failed](#)
- [Clearing System Event Log failed](#)
- [Maintenance mode](#)
- [Auto update](#)
- [Unable to edit device credentials](#)
- [Automatic case creation](#)
- [Scheduled tasks](#)
- [SupportAssist Enterprise services](#)
- [Other services](#)
- [Security](#)

## 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](http://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](http://Dell.com/storagemanuals).
- If the device was inventoried through an adapter, ensure that the credentials of the device are correct. To resolve credential errors, you can edit the device credentials, update the credential account, or assign another Credential Profile.
- 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 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](http://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](http://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](http://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](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.

## Software

- For troubleshooting HITKIT collection:
  - Ensure that Secure Shell (SSH) service is running on the system.
  - Ensure that you have root credentials for the SSH connection. SupportAssist Enterprise uses the SSH protocol to connect to the system.
- For troubleshooting SAN HQ device:
  - Check the server installation details of Dell EqualLogic SAN Headquarters device from the registry entry: **HKLM\SOFTWARES\EqualLogic\PerformanceMonitor**.
  - Ensure that the value of the install type attribute is "Full" and logdir attribute has a value.

# Unable to add adapter

If the **Adapters** page displays an  **Unable to add adapter** status:


- Verify if the server where you want to add the adapter is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that the system where you want to set up the adapter has more than 500 MB of free disk space required for installation of the adapter.
- Verify if port 135 is open on the system where you want to set up the adapter.
- For setting up an OpenManage Essentials (OME) adapter, the system where you want to set up the adapter must be running OpenManage Essentials version 2.3.
- For setting up the Microsoft System Center Operations Manager (SCOM) adapter, Dell Server Management Pack Suite Version 7.x For Microsoft System Center Operations Manager and System Center Essentials must be installed on the system.
- Ensure that Microsoft .NET Framework 4 is installed on the system where you want to set up the adapter.
- Ensure that the adapter is not already installed on the server where you are trying to set up the adapter.

# Unable to add Remote Collector

If the **Remote Collectors** page displays  **Unable to add Remote Collector** status:

- Verify if the server where you want to add the Remote Collector is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that the system where you want to set up the Remote Collector has more than 500 MB of free disk space required for installation of the Remote Collector.
- Verify if port 135 is open on the system where you want to set up the Remote Collector.
- Ensure that SupportAssist Enterprise is not previously installed on the server where you want to add the Remote Collector.
- Ensure that the Remote Collector is not already installed on the server where you are trying to set up the Remote Collector.

# Disconnected

A  **Disconnected** status may be displayed on header area if the server running SupportAssist Enterprise is unable to connect to an adapter or Remote Collector that you have set up. When this issue occurs, a **Disconnected** status is also displayed on the **Adapters** or **Remote Collectors** page depending on the connectivity status of SupportAssist Enterprise with an adapter or Remote Collector. If the **Disconnected** status is displayed:

- Ensure that server where you have set up the adapter or Remote Collector is reachable from the server where SupportAssist Enterprise is installed.
- For Remote Collectors, ensure that the **Dell EMC SupportAssist Enterprise** service is running on the server where you have set up the Remote Collector.
- For adapters, ensure that the **Dell EMC SupportAssist Enterprise OME Adapter** or **Dell EMC SupportAssist Enterprise SCOM Adapter** service is running on the server where you have set up the adapter.
- Ensure that port 5700 is open on the server where SupportAssist Enterprise is installed.

# 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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](http://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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](http://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](#).
- If the server is running a Linux operating system, restart the snmpdtrapd service.

## 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](http://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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](http://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 *SupportAssist Enterprise Version 1.1 Support Matrix* at [Dell.com/ServiceabilityTools](https://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 the required network ports 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:
  - Download the [Zulu Cryptographic Extension Kit](#) available at the Azul Systems website.
  - Extract the downloaded file.
  - 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`
  - 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](#).

## Hypervisors

For devices running VMware ESX and ESXi:

- Ensure that SFCBD and CIMOM are enabled on your device.
  - To enable SFCBD, use the following command: `/etc/init.d/sfcbd-watchdog start`.
  - To enable WBEM, use the following command: `esxcli system wbem set --enable true`.

Depending on your scenario, you may have to run the following commands.

- To check the status of the agent: `/etc/init.d/sfcbd-watchdog status`.
- To reset WBEM, perform the following:
  - Disable WBEM on your device: `esxcli system wbem set --enable false`.
  - Enable WBEM on your device: `esxcli system wbem set --enable true`.
- To disable SFCBD, use the following command: `/etc/init.d/sfcbd-watchdog stop`.

## 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 SupportAssist Enterprise.

## Chassis

Ensure that Secure Shell (SSH) service is running on the device.

## Software

- For troubleshooting HITKIT collection:
  - Ensure that Secure Shell (SSH) service is running on the system.
  - Ensure that you have root credentials for the SSH connection. SupportAssist Enterprise uses the SSH protocol to connect to the system.
- For troubleshooting SAN HQ device:
  - Check the server installation details of Dell EqualLogic SAN Headquarters device from the registry entry: **HKLM\SOFTWARES\EqualLogic\PerformanceMonitor**.
  - Ensure that the value of the install type attribute is "Full" and logdir attribute has a value.

## 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 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](#).
- If the device is associated to a Remote Collector, then verify if the system where Remote Collector is setup has internet connectivity.

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.

## Software

- For troubleshooting HITKIT collection:
  - Ensure that Secure Shell (SSH) service is running on the system.
  - Ensure that you have root credentials for the SSH connection. SupportAssist Enterprise uses the SSH protocol to connect to the system.
- For troubleshooting SAN HQ device:
  - Check the server installation details of Dell EqualLogic SAN Headquarters device from the registry entry: **HKLM\SOFTWARES\EqualLogic\PerformanceMonitor**.
  - Ensure that the value of the install type attribute is "Full" and logdir attribute has a value.

## 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 clrse`

## 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 of SupportAssist Enterprise, product support files, or policy files 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.

## Software

- For troubleshooting HITKIT collection:
  - Ensure that Secure Shell (SSH) service is running on the system.
  - Ensure that you have root credentials for the SSH connection. SupportAssist Enterprise uses the SSH protocol to connect to the system.
- For troubleshooting SAN HQ device:
  - Check the server installation details of Dell EqualLogic SAN Headquarters device from the registry entry: **HKLM\SOFTWARE\EqualLogic\PerformanceMonitor**.
  - Ensure that the value of the install type attribute is "Full" and logdir attribute has a value.

## 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, storage, 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.
- If the device was inventoried through an OpenManage Essentials adapter, ensure that the device is configured to forward alerts to the server where OpenManage Essentials is installed.

## 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 Enterprise services

SupportAssist Enterprise has two services that run in the background: **Dell EMC SupportAssist Enterprise** and **Dell EMC SupportAssist Enterprise DB**. If the SupportAssist Enterprise application does not respond appropriately, ensure the following:

- 1 On the server where SupportAssist Enterprise is installed, verify if the SupportAssist Enterprise services are running. For information on verifying the status of the SupportAssist Enterprise services, see [Verifying the status of SupportAssist Enterprise services \(Windows\)](#) or [Verifying the status of SupportAssist Enterprise services \(Linux\)](#).
- 2 If the services cannot or do 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 services. 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 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 status of SupportAssist Enterprise services (Windows)

To verify the status of the SupportAssist Enterprise services 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 EMC SupportAssist Enterprise** and **Dell EMC SupportAssist Enterprise DB** services display the status as **Running**.
- 4 If the services are not running, right-click each service and select **Start**.

**NOTE:** If you stop one or both of the SupportAssist Enterprise services, ensure that you restart both the services.

**NOTE:** To verify if the adapter service is running, check for the status of the Dell EMC SupportAssist Enterprise OME Adapter or Dell EMC SupportAssist Enterprise SCOM Adapter service on the server where you have set up the adapter.

**NOTE:** To verify if the Remote Collector service is running, check for the status of the Dell EMC SupportAssist Enterprise and Dell EMC SupportAssist Enterprise DB service on the server where you have set up the Remote Collector.

# Verifying the status of SupportAssist Enterprise services (Linux)

To verify the status of the SupportAssist Enterprise services on Linux operating systems:

- 1 Open the terminal window on the system where SupportAssist Enterprise is installed.
- 2 Type `service Dell EMC SupportAssist Enterprise status` and press Enter.  
The status of the Dell EMC SupportAssist Enterprise service is displayed.
- 3 Type `service Dell EMC SupportAssist Enterprise DB status` and press Enter.  
The status of the Dell EMC SupportAssist Enterprise DB service is displayed.
- 4 If the services are not running, type `service <service name> start` and press Enter.

**NOTE:** If you stop one or both of the SupportAssist Enterprise services, ensure that you restart both the services.

## 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 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 the available options to access following pages:
  - **Manage Device Groups** — Enables you to create and manage devices groups.
  - **Manage Credentials** — Enables you to provide the credentials for the device types.
    - **Account Credentials** — Enables you to connect to your remote devices and collect system information.
    - **Credential Profiles** — Enables you to apply a set of credentials to a device or group of devices, instead of entering the credentials for each device manually.
- **Collections** — Displays the list of collections that have been performed successfully.
- **Extensions** — Enable you to set up adapters and Remote Collectors.
- **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:
  - **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.
-  **Disconnected** — Displayed when SupportAssist Enterprise is unable to connect to an adapter or Remote Collector.

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 22. 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>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>Network 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 Network 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 23. 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> <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>The three types of banners displayed are:</p> <ul style="list-style-type: none"> <li>• SupportAssist Enterprise</li> <li>• Product Support</li> <li>• Policy Update</li> </ul> <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>

Topics:

- [SupportAssist Enterprise Registration Wizard](#)
- [Login page](#)
- [Cases page](#)
- [Devices page](#)
- [Device Groups page](#)
- [Manage Account Credentials](#)
- [Manage Credential Profiles](#)
- [Collections page](#)
- [Extensions](#)
- [Settings](#)
- [Network Connectivity Test](#)
- [SupportAssist Enterprise test](#)

## Related links

- [SupportAssist Enterprise Registration Wizard](#)
- [Login page](#)
- [Cases page](#)
- [Devices page](#)
- [Settings](#)
- [Collections page](#)
- [Network Connectivity Test](#)
- [SupportAssist Enterprise test](#)

# 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 24. 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 25. 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 26. Login page**

Field	Description
<b>Username</b>	User name required to log in to SupportAssist Enterprise.
<b>Password</b>	Password required to log in to SupportAssist Enterprise.
<b>Login</b>	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 following options available at the top of the cases page are:


- **Search by** — To search by a specific category of displayed data. The available options are:
  - **Service Tag**
  - **Name / IP Address**
  - **Number**
  - **Title**
  - **Status**
- **Search term** — To enter the search keyword.
- **Case Options** — 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 Technical Support to suspend activities related to a support case for 24 hours. After 24 hours, Technical Support automatically resumes activities related to the support case.
  - **Resume Activity** — To request 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 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.**
- **Refresh** — To refresh the case list view.
- **Fetching Cases** — A progress indicator that is displayed when SupportAssist Enterprise is verifying if cases are present for your devices.

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 27. Cases page**

Column name	Description
Check box	Use to select a support case for performing case management actions. <p> <b>NOTE: The check box is displayed only for cases that were automatically created by SupportAssist Enterprise.</b></p>
<b>Name/IP Address</b>	The 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.
<b>Number</b>	The numeric identifier assigned to the support case.
<b>Status</b>	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> — Technical Support has opened the submitted support case.</li> <li>• <b>In Progress</b> — Technical Support is working on the support case.</li> <li>• <b>Customer Deferred</b> — 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> — Technical Support has suspended activities related to the support case for 24 hours based on your request.</li> <li>• <b>Closure Requested</b> — You have requested 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> </ul>

Column name	Description
	<ul style="list-style-type: none"> <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 Technical Support over phone.</li> <li>• <b>Email</b> — The support case was created by contacting Technical Support through email.</li> <li>• <b>Chat</b> — The support case was created by contacting 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 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**
  - **Software**

- **Solution**
- **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**

#### 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 the 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 enables you to perform certain tasks:
















- **Search by** — To search by a specific category of displayed data. The available options are:
  - **Service Tag**
  - **Model**
  - **Name / IP Address**
  - **Operating System**
- **Search term** — To enter the search keyword.
- **Add Device** — To add a single device or to import multiple devices.
- **Start Collection** — To initiate a single device or multiple device collections.
- **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.
- **Assign Profile** — To assign credentials for devices.













- **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 28. 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:</b> The check box is disabled while the following SupportAssist Enterprise initiated tasks are in progress:</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 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:</b> 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.</p> <p><b>NOTE:</b> You can cancel a collection only when SupportAssist Enterprise is collecting system information from the device. You cannot cancel a collection while the collected system information is being sent to Dell.</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:</b> 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.</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> <p><b>NOTE:</b> 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:</p> <ul style="list-style-type: none"> <li>• Manual collection</li> <li>• Support case collection</li> <li>• Periodic collection</li> </ul> </li> </ul> </li> </ul>

Column name	Description
	<ul style="list-style-type: none"> <li>Maintenance mode — If the device is placed in maintenance mode, the maintenance mode icon  is displayed.</li> </ul>
<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> <li> <b>Revalidating device</b> — SupportAssist Enterprise is validating the prerequisites and the credentials of the device.</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> </ul>

Column name	Description
	<ul style="list-style-type: none"> <li>·  <b>Unable to install OMSA</b> — Installation of OMSA could not be completed.</li> <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 data-bbox="400 1171 1458 1272">  <b>NOTE:</b> 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. </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**
  - **Software**
  - **Solution**
- **Groups**
  - **Default**
  - **Staging**
  - Custom groups
- **Adapter**
- **Remote Collector**

The **Devices** page also displays 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 collections 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](#)
- [Viewing 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 29. Add Single Device**

Field	Description
<b>Device Type</b>	<p>Displays a list of device types that you can add. The available device types are:</p> <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>Software</b></li> <li>• <b>Solution</b></li> <li>• <b>Storage Center (SC) / Compellent</b></li> </ul>
<b>IP Address / Host Name</b>	<p>IP address or host name of the device that you want to add.</p> <p> <b>NOTE:</b> For adding an EqualLogic storage array, enter the management IP address.</p>

Field	Description
<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.  <i>i</i> <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 issues. By configuring the SNMP settings, alerts (SNMP traps) from device are forwarded to the server where SupportAssist Enterprise is installed.  <i>i</i> <b>NOTE: The Configure SNMP settings option is displayed only for the following Device Types: Server, iDRAC, and Hypervisor.</b>
<b>Install or upgrade OMSA</b>	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.  <i>i</i> <b>NOTE: The Install, or upgrade OMSA option is displayed only for the following Device Types: Server and Hypervisor.</b>

*i* **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 Networking device](#)
- [Adding a PowerVault MD Series storage array](#)
- [Adding an EqualLogic PS Series storage solution](#)
- [Adding a Compellent SC Series storage solution](#)
- [Adding a Fluid File System \(FluidFS\) NAS device](#)
- [Adding a software](#)
- [Adding a solution](#)

## 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 30. 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.

① **NOTE:** The Enable Password and Community String are applicable only for Dell Networking devices.

① **NOTE:** The Community String is also applicable for Dell EqualLogic storage arrays.

① **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 31. 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 32. 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 33. Device overview pane**

Field	Description
Tasks	<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> </ul> </li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>· <b>Configure SNMP</b> — To configure the SNMP settings of the device.</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 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 collection history. You can select a date and time from the list to view the system information that was collected.</p> <p><b>NOTE: The Collections field displays No Collections in the following scenarios:</b></p> <ul style="list-style-type: none"> <li>· No collections have been performed from the device</li> <li>· The device is associated with a Remote Collector</li> </ul>
<b>Next Scheduled Collection</b>	Displays the date and time of the next scheduled 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 34. Multiple Device Collection window**

Field	Description
<b>Collection Name</b> (Optional)	The name that you want to assign to the collection.
<b>Dell EMC Support Request/case number</b> (Optional)	The case identifier that you want to associate with the collection.
<b>Dell EMC Technician Email</b> (Optional)	The email address or name of the Technical Support contact.
<b>Project ID</b> (Optional)	The project identification information.

Field	Description
<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 system information 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 system information 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.

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 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 35. Device Groups**

Column name	Description
Check box	Use to select a device group for performing an action.
<b>Name</b>	The name of the device group and the total number of devices in the device group.
<b>Description</b>	The description that you have provided for the device group.

### Related links

[Manage Devices](#)

[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 36. Manage Devices**

Field	Description
<b>Name</b>	Displays the 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>	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 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 37. Manage Contacts**

Field	Description
<b>Use default</b>	Select to use the contact information already available in the <b>Settings &gt; 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>	The first name of the primary or secondary contact.
<b>Last Name</b>	The last name of the primary or secondary contact.
<b>Phone</b>	The phone number of the primary or secondary contact.
<b>Alternate Phone</b>	The alternate phone number of the primary or secondary contact.
<b>Email Address</b>	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:

Field	Description
	<ul style="list-style-type: none"> <li>· <b>Phone</b></li> <li>· <b>Email</b></li> </ul>
<b>Preferred Contact Hours</b>	The preferred hours when Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.
<b>Time Zone</b>	Use 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>	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 38. Edit/Delete Device Group**

Field	Description
<b>Name</b>	The name of the device group.
<b>Description</b>	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](#)

# Manage Account Credentials

The **Manage Account Credentials** section enables you to configure SupportAssist Enterprise with administrator credentials for each supported device type and credential type. The following table provides information about the options displayed in the **Manage Account Credentials** section.

**Table 39. Manage Account Credentials**

Field	Description
<b>Add Credentials</b>	Click to add Account Credentials.
<b>Edit</b>	Click to edit Account Credentials.
<b>Delete</b>	Click to delete Account Credentials.
<b>Name</b>	The name that you have provided for the Account Credentials.
<b>Device Type</b>	The device type to which the Account Credentials is applicable.

## Related links

- [Account Credentials](#)
- [Adding Account Credentials](#)
- [Editing Account Credentials](#)
- [Deleting Account Credentials](#)

# Add Account Credentials

The **Add Account Credentials** window allows you to add Account Credentials. The following table provides information about the items displayed in the **Add Account Credentials** window.

**Table 40. Add Account Credentials**

Field	Description
<b>Name</b>	Type a name for the Account Credentials.
<b>Device Type</b>	The 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>Software</b></li><li>• <b>Solution</b></li><li>• <b>Storage Center (SC) / Compellent</b></li></ul>
<b>Username</b>	The user name required to connect to the device type.
<b>Password</b>	The password required to connect to the device type.
<b>Community String</b>	The community string assigned to the device.

Field	Description
	<p><b>NOTE:</b> The <b>Community String</b> option is displayed only for the <b>Networking and Peer Storage (PS) / EqualLogic</b> device types.</p>
<b>Enable Password</b>	<p>The enable password configured on the device.</p> <p><b>NOTE:</b> The <b>Enable Password</b> option is displayed only for the <b>Networking</b> device type.</p>
<b>Operating system type</b>	<p>The list of operating system types. The available operating system types are:</p> <ul style="list-style-type: none"> <li>Windows</li> <li>Linux</li> <li>ESX</li> <li>ESXi</li> </ul> <p><b>NOTE:</b> The <b>Operating system type</b> option is displayed only for the <b>Server / Hypervisor</b> device type.</p>
<b>Software Type</b>	<p>The list of software types. The available software types are:</p> <ul style="list-style-type: none"> <li>SCVMM</li> <li>vCenter</li> <li>SAN HQ</li> <li>HIT Kit / VSM for VMware</li> </ul> <p><b>NOTE:</b> The <b>Software Type</b> option is displayed only for the <b>Software</b> device type.</p> <p><b>NOTE:</b> If <b>SupportAssist Enterprise</b> is installed on a <b>Linux</b> operating system, adding <b>SCVMM</b> and <b>SAN HQ</b> is not supported.</p>
<b>Solution Type</b>	<p>The type of solution. The available type of solution is <b>Web Scale</b>.</p> <p><b>NOTE:</b> The <b>Solution Type</b> option is displayed only for the <b>Solution</b> device type.</p>

#### Related links

[Adding Account Credentials](#)

## Edit Account Credentials

The **Edit Account Credentials** window allows you to edit the Account Credentials. The following table provides information about the items displayed in the **Edit Account Credentials** window.

**Table 41. Edit Account Credentials**

Field	Description
<b>Name</b>	Type a name for the Account Credentials.
<b>Device Type</b>	The list of device types that you can add. The available device types are:

Field	Description
	<ul style="list-style-type: none"> <li>· Chassis</li> <li>· Fluid File System (FluidFS)</li> <li>· iDRAC</li> <li>· Networking</li> <li>· Peer Storage (PS) / EqualLogic</li> <li>· PowerVault</li> <li>· Server / Hypervisor</li> <li>· Software</li> <li>· Solution</li> <li>· Storage Center (SC) / Compellent</li> </ul>
<b>Username</b>	The user name required to connect to the device type.
<b>Password</b>	The password required to connect to the device type.
<b>Community String</b>	<p>The community string assigned to the device.</p> <p><b>NOTE:</b> The Community String option is displayed only for the Networking and Peer Storage (PS) / EqualLogic device types.</p>
<b>Enable Password</b>	<p>The enable password configured on the device.</p> <p><b>NOTE:</b> The Enable Password option is displayed only for the Networking device type.</p>
<b>Operating system type</b>	<p>The list of operating system types. The available operating system types are:</p> <ul style="list-style-type: none"> <li>· Windows</li> <li>· Linux</li> <li>· ESX</li> <li>· ESXi</li> </ul> <p><b>NOTE:</b> The Operating system type option is displayed only for the Server / Hypervisor device type.</p>
<b>Software Type</b>	<p>The list of software types. The available software types are:</p> <ul style="list-style-type: none"> <li>· SCVMM</li> <li>· vCenter</li> <li>· SAN HQ</li> <li>· HIT Kit / VSM for VMware</li> </ul> <p><b>NOTE:</b> The Software Type option is displayed only for the Software device type.</p> <p><b>NOTE:</b> If SupportAssist Enterprise is installed on a Linux operating system, adding SCVMM and SAN HQ is not supported.</p>
<b>Solution Type</b>	<p>The type of solution. The available type of solution is <b>Web Scale</b>.</p> <p><b>NOTE:</b> The Solution Type option is displayed only for the Solution device type.</p>

## Related links

[Editing Account Credentials](#)

# Manage Credential Profiles

The **Manage Credential Profiles** section enables you to apply a set of credentials to a device or group of devices. The following table provides information about the options displayed in the **Manage Credential Profiles** section.

**Table 42. Manage Credential Profiles**

Field	Description
<b>Add Profile</b>	Click to add a Credential Profile.
<b>Edit</b>	Click to edit a Credential Profile.
<b>Delete</b>	Click to delete a Credential Profile.
<b>Name</b>	The name that you have provided for the Credential Profile.

## Related links

[Credential Profiles](#)  
[Creating Credential Profile](#)  
[Assigning Credential Profile](#)  
[Editing Credential Profile](#)  
[Deleting Credential Profile](#)

# Add Credential Profile

The **Add Credential Profile** window allows you to add Credential Profiles. The following table provides information about the items displayed in the **Add Credential Profile** window.

**Table 43. Add Credential Profile**

Field	Description
<b>Name</b>	Type a name for the Credential Profile.
Check box	Use to select a device type.
<b>Device Type</b>	The list of device types that you can select. 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>Software</b></li><li>• <b>Solution</b></li><li>• <b>Storage Center (SC) / Compellent</b></li></ul>

Field	Description
<b>Account Credentials</b>	The Account Credentials that you have created for the specific device type.
<b>Add Account Credentials</b>	Click to add new account credentials.

**Related links**

[Creating Credential Profile](#)

## Edit Credential Profile

The **Edit Credential Profile** window allows you to edit Credential Profiles. The following table provides information about the items displayed in the **Edit Credential Profile** window.

**Table 44. Edit Credential Profile**

Field	Description
<b>Name</b>	The name of the Credential Profile.
Check box	Use to select a device type.
<b>Device Type</b>	The list of device types that you can select. 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>Software</b></li> <li>· <b>Solution</b></li> <li>· <b>Storage Center (SC) / Compellent</b></li> </ul>
<b>Account Credentials</b>	The Account Credentials that you have created for the specific device type.

**Related links**

[Editing Credential Profile](#)

## Collections page

The **Collections** page displays the collections that have been performed successfully. From the **Collections** page, you can view the collected system information, download multi-device collections, and also upload collections to Dell.

At the top of the **Collections** page, the navigation trail is displayed.

The following options available at the top of the collections page are:

- **Date Range** — To search the collections by a specific date range.
- **Search by** — To search by a specific category of displayed data. The available options are:
  - **Service Tag**

- **Name / IP Address**
- **Search term** — To enter the search keyword.
- **Upload** — To upload a collection to Dell.

The following table describes the information displayed in the **Collections** page.

**Table 45. 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 and collection type. 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 when the collection was started.
<b>Collection Purpose</b>	The reason selected while performing a multiple device collection.
<b>Case Number</b>	The numeric support case identifier.
<b>Upload Status</b>	The upload status of the collection.

You can choose to refine the displayed collections based on the collection type, device type, or adapter. The following are the available options for refining the displayed data:

- **Collection Type**
  - **Manual Collection**
  - **Periodic Collection**
  - **Case Collection**
  - **Multi Collection**
- **Device Type**
  - **Server**
  - **Storage**
  - **Networking**
  - **Chassis**
  - **Software**
  - **Solution**
- **Adapter**

## Collection overview pane

The collection overview pane displays the details of a collection and enables you to view or download the collected system information. 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 46. 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.
<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 collections from all other device types and multiple device collections)	Click to download the collection as a .zip file.

 **NOTE:** The **View Collection** or **Download Collection** option is disabled if the collection was performed by a **Remote Collector**.

## Extensions

The extensions available in SupportAssist Enterprise enables you to extend the SupportAssist Enterprise capability to many devices. You can use the extensions to inventory and add devices that are managed by a systems management console such as Dell OpenManage Essentials or Microsoft System Center Operations Manager.

Two types of extensions are available in SupportAssist Enterprise:

- **Adapter** — An application that acts as an interface between SupportAssist Enterprise and a systems management console.
- **Remote Collector** — A remote instance of SupportAssist Enterprise that collects and uploads system information from devices within a specific IP address range.

### Related links

- [Adapters](#)
- [Remote Collectors](#)

## Adapters

The adapter is an application that acts as an interface between SupportAssist Enterprise and systems management consoles. The following table provides information about the options displayed in the **Adapters** tab.

**Table 47. Adapters**

Field	Description
<b>Set Up Adapter</b>	Click to set up an adapter.
<b>Edit</b>	Click to edit the details of an adapter.
<b>Delete</b>	Click to delete an adapter.
Check box	Use to select an adapter that you have set up.

Field	Description
<b>Name</b>	The name that you have provided for the adapter and the host name or IP address of the server where the adapter is set up.
<b>Type</b>	The adapter type.
<b>Assigned Devices</b>	The total number of devices that are added through the adapter.
<b>Version</b>	The version of the adapter application.
<b>Status</b>	<p>The status of the adapter.</p> <p>The status of an adapter may be:</p> <ul style="list-style-type: none"> <li>• <b>Connected</b> — SupportAssist Enterprise is able to connect successfully to the adapter.</li> <li>• <b>Disconnected</b> — SupportAssist Enterprise is unable to connect to the adapter.</li> <li>• <b>Initial Synchronization</b> — Initial inventory of devices in progress.</li> <li>• <b>Periodic Synchronization</b> — Automatic periodic inventory of devices is in progress.</li> <li>• <b>Manual Synchronization</b> — Manually-initiated inventory of devices is in progress.</li> <li>• <b>Connection lost</b> — The server running SupportAssist Enterprise is unable to connect to the server where the adapter is set up.</li> <li>• <b>Copy in progress</b> — The adapter installer package is being copied to the system.</li> <li>• <b>Installation in progress</b> — Installation of the adapter is in progress.</li> <li>• <b>Validation in progress</b> — SupportAssist Enterprise is verifying if the adapter meets the prerequisites for setting up the adapter.</li> <li>• <b>Configuration in progress</b> — SupportAssist Enterprise is configuring the settings of the adapter.</li> <li>• <b>Starting service</b> — SupportAssist Enterprise had installed the adapter and the adapter service is started.</li> <li>• <b>Awaiting connection</b> — SupportAssist Enterprise is waiting for the adapter service to start.</li> <li>• <b>Connection in progress</b> — SupportAssist Enterprise is trying to connect to the adapter.</li> <li>• <b>Assigning Profile</b> — The Credential Profile is being applied to the inventoried devices. The total number of inventoried devices and the count of devices to which the profile is applied is also displayed.</li> </ul>

#### Related links

- [Setting up OpenManage Essentials adapter](#)
- [Setting up the Microsoft System Center Operations Manager adapter](#)
- [Viewing adapter overview pane](#)
- [Viewing devices inventoried by the adapter](#)
- [Synchronizing adapter](#)
- [Editing adapter](#)
- [Deleting adapter](#)

## Set Up Adapter (OpenManage Essentials)

The **Set Up Adapter** window allows you to add an adapter. The following table provides information about the items displayed in the **Set Up Adapter** window.

**Table 48. Set Up Adapter (OpenManage Essentials)**

Field	Description
<b>Adapter type</b>	Use to select the type of adapter that you want to set up. The available adapter types are: <ul style="list-style-type: none"> <li>• <b>OpenManage Essentials</b> — Select to set up the Open Manage Essentials adapter.</li> <li>• <b>System Center Operations Manager</b> — Select to set up the System Center Operations Manager adapter.</li> </ul>
<b>Host name / IP address</b>	The host name or IP address of the server where OpenManage Essentials is installed.
<b>Name</b> (Optional)	An optional name that you want to use for identifying the adapter in SupportAssist Enterprise.
<b>User name</b>	The user name required to connect to the server where OpenManage Essentials is installed.
<b>Password</b>	The password required to connect to the server where OpenManage Essentials is installed.
<b>Credential Profile</b>	Use to select a Credential Profile that is required to add the devices that are inventoried by the adapter.
<b>Update device inventory</b>	Use to select the frequency at which the adapter must inventory devices from the adapter. The available options are: <ul style="list-style-type: none"> <li>• <b>Every 12 hours</b></li> <li>• <b>Daily</b></li> <li>• <b>Weekly</b></li> <li>• <b>Every two weeks</b></li> <li>• <b>Monthly</b></li> </ul>

### Related links

[Setting up OpenManage Essentials adapter](#)

## Set Up Adapter (Microsoft System Center Operations Manager)

The **Set Up Adapter** window allows you to add an adapter. The following table provides information about the items displayed in the **Set Up Adapter** window.

**Table 49. Set Up Adapter (Microsoft System Center Operations Manager)**

Field	Description
<b>Adapter type</b>	Use to select the type of adapter that you want to set up. The available adapter types are:

Field	Description
	<ul style="list-style-type: none"> <li>• <b>OpenManage Essentials</b> — Select to set up the OpenManage Essentials adapter.</li> <li>• <b>System Center Operations Manager</b> — Select to set up the System Center Operations Manager adapter.</li> </ul>
<b>Name</b> (Optional)	An optional name that you want to use for identifying the adapter in SupportAssist Enterprise.
<b>Establish a remote connection with the management group</b>	Select this option if you are setting up the adapter on the server hosting the Remote Console.
Management group <b>Host name / IP address</b>	The host name or IP address of the server that hosts the management group.
<b>User Name</b>	The user name required to connect to the server that hosts the management group.
<b>Password</b>	The password required to connect to the server that hosts the management group.
Remote Console <b>Host name / IP address</b>	The host name or IP address of the server that hosts the Remote Console.
<b>User Name</b>	The user name required to connect to the server that hosts the Remote Console.
<b>Password</b>	The password required to connect to the server that hosts the Remote Console.
<b>Credential Profile</b>	Use to select a Credential Profile that is required to add the devices that are inventoried by the adapter.
<b>Update device inventory</b>	<p>Use to select the frequency at which the adapter must inventory devices from the adapter. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Every 12 hours</b></li> <li>• <b>Daily</b></li> <li>• <b>Weekly</b></li> <li>• <b>Every two weeks</b></li> <li>• <b>Monthly</b></li> </ul>

#### Related links

[Setting up the Microsoft System Center Operations Manager adapter](#)

## Adapter overview pane

The adapter overview pane displays the details of an adapter and allows you to perform certain operations on that adapter. This pane is displayed when you select an adapter on the **Adapters** page.

**Table 50. Adapter overview pane**

Field	Description
<b>Name</b>	The name that you have provided for the adapter.
<b>IP address</b>	The IP address or host name of the server where the adapter is set up.
<b>Status</b>	The status of the adapter.
<b>Sync now</b>	Click to inventory devices from the systems management console.
<b>Last sync</b>	The date and time when the devices were last inventoried.
<b>Adapter type</b>	The type of adapter.
<b>OS Type</b>	The operating system running on the server where the adapter is set up.
<b>Assigned devices</b>	The total number of devices that are added successfully through the adapter.
<b>Staging devices</b>	Displays the total number of inventoried devices that are added to the staging group. Devices may be added to the staging group because they did not meet certain prerequisites.
<b>Version</b>	The version of the adapter application.

**Related links**

[Viewing adapter overview pane](#)

## Remote Collectors

The Remote Collector is a remote instance of SupportAssist Enterprise that collects and uploads system information from devices within a specific IP address range. The following table provides information about the options displayed on the **Remote Collectors** page.

**Table 51. Remote Collectors**

Field	Description
<b>Set Up Remote Collector</b>	Click to set up a Remote Collector.
<b>Edit</b>	Click to edit the details of a Remote Collector.
<b>Delete</b>	Click to delete a Remote Collector.
Check box	Use to select a Remote Collector that you have set up.
<b>Name</b>	The name that you have provided for the Remote Collector and the host name or IP address of the server where the Remote Collector is set up.
<b>Assigned Devices</b>	The total number of devices that are associated with the Remote Collector.
<b>Version</b>	The version of the Remote Collector application.
<b>Status</b>	The status of the Remote Collector.

Field	Description
	<p>The status of a Remote Collector may be:</p> <ul style="list-style-type: none"> <li>• <b>Connected</b> — The server where SupportAssist Enterprise is installed is able to connect to the server where the Remote Collector is set up.</li> <li>• <b>Disconnected</b> — The server where SupportAssist Enterprise is installed is not able to connect to the server where the Remote Collector is set up.</li> <li>• <b>Connection failed</b> — Displayed when a connection fails while connecting to the SupportAssist server.</li> <li>• <b>Registration failed</b> — Displayed when a Remote Collector fails to connect to SupportAssist Enterprise.</li> <li>• <b>Registration initiated</b> — Displayed when the Remote Collector connects to SupportAssist Enterprise.</li> <li>• <b>Copy in progress</b> — The Remote Collector installer package is being copied to the remote system.</li> <li>• <b>Validation in progress</b> — SupportAssist Enterprise is verifying if the remote server meets the prerequisites for setting up the Remote Collector.</li> <li>• <b>Configuration in progress</b> — SupportAssist Enterprise is configuring the settings of the Remote Collector.</li> <li>• <b>Registration in progress</b> — The server running SupportAssist Enterprise is communicating with the Remote Collector after the configuration is complete.</li> <li>• <b>Installation in progress</b> — Installation of the Remote Collector application is in progress.</li> <li>• <b>Installer not found</b> — The Remote Collector installer file is corrupted or deleted manually from the server running SupportAssist Enterprise.</li> <li>• <b>Copy failed</b> — The Remote Collector could not be copied to the remote server.</li> <li>• <b>Installation failed</b> — Installation of the Remote Collector could not be completed successfully.</li> <li>• <b>Configuration failed</b> — SupportAssist Enterprise could not complete the configuring the settings of the Remote Collector.</li> <li>• <b>Validation failed</b> — SupportAssist Enterprise could not verify if the remote server meets the prerequisites for setting up the Remote Collector.</li> <li>• <b>Low disk space</b> — The free hard-drive space on the server where the Remote Collector is set up is less than 500 MB.</li> <li>• <b>Connection initiated</b> — Displayed when a connection is initiated while connecting to the SupportAssist server.</li> </ul>

#### Related links

- [Setting up Remote Collector](#)
- [Viewing collections for devices associated with a Remote Collector](#)
- [Viewing the Remote Collector overview pane](#)
- [Viewing devices associated with a Remote Collector](#)
- [Editing Remote Collector](#)
- [Deleting Remote Collector](#)

## Set Up Remote Collector

The **Set Up Remote Collector** window allows you to set up a Remote Collector. The following table provides information about the items displayed in the **Set Up Remote Collector** window.

**Table 52. Set Up Remote Collector**

Field	Description
<b>Host name / IP address</b>	The host name or IP address of the server where you want to set up the Remote Collector.
<b>Name</b> (Optional)	An optional name that you want to use for identifying the Remote Collector in SupportAssist Enterprise.
<b>User name</b>	The user name required to connect to the server where you want to set up the Remote Collector.
<b>Password</b>	The password required to connect to the server where you want to set up the Remote Collector.
<b>IP address / range</b>	The IP address or IP address range of the devices that you want to associate with the Remote Collector.
<b>Add IP address range</b>	Click to open an additional IP address or IP address range field.
<b>The remote server connects to the internet through a proxy server</b>	Select to enter details of the proxy server through which the remote server connects to the internet.
<b>Host name / IP address</b>	The host name or IP address of the proxy server.
<b>Port</b>	The port number used by the proxy server.
<b>Requires authentication</b>	Select this option if a user name and password are required to connect to the proxy server.
<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.
<b>Proxy Exclusion List</b>	The IP address range or ranges of devices to which the Remote Collector must communicate directly and not through the proxy server. IP address of devices that communicate through https protocol must be included in the proxy exclusion list. Examples of devices that communicate through https protocol include iDRAC, Compellent storage arrays, VMware ESX and ESXi, and XC Series of Web-scale Hyper-converged appliances.

**Related links**

[Setting up Remote Collector](#)

## Remote Collector overview pane

The Remote Collector overview pane displays details of a Remote Collector. This pane is displayed when you select a Remote Collector in the **Remote Collectors** page.

**Table 53. Remote Collector overview pane**

Field	Description
<b>Name</b>	The name that you have provided for the Remote Collector.
<b>IP address</b>	The IP address or host name of the server where the Remote Collector.

Field	Description
Status	The status of the Remote Collector.
Collector Type	The type of the collector.
Version	The version of the Remote Collector application.
OS	The operating system running on the server where the Remote Collector is set up.
Assigned devices	The total number of devices associated with the Remote Collector.
Collection Range	The IP address ranges that are assigned to the Remote Collector.
View all devices	Click to open the <b>Devices</b> page where all devices that are associated with the Remote Collector are displayed.

**Related links**

[Viewing the Remote Collector overview pane](#)

# 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:

- **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, collection of system information, 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**

- [Proxy Settings](#)
- [Preferences](#)
- [Contact Information](#)
- [SMTP Settings](#)

# 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.

**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 54. Proxy Settings**

Field	Description
<b>Use proxy server</b>	Select this option to enable configuring the proxy server settings.
<b>Host Name / IP Address</b>	The host name or IP address of the proxy server.
<b>Port</b>	The port number used by the proxy server.
<b>Requires authentication</b>	Select this option if a user name and password are required to connect to the proxy server.
<b>User Name</b>	The user name required to connect to the proxy server.
<b>Password</b>	The password required to connect to the proxy server.
<b>Proxy exclusion list</b>	The IP address range or ranges of devices to which SupportAssist Enterprise must communicate directly and not through the proxy server. IP address of devices that communicate through https protocol must be included in the proxy exclusion list. Examples of devices that communicate through https protocol include iDRAC, Compellent storage arrays, VMware ESX and ESXi, and XC Series of Web-scale Hyper-converged appliances.

**Related links**

[Configuring proxy server settings](#)

## Preferences

The **Preferences** page enables you to configure 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 55. Preferences**

Field	Description
<b>Automated Tasks</b>	
<b>Automatically update the following features in SupportAssist Enterprise:</b>	<p>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.</p> <p><b>NOTE:</b> Dell recommends that you select automatic updates to ensure that SupportAssist Enterprise is up-to-date with the latest features and enhancements.</p>
<b>SupportAssist Enterprise application</b>	Select this option to automatically download and install the SupportAssist Enterprise application update whenever it is available.

Field	Description
Policy files	Select this option to automatically download and install the policy files update whenever it is available.
Product support files	Select this option to automatically download and install the device support update whenever it is available.
<b>Automatically collect system state information:</b>	
Starting from day N of every month at 11 PM	Select this option to automatically collect system state information from each device type on a randomly determined day of every month at 11 PM.
When a new support case is created	Select this option to automatically start a system log collection when a new support case is generated.
<b>Email Settings</b>	
Automatically upload system state information collected from devices to Dell	Select to automatically upload collections to Dell.
Receive email notification when a new support case is opened	Select this option to receive an email notification when a new support case is opened.
Preferred email Language	Select the preferred language for email notifications.
<b>Recommendation Report Settings</b>	
Automatically receive recommendation reports via email	Select this option to automatically receive ProSupport Plus server recommendation reports through email.
<b>Collection Data Settings</b>	
Server / Hypervisor	<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:</b> For information on the logs that are collected by SupportAssist Enterprise, see the <i>SupportAssist Enterprise Version 1.1 Reportable Items</i> document at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</p>
Storage: Fluid File System (FluidFS)	Select <b>Logs</b> to collect logs from the device.
Storage: Peer Storage (PS) / EqualLogic	<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>
Storage: PowerVault	Select <b>Support Data</b> to collect support data from the device.
Storage: Storage Center (SC) / Compellent	Select <b>Logs</b> to collect logs from the device.
Software: HIT Kit/VSM for VMware	Select <b>Advanced Logs</b> to collect logs from the device.
<b>Identification Information Settings</b>	
Include identification information in data sent to Dell	<p>Select this option to allow sending identity information to Dell.</p> <p><b>NOTE:</b> If you clear this option, settings for the collection of logs and diagnostic data under <b>Collection Data Settings</b> are automatically disabled.</p>

Field	Description
<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.

**NOTE:** It is mandatory to provide information for all fields, except the alternate phone number.

**Table 56. Contact Information**

Field	Description
<b>Company name</b>	The name of your company.
<b>Primary</b>	Select this option to view or edit the primary contact information.
<b>Secondary</b>	Select this option to view or edit the secondary contact information.
<b>First name</b>	The first name of the primary or secondary contact.
<b>Last name</b>	The last name of the primary or secondary contact.
<b>Phone number</b>	The phone number of the primary or secondary contact.
<b>Alternate phone number</b>	The alternate phone number of the primary or secondary contact.
<b>Email address</b>	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>	The preferred hours when Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.

Field	Description
Time Zone	The time zone of the primary or secondary contact.
<b>Part dispatch (Optional)</b>	
Address City / Town Country / Territory State / Province / Region Zip / Postal code	The address where a replacement part must be dispatched.
CNPJ IE	For Brazil only: 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.

**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 57. SMTP Settings**

Field	Description
Use SMTP server	Select this option to enable configuring the email server settings.
Host Name / IP Address	The host name or IP address of the email server.
Port	The port number used by the email server.
Requires authentication	Select this option if a user name and password are required to connect to the email server.
User Name	The user name required to connect to the email server.
Password	The password required to connect to the email server.
Use SSL	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.

The following table describes the fields displayed on the **Network Connectivity Test** page.

**Table 58. Connectivity Test**

Field	Description
Check box	Select the appropriate check boxes to test the connectivity status you want to verify.
<b>Test</b>	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 Enterprise 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> <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:</b> The Error status is displayed as a link that you can click to view a description of the issue and the possible resolution steps.</p>
<b>Last Verified</b>	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](#)




# SupportAssist Enterprise test

The **SupportAssist Enterprise test** page enables you to verify the ability of SupportAssist Enterprise to run specific tasks.

At the top of the **SupportAssist Enterprise 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 that are displayed in the **SupportAssist Enterprise test** page.

**Table 59. SupportAssist Enterprise test**

Field	Description
Check box	Select the appropriate check box to test the task that you want to verify.
<b>Test</b>	The feature 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 Technical Support.
<b>Description</b>	Describes the purpose of the test.
<b>Status</b>	<p>Displays an icon and a message that indicates the test status. The possible statuses are:</p> <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>	The date and time the status was last verified.
<b>Run Tests</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 60. 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>SupportAssist Enterprise Version 1.1 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact 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 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>SupportAssist Enterprise version 1.1 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact 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 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> .	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>SupportAssist Enterprise version 1.1 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> If the problem persists, contact Technical Support for assistance.
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> .	Make sure that the device is reachable and the configured device credentials have Administrator rights, 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>SupportAssist Enterprise version 1.1 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> If the problem persists, contact Technical Support for assistance.
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> For more information, see <a href="#">Other services</a> .
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	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <i>device_name</i> .	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>SupportAssist Enterprise version 1.1 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> If the problem persists, contact Technical Support for assistance.

Error code	Error message	Possible resolution
3000_37 3000_38 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> .	<p>Make sure that port 22 is open and SSH is enabled on the system, 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>SupportAssist Enterprise version 1.1 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Technical Support for assistance.</p>
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>SupportAssist Enterprise version 1.1 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Technical Support for assistance.</p>
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 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	Ensure that the health of this device is restored for optimal SupportAssist Enterprise operations.

Error code	Error message	Possible resolution
	mode. During this period, SupportAssist Enterprise will not process any alerts from this device.	
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 &gt; 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 &gt; 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 &gt; 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 &gt; 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 &gt; 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 &gt; 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>SupportAssist Enterprise Version 1.1 Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a> .

Error code	Error message	Possible resolution
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 &gt; 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 &gt; 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 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 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 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.
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.

Error code	Error message	Possible resolution
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>SupportAssist Enterprise Version 1.1 Support Matrix</i> at <a href="https://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.
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>SupportAssist Enterprise Version 1.1 Support Matrix</i> at <a href="https://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a> . If the problem persists, contact Technical Support for assistance.

Error code	Error message	Possible resolution
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 <i>name</i> is already in use by another device.	Retry adding the device with any other 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>SupportAssist Enterprise Version 1.1 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>SupportAssist Enterprise Version 1.1 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.
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.

Error code	Error message	Possible resolution
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>SupportAssist Enterprise Version 1.1 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>SupportAssist Enterprise Version 1.1 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>
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.

Error code	Error message	Possible resolution
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 it is already in use by another device.	Enter any other 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 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 Technical Support.	Not applicable.
SA-4015 SA-4020 SA-4025 SA-4030 SA-4035 SA-4040 SA-4045 SA-4050 SA-4055 SA-4060	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 Technical Support for assistance.

Error code	Error message	Possible resolution
SA-4065 SA-4070 SA-4071 SA-4072		
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 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 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 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 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 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 Technical Support for assistance.</li> </ul>
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> </ul>

Error code	Error message	Possible resolution
		<ul style="list-style-type: none"> <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 <a href="#">SupportAssist Enterprise Version 1.1 Support Matrix at 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 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 Technical Support for assistance.
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>

Error code	Error message	Possible resolution
		If the problem persists, contact Technical Support for assistance.
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 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>
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 device <i>device_name</i> because the hard-drive space available on the server where SupportAssist Enterprise is installed is critically low.	For information about the hard-drive space requirements for installing and using SupportAssist Enterprise, see <a href="#">Hardware requirements</a> .
SA-30130	SupportAssist Enterprise has placed the device <i>device_name</i> in the <b>Staging</b> group because a required verification could not be completed.	To add the device, revalidate the device later.

Error code	Error message	Possible resolution
SA-30180	SupportAssist Enterprise has placed the device <i>device_name</i> in the <b>Staging</b> group because the device does not have the 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 device <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 is enabled in Enterprise Manager, and then revalidate the device.
SA-20005	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the adapter is already installed on the system or the devices associated with the adapter are already added.	Not applicable.
SA-20010	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the <i>name</i> is already in use by another adapter.	Retry adding the adapter with another name.
SA-20015	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because of an unknown error.	Retry adding the adapter.
SA-20020	SupportAssist is unable to set up the adapter <i>adapter_name</i> because the Management Group credentials are incorrect.	Enter the correct Management Group credentials and retry.
SA-20025	SupportAssist Enterprise is unable to reach the system where the adapter is set up or the adapter service is not running on the remote system.	Verify the following and then retry: <ul style="list-style-type: none"> <li>• The adapter is reachable from the server where SupportAssist Enterprise is installed.</li> <li>• Port 5700 is open on the server where SupportAssist Enterprise is installed.</li> <li>• SupportAssist Enterprise Adapter service is running.</li> </ul>
SA-20030	SupportAssist Enterprise is unable to reach the system where the adapter is installed.	Verify the following and then retry: <ul style="list-style-type: none"> <li>• Management Group credentials are correct.</li> <li>• Adapter is connected to the Management Group.</li> <li>• SupportAssist Enterprise Adapter service is running.</li> </ul>
SA-20035	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the adapter has an invalid key.	Retry adding the adapter with a valid key.
SA-20040	SupportAssist Enterprise is unable to reach the adapter <i>adapter_name</i> because the Microsoft System Center Operations Manager instance is not available or Microsoft System Center Operations Manager service may not be running.	Verify the following and then retry: <ul style="list-style-type: none"> <li>• Microsoft System Center Operations Manager instance is available.</li> <li>• Microsoft System Center Operations Manager Service is running.</li> </ul>
SA-20045	SupportAssist Enterprise is unable to reach the adapter <i>adapter_name</i> because the Management Group credentials are incorrect or does not have sufficient privileges.	Enter the correct Management Group credentials and retry.
SA-20050 SA-20065 SA-20070 SA-20075	SupportAssist Enterprise is unable to reach the adapter <i>adapter_name</i> because of an unknown error.	Not applicable.

Error code	Error message	Possible resolution
SA-20080 SA-20085 SA-20090		
SA-20404	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the adapter is not available or not reachable.	Ensure that the adapter is available and details of the adapter are correct and retry again.
SA-21005	SupportAssist Enterprise is unable to edit the details of the adapter <i>adapter_name</i> because the <i>name</i> is already in use by another adapter.	Enter any other name for the adapter and retry.
SA-21010	SupportAssist Enterprise is unable to edit the details of the adapter <i>adapter_name</i> because of an unknown error.	Retry editing the details of the adapter after some time.
SA-21015	SupportAssist Enterprise is unable to edit the details of the adapter <i>adapter_name</i> because the details of the adapter are incorrect.	Ensure that the details of the adapter are correct and then retry.
SA-21404	SupportAssist Enterprise is unable to edit the adapter <i>adapter_name</i> because the adapter is not reachable.	Ensure that the details of the adapter are correct and then retry.
SA-20095	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because a connection could not be established with the system.	Ensure the following and retry the operation: <ul style="list-style-type: none"> <li>• Ensure that the credentials are valid.</li> <li>• Ensure that you have administrator privileges.</li> </ul>
SA-20100	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because of low disk space on the system.	Ensure that the remote system has sufficient free hard-drive space required for installing the adapter and retry the operation.
SA-20105	SupportAssist Enterprise is unable to copy installer file to the system.	Ensure that the system is reachable and the installer file is present at the required location.
SA-20110	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the installation of the adapter could not be completed successfully.	Retry setting up the adapter.
SA-20115	SupportAssist Enterprise is unable to start the adapter service on the system.	Ensure that the installation of the adapter is successful and the configuration file has the correct values.
SA-20120	SupportAssist Enterprise is unable to copy the configuration file.	Ensure that the configuration file that is generated is not empty and the system is reachable.
SA-20125	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the OpenManage Essentials adapter is already installed on the system.	Ensure that the OpenManage Essentials adapter is not installed on the system and then retry the operation.
SA-20130	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the status of the required network port could not be verified.	Ensure that the system is running a Windows operating system and the WMI port (135) is open on the system.
SA-20135	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the OpenManage Essentials services are not running on the remote system.	Ensure that OpenManage Essentials services are running and retry the operation.

Error code	Error message	Possible resolution
SA-20140	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> on the system <i>device_name</i> because of one of the following: <ul style="list-style-type: none"> <li>OpenManage Essentials is not installed on the system</li> <li>The adapter is not compatible with the version of OpenManage Essentials installed on the system</li> </ul>	Ensure that OpenManage Essentials version 2.3 or later is installed on the system and then retry the operation.
SA-20145	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the installer for OpenManage Essentials adapter is not present at the required location.	Reinstall SupportAssist Enterprise and then retry the operation.
SA-20150	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the operating system installed on the remote system is not of 64-bit architecture.	Ensure that the remote system is running a 64-bit Windows Operating System and retry the operation.
SA-20155	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the version of OpenManage Essentials installed on the system is not compatible with the OpenManage Essentials adapter.	Ensure that the OpenManage Essentials version 2.3 or later is installed on the system and then retry the operation.
SA-20160	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the Microsoft .NET package is not installed on the system.	Ensure that the Microsoft .NET package is installed on the remote system and then retry the operation.
SA-20165	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the version of the Microsoft .NET package installed on the remote system is not compatible with the OpenManage Essentials adapter.	Ensure that the Microsoft .NET package version 4.0 or later is installed on the remote system and then retry the operation.
SA-20170	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because Microsoft System Center Operations Manager is not installed on the remote system.	Ensure that the Microsoft System Center Operations Manager is installed on the remote system and then retry the operation.
SA-20175	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the version of Microsoft System Center Operations Manager installed on the remote system is not compatible with Microsoft System Center Operations Manager adapter.	Ensure that the Microsoft System Center Operations Manager version 7.0 or later is installed on the remote system and then retry the operation.
SA-20180	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the Microsoft System Center Operations Manager service is not running on the remote system.	Ensure that the Microsoft System Center Operations Manager service is running and then retry the operation.
SA-20185	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because the Microsoft System Center Operations Manager adapter is already installed on the remote system.	Ensure that the Microsoft System Center Operations Manager adapter is not previously installed on the remote system and then retry the operation.
SA-20190	SupportAssist Enterprise is unable to edit the adapter <i>adapter_name</i> because a connection could not be established with the remote system.	Ensure the following and retry the operation : <ul style="list-style-type: none"> <li>Ensure that the credentials are valid.</li> <li>Ensure that you have administrator privileges.</li> </ul>
SA-20200	SupportAssist Enterprise is unable to edit the adapter <i>adapter_name</i> because the adapter is uninstalled on the remote system.	Not applicable.

<b>Error code</b>	<b>Error message</b>	<b>Possible resolution</b>
SA-20205	SupportAssist Enterprise is unable to set up the adapter <i>adapter_name</i> because of an error during validation.	Delete the adapter and then try setting up the adapter again
SA-20210	SupportAssist Enterprise is unable to synchronize devices through the adapter <i>adapter_name</i> .	Select the adapter and then perform a manual device synchronization
SA-20215	SupportAssist Enterprise is unable to delete the adapter <i>adapter_name</i> because the adapter is not present on the system.	Not applicable.
SA-30005	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the Remote Collector is already added.	You may have already added the Remote Collector by using another IP address.
SA-30010	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the provided name <i>name</i> is already in use by another Remote Collector.	Provide any other name and retry.
SA-30015	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the provided IP address range <i>IP address_range</i> overlaps with the IP address range of another Remote Collector.	Provide a mutually exclusive IP address range and retry.
SA-30020	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because another operation is in progress.	Retry the operation after some time.
SA-30025	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the credentials provided for the remote system are incorrect.	Provide the correct credentials and retry.
SA-30404	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the Remote Collector is either not valid or not reachable.	Verify the details of the Remote Collector and retry.
SA-30405	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because Start IP Address is greater than the End IP Address.	Provide the correct IP address range and retry.
SA-30406	SupportAssist Enterprise is unable to delete the Remote Collector <i>Remote Collector_name</i> because another operation is currently in progress.	Retry the operation after some time.
SA-30408	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the <i>name</i> is already in use by another Remote Collector.	Provide any other name and retry.
SA-30409	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the credentials of the Remote Collector are incorrect.	Verify the credentials of the Remote Collector and retry.
SA-30410	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because Remote Collector is either not valid or not reachable.	Verify the details of the Remote Collector and retry.
SA-30411	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the provided IP address range <i>IP address_range</i> overlaps with the IP address range of another Remote Collector.	Provide a mutually exclusive IP address range and retry.

<b>Error code</b>	<b>Error message</b>	<b>Possible resolution</b>
SA-30412	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the Start IP Address is greater than the End IP Address.	Provide the correct IP address range and retry.
SA-30413	SupportAssist Enterprise is unable to update the Remote Collector <i>Remote Collector_name</i> because another operation is in progress.	Retry the operation after some time.
SA-30414	SupportAssist Enterprise is unable to connect to the Remote Collector <i>Remote Collector_name</i> because of an internal error.	Ensure that the Remote Collector application is running and then retry the operation.
SA-30415	SupportAssist Enterprise is unable to connect to the Remote Collector <i>Remote Collector_name</i> because of an internal error.	Update the credentials of the Remote Collector, ensure that the Remote Collector application is running, and then retry.
SA-30416	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the provided IP address range <i>IP address_range</i> overlaps with the IP address range of same Remote Collector.	Provide a mutually exclusive IP address range and retry.
SA-30417	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the installer for Remote Collector could not be found at the required location.	Reinstall SupportAssist Enterprise and then retry the operation.
SA-30418	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because a connection could not be established with the remote system.	Ensure the following and retry the operation: <ul style="list-style-type: none"> <li>• Ensure that the credentials are valid.</li> <li>• Ensure that you have administrator privileges.</li> </ul>
SA-30419	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the Remote Collector installer could not be copied to the remote system.	Ensure that the remote system is reachable. Verify the credentials of the remote system and then retry the operation.
SA-30420	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the Remote Collector installation on the remote system was unsuccessful.	Ensure that the remote system is compatible with the hardware and software requirements for setting up a Remote Collector.
SA-30421	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the Remote Collector installation was not successful.	Ensure that the remote system is compatible with the hardware and software requirements for setting up a Remote Collector.
SA-30422	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the installation of the Remote Collector was unsuccessful.	Reinstall SupportAssist Enterprise and then retry the operation.
SA-30423	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the Remote Collector configuration was unsuccessful.	Reinstall SupportAssist Enterprise and then retry the operation.
SA-30424	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the remote system does not have sufficient free hard-drive space.	Ensure that the remote system has at least 500 MB of free hard-drive space.

<b>Error code</b>	<b>Error message</b>	<b>Possible resolution</b>
SA-30425	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because SupportAssist Enterprise is already installed on the remote system.	Uninstall SupportAssist Enterprise from the remote system and then retry the operation.
SA-30426	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the IP address or hostname that has been provided is of the local system.	Provide the correct IP address or hostname of a remote system and retry the operation.
SA-30427	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the remote system is not reachable.	Ensure that the remote system is reachable and then retry the operation.
SA-30428	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the Remote Collector is not supported on a non-Windows operating system.	Ensure you provide the details of a remote system that is running a Windows operating system and then retry the operation.
SA-30429	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the provided IP address range <i>IP address_range</i> overlaps with the IP address range of the same Remote Collector <i>Remote Collector_name</i> .	Provide a mutually exclusive IP address range and retry.
SA-30430	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the credentials of the Remote Collector are incorrect.	Verify the credentials of the Remote Collector and retry the operation.
SA-30431	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the Remote Collector configuration on the remote system was not successful.	Ensure that the remote system is reachable. Verify the credentials of the remote system and then retry the operation.
SA-30432	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the SupportAssist Enterprise service is not running on the remote system.	Start the SupportAssist Enterprise service on the remote system and then retry the operation.
SA-30433	SupportAssist Enterprise is unable to update the details of the Remote Collector <i>Remote Collector_name</i> because the Remote Collector application is not installed on the remote system.	Not applicable.
SA-30434	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the operating system installed on the remote system is not of 64-bit architecture.	Ensure that you provide the details of a remote system that is running a 64-bit Windows operating system and then retry the operation.
SA-30435	SupportAssist Enterprise is unable to set up the Remote Collector <i>Remote Collector_name</i> because the validation of the Remote Collector was unsuccessful.	Ensure that the remote system is compatible with the hardware and software requirements for setting up a Remote Collector.

## Related documents and resources

In addition to this guide you can access the following guides available on the Dell Support website.

**Table 61. Related documents**

Document title	How to access the document
<i>SupportAssist Enterprise Version 1.1 Online Help</i>	Click the help icon in the SupportAssist Enterprise user interface.
<i>SupportAssist Enterprise Version 1.1 User's 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>SupportAssist Enterprise Version 1.1 Quick Setup Guide</i>	
<i>SupportAssist Enterprise Version 1.1 Reportable Items</i>	
<i>SupportAssist Enterprise Version 1.1 Release Notes</i>	
<i>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>OpenManage Server Administrator User's Guide</i>	
<i>iDRAC User's Guide</i>	Visit <a href="https://Dell.com/idracmanuals">Dell.com/idracmanuals</a> .
SupportAssist on Dell EMC's 14th generation of PowerEdge servers	Visit the <a href="#">iDRAC Dell TechCenter</a> page.
SupportAssist Collections on Dell EMC's 14th generation of PowerEdge servers	Visit the <a href="#">iDRAC Dell TechCenter</a> page.

## Video tutorials

You can access the following video tutorials related to SupportAssist Enterprise.

**Table 62. Video tutorials**

Video title	How to access the videos
SupportAssist Enterprise: Installing and Registering (Windows)	Visit the <b>Dell TechCenter</b> channel on YouTube, and click <b>Playlist</b> . On the playlist, click <b>SupportAssist Enterprise</b> .
SupportAssist Enterprise: Installing and Registering (Linux)	
SupportAssist Enterprise: Checking for Cases	
SupportAssist Enterprise: Importing Multiple Devices	
SupportAssist Enterprise: Revalidating a Device	
SupportAssist Enterprise: Testing Case Creation	
SupportAssist Enterprise: Monitoring the Local System	
SupportAssist Enterprise: Adding Devices	
SupportAssist Enterprise: Case Management	
SupportAssist Enterprise: Managing Device Groups	

Video title	How to access the videos
SupportAssist Enterprise: Testing Network Connectivity	
SupportAssist Enterprise: Viewing Collections	
SupportAssist Enterprise: Collecting System Information	
SupportAssist Enterprise: Uploading Collections from a Disconnected Site	
SupportAssist Enterprise: Setting up OpenManage Essentials adapter	
SupportAssist Enterprise: Setting up System Center Operations Manager adapter	
SupportAssist Enterprise: Setting up Remote Collector	
SupportAssist Enterprise: Creating Account Credentials	
SupportAssist Enterprise: Creating Credential Profiles	

## SupportAssist 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).

Topics:

- [Accessing documents from the Dell EMC support site](#)
- [Contacting Dell](#)

## Accessing documents from the Dell EMC support site

You can access the required documents using the following links:

- For Dell EMC Enterprise Systems Management documents — [Dell.com/SoftwareSecurityManuals](https://Dell.com/SoftwareSecurityManuals)
- For Dell EMC OpenManage documents — [Dell.com/OpenManageManuals](https://Dell.com/OpenManageManuals)
- For Dell EMC Remote Enterprise Systems Management documents — [Dell.com/esmanuals](https://Dell.com/esmanuals)
- For iDRAC and Dell EMC Lifecycle Controller documents — [Dell.com/idracmanuals](https://Dell.com/idracmanuals)
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — [Dell.com/OMConnectionsEnterpriseSystemsManagement](https://Dell.com/OMConnectionsEnterpriseSystemsManagement)
- For Dell EMC Serviceability Tools documents — [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools)
- For Client Command Suite Systems Management documents — [Dell.com/DellClientCommandSuiteManuals](https://Dell.com/DellClientCommandSuiteManuals)
- a Go to [Dell.com/Support/Home](https://Dell.com/Support/Home).
- b Click **Choose from all products**.
- c From **All products** section, click **Software & Security**, and then 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.