Notes, cautions, and warnings

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

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

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

1 Overview ........................................................................................................................................ 11
   What is new in this release .............................................................................................................. 11
   Overview of supported device types .............................................................................................. 11
   How SupportAssist Enterprise works ............................................................................................ 13
   SupportAssist Enterprise capabilities available with Dell service contracts ...................................... 13
   System information collected by SupportAssist Enterprise ............................................................. 14

2 Getting started with SupportAssist Enterprise ............................................................................. 16
   Setting up SupportAssist Enterprise for the local system .............................................................. 16
   Setting up SupportAssist Enterprise for remote devices ............................................................... 17
   Evaluating SupportAssist Enterprise ............................................................................................. 17
      Evaluating the monitoring capability ....................................................................................... 17
      Evaluating the system information collection capability ......................................................... 17
   Download the SupportAssist Enterprise installation package ....................................................... 18
   Installing or Upgrading SupportAssist Enterprise ........................................................................... 18
   Minimum requirements for installing and using SupportAssist Enterprise ...................................... 19
      Hardware requirements ............................................................................................................... 19
      Software requirements .............................................................................................................. 20
      Network requirements ............................................................................................................. 21
   Installing SupportAssist Enterprise ............................................................................................... 25
      Operating system considerations for installing SupportAssist Enterprise ................................. 25
   Installing SupportAssist Enterprise by using the SupportAssist Enterprise installer package .......... 26
   Install SupportAssist Enterprise by using the OpenManage Essentials installation package ......... 31
   Upgrading SupportAssist Enterprise .............................................................................................. 32
      Upgrade SupportAssist Enterprise by using the SupportAssist Enterprise installation package .... 32
      Upgrade SupportAssist Enterprise by using the OpenManage Essentials installer package ......... 33
   Migrating to SupportAssist Enterprise ......................................................................................... 33
   Using SupportAssist Enterprise without registration .................................................................... 34
   Register SupportAssist Enterprise .................................................................................................. 34
   Set up an SELinux enabled system to receive alerts ...................................................................... 37
   Open the SupportAssist Enterprise user interface ..................................................................... 37
   Log in to SupportAssist Enterprise .............................................................................................. 38
   Log out of SupportAssist Enterprise ............................................................................................ 38

3 Adding devices ............................................................................................................................. 39
   Methods of adding devices ............................................................................................................. 39
   Device types and applicable devices ............................................................................................. 40
   Add a server or hypervisor .............................................................................................................. 41
   Add an iDRAC ................................................................................................................................ 44
   Add a chassis .................................................................................................................................. 45
   Add a Networking device ............................................................................................................... 47
   Add a PowerVault storage array ..................................................................................................... 48
Add an EqualLogic PS Series storage solution ................................................................. 49
Add a Compellent SC Series storage solution................................................................. 50
Add a Fluid File System NAS device ........................................................................... 51
Add a software ............................................................................................................ 52
Add a solution ............................................................................................................ 53
Add a virtual machine ............................................................................................... 54
SupportAssist Enterprise features available for virtual machines ......................... 55
Add a device by duplication ....................................................................................... 56

4 Managing device discovery rules .............................................................................. 59
Create device discovery rule ...................................................................................... 59
View the device discovery rule overview pane ......................................................... 61
Edit device discovery rule ......................................................................................... 62
Delete device discovery rule ..................................................................................... 63
Run the discovery rule ............................................................................................... 63

5 Viewing cases and devices ....................................................................................... 65
Viewing all support cases ......................................................................................... 65
View support cases for a specific device .................................................................... 66
Case management options ....................................................................................... 67
Request to suspend case activities for 24 hours ....................................................... 68
Request to resume support activities ....................................................................... 69
Request to close a support case .............................................................................. 69
View the device inventory ....................................................................................... 70
View the device overview pane .............................................................................. 71
Sorting the displayed data ........................................................................................ 72

6 Monitoring site health ............................................................................................. 73
View site health .......................................................................................................... 74
Current SupportAssist Enterprise Hostname Details ................................................ 74
Current SupportAssist Overview .............................................................................. 74
Sitewide Inventory Validation .................................................................................... 74
Network Connectivity ............................................................................................... 75
Extensions Tree View ............................................................................................... 75

7 Using Extensions ..................................................................................................... 76
Types of extensions ................................................................................................... 76
Support for setting up adapter or Remote Collector ............................................... 76
Getting started with adding devices managed by systems management consoles .... 77
Adapters overview ................................................................................................... 77
Set up OpenManage Essentials adapter ................................................................... 78
Set up the Microsoft System Center Operations Manager adapter ....................... 80
Management Packs for inventorying devices managed by Operations Manager .... 83
Set up OpenManage Enterprise adapter ................................................................... 83
View the adapter overview pane ............................................................................ 85
View devices inventoried by the adapter ................................................................... 85
Synchronize adapter ................................................................. 85
Edit adapter ........................................................................... 86
Delete adapter ....................................................................... 86
Approximate time required to assign Credential Profile .......... 87
Remote Collectors overview .................................................. 87
Minimum requirements for setting up a Remote Collector ...... 88
Set up Remote Collector ......................................................... 91
View collections for devices associated with a Remote Collector 93
View the Remote Collector overview pane ............................. 94
View devices associated with a Remote Collector ................. 94
Edit Remote Collector ............................................................. 95
Delete Remote Collector ........................................................ 96

8 Device grouping ..................................................................... 97
Predefined device groups ........................................................ 98
View device groups ............................................................... 98
Creating a device group ......................................................... 98
Manage devices in a device group ........................................... 99
Manage the credentials of a device group .............................. 100
View and update device group information ............................ 101
Delete a device group ........................................................... 102

9 Managing device credentials .............................................. 103
Account Credentials ............................................................. 103
Add Account Credentials ..................................................... 103
Reassign Account Credentials ............................................. 105
Edit Account Credentials ..................................................... 106
Delete Account Credentials ................................................ 106
Credential Profiles ............................................................... 107
Create Credential Profile ..................................................... 107
Assign Credential Profile ..................................................... 109
View devices associated with a Credential Profile ................. 109
Edit Credential Profile ........................................................ 109
Delete Credential Profile ..................................................... 110

10 Validating device inventory ............................................... 111
View the Site Inventory Validation page ............................... 111
Start inventory validation manually ..................................... 112
Schedule automatic inventory validation .............................. 112

11 Maintaining SupportAssist Enterprise capability ............... 113
Enable or disable monitoring of a device ............................. 113
Perform deep discovery ....................................................... 114
Install or upgrade OMSA by using SupportAssist Enterprise .. 115
Configure SNMP settings by using SupportAssist Enterprise .. 116
View and update the contact information ............................. 118
View and update parts dispatch information................................................................. 118
Integrate SupportAssist Enterprise with your TechDirect account................................ 119
Configure proxy server settings.................................................................................. 120
Connectivity test........................................................................................................... 121
View the connectivity status....................................................................................... 121
Perform the connectivity test...................................................................................... 122
Test the case creation capability................................................................................ 122
Clear the System Event Log....................................................................................... 122
Automatic update........................................................................................................ 124
Enable or disable automatic updates........................................................................ 124
Delete a device............................................................................................................ 125

12 Configuring email notifications.............................................................................. 127
Configure email notification settings.......................................................................... 127
Configure SMTP server settings................................................................................ 128
Types of email notifications....................................................................................... 128

13 Configuring collection settings............................................................................. 131
Prerequisites for collecting system information....................................................... 131
Enable or disable the automatic collection of system information on case creation... 132
Enable or disable the periodic collection of system information from all devices.... 132
Enable or disable the collection of identity information.......................................... 133
Enable or disable the collection of system information.......................................... 134
Enable or disable the automatic upload of collections............................................. 134

14 Viewing collections............................................................................................... 135
View a collection from the Devices page................................................................. 135
View a collection from the Collections page........................................................... 136
Refine collections based on a date range................................................................. 137
Configuration Viewer............................................................................................... 137
Log types................................................................................................................ 139
Items reported in periodic collections from servers.................................................. 139
Download and view a multiple device collection..................................................... 141

15 Using SupportAssist Enterprise to collect and send system information.......... 143
Set up SupportAssist Enterprise for collecting and sending system information...... 143
Start the collection of system information from a single device............................. 144
Start the collection of system information from multiple devices......................... 146
Upload a collection................................................................................................. 148
Upload a collection from a disconnected site......................................................... 148

16 Understanding maintenance mode...................................................................... 150
Global-level maintenance mode.............................................................................. 150
Device-level maintenance mode.............................................................................. 150
Enable or disable global-level maintenance mode.................................................. 151
Enable or disable device-level maintenance mode.................................................. 151
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>History of inventory validation</td>
<td>216</td>
</tr>
<tr>
<td>Device Groups page</td>
<td>216</td>
</tr>
<tr>
<td>Manage Devices</td>
<td>217</td>
</tr>
<tr>
<td>Create or Edit Device Group</td>
<td>218</td>
</tr>
<tr>
<td>Manage Device Discovery Rule</td>
<td>219</td>
</tr>
<tr>
<td>Create or Edit Device Discovery Rule</td>
<td>220</td>
</tr>
<tr>
<td>Discovery Rule Details</td>
<td>221</td>
</tr>
<tr>
<td>Discovery Rule Current Iteration Status</td>
<td>222</td>
</tr>
<tr>
<td>Recent Activity</td>
<td>222</td>
</tr>
<tr>
<td>Current versus Previous Discovery Rule Status</td>
<td>222</td>
</tr>
<tr>
<td>Manage Account Credentials</td>
<td>223</td>
</tr>
<tr>
<td>Add Account Credentials</td>
<td>224</td>
</tr>
<tr>
<td>Edit Account Credentials</td>
<td>225</td>
</tr>
<tr>
<td>Manage Credential Profiles</td>
<td>226</td>
</tr>
<tr>
<td>Add Credential Profile</td>
<td>227</td>
</tr>
<tr>
<td>Edit Credential Profile</td>
<td>227</td>
</tr>
<tr>
<td>Collections page</td>
<td>228</td>
</tr>
<tr>
<td>Collection overview pane</td>
<td>230</td>
</tr>
<tr>
<td>Extensions</td>
<td>230</td>
</tr>
<tr>
<td>Adapters</td>
<td>230</td>
</tr>
<tr>
<td>Remote Collectors</td>
<td>235</td>
</tr>
<tr>
<td>Settings</td>
<td>238</td>
</tr>
<tr>
<td>Proxy Settings</td>
<td>239</td>
</tr>
<tr>
<td>Preferences</td>
<td>239</td>
</tr>
<tr>
<td>Contact Information</td>
<td>242</td>
</tr>
<tr>
<td>TechDirect Login</td>
<td>243</td>
</tr>
<tr>
<td>SMTP Settings</td>
<td>244</td>
</tr>
<tr>
<td>Network Connectivity Test</td>
<td>244</td>
</tr>
<tr>
<td>SupportAssist Enterprise test</td>
<td>245</td>
</tr>
</tbody>
</table>

23 Error code appendix ........................................................................................................ 247

24 Related documents and resources ..................................................................................... 270

Video tutorials ......................................................................................................................... 270
SupportAssist community .......................................................................................................... 271
Accessing documents from the Dell EMC support site ............................................................... 271
Contacting Dell .......................................................................................................................... 271
SupportAssist Enterprise is an application that automates technical support for your Dell server, storage, and networking devices. SupportAssist Enterprise monitors your 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. SupportAssist Enterprise automatically collects the system state information required for troubleshooting the issue and sends it securely to Dell. 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, Microsoft System Center Operations Manager (SCOM), or OpenManage Enterprise.

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

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

**NOTE:** In this document, the term *local system* refers to the server where SupportAssist Enterprise is installed; *remote device* refers to any other device 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 link**

System information collected by SupportAssist Enterprise

**What is new in this release**

- Retention of installer and migration logs while upgrading SupportAssist Enterprise, for troubleshooting purposes
- Support for additional device models, operating systems, and newer firmware versions
- Support for newer collection attributes from Server, Storage, and Networking devices

**Overview of supported device types**

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

**NOTE:** SupportAssist Enterprise can monitor hardware issues on Dell server, Dell networking, Storage MD series, and Storage PS series devices. For Storage MD Series devices, monitoring of hardware issues is supported when the device is added either directly or through the OpenManage Essentials adapter. For Storage PS Series devices, monitoring of hardware issues is supported only if the device is added through the OpenManage Essentials adapter. For more information on adapters, see Using Extensions. Automatic case creation is supported only for devices that are monitored by SupportAssist Enterprise.
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.

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 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

NOTE: Remote monitoring, case creation, and periodic collection of system information from Storage SC Series devices is supported through the SupportAssist solution that is available on the device.

- Servers
  - 9th and later generations of PowerEdge servers
  - PowerEdge C Series servers
  - Datacenter Scalable Solutions
  - Storage NX devices
  - Storage DL devices
  - OEM-ready servers
- Storage
  - Storage PS Series arrays (previously EqualLogic)
  - Storage MD Series arrays (previously PowerVault)
  - Storage ME4 Series arrays
  - Storage SC Series arrays (previously Compellent)
  - Fluid File System (FluidFS) Network attached storage (NAS) devices
  - OEM-ready storage devices
- Networking
  - PowerConnect switches
  - Force10 switches
  - Dell Networking switches
  - Networking X-Series switches
  - Networking Wireless Controllers Mobility Series
  - Other supported Networking devices (Brocade and Cisco)
- Chassis
  - PowerEdge FX2/FX2s
  - PowerEdge VRTX
  - PowerEdge M1000e
  - PowerEdge MX7000
- Software
  - HIT Kit / VSM for VMware
  - SAN HQ
  - vCenter
  - SCVMM
- Solution
  - XC Series of web-scale hyper-converged appliances

NOTE: You can also add non-Dell branded servers or non-Dell Networking devices in SupportAssist Enterprise. For such servers and devices, only collection of host information is supported.
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.

**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](#).

**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.

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

SupportAssist Enterprise capabilities available with Dell service contracts

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

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

<table>
<thead>
<tr>
<th>SupportAssist Enterprise capability</th>
<th>Description</th>
<th>Basic Hardware</th>
<th>ProSupport</th>
<th>ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive detection of hardware failures</td>
<td>SupportAssist Enterprise receives alerts for hardware events that occur in monitored devices and proactively determines if the alerts indicate a hardware failure.</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Predictive detection of hardware failures*</td>
<td>Intelligent analysis of system information collected from a monitored device is used to predict hardware failures that may occur in future.</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Automated collection of system information</td>
<td>The system information required for troubleshooting an issue is automatically collected and sent to Dell.</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>SupportAssist Enterprise capability</td>
<td>Description</td>
<td>Basic Hardware</td>
<td>ProSupport</td>
<td>ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>collected from the monitored device and sent securely to Dell.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated support case creation</td>
<td>When a hardware failure is detected either proactively or predictively, a Service Request is automatically created with Technical Support.</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Automated email notification</td>
<td>An email notification about the support case or issue is automatically sent to your company’s primary and secondary SupportAssist Enterprise contacts.</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Proactive response from Technical Support</td>
<td>A Technical Support agent contacts you proactively about the support case and helps you resolve the issue.</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Proactive parts dispatch</td>
<td>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 based on the dispatch preferences that you configure in SupportAssist Enterprise.</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ProSupport Plus reporting</td>
<td>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.</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

**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 10. 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](http://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 View 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 Enable or disable the collection of identity information and Enable or disable 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
- Download the SupportAssist Enterprise installation package
- Installing or Upgrading 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
- Register SupportAssist Enterprise
- Set up an SELinux enabled system to receive alerts
- Open the SupportAssist Enterprise user interface
- Log in to SupportAssist Enterprise
- Log 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 Download the SupportAssist Enterprise installation package.
2. Review the requirements for installing SupportAssist Enterprise. See Minimum requirements for installing and using SupportAssist Enterprise.
4. (Optional) Complete the registration of SupportAssist Enterprise. See Register SupportAssist Enterprise.

**CAUTION:** Completing the registration is a prerequisite to receive 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 Install or upgrade OMSA by using SupportAssist Enterprise.
   b. Configure the SNMP settings of the local system. See Configure SNMP settings by using SupportAssist Enterprise.
   c. Enable SupportAssist Enterprise to monitor hardware issues that may occur on the local system. See Enable or disable monitoring of a device.
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 Add devices.
4. (Optional) Set up an adapter to inventory and add devices from OpenManage Essentials, Microsoft System Center Operations Manager (SCOM), or OpenManage Enterprise. See Adapters.
5. (Optional) If you have more than 4,000 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 Configure the SMTP server settings.
7. (Optional) If you want to manage SupportAssist Enterprise alerts in TechDirect, set up TechDirect. See Managing SupportAssist Enterprise alerts in TechDirect.

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 Enable or disable 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 Enable or disable 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 Enable or disable 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 View 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 Enable or disable the collection of identity information.
- You can disable the collection of software information and the system log from certain devices. See Enable or disable the collection of system information.
- You can disable the periodic collection of system information from all devices. See Enable or disable 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 Enable or disable the automatic collection of system information.
- You can also prevent the upload of collections. See Disable 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.

**Download the SupportAssist Enterprise installation package**

**Prerequisite**
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.
   The Dell SupportAssist portal is displayed.
2. In the Available Versions section, click the Learn More link that is displayed under SupportAssist for Enterprise Systems.
   The SupportAssist for enterprise systems 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 or Upgrading 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.
- If you have already installed SupportAssist Enterprise version 1.1 or 1.2, upgrade to SupportAssist Enterprise version 2.0.21. For more information, see Upgrading SupportAssist Enterprise.
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 by either collection of system information only or both monitoring and collection of system information

You can install SupportAssist Enterprise on a Virtual Machine (VM) or on a 9th or later generation PowerEdge server.

NOTE: For more information on the hardware requirements for installing and using SupportAssist Enterprise, see the Dell EMC SupportAssist Enterprise Version 2.0.21 User’s Guide at Dell.com/ServiceabilityTools.

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

<table>
<thead>
<tr>
<th>Devices</th>
<th>Monitoring</th>
<th>Collecting System Information</th>
<th>Processor</th>
<th>Installed memory (RAM)</th>
<th>Hard drive (free space)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>1 core</td>
<td>4 GB</td>
<td>1 GB</td>
</tr>
<tr>
<td>20</td>
<td>Yes</td>
<td>Yes</td>
<td>2 cores</td>
<td>4 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Up to 100</td>
<td>Yes</td>
<td>Yes</td>
<td>4 cores</td>
<td>8 GB</td>
<td>12 GB</td>
</tr>
<tr>
<td>Up to 300</td>
<td>Yes</td>
<td>Yes</td>
<td>4 cores</td>
<td>8 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Up to 1000</td>
<td>Yes</td>
<td>Yes</td>
<td>8 cores</td>
<td>8 GB</td>
<td>60 GB</td>
</tr>
<tr>
<td>Up to 4000</td>
<td>Yes</td>
<td>Yes</td>
<td>8 cores</td>
<td>16 GB</td>
<td>90 GB</td>
</tr>
</tbody>
</table>

NOTE: You can extend the monitoring and collection capabilities of SupportAssist Enterprise for up to 18,000 devices by setting up multiple remote collectors.

NOTE: For monitoring more than 100 devices in your environment, Dell recommends that you install SupportAssist Enterprise on a 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.
NOTE: If SupportAssist Enterprise is installed in a virtual environment, hardware resources of the system such as processor, memory, and I/O are shared among the virtual machines. Therefore, more hardware resources may be utilized by the virtual machine where SupportAssist Enterprise is installed. For optimal performance, ensure that you allocate dedicated processor and memory to the VM as specified in the hardware requirements for SupportAssist Enterprise.

To change the amount of processor resources allocated to a VM by using the shares, reservations, and limits settings, see the following:

- For ESX, see the "Allocate CPU Resources" section in the VMware vSphere documentation at docs.vmware.com.
- For Hyper-V, see the "Hyper-V CPU Scheduling" blog post at msdn.microsoft.com.
- For other virtual environments, see the respective documentation.

The following table provides a summary of the minimum hardware requirements on the server running SupportAssist Enterprise for performing multiple device collections.

Table 3. Hardware requirements for performing multiple device collections

<table>
<thead>
<tr>
<th>Devices</th>
<th>Processor</th>
<th>Installed memory (RAM)</th>
<th>Hard drive (free space)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 30 devices</td>
<td>2 cores</td>
<td>4 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Up to 50 devices</td>
<td>4 cores</td>
<td>8 GB</td>
<td>15 GB</td>
</tr>
<tr>
<td>Up to 100 devices</td>
<td>8 cores</td>
<td>8 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>Up to 300 devices</td>
<td>8 cores</td>
<td>16 GB</td>
<td>75 GB</td>
</tr>
</tbody>
</table>

NOTE: Performing a multiple device collection for Deployment, System Maintenance, or Consulting purposes may result in high system resource utilization at irregular intervals.

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

NOTE: SupportAssist Enterprise can only 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
- Windows Server 2019 Essentials and Datacenter
- Windows 2008 Small Business Server
- Windows 2011 Small Business Server
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016
NOTE: SupportAssist Enterprise can also be installed on a Microsoft Windows domain controller.

**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
- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Server 12 SP1
- SUSE Linux Enterprise Server 12 SP2
- SUSE Linux Enterprise Server 12 SP3
- 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
- Debian 7.x
- Debian 8.x
- Debian 9.x
- Ubuntu 14.x
- Ubuntu 16.04.x
- Ubuntu 18.04.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
- Google Chrome 59 or later
- Microsoft Edge 38 or later

NOTE: Transport Layer Security (TLS) version 1.1 or later must be enabled on the web browser.

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 networking 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://is.us.dell.com/*` — The file upload server and related services.
- `https://downloads.dell.com/*` — For downloading Dell OpenManage Server Administrator (OMSA) and receiving new SupportAssist Enterprise release information, policy files, and product support files.

[NOTE: The downloads.dell.com page uses the Akamai third-party vendor for improved download experience.]


[NOTE: During registration, SupportAssist Enterprise verifies connectivity to the Internet by trying to connect to `http://www.dell.com`, which then gets redirected to `https://www.dell.com`.]

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

### Table 4. Network bandwidth requirements

<table>
<thead>
<tr>
<th>Devices</th>
<th>Monitoring</th>
<th>Collecting System Information</th>
<th>LAN bandwidth*</th>
<th>WAN bandwidth**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>10 Mbps</td>
<td>5 Mbps</td>
</tr>
<tr>
<td>20</td>
<td>Yes</td>
<td>Yes</td>
<td>0.5 Gbps</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Up to 100</td>
<td>Yes</td>
<td>Yes</td>
<td>0.5 Gbps</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Up to 300</td>
<td>Yes</td>
<td>Yes</td>
<td>0.5 Gbps</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Up to 1000</td>
<td>Yes</td>
<td>Yes</td>
<td>1 Gbps</td>
<td>20 Mbps</td>
</tr>
<tr>
<td>Up to 4000</td>
<td>Yes</td>
<td>Yes</td>
<td>1 Gbps</td>
<td>20 Mbps</td>
</tr>
</tbody>
</table>

* 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 figure illustrates network port connectivity between SupportAssist Enterprise and other monitored devices.
Figure 1. Managed devices

- 1 — Network ports required for discovering devices and collecting system information
- 2 — Network ports required for uploading the collected system information (collection)
- 3 — Network ports required for adapters
- 4 — Network ports on devices for collecting system information

The following table lists the network ports required for discovering devices and collecting system information.
<table>
<thead>
<tr>
<th>Device</th>
<th>Protocol for discovery and collection</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server - Windows</td>
<td>WMI</td>
<td>135</td>
</tr>
<tr>
<td>Server - Linux</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>ESX or ESXi</td>
<td>SSH and VMware SDK</td>
<td>22 and 443</td>
</tr>
<tr>
<td>Storage PS Series arrays (previously EqualLogic)</td>
<td>SNMPv2, SSH2, and FTP</td>
<td>161, 22, and 21</td>
</tr>
<tr>
<td>Storage MD Series arrays (previously PowerVault)</td>
<td>SYMbolSDK</td>
<td>2463</td>
</tr>
<tr>
<td>Storage ME4 Series arrays</td>
<td>REST and SFTP</td>
<td>443 and 1022</td>
</tr>
<tr>
<td>Storage SC Series arrays (previously Compellent)</td>
<td>REST</td>
<td>3033</td>
</tr>
<tr>
<td>Fluid File System (FluidFS) Network attached storage (NAS) devices</td>
<td>SSH and FTP</td>
<td>22 and 44421</td>
</tr>
<tr>
<td>PowerConnect switches</td>
<td>SNMP and SSH</td>
<td>22 and 161</td>
</tr>
<tr>
<td>Force10 switches</td>
<td>SNMP and SSH</td>
<td>161 and 22</td>
</tr>
<tr>
<td>Networking switches</td>
<td>SNMP and SSH</td>
<td>22 and 161</td>
</tr>
<tr>
<td>W series switches</td>
<td>SNMP and SSH</td>
<td>22 and 161</td>
</tr>
<tr>
<td>PowerEdge FX2/FX2s</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>PowerEdge VRTX</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>PowerEdge M1000e</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>PowerEdge MX7000</td>
<td>REST</td>
<td>443</td>
</tr>
<tr>
<td>SAN HQ</td>
<td>WMI</td>
<td>135</td>
</tr>
<tr>
<td>HIT Kit / VSM for VMware</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>vCenter</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>SCVMM</td>
<td>WMI</td>
<td>135</td>
</tr>
<tr>
<td>XC Series of Web-Scale hyper-converged appliances</td>
<td>REST and SSH</td>
<td>9440 and 22</td>
</tr>
<tr>
<td>Virtual Machine - Windows</td>
<td>WMI</td>
<td>135</td>
</tr>
<tr>
<td>Virtual Machine - Linux</td>
<td>SSH</td>
<td>22</td>
</tr>
</tbody>
</table>

The following table lists the network ports required for uploading the collected system information.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SupportAssist Enterprise</td>
<td>SupportAssist Server</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>File Upload Server (FUS)</td>
<td></td>
</tr>
</tbody>
</table>
### Table 7. Network ports required for adapters

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SupportAssist Enterprise</td>
<td>OpenManage Essentials adapter</td>
<td>5700 (web socket)</td>
</tr>
<tr>
<td>OpenManage Essentials adapter</td>
<td>OpenManage Essentials</td>
<td>443</td>
</tr>
<tr>
<td>SupportAssist Enterprise</td>
<td>System Center Operations Manager adapter</td>
<td>5700 (web socket)</td>
</tr>
<tr>
<td>System Center Operations Manager adapter</td>
<td>System Center Operations Manager</td>
<td>Not applicable (SCOM SDK)</td>
</tr>
<tr>
<td>SupportAssist Enterprise</td>
<td>OpenManage Enterprise</td>
<td>443</td>
</tr>
</tbody>
</table>

The following table lists the network ports required for collecting system information.

### Table 8. Network ports on devices for collecting system information

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage SC Series arrays (previously Compellent)</td>
<td>SupportAssist Enterprise</td>
<td>5701, 5702, 5703, and 5704</td>
</tr>
<tr>
<td>Server SupportAssist agent</td>
<td>SupportAssist Enterprise</td>
<td>5701, 5702, 5703, and 5704</td>
</tr>
<tr>
<td>Server (In band)</td>
<td>SupportAssist Enterprise</td>
<td>5701, 5702, 5703, and 5704</td>
</tr>
</tbody>
</table>

## 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 installed on a Linux operating system, servers running a Windows operating system can only be added in SupportAssist Enterprise with the device type as iDRAC. For instructions to add an iDRAC, 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 9. Features available based on the operating system where SupportAssist Enterprise is installed

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum device support</td>
<td>Up to 18,000 devices</td>
<td>Up to 18,000 devices</td>
</tr>
<tr>
<td>Adding devices</td>
<td>Adding all device types is supported</td>
<td>Adding all device types is supported, except for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Servers running Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SCVMM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SAN HQ</td>
</tr>
<tr>
<td>Installing or upgrading OMSA on a remote server through SupportAssist Enterprise</td>
<td>Supported on Windows and Linux operating systems</td>
<td>Supported on Linux operating systems only</td>
</tr>
<tr>
<td>Set up Remote Collectors to enable a remote device to collect and upload system information to Dell</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Set up adapters to inventory and add devices that are managed by OpenManage Essentials, Microsoft System Center Operations Manager, or OpenManage Enterprise</td>
<td>Supported</td>
<td>Supported (For OpenManage Enterprise only)</td>
</tr>
</tbody>
</table>

NOTE: For more information about setting up adapters and Remote Collectors, see Using Extensions.

Installing SupportAssist Enterprise by using the SupportAssist Enterprise installer package

Install SupportAssist Enterprise on Windows

Prerequisites

- Download the SupportAssist Enterprise installation package for Windows operating systems. See Download 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 Next.

The Destination Folder page is displayed.

5 The default installation folder for SupportAssist Enterprise is <Drive where SupportAssist Enterprise is installed>\Program Files\Dell\SupportAssist. If you want to install SupportAssist Enterprise on any other location, click Browse and select a folder.

6 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.

7 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.

8 Click Finish to exit the SupportAssist Enterprise installer.

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

![Login page](image)

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 Open 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.

9 Enter the Microsoft Windows operating system user name and password, and then click Login.

The SupportAssist Enterprise Registration Wizard is displayed.

NOTE: The server or virtual machine where you have installed SupportAssist Enterprise is automatically added as a device.

Next step (Optional) Follow the instructions in the SupportAssist Enterprise Registration Wizard to complete the registration of SupportAssist Enterprise.
Install SupportAssist Enterprise on Windows Server Core

Prerequisites

- You must be logged in to a system that has PowerShell ISE version 5.1 or later.
- You must be logged in to the system with Administrator Privileges.
- You must have the SupportAssist Enterprise installation package for Windows.

About this task

You can install SupportAssist Enterprise by remotely accessing the system running Windows Server Core.

Steps

1. Open the PowerShell ISE window.
2. Type `get-service winrm` and press Enter.
3. Type `Enable-PSRemoting -force` and press Enter.
4. Type `set-item wsman:\localhost\Client\TrustedHosts -value "<Windows Server Core Operating System IP address>" -Force` and press Enter.
   Example: `set-item wsman:\localhost\Client\TrustedHosts -value "10.49.18.20" -Force`
5. Type `$TargetSession = New-PSSession -ComputerName "<Windows Server Core Operating System IP address>" -Credential ~\<Username>` and press Enter.
   Example: `$TargetSession = New-PSSession -ComputerName "10.49.18.20" -Credential ~\Administrator`
6. Type `Enter-PSSession -ComputerName <HostName/IP address of the Windows Server Core device> -Credential ~\<Username of Windows Server Core machine>` and press Enter.
   Example: `Enter-PSSession -ComputerName "10.49.18.20" -Credential ~\Administrator`
7. Type the password and press Enter.
8. Create a folder.
9. Type `Exit` and press Enter to end the remote connection.
10. To copy the installer file to Windows Server Core, type `Copy-Item -ToSession $TargetSession -Path "<Location where the SupportAssist Enterprise installer is available>" -Destination "<Destination Path>" -Recurse` and press Enter.
   Example: `Copy-Item -ToSession $TargetSession -Path "C:\installer\SupportAssistEnterprise_2.0.10.exe" -Destination "C:\Users \Administrator\Documents\SupportAssistEnterprise_2.0.10.exe" -Recurse`
11. To enable remote login, type `set-itemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -name "UserAuthentication" -Value 1` and press Enter.
12. Open a remote desktop connection to the system running Windows Server Core and run the SupportAssist Enterprise installer.exe file.

Install SupportAssist Enterprise on 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.

On Debian operating systems, ensure that `en_US.utf8` locale package is installed.
- If locales are not installed, use the `apt-get install locales` command to install the locales.
- If any other locale is installed, you can install the `en_US.utf8` locale by using the `dpkg-reconfigure locales` command.

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_2.x.x.bin` and press Enter.
   - Type `chmod +x supportassistenterprise_2.x.x.bin` and press Enter.
4. Type `/supportassistenterprise_2.x.x.bin` and press Enter.
   The Welcome to the SupportAssist Enterprise Installer message is displayed.
5. To continue, type c.
   The SupportAssist Enterprise License Agreement is displayed.
6. Read the license agreement and type y to start the installation.

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.

![SupportAssist Enterprise Login Page](image)

**Figure 3. 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`

  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`

  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 step
(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 receive 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.

Install SupportAssist Enterprise on Linux in silent mode

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 Install 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.
- On Debian operating systems, ensure that en_US.utf.8 locale package is installed.
  - If locales are not installed, use the `apt-get install locales` command to install the locales.
  - If any other locale is installed, you can install the en_US.utf.8 locale by using the `dpkg-reconfigure locales` command.

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_2.x.x.bin` and press Enter.
   - Type `chmod +x supportassistenterprise_2.x.x.bin` and press Enter.
4 Type `./supportassistenterprise_2.x.x.bin silent` and press Enter.

Next step
(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 receive 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.
Install 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/*
  - https://downloads.dell.com/*
  - https://sa-is.us.dell.com/*

**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 `<System drive>:\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 2.5 or later 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**.
6. The **License Agreement** window is displayed.
7. Read the terms in the communication requirements and click **I Agree**.
8. 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.
9. Click **Finish**.

**Next step**

(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 receive 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 1.1 or 1.2, you can upgrade to SupportAssist Enterprise version 2.0.21 by using one of the following installation packages:

- SupportAssist Enterprise version 2.0.21 installation package available at Dell.com/SupportAssistGroup.
- OpenManage Essentials installation package available at DellTechCenter.com/OME.

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

Upgrade SupportAssist Enterprise by using the SupportAssist Enterprise installation package

**Prerequisite**
The system must have internet connectivity.

**Steps**

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.

   **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.
NOTE: If a newer version of the adapter or Remote Collector is available, the adapter or Remote Collector is also upgraded during the upgrade of SupportAssist Enterprise.

NOTE: If previous version on SupportAssist Enterprise was installed in a custom folder path, the upgraded version of SupportAssist Enterprise is also installed in the same custom folder path.

Upgrade SupportAssist Enterprise by using the OpenManage Essentials installer package

Prerequisite
The system must have internet connectivity.

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

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.

NOTE: If a newer version of the adapter or Remote Collector is available, the adapter or Remote Collector is also upgraded during the upgrade of SupportAssist Enterprise.

Migrating to SupportAssist Enterprise

If you are already using 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 also migrated.

NOTE: Direct migration from SupportAssist for OpenManage Essentials or SupportAssist for Microsoft System Center Operations Manager to SupportAssist Enterprise version 2.0.1 is not supported. If necessary, migrate to SupportAssist Enterprise version 1.1 or 1.2, and then upgrade to SupportAssist Enterprise version 2.0.1. For information on migrating to SupportAssist Enterprise version 1.1 or 1.2, see the SupportAssist Enterprise Version 1.2 User's Guide at Dell.com/ServiceabilityTools.
Using SupportAssist Enterprise without registration

Registration of SupportAssist Enterprise is a prerequisite to receive 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>
<thead>
<tr>
<th>Capabilities or features that are available</th>
<th>Capabilities or features that are not available</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Add devices</td>
<td>• Monitor devices for hardware issues</td>
</tr>
<tr>
<td>• Manually start the collection and upload</td>
<td>• Automatic case creation on issue detection</td>
</tr>
<tr>
<td>of system information to Dell from a</td>
<td>• Automated periodic collection of system</td>
</tr>
<tr>
<td>single device or multiple devices</td>
<td>information</td>
</tr>
<tr>
<td></td>
<td>• View support cases that are open for your</td>
</tr>
<tr>
<td></td>
<td>devices</td>
</tr>
<tr>
<td></td>
<td>• Update contact and parts dispatch information</td>
</tr>
<tr>
<td></td>
<td>• Set up adapter</td>
</tr>
<tr>
<td></td>
<td>• Set up Remote Collector</td>
</tr>
<tr>
<td></td>
<td>• Set up automated parts dispatch</td>
</tr>
</tbody>
</table>

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

Register 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 receive 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 cannot monitor your devices for hardware issues or 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, 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 by trying to connect to **http://www.dell.com**, which then gets redirected to **https://www.dell.com**.
   - If SupportAssist Enterprise can 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 hostname 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.

3 On the **Registration** page, provide the following information:
   a. In the **Company Information** section, type the company name, and select your country or territory, in the appropriate fields.
   b. In the **IT Administrator Contact Information** section, type your first name, last name, phone number, alternate phone number, and email address in the appropriate fields.
   c. From the **Time zone** list, select the time zone.

   **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 EMC contacts 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 about updating the contact information, see **View and update the contact information**.

4 Click **Next**.

The **Parts Replacement Preferences for Dell Servers** page is displayed.
By default, the I want Dell server replacement parts shipped automatically is selected. If you clear the option, the shipment of Dell server replacement parts could be delayed.

5. To copy the already provided contact information, click the appropriate link.

The Primary Shipping Contact information is populated.

6. In the Secondary Shipping Contact section, type the first name, last name, phone number, and email address of the secondary contact.

   **NOTE:** Contact details of the primary and secondary contact must be unique.

7. In the Shipping Address section, perform the following:
   a. Select the preferred contact hours during which Dell can contact you, if necessary.
   b. Select the time zone, country, and type your shipping address in the appropriate fields.
   c. Type any specific dispatch related information in the Dispatch Notes section.

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

   d. If you want an onsite technician to replace the dispatched hardware component, select I want a technician to replace my parts onsite (if included in my service plan).

8. Click Next.

The Integrate With TechDirect (Optional) page is displayed.

9. Select I agree to integrate SupportAssist Enterprise with TechDirect, and perform the following:
   a. Click Sign In to log in to your company’s TechDirect Administrator account to get the One-Time Password (OTP).
   b. Enter the OTP to verify your TechDirect account.

10. Click Submit.

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.

11. Click Finish.

The SupportAssist Enterprise Site Health page is displayed.

**Next steps**

- To enable 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 Install or upgrade OMSA by using SupportAssist Enterprise.
  b. Configure the SNMP settings of the local system. See Configure SNMP settings by using SupportAssist Enterprise.
  c. Enable SupportAssist Enterprise to monitor hardware issues that may occur on the local system. See Enable or disable 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 Set up an SELinux enabled system to receive alerts.

- Add devices in SupportAssist Enterprise. For more information, see Adding devices.

- (Optional) If your company uses an SMTP server (email server), configure the SMTP server settings in SupportAssist Enterprise. This enables SupportAssist Enterprise to use the SMTP server to send you device status and connectivity status email notifications. For more information, see Configure the SMTP server settings.

- (Optional) Update the contact details of the primary and secondary SupportAssist Enterprise contacts and provide a parts dispatch address. See View and update 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.

**Related links**

- View and update parts dispatch information
- Open the SupportAssist Enterprise user interface
Set 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, SUSE Linux Enterprise Server 12, 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:

```plaintext
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.

Open 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 SupportAssist Enterprise desktop icon.
  - Open a web browser and type the address in the following format:
    ```plaintext
    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:
  ```plaintext
  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.

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

### Log in to SupportAssist Enterprise

#### Prerequisite
You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See Granting elevated or administrative privileges to users.

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

   - **NOTE:** 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 Site Health 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.

### Log 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 or virtual machine 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 add each device in SupportAssist Enterprise.

**NOTE:** For the complete list of device types and device models that you can add in SupportAssist Enterprise, see the SupportAssist Enterprise Version 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

**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.

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

**NOTE:** If the device is part of a domain, you must configure its Domain Name System (DNS) correctly to view the host name in the Devices page.

Topics:
- Methods of adding devices
- Device types and applicable devices
- Add a server or hypervisor
- Add an iDRAC
- Add a chassis
- Add a Networking device
- Add a PowerVault storage array
- Add an EqualLogic PS Series storage solution
- Add a Compellent SC Series storage solution
- Add a Fluid File System NAS device
- Add a software
- Add a solution
- Add a virtual machine
- Add a device by duplication

**Methods of adding devices**

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

- Add a single device — Add each device individually by entering details of the device
- Create a device discovery rule — Add devices based on a specific IP address ranges. For more information on discovery rules, see Managing device discovery rules.
Device types and applicable devices

While adding devices 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.

1. **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 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Devices that you can add</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>• PowerEdge M1000e</td>
</tr>
<tr>
<td></td>
<td>• PowerEdge VRTX</td>
</tr>
<tr>
<td></td>
<td>• PowerEdge FX2/FX2s</td>
</tr>
<tr>
<td></td>
<td>• PowerEdge MX7000</td>
</tr>
<tr>
<td>Fluid File System (FluidFS)</td>
<td>• Storage PS Series with FluidFS</td>
</tr>
<tr>
<td></td>
<td>• Storage MD Series with FluidFS</td>
</tr>
<tr>
<td></td>
<td>• Storage SC Series with FluidFS</td>
</tr>
<tr>
<td>iDRAC</td>
<td>12th and later generations of PowerEdge servers</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> To add an iDRAC, you must provide the iDRAC IP address of the server.</td>
</tr>
<tr>
<td>Networking</td>
<td>• PowerConnect</td>
</tr>
<tr>
<td></td>
<td>• Force10</td>
</tr>
<tr>
<td></td>
<td>• Dell Networking</td>
</tr>
<tr>
<td></td>
<td>• Networking X-Series switches</td>
</tr>
<tr>
<td></td>
<td>• Networking Wireless Controllers Mobility Series</td>
</tr>
<tr>
<td></td>
<td>• Other supported Networking devices (Brocade and Cisco)</td>
</tr>
<tr>
<td>Peer Storage (PS) / EqualLogic</td>
<td>Storage PS Series arrays</td>
</tr>
<tr>
<td>PowerVault</td>
<td>• Storage MD Series arrays</td>
</tr>
<tr>
<td></td>
<td>• Storage ME4 Series arrays</td>
</tr>
<tr>
<td>Server / Hypervisor</td>
<td>9th or later generation of PowerEdge servers running:</td>
</tr>
<tr>
<td></td>
<td>• Windows</td>
</tr>
<tr>
<td></td>
<td>• Linux</td>
</tr>
<tr>
<td></td>
<td>• VMware ESX or ESXi</td>
</tr>
<tr>
<td></td>
<td>• Citrix XenServer</td>
</tr>
<tr>
<td></td>
<td>• Oracle Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Hyper-V</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> To add a Server / Hypervisor, you must provide the operating system IP address of the server.</td>
</tr>
</tbody>
</table>
### Add 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, Ctxix 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](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 wizard is displayed.
3. From the Select device type list, select Server / Hypervisor.

Figure 5. Add single device window

4. Type the host name or IP address 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. To discover and add other supported device types that may be associated with the server, select Perform deep discovery. See Deep discovery.
6. If desired, type a name for the device in the appropriate field.
   The name that 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.
7. Perform one of the following:
   - If you selected the Perform deep discovery option, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, select Create New Profile and click Create. To enter the profile details, follow steps 3 to 7 in Create Credential Profile.
   - If you did not select the Perform deep discovery option, select the Account Credentials that you want to assign to the device. To create new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.
8. 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.

1. **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.

9. 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.

10. 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**.

11. Click **Finish**.

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

12. 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 **Add 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 **Success**. 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 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 **Add 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. Perform inventory validation on the device. See Start inventory validation manually.

Related links
- Add Single Device
- Deep discovery

Add 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.
- To add an iDRAC7 or iDRAC8, Enterprise or Express license must be installed on the iDRAC. To add an iDRAC9, Basic, 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.

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.

1. 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 wizard is displayed.
3. From the Select device type list, select iDRAC.
4. Type the host name or IP address 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 that 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. From the Account Credentials list, select an account credentials that you want to assign to the device. To create a new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.
7. 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.

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

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**.
    **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.

1. **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 **Success**. If an issue occurs during the configuration of SNMP, the device displays an appropriate status in the **Devices** page.

2. **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 **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 **Add 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. Perform inventory validation on the device. See **Start inventory validation manually**.

**Related link**
- **Add Single Device**

**Add 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, 161, and 443 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
• Dell PowerEdge MX7000

Steps
1. Point to Devices and click View Devices.
   The Devices page is displayed.
2. Click Add Devices.
   The Add Single Device wizard is displayed.
3. From the Select device type list, select Chassis.
4. Type the host name or IP address 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. To discover and add other supported device types that may be associated with the chassis, select Perform deep discovery. See Deep discovery.
6. If desired, type a name for the device in the appropriate field.
   The name that 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.
7. Perform one of the following:
   • If you selected the Perform deep discovery option, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, select Create New Profile and click Create. To enter the profile details, follow steps 3 to 7 in Create Credential Profile.
   • If you did not select the Perform deep discovery option, select the Account Credentials that you want to assign to the device. To create new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.
8. 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 configure the alert destination of a chassis by using the web interface.]
9. 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.
10. 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.
11. Click Finish.
    The device is added to the device inventory and the Summary page is displayed.
12  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 configure 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. Perform inventory validation on the device. See Start inventory validation manually.

Related links

- Add Single Device
- Deep discovery

---

**Add 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.
- Port 22 and 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 wizard is displayed.
3. From the Select device type list, select Networking.
4. Type the host name or IP address 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. To discover and add other supported device types that may be associated with the networking device, select Perform deep discovery. See Deep discovery.
6. If desired, type a name for the device in the appropriate field.
   The name that 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.
7. Perform one of the following:
If you selected the **Perform deep discovery** option, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, select **Create New Profile** and click **Create**. To enter the profile details, follow steps 3 to 7 in [Create Credential Profile](#).

If you did not select the **Perform deep discovery** option, select the Account Credentials that you want to assign to the device. To create new account credentials, select **Create New Account** and click **Create**. To enter the account details, follow steps 3 to 6 in [Add Account Credentials](#).

8 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 configure the alert destination of a networking device](#).

9 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.

10 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](#).

11 Click **Finish**.

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

12 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 configure the alert destination of a networking device](#).

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

1 Ensure that all prerequisites for adding the device are met.
2 Perform inventory validation on the device. See [Start inventory validation manually](#).

**Related links**

- [Add Single Device](#)
- [Deep discovery](#)

**Add a PowerVault 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.
- For adding an Storage MD Series array, port 2463 must be open on the device.
- For adding an Storage ME4 Series array, port 443 must be open on the device.

**About this task**

SupportAssist Enterprise can collect system information from the Storage MD Series arrays and Storage ME4 Series arrays. By adding a Storage MD Series or Storage ME4 Series 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** wizard is displayed.

3. From the **Select device type** list, select **PowerVault**.

4. Type the host name or IP address 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. To discover and add other supported device types that may be associated with the device, select **Perform deep discovery**.

6. If desired, type a name for the device in the appropriate field.
   The name that 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.

7. Perform one of the following:
   - If you selected the **Perform deep discovery** option, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, select **Create New Profile** and click **Create**. To enter the profile details, follow steps 3 to 7 in **Create Credential Profile**.
   - If you did not select the **Perform deep discovery** option, select the Account Credentials that you want to assign to the device. To create new account credentials, select **Create New Account** and click **Create**. To enter the account details, follow steps 3 to 6 in **Add Account Credentials**.

   **NOTE:**
   - Account Credentials are mandatory for adding a Storage ME4 Series device.
   - Account Credentials are not required for adding a Storage MD Series device.

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 step

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. Perform inventory validation on the device. See **Start inventory validation manually**.

Related link

**Add 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 Storage PS Series (previously EqualLogic) arrays. By adding a Storage PS Series 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 wizard is displayed.
3. From the Select device type list, select Peer Storage (PS) / EqualLogic.
4. Type the host name or IP address of the Storage PS Series group 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. To discover and add other supported device types that may be associated with the Storage PS Series device, select Perform deep discovery. See Deep discovery.
6. If desired, type a name for the device in the appropriate field.
   The name that 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.
7. Perform one of the following:
   • If you selected the Perform deep discovery option, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, select Create New Profile and click Create. To enter the profile details, follow steps 3 to 7 in Create Credential Profile.
   • If you did not select the Perform deep discovery option, select the Account Credentials that you want to assign to the device. To create new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.
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 step
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. Perform inventory validation on the device. See Start inventory validation manually.

Related link
Add Single Device

Add 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 for Compellent devices with SC Series storage solution 7.1 and below.

About this task
SupportAssist Enterprise can only collect system information from the Storage SC Series solutions. By adding a Storage SC Series 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 wizard is displayed.
3. From the Select device type list, select Storage Center (SC) / Compellent.
4. Type the host name or IP address 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 that 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. From the Account Credentials list, select an account credentials that you want to assign to the device. To create a new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.
7. 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 step
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. Perform inventory validation on the device. See Start inventory validation manually.

Related link
Add Single Device

Add a Fluid File System 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:
- Storage SC Series
- Storage PS Series
- Storage MD Series

**Steps**
1. Point to Devices and click View Devices. The Devices page is displayed.
2. Click Add Devices. The Add Single Device wizard is displayed.
3. From the Select device type list, select Fluid File System (FluidFS).
4. Type the host name or IP address 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 that 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. From the Account Credentials list, select an account credentials that you want to assign to the device. To create a new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.
7. 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 step**
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. Perform inventory validation on the device. See Start inventory validation manually.

**Related link**
Add Single Device

**Add 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 / Virtual Storage Manager).

Steps
1. Point to Devices and click View Devices.
   The Devices page is displayed.
2. Click Add Devices.
   The Add Single Device wizard is displayed.
3. From the Select device type list, select Software.
4. From the Select Software type list, select the software type.
5. Type the host name or IP address 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.
6. If desired, type a name for the device in the appropriate field.
   The name that 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.
7. From the Account Credentials list, select an account credentials that you want to assign to the device. To create a new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.
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 step
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. Perform inventory validation on the device. See Start inventory validation manually.

Related link
Add Single Device

Add 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 9440 and 22 must be open on the device.
- For web-scale solution, 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 wizard is displayed.
From the Select device type list, select Web-Scale.

From the Select solution type list, select the solution.

Type the host name or IP address 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.

To discover and add other supported device types that may be associated with the solution, select Perform deep discovery. See Deep discovery.

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

The name that 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.

Perform one of the following:

- If you selected the Perform deep discovery option, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, select Create New Profile and click Create. To enter the profile details, follow steps 3 to 7 in Create Credential Profile.
- If you did not select the Perform deep discovery option, select the Account Credentials that you want to assign to the device. To create new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.

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 step**

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. Perform inventory validation on the device. See Start inventory validation manually.

**Related links**

Add Single Device
Deep discovery

**Add a virtual machine**

**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.
- The system hosting the virtual machine must be reachable from the server where SupportAssist Enterprise is installed.
- The virtual machine you want to add must be created on VMware ESX, ESXi, and Microsoft Hyper-V.

**About this task**

SupportAssist Enterprise can only collect system information from virtual machines. You can perform the following steps to add a virtual machine.

**Steps**

1. Point to Devices and click View Devices.
   The Devices page is displayed.
2. Click Add Devices.
   The Add Single Device wizard is displayed.
3. From the Select device type list, select Virtual Machine.
4 Type the host name or IP address 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 that 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 From the Account Credentials list, select an account credentials that you want to assign to the device. To create a new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.

7 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.

**Related link**
Add Single Device

---

**SupportAssist Enterprise features available for virtual machines**

The following table lists the SupportAssist Enterprise features that are available for virtual machines.

**Table 12. SupportAssist Enterprise features available for virtual machines**

<table>
<thead>
<tr>
<th>SupportAssist Enterprise features</th>
<th>Support status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add devices</td>
<td>✔️</td>
</tr>
<tr>
<td>Create device discovery rule</td>
<td>✔️</td>
</tr>
<tr>
<td>Collect software information</td>
<td>✔️</td>
</tr>
<tr>
<td>Collect system logs</td>
<td>✔️</td>
</tr>
<tr>
<td>Upload system information to Dell</td>
<td>✔️</td>
</tr>
<tr>
<td>Collect system information periodically</td>
<td>✔️</td>
</tr>
<tr>
<td>View device type filters in Devices and Collection page</td>
<td>✔️</td>
</tr>
<tr>
<td>Perform inventory validation</td>
<td>✔️</td>
</tr>
<tr>
<td>Revalidate a device</td>
<td>✔️</td>
</tr>
<tr>
<td>SupportAssist Enterprise features</td>
<td>Support status</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Edit device credentials</td>
<td>✓</td>
</tr>
<tr>
<td>Assign Credential profiles to devices</td>
<td>✓</td>
</tr>
<tr>
<td>Set up, edit, or delete an adapter or Remote Collector</td>
<td>✗</td>
</tr>
<tr>
<td>Perform deep discovery</td>
<td>✗</td>
</tr>
<tr>
<td>Install/upgrade OMSA by using SupportAssist Enterprise</td>
<td>✗</td>
</tr>
<tr>
<td>Monitor devices</td>
<td>✗</td>
</tr>
<tr>
<td>Create cases</td>
<td>✗</td>
</tr>
<tr>
<td>Collect hardware information</td>
<td>✗</td>
</tr>
<tr>
<td>Collect smart logs</td>
<td>✗</td>
</tr>
<tr>
<td>Clear SEL logs</td>
<td>✗</td>
</tr>
<tr>
<td>Enable or disable maintenance mode</td>
<td>✗</td>
</tr>
<tr>
<td>Configure SNMP by using SupportAssist Enterprise</td>
<td>✗</td>
</tr>
<tr>
<td>Graphic of the virtual machine type in the device overview page</td>
<td>✗</td>
</tr>
</tbody>
</table>

Add 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.
Figure 6. Duplicate option

The device overview pane is displayed.

3 Click Duplicate.
   The Duplicate Device wizard is displayed.

4 Type the host name or IP address 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 that 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 From the Account Credentials list, select an account credentials that you want to assign to the device. To create a new account credentials, select Create New Account and click Create. To enter the account details, follow steps 3 to 6 in Add Account Credentials.

7 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 step

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. Perform inventory validation on the device. See *Start inventory validation manually*. 
Managing device discovery rules

A device discovery rule enables you to discover and add devices that are present within one or more IP address ranges. Creating a device discovery rule helps you add multiple devices, and reduces the effort involved in adding each device individually.

Topics:
• Create device discovery rule
• View the device discovery rule overview pane
• Edit device discovery rule
• Delete device discovery rule
• Run the discovery rule

Create device discovery rule

Prerequisite
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 creating a discovery rule, you can discover and add devices based on IP address ranges or hostname. While you create the discovery rule, you can select a Credential Profile that must be applied to the devices. After creating the device discovery rule, you can run the rule immediately or based on a schedule to discover devices.

Steps
1. Point to Devices and click Manage Rules for Device Discovery.
   The Manage Discovery Rules page is displayed.
2. Click Create Discovery Rule.
   The Create Device Discovery Rule window is displayed.
3 Type a name for the discovery rule in the appropriate field.

4 From the Credential profile list, select a Credential Profile that contains the Account Credentials for the device types that are present within the IP address ranges. To create a new credential profile, select Create New Profile and click Create. To enter the profile details, follow steps 3 to 7 in Create Credential Profile.

5 To discover devices by using IP address ranges:
   a Select IP address / range.
   b Type the IP address or IP address range of the devices that you want to discover. To add another IP address range, click Add another range, and then type the IP address range of the devices.

   **NOTE:** You can add up to five different IP address ranges in the following formats:
   - 10.34.*.*
   - 10.34.1-10.*
   - 10.34.*.1-10
   - 10.34.1-10.1-10
   - 10.34.1.1/24

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

   **NOTE:** For an IP address entered in Classless-Inter Domain Routing (CIDR) notation, for example 10.34.1.1/24, the subnet mask entry is not considered.

   c Type the Subnet Mask of the specified IP address range in the appropriate field.

6 To discover devices by using the hostname or IP addresses:
   a Select Devices.
   b Enter the hostname or IP address of devices as comma-separated values in the following formats:
      - 10.34.10.2, 10.34.10.3, 10.34.10.22
      - hostname1, hostname2, hostname3
      - 10.34.10.22, hostname2, 10.34.10.24

7 Select an option based on your preference:
   - Run now — Discover the devices immediately.
   - Run once — Discover the devices at a specific date and time.
Recur — Schedule the discovery of devices at periodic intervals.

8 Click Next.

The Discovering Devices window is displayed. Based on the device types included in the Credential Profile, the device types are selected automatically.

9 If desired, clear the device types that you do not want to discover.

10 In the Configuration Settings section, clear the following options based on your preference:
   - Perform deep discovery — Discover a device and its associated device types. See Deep discovery.
   - Enable Monitoring — Enables SupportAssist Enterprise to detect hardware issues that may occur on the discovered devices.
   - Configure SNMP to receive alerts from this device — Automatically configure the SNMP settings of the discovered device to forward alerts (SNMP traps) to SupportAssist Enterprise.
   - Install latest version of OMSA — Enables SupportAssist Enterprise to install the latest version of OMSA or iDRAC Service Module (iSM) on the discovered servers. OMSA or iSM is required for collecting system information and to generate alerts from servers.

11 Click Add Rule.

The discovery rule is added and listed on the Manage Discovery Rules page. If you selected Run now, discovery of devices is initiated.

Related links
Manage Device Discovery Rule
Create or Edit Device Discovery Rule

View the device discovery rule overview pane

About this task

The Manage Discovery Rules page enables you to view the Discovery Rule Details, Discovery Rule Current Iteration Status, Recent Activity, and Current v/s Previous Discovery Rule Status panes. For more information about the attributes displayed in these panes, see Discovery Rule Details, Discovery Rule Current Iteration Status, Recent Activity, and Current v/s Previous Discovery Rule Status.

Steps

1 Point to Devices and click Manage Rules for Device Discovery.

   The Manage Discovery Rules page is displayed.

2 Select a discovery rule.

   The Discovery Rule Details, Discovery Rule Current Iteration Status, Recent Activity, and Current v/s Previous Discovery Rule Status panes are displayed.
Edit device discovery rule

Prerequisite
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 discovery rule based on your requirement.

NOTE: You cannot edit a discovery rule when the device discovery is in progress.

Steps
1. Point to Devices and click Manage Rules for Device Discovery.

The Manage Discovery Rules page is displayed.

2. Select the discovery rule that you want to edit and click Edit.

The Edit Device Discovery Rule window is displayed.

3. To discover devices by using IP address ranges:
   a. Select IP address/range.
   b. Type the IP address or IP address range of the devices that you want to discover. To add another IP address range, click Add another range, and then type the IP address range of the devices.
NOTE: You can add up to five different IP address ranges in the following formats:

- 10.34.*.*
- 10.34.1-10.*
- 10.34.*.1-10
- 10.34.1-10.1-10
- 10.34.1/24

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

NOTE: For an IP address entered in Classless-Inter Domain Routing (CIDR) notation, for example 10.34.1.1/24, the subnet mask entry is not considered.

c Type the Subnet Mask of the specified IP address range in the appropriate field.

4 To discover devices by using the hostname or IP addresses:
   a Select Devices.
   b Enter the hostname or IP address of devices as comma-separated values in the following formats:
      - 10.34.10.2, 10.34.10.3, 10.34.10.22
      - hostname1, hostname2, hostname3
      - 10.34.10.22, hostname2, 10.34.10.24

5 Click Next.
   The Discovering Devices window is displayed.

6 Select or clear the devices types and the configuration settings.

7 Click Edit Rule.
   The discovery rule is updated.

Related links
Manage Device Discovery Rule
Create or Edit Device Discovery Rule

Delete device discovery rule

Prerequisite
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 discovery rule based on your preference.

Steps
1 Point to Devices and click Manage Rules for Device Discovery.
   The Manage Discovery Rules page is displayed.
2 Select the discovery rule that you want to delete and click Delete.
   The Delete Device Discovery Rule window is displayed.
3 Click Yes.

Related link
Manage Device Discovery Rule

Run the discovery rule

Prerequisite
You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See Granting elevated or administrative privileges to users.
About this task
After creating a discovery rule, you can run the rule at any time.

Steps
1. Point to Devices and click Manage Rules for Device Discovery. The Manage Discovery Rules page is displayed.
2. Select the discovery rule that you want to run and click Run now. The devices associated with the discovery rule are discovered immediately.

NOTE: Devices that were discovered by the discovery rule, but are later unreachable are moved to the Inactive status. If a device is in an Inactive status even after the discovery rule is run for three consecutive times, the device is deleted automatically from SupportAssist Enterprise.

Related link
Manage Device Discovery Rule
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 that is received from a monitored device. A support case is created only if the alert type and number of alerts that are received from the device match with the criteria defined by Dell for support case creation.

**Topics:***
- Viewing all support cases
- View support cases for a specific device
- Case management options
- View the device inventory
- View the device overview pane
- 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.

![Figure 9. Cases page](image)
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.

**View support cases for a specific device**

**Prerequisite**
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**.
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.

- If no support cases are present for the device, an appropriate message is displayed.

**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.
Request to suspend case activities for 24 hours

**Prerequisite**
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** 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 link**
[Test the case creation capability](#)
Request to resume support activities

Prerequisite
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.
   
   \[ \text{NOTE: The Case Options list is enabled only if the support case that you have selected was opened by SupportAssist.} \]

   \[ \text{NOTE: The Resume Activity option is enabled only if you had previously requested to suspend notifications for the selected support case.} \]

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.

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

Related link
Test the case creation capability

Request to close a support case

Prerequisite
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.

\[ \text{NOTE: You can request Technical Support to close a support case only if the support case was opened by SupportAssist.} \]

\[ \text{NOTE: You can request Technical Support to close a support case that is in any status, except the Closed and Closure Requested status.} \]

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 link**

Test the case creation capability

**View the device inventory**

To view the device inventory, point to **Devices** and click **View Devices**.

![Device Inventory page](image)

**Figure 12. Device Inventory page**

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

For information on the fields and details displayed on the **Devices** page, see **Device inventory**.
View 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
- Perform deep discovery
- 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
- 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.

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

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

The device overview pane is displayed.
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.
SupportAssist Enterprise enables you to view the overall site health connectivity and status of your devices. Site health contains key connectivity result information that enables you to identify and prioritize the most important issue on your site.

The **Site Health** page contains the following panes:

- **Current SupportAssist Enterprise (Hostname) Details**
- **Current SupportAssist Overview**
- **Sitewide Inventory Validations**
- **Network Connectivity**
- **Extensions Tree View**

If your devices are placed in the Staging group, the count of the devices, details about the error, and the appropriate solution for the error is displayed in the **Site Health** page. You can also export this information as a .csv file.

**Figure 14. Site Health page**

Topics:
- View site health
- Current SupportAssist Enterprise Hostname Details
- Current SupportAssist Overview
- Sitewide Inventory Validation
- Network Connectivity
View site health

1. Open SupportAssist Enterprise. By default, the Site Health page is displayed.
2. If you are on any another page, then point to Site Health, and then click View Site Health.

Current SupportAssist Enterprise Hostname Details

The Current SupportAssist Enterprise (Hostname) Details pane displays information about devices you have discovered or added in SupportAssist Enterprise. This section displays the following information in a chart format:

- **Managed** — Devices monitored by SupportAssist Enterprise
- **Staging** — Devices in the Staging group
- **Inactive** — Devices that are classified as Inactive
- **Not managed** — Devices not monitored by SupportAssist Enterprise

Current SupportAssist Overview

The Current SupportAssist Overview pane displays the number of devices that are monitored and the number of open support cases. You can click the cases link to go to the Cases page.

Sitewide Inventory Validation

The Sitewide Inventory Validation pane displays the roll-up status of the inventory validation for devices that are discovered or added in SupportAssist Enterprise. The result is displayed in the following format:

- **Success** — Number of devices for which tests for connectivity, collection capability, and monitoring capability were successful.
- **Failed** — Number of devices for which tests for connectivity, collection capability, or monitoring capability was not successful.

**NOTE:** The total count of devices in Site Inventory Validation may not match with the total number of devices that you have added or discovered in SupportAssist Enterprise. This variance is because inventory validation does not support validating:

- Devices added in SupportAssist Enterprise through the adapter
- Devices that require manual configuration of SNMP settings, for example, networking devices
Network Connectivity

The **Network Connectivity** pane displays the status of SupportAssist Enterprise connectivity to the following network resources:

- Internet Connectivity
- SMTP Server
- Dell EMC FTP Server
- Dell EMC Upload Server
- SupportAssist Server

Related link  
Monitoring site health

Extensions Tree View

The **Extensions Tree View** pane displays the adapters and remote collectors that you have set up in the current SupportAssist Enterprise installation.

This pane also displays the number of devices associated with each remote collector and adapter.

Related link  
Monitoring site health
The extensions that are 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, Microsoft System Center Operations Manager (SCOM), or OpenManage Enterprise. 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 adding devices managed by systems management consoles
- Adapters overview
- Remote Collectors overview

## 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
  - OpenManage Enterprise adapter — For inventorying devices managed by OpenManage Enterprise – Tech Release and OpenManage Enterprise Version 3.0

- **Remote Collector** — A remote instance of SupportAssist Enterprise that collects and uploads system information from devices that are present 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.
Getting started with adding devices managed by systems management consoles

To inventory and add devices that are managed by a systems management console such as OpenManage Essentials, Microsoft System Center Operations Manager, OpenManage Enterprise - Tech Release, or OpenManage Enterprise Version 3.0:

1. Add Account Credentials in SupportAssist Enterprise for the devices that you want to add from the systems management console. See Add Account Credentials.
2. Create one or more Credential Profiles depending on the type of devices that you want to add. See Create Credential Profile.
3. Set up the adapter in SupportAssist Enterprise. See Set up OpenManage Essentials adapter, Set up Microsoft System Center Operations Manager adapter, or Set up OpenManage Enterprise adapter.
4. If you are adding more than 4,000 devices, set up a Remote Collector. See Set up Remote Collector.

Adapters overview

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 Dell EMC devices that are managed by Microsoft System Center Operations Manager by using the Dell Server Management Pack Suite
- OpenManage Enterprise adapter — To inventory devices that are managed by OpenManage Enterprise – Tech Release and OpenManage Enterprise Version 3.0

<table>
<thead>
<tr>
<th>Operating system where SupportAssist Enterprise is installed</th>
<th>Support for setting up an adapter on a local or remote server running Windows</th>
<th>Support for setting up an adapter on a local or remote server running Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Yes</td>
<td>Yes (For OpenManage Enterprise only)</td>
</tr>
<tr>
<td>Linux</td>
<td>No</td>
<td>Yes (For OpenManage Enterprise only)</td>
</tr>
</tbody>
</table>

Table 13. Support for setting up an adapter

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 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

<table>
<thead>
<tr>
<th>Operating system where SupportAssist Enterprise is installed</th>
<th>Support for setting up Remote Collector on a remote server running Windows</th>
<th>Support for setting up Remote Collector on a remote server running Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Linux</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 14. Support for setting up a Remote Collector

NOTE: For the devices that you can assign to a Remote Collector, see the list of devices in the SupportAssist Enterprise Version 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

1. NOTE: Setting up an OpenManage Enterprise adapter is supported only on a local or remote server running Linux.
2. NOTE: Servers running Debian and Ubuntu operating systems can only be added directly in SupportAssist Enterprise, and not through the adapters.
Related links
- Extensions
- Set up OpenManage Essentials adapter
- Set up the Microsoft System Center Operations Manager adapter
- Set up OpenManage Enterprise adapter
- Synchronize adapter
- Edit adapter
- Delete adapter
- Set Up OpenManage Essentials Adapter
- Set Up Microsoft System Center Operations Manager Adapter
- Set Up OpenManage Enterprise adapter

Set 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 2.5 or later.
- 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 Create Account Credentials and Create Credential Profile.
- The server running SupportAssist Enterprise must have internet connectivity.
- You must have read-write access to the system drive of the target device.
- Ensure that Microsoft .NET Framework 4.5 is installed on the system where you want to set up the adapter.
- Ensure that one of the following requirements are met:
  - The Secure Socket Layer (SSL) protocol is enabled
  - The Transport Layer Security (TLS) protocol is enabled and its version is 1.0, 1.1, or 1.2

About this task
Setting up the OME adapter enables you to inventory and add 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.

- **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.
- **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 and added in SupportAssist Enterprise.
- **NOTE:** One OpenManage Essentials adapter can only inventory and add devices from a single OpenManage Essentials installation.
- **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 2.0.21 Support Matrix at 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.
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.

   **NOTE:** The password must not exceed 50 characters.

   **NOTE:** If you change the credentials of the system running OpenManage Essentials because of the security policy requirements of your company or for other reasons, ensure that you also update the adapter credentials in SupportAssist Enterprise. Dell recommends that you create a service account with credentials that do not expire, and enter the service account credentials in SupportAssist Enterprise.

   **NOTE:** After SupportAssist Enterprise makes two consecutive failed authentication attempts to connect to OpenManage Essentials, a lock file is created by SupportAssist Enterprise. The lock file, SupportAssist_RestError.xml, is created on the system where OpenManage Essentials is installed and is available at C:\ProgramData. The lock file is automatically deleted after one hour or you can delete the lock file manually. During the lock out period, there is no communication between SupportAssist Enterprise and OpenManage Essentials.

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**.

   The **Adapter Details** overview pane is displayed and devices that are managed by OpenManage Essentials 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.

NOTE: While assigning a Credential Profile, SupportAssist Enterprise performs additional classification tasks in the background for each device. Therefore, assigning Credential Profiles may be prolonged depending on the device types, number of devices, and your network bandwidth. For more information on the approximate time taken to assign Credential Profiles, see Approximate time taken to assign Credential Profiles.

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:

1. In the Refine by pane, expand Groups and select Staging. You can also select the adapter under Devices Added in the Refine by pane to view devices that are inventoried by an adapter. If necessary, use the Search by option to filter the displayed list of devices.

2. Perform one of the following:
   - Select the devices and assign a Credential Profile that contains the credentials of the selected devices.
   - Select a device and click Edit to assign a Credential Account.

3. Repeat step 2 until you have assigned the correct Credential Profile or Account Credentials to all devices.

NOTE: For Storage PS Series devices, only the Storage PS Series management group is added through the adapter. The Storage PS Series members are not added through the adapter.

Related links
Adapters
Set Up OpenManage Essentials Adapter
Adapters overview

Set 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 6.3 or 7.0 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.
- The server running SupportAssist Enterprise must have internet connectivity.
- 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 Create Account Credentials and Create Credential Profile.
- You must have read-write access to the system drive of the target device.

About this task
Setting up the System Center Operations Manager (SCOM) adapter enables you to inventory and add 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.

**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.

**NOTE:** One System Center Operations Manager adapter can only inventory and add devices from a single System Center Operations Manager instance.

**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 2.0.21 Support Matrix at 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 17. 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.

   **NOTE:** The password must not exceed 50 characters.

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.

   **NOTE:** If you change the credentials of the system running the Management Group or Remote Console because of the security policy requirements of your company or for other reasons, ensure that you also update the adapter credentials in SupportAssist Enterprise. Dell recommends that you create a service account with credentials that do not expire, and enter the service account credentials in SupportAssist Enterprise.

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.
   The Adapter Details overview pane is displayed and 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.

   **NOTE:** While assigning a Credential Profile, SupportAssist Enterprise performs additional classification tasks in the background for each device. Therefore, assigning Credential Profiles may be prolonged depending on the device types, number of devices, and your network bandwidth. For more information on the approximate time taken to assign Credential Profiles, see Approximate time taken to assign Credential Profiles.

**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:

1 In the Refine by pane, expand Groups and select Staging. You can also select the adapter under Devices Added in the Refine by pane to view devices that are inventoried by an adapter. If necessary, use the Search by option to filter the displayed list of devices.

2 Perform one of the following:
   • Select the devices and assign a Credential Profile that contains the credentials of the selected devices.
   • Select a device and click Edit to assign a Credential Account.

3 Repeat step 2 until you have assigned the correct Credential Profile or Account Credentials to all devices.

**Related links**
Adapters
Set Up Microsoft System Center Operations Manager Adapter
Adapters overview
Management Packs for inventorying devices managed by Operations Manager

The following table lists the Dell Server Management Pack Suite Version 6.3 or 7.0 required for SupportAssist Enterprise to inventory devices that are managed by System Center Operations Manager (SCOM).

Table 15. Management Packs for inventorying devices managed by Operations Manager

<table>
<thead>
<tr>
<th>Devices to be monitored</th>
<th>Monitoring Feature</th>
<th>Required Management Packs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell’s 9th or later generation of PowerEdge servers</td>
<td>Servers and Rack Workstations Agent-based Monitoring</td>
<td>• Dell Base Hardware Library</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell Server Model</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell Server Operations Library</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell Server View Library</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell Windows Server (Scalable Edition)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell Operations Library Common</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell Server and Rack Workstation Monitoring (Licensed)</td>
</tr>
<tr>
<td>iDRAC</td>
<td>DRAC Monitoring</td>
<td>• Dell Feature Monitoring (optional)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell Base Hardware Library</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell Operations Library Common</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell DRAC Model</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell DRAC View</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell DRAC Operations Library</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell DRAC (SC2012 OM)</td>
</tr>
</tbody>
</table>

**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.

Set up OpenManage Enterprise adapter

**Prerequisites**

- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See *Granting elevated or administrative privileges to users*.
- You must have administrator privileges on the system running OpenManage Enterprise – Tech Release or OpenManage Enterprise Version 3.0.
- 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 *Create Account Credentials* and *Create Credential Profile*.

**About this task**

Setting up the OpenManage Enterprise adapter enables you to inventory devices that are managed by OpenManage Enterprise – Tech Release and OpenManage Enterprise Version 3.0. During the set up, SupportAssist Enterprise installs the adapter on the system running SupportAssist Enterprise and then inventories the devices.
You can only inventory and add the following devices through the OpenManage Enterprise adapter:

- iDRAC of 12th to 14th generation of PowerEdge servers
- Servers running Linux, ESXi, and HyperV
- Chassis
- Storage SC Series devices (previously Compellent)
- Dell Networking devices (previously Force10)
- OEM devices
- IOM devices

**NOTE:** One OpenManage Enterprise adapter can inventory and add devices from multiple OpenManage Enterprise instances.

**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.
3. From the **Adapter type** list, select **OpenManage Enterprise**.
4. Perform the following:
   a. Type the hostname or IP address of the server where OpenManage Enterprise 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.

   **NOTE:** The password must not exceed 50 characters.

5. 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.
6. From the **Update device inventory** list, select the desired frequency for inventorying devices through the adapter.
7. Click **OK**. The **Adapter Details** overview pane is displayed and devices that are managed by OpenManage Enterprise are inventoried in SupportAssist Enterprise.

**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.

**NOTE:** For Storage PS Series devices, only the Storage PS Series management group is added through the adapter. The Storage PS Series members are not added through the adapter.

To add devices that are placed in the **Staging** group:

1. In the **Refine** pane, expand **Groups** and select **Staging**. You can also select the adapter under **Devices Added** in the **Refine by** pane to view devices that are inventoried by an adapter. If necessary, use the **Search by** option to filter the displayed list of devices.
2. Perform one of the following:
   - Select the devices and assign a Credential Profile that contains the credentials of the selected devices.
   - Select a device and click **Edit** to assign a Credential Account.
3. Repeat step 2 until you have assigned the correct Credential Profile or Account Credentials to all devices.
NOTE: When the OpenManage Enterprise services are suspended and resumed, the OpenManage Enterprise adapter will only retrieve alerts that have occurred in the last 12 hours for devices that are added in SupportAssist Enterprise through the OpenManage Enterprise adapter.

NOTE: After synchronization of the OpenManage Enterprise adapter, some of the iDRACs may not be displayed in SupportAssist Enterprise. This may occur if the iDRAC version cannot be retrieved from OpenManage Enterprise.

**View the adapter overview pane**

**Prerequisite**
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

**View devices inventoried by the adapter**

**Prerequisite**
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, under **Devices Added**, click + to expand the adapter list, and then select the adapter.
   - The devices that are inventoried by the adapter are displayed.

**Related link**
- Adapters

**Synchronize adapter**

**Prerequisite**
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
Adapters overview

Edit adapter

Prerequisite
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
Adapters overview

Delete adapter

Prerequisite
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.

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

**NOTE:** Uninstallation of the OpenManage Enterprise adapter occurs only if all the OpenManage Enterprise adapters are deleted in SupportAssist Enterprise.

### 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.

### Related links

- Adapters
- Adapters overview

### Approximate time required to assign Credential Profile

Assigning a Credential Profile may be prolonged depending upon the device types, number of devices, and your network bandwidth. The following table provides the approximate time required to assign a Credential Profile depending upon the number of devices.

#### Table 16. Device count and Credential Profile assignment duration

<table>
<thead>
<tr>
<th>Number of devices</th>
<th>Time taken to assign a Credential Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3 minutes</td>
</tr>
<tr>
<td>50</td>
<td>15 minutes</td>
</tr>
<tr>
<td>100</td>
<td>30 minutes</td>
</tr>
<tr>
<td>1000</td>
<td>6 hours</td>
</tr>
<tr>
<td>1500</td>
<td>9 hours</td>
</tr>
<tr>
<td>2000</td>
<td>12 hours</td>
</tr>
<tr>
<td>3000</td>
<td>17 hours</td>
</tr>
</tbody>
</table>

### Remote Collectors overview

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 4,000 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
- Set Up Remote Collector
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 17. Hardware requirements

<table>
<thead>
<tr>
<th>Devices</th>
<th>Monitoring</th>
<th>Collecting System Information</th>
<th>Processor</th>
<th>Installed memory (RAM)</th>
<th>Hard drive (free space)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>1 core</td>
<td>4 GB</td>
<td>1 GB</td>
</tr>
<tr>
<td>20</td>
<td>Yes</td>
<td>Yes</td>
<td>2 cores</td>
<td>4 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Up to 100</td>
<td>Yes</td>
<td>Yes</td>
<td>4 cores</td>
<td>8 GB</td>
<td>12 GB</td>
</tr>
<tr>
<td>Up to 300</td>
<td>Yes</td>
<td>Yes</td>
<td>4 cores</td>
<td>8 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Up to 1000</td>
<td>Yes</td>
<td>Yes</td>
<td>8 cores</td>
<td>8 GB</td>
<td>60 GB</td>
</tr>
<tr>
<td>Up to 4000</td>
<td>Yes</td>
<td>Yes</td>
<td>8 cores</td>
<td>16 GB</td>
<td>90 GB</td>
</tr>
</tbody>
</table>

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 https://is.us.dell.com/*, the file upload server and related services.

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

Table 18. Network bandwidth requirements

<table>
<thead>
<tr>
<th>Devices</th>
<th>Monitoring</th>
<th>Collecting System Information</th>
<th>LAN bandwidth*</th>
<th>WAN bandwidth**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>Yes</td>
<td>10 Mbps</td>
<td>5 Mbps</td>
</tr>
<tr>
<td>20</td>
<td>Yes</td>
<td>Yes</td>
<td>0.5 Gbps</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Up to 100</td>
<td>Yes</td>
<td>Yes</td>
<td>0.5 Gbps</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Up to 300</td>
<td>Yes</td>
<td>Yes</td>
<td>0.5 Gbps</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Up to 1000</td>
<td>Yes</td>
<td>Yes</td>
<td>1 Gbps</td>
<td>20 Mbps</td>
</tr>
<tr>
<td>Up to 4000</td>
<td>Yes</td>
<td>Yes</td>
<td>1 Gbps</td>
<td>20 Mbps</td>
</tr>
</tbody>
</table>

* 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 figure illustrates network port connectivity between SupportAssist Enterprise and other monitored devices.

**Figure 18. Managed devices**

- 1 — Network ports required for discovering devices and collecting system information
- 2 — Network ports required for uploading the collected system information (collection)
- 3 — Network ports required for adapters
- 4 — Network ports on devices for collecting system information

The following table lists the network ports required for discovering devices and collecting system information.
### Table 19. Network ports required for discovering devices and collecting system information

<table>
<thead>
<tr>
<th>Device</th>
<th>Protocol for discovery and collection</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server - Windows</td>
<td>WMI</td>
<td>135</td>
</tr>
<tr>
<td>Server - Linux</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>ESX or ESXi</td>
<td>SSH and VMware SDK</td>
<td>22 and 443</td>
</tr>
<tr>
<td>Storage PS Series arrays (previously EqualLogic)</td>
<td>SNMPv2, SSH2, and FTP</td>
<td>161, 22, and 21</td>
</tr>
<tr>
<td>Storage MD Series arrays (previously PowerVault)</td>
<td>SYMbolSDK</td>
<td>2463</td>
</tr>
<tr>
<td>Storage ME4 Series arrays</td>
<td>REST and SFTP</td>
<td>443 and 1022</td>
</tr>
<tr>
<td>Storage SC Series arrays (previously Compellent)</td>
<td>REST</td>
<td>3033</td>
</tr>
<tr>
<td>Fluid File System (FluidFS) Network attached storage (NAS) devices</td>
<td>SSH and FTP</td>
<td>22 and 44421</td>
</tr>
<tr>
<td>PowerConnect switches</td>
<td>SNMP and SSH</td>
<td>22 and 161</td>
</tr>
<tr>
<td>Force10 switches</td>
<td>SNMP and SSH</td>
<td>161 and 22</td>
</tr>
<tr>
<td>Networking switches</td>
<td>SNMP and SSH</td>
<td>22 and 161</td>
</tr>
<tr>
<td>W series switches</td>
<td>SNMP and SSH</td>
<td>22 and 161</td>
</tr>
<tr>
<td>PowerEdge FX2/FX2s</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>PowerEdge VRTX</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>PowerEdge M1000e</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>PowerEdge MX7000</td>
<td>REST</td>
<td>443</td>
</tr>
<tr>
<td>SAN HQ</td>
<td>WMI</td>
<td>135</td>
</tr>
<tr>
<td>HIT Kit / VSM for VMware</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>vCenter</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>SCVMM</td>
<td>WMI</td>
<td>135</td>
</tr>
<tr>
<td>XC Series of Web-Scale hyper-converged appliances</td>
<td>REST and SSH</td>
<td>9440 and 22</td>
</tr>
<tr>
<td>Virtual Machine - Windows</td>
<td>WMI</td>
<td>135</td>
</tr>
<tr>
<td>Virtual Machine - Linux</td>
<td>SSH</td>
<td>22</td>
</tr>
</tbody>
</table>

The following table lists the network ports required for uploading the collected system information.

### Table 20. Network ports required for uploading the collected system information

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SupportAssist Enterprise</td>
<td>SupportAssist Server</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>File Upload Server (FUS)</td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Port</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Storage SC Series arrays (previously</td>
<td>SupportAssist Enterprise</td>
<td>5701, 5702, 5703,</td>
</tr>
<tr>
<td>Compellent)</td>
<td></td>
<td>and 5704</td>
</tr>
<tr>
<td>Server SupportAssist agent</td>
<td>SupportAssist Enterprise</td>
<td>5701, 5702, 5703,</td>
</tr>
<tr>
<td>Server (In band)</td>
<td>SupportAssist Enterprise</td>
<td>and 5704</td>
</tr>
</tbody>
</table>

The following table lists the network ports required for collecting system information.

**Table 21. Network ports on devices for collecting system information**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Retrieval Service (FRS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Collector</td>
<td>File Upload Server (FUS)</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>File Retrieval Service (FRS)</td>
<td></td>
</tr>
</tbody>
</table>

**Set 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](#).
- The server running SupportAssist Enterprise must have internet connectivity.
- You must have read-write access to the system drive of the target device.
- Ensure that sudo access is configured for the non-root user account. For information on configuring sudo access, see [Configure sudo access for SupportAssist Enterprise in Linux](#).

**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.
Figure 19. 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 To assign devices to the Remote Collector by using hostname expressions:
   a Select **Hostname**.
   b Type the hostname expression or hostname expressions of the devices that you want to assign to the Remote Collector.
   
   **NOTE:** The hostname expression can only include special characters such as *, ?, or alphanumeric characters.
   c To add multiple hostname expressions, click **Add another expression**, and then type the hostname expressions of the devices.
7 To assign devices to the Remote Collector by using IP address ranges:
   a Select **IP address / range**.
   b Type the IP address or IP address ranges of the devices that you want to associate with the Remote Collector.
   c To add multiple IP address ranges, click **Add IP address range**, and then type the IP address range of the devices.
   You can add up to five different IP address ranges by using one of the following formats:
     - 193.109.112.99
     - 193.109.112.*
     - 193.104.20-40.*
     - 192.168.2-51.3-91
     - 193.109.112.45-99
   
   **NOTE:** Ensure that the IP address ranges you have entered do not overlap with each other.
If the remote server connects to the internet through a proxy server, select the **The remote system 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 ranges or host name expressions 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, Storage SC Series 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.](image)

You can enter a list of IP address ranges in the following formats:

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

The following IP address range formats are not supported:

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

![NOTE: If you have assigned devices to the Remote Collector by using IP address ranges, ensure that you only enter IP address ranges in the Proxy Exclusion List. If you have assigned devices to the Remote Collector by using hostname expressions, ensure that you only enter hostname expressions in the Proxy Exclusion List.](image)

9. Click **OK**.

The **Set Up Remote Collector** overview pane is displayed and 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.](image)

**View 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. Perform one of the following:

   - If you have set up the Remote Collector on a server running Windows — Browse to `<Drive where SupportAssist Enterprise is installed>`\Program Files\Dell\SupportAssist\Reports` folder.
3. If you have set up the Remote Collector on a server running Linux — Browse to \opt\Dell\supportassist\reports folder.

   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.

**View the Remote Collector overview pane**

**Prerequisite**
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 20. Remote Collector overview pane](image)

**Related links**
Remote Collectors
Remote Collector overview pane

**View devices associated with a Remote Collector**

**Prerequisite**
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.

3. Click View all devices.

Devices that are associated with the Remote Collector are displayed on the Devices page.

Related link
Remote Collectors

Edit Remote Collector

Prerequisite
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 that you want to update 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.

   If SupportAssist Enterprise is unable to connect to the remote system using the entered credentials:

   - The existing credentials are retained
   - The Remote Collector and the Upload Connectivity on the Remote Collectors page retain the status that was displayed prior to editing the credentials

   If the remote system is unable to connect to the proxy server using the entered proxy server credentials:

   - The entered proxy server credentials are saved in SupportAssist Enterprise, but the existing proxy server credentials are retained in the Remote Collector.
   - The Remote Collector displays a proxy validation failed status, but the Upload connectivity retains the status that was displayed prior to editing the proxy server credentials.

Related link
Remote Collectors
Delete Remote Collector

Prerequisite
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. If the IP address range or hostname expression of devices that were assigned to the Remote Collector overlap with that of another Remote Collector, the applicable devices are assigned to the other Remote Collector. Otherwise, the devices are assigned to the server running SupportAssist Enterprise.

Related link
Remote Collectors
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 on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

**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
- View device groups
- Creating a device group
- Manage devices in a device group
- Manage the credentials of a device group
- View and update device group information
- Delete a device group

Related links

View device groups
Creating a device group
Manage devices in a device group
Manage the credentials of a device group
View and update device group information
Delete 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 the required 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

View device groups

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

**About this task**

To view the device groups:

**Step**

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

The **Device Groups** page is displayed.

![Device Groups page](image)

Creating a device group

**Prerequisite**

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 Group**.
   
   The **Create Device Group** window is displayed.

3. On the **Group and Contact Information** page, in the **Group Details** section, type the group name and a description for the group.

4. Select **IT Administrator Contact Information**, and provide the following information:
   a. If you want to use the IT Administrator contact information provided in the **Settings > Contact Information** page, click the appropriate link.
b Select one of the following:
   - Primary
   - Secondary

c Type your first name, last name, phone number, alternate phone number, and email address in the appropriate fields.

d Select the preferred contact method, preferred contact hours, and time zone.

5 Click Next.

The Parts Replacement Preferences for Dell Servers page is displayed.

By default, the I want Dell server replacement parts shipped automatically is selected. If you clear the option, the shipment of Dell server replacement parts could be delayed.

6 To copy the already provided contact information, click the appropriate link.

The Primary Shipping Contact information is populated.

7 In the Secondary Shipping Contact section, type the first name, last name, phone number, and email address of the secondary contact.

   🔄| NOTE: Contact details of the primary and secondary contact must be unique.

8 In the Shipping Address section, perform the following:
   a Select the preferred contact hours during which Dell can contact you, if necessary.
   b Select the time zone, country, and type your shipping address in the appropriate fields.
   c Type any specific dispatch related information in the Dispatch Notes section.

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

   d If you want an onsite technician to replace the dispatched hardware component, select I want a technician to replace my parts onsite (if included in my service plan).

9 Click Create.

The device group that you created is displayed in the Device Groups page.

## Manage 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. Before you begin, makes sure that you have already created a device group. See Creating a device group.

唵| NOTE: You can add or remove devices from a device groups only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

To manage devices in a device group:

唵| 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.
To add devices to the device group, select the devices in the Ungrouped pane, and click \( \rightarrow \). The selected devices are moved to the Devices in current group pane.

To remove devices from the device group, select the devices in the Devices in current group pane, and click \( \leftarrow \). The selected devices are moved to the Ungrouped pane.

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.

### Manage the credentials of a device group

If the device types within a device group differ from the default credentials, you must provide the credentials of those device types. 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 Create 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.

**NOTE:** You can manage credentials of a device group only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

**NOTE:** The device group credentials override the default credentials configured in the Settings > System Logs page. When the device group credentials are configured:

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

To manage the credentials of a device group:
View and update device group information

Prerequisite
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 or update the contact information, preferred contact method and time, and the parts dispatch information of a device group. You can also integrate automated parts dispatch with specific TechDirect accounts.

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 Group.
   The Edit Device Group window is displayed.
4. Select IT Administrator Contact Information, and provide the following information:
   a. If you want to use the IT Administrator contact information provided in the Settings > Contact Information page, click the appropriate link.
   b. Select one of the following:
      - Primary
      - Secondary
   c. Type your first name, last name, phone number, alternate phone number, and email address in the appropriate fields.
   d. Select the preferred contact method, preferred contact hours, and time zone.
5. Click Next.
   The Parts Replacement Preferences for Dell Servers page is displayed.
6. Select I want Dell server replacement parts shipped automatically.
   NOTE: If you do not wish to set up parts replacement preferences, the shipment of Dell server replacement parts could be delayed.
7. To copy the already provided contact information, click the appropriate link.
   The Primary Shipping Contact information is populated.
8. In the Secondary Shipping Contact section, type the first name, last name, phone number, and email address of the secondary contact.
   NOTE: Contact details of the primary and secondary contact must be unique.
9. In the Shipping Address section, perform the following:
a. Select the preferred contact hours during which Dell can contact you, if necessary.

b. Select the time zone, country, and type your shipping address in the appropriate fields.

c. Type any specific dispatch related information in the Dispatch Notes section.

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

d. If you want an onsite technician to replace the dispatched hardware component, select I want a technician to replace my parts onsite (if included in my service plan).

10. Click Update.

---

**Delete a device group**

**Prerequisite**
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:** You can delete a device group only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

**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, and then click Delete.
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 device
- By using the Edit option
- By assigning an Account Credentials or a Credential Profile

Topics:
- Account Credentials
- Credential Profiles

Account Credentials

An Account Credential consists of the credentials of a specific device type. The Account Credentials is used by SupportAssist Enterprise to 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
- Add Account Credentials
- Reassign Account Credentials
- Edit Account Credentials
- Delete Account Credentials

Add Account Credentials

Prerequisite
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 add a device or 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.
2 Click **Add Credentials**.

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

**Figure 25. Add Account Credentials window**

3 In the **Name** field, 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:

   - **NOTE**: The credentials that you enter must have Administrator rights.

   - 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.

     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 Configure 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

- 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, enter the SSH and REST credentials in the appropriate fields.
- For Networking devices, type the user name, password, community string, and enable password of the device in the appropriate fields.

**NOTE:** Community string is required for the following network devices:
- PowerConnect family 28xx and X series
- Cisco
- Wireless controller

**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.

**NOTE:**
- Account Credentials are mandatory for adding a Storage ME4 Series device.
- Account Credentials are not required for adding a Storage MD Series device.

6. Click Save.

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

**Related links**
- Account Credentials
- Manage Account Credentials
- Add Account Credentials

**Reassign Account Credentials**

**Prerequisite**
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 a device and click Edit.
   
   The Edit Account window is displayed.

3. From the Account Credentials list, select an account credential.

   **NOTE:** Only Account Credentials that you have already created for the selected device type are present in the Account Credentials list.

4. Click Save (if the device is in the Default group) or Revalidate (if the device is in the Staging group).

**Related links**
- Account Credentials
- Manage Account Credentials
Edit Account Credentials

**Prerequisite**
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.

⚠️ **NOTE:** Changing the device type is not supported.

**Steps**

1. Point to **Devices > Manage Credentials** and click **Account Credentials**.
   
   The **Manage Account Credentials** page is displayed.

   ![Manage Account Credentials](#)

   **Figure 26. 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](#)

Delete Account Credentials

**Prerequisites**

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

- The Account Credentials that you want to delete must not be assigned to any device.

**About this task**
You can delete the Account Credentials based on your preference.
Steps
1. Point to Devices > Manage Credentials and click Account Credentials. The Manage Account Credentials page is displayed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Device type</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT</td>
<td>Server / Hypervisor - WINDOWS</td>
</tr>
<tr>
<td>Marketing</td>
<td>Server / Hypervisor - WINDOWS</td>
</tr>
<tr>
<td>Support</td>
<td>Server / Hypervisor - WINDOWS</td>
</tr>
<tr>
<td>Admin A</td>
<td>iDRAC</td>
</tr>
<tr>
<td>Admin B</td>
<td>Chassis</td>
</tr>
</tbody>
</table>

Figure 27. 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
- Create Credential Profile
- Assign Credential Profile
- Edit Credential Profile
- Delete Credential Profile

Create Credential Profile

Prerequisite
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.
2. Click **Create Profile**. The **Create Credential Profile** window is displayed.

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 new Account Credentials, click Add Account Credentials. For more information on 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
Assign Credential Profile

Prerequisite
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

View devices associated with a Credential Profile

1. Point to Devices > Manage Credentials and click Credential Profiles.
   The Manage Credential Profiles page is displayed.
2. Select a credential profile.
   Devices that are associated with the Credential Profile are displayed on the Credential Profile overview pane.

Edit Credential Profile

Prerequisite
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.

NOTE: Updating the name of the Credential Profile is not supported.

Steps
1. Point to Devices > Manage Credentials and click Credential Profiles.
   The Manage Credential Profiles page is displayed.
2. Select the Credential Profile that you want to edit and click Edit.
   The Edit Credential Profile window is displayed.

Figure 30. Manage Credential Profiles window
Select the device type for which you want to edit Account Credentials. The **Account Credentials** list is enabled for selection.

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

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

## Delete Credential Profile

**Prerequisites**
- You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- The Credential Profile that you want to delete must not be assigned to any device.

**About this task**
You can delete a Credential Profile based on your preference.

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

   ![Manage Credential Profiles page](#)

   **Figure 31. 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
Validating device inventory

Site inventory validation verifies the availability of the following capabilities of SupportAssist Enterprise for your devices:

- **Connectivity Status** — Verifies if the device has internet connectivity and if the required ports are open on the device. It also verifies if the required credentials of the device are correct and available.
- **Collection Capability Status** — Verifies if the requirements for collecting system information are met on the device.
- **Monitoring Status** — Verifies if the latest version of OMSA is installed on servers. It also verifies if the SNMP trap destination and the iDRAC trap destination are configured.

*NOTE:* Monitoring capability test is supported only on Windows, Linux, and iDRAC.

During inventory validation, the device status is updated.

- If the validation is successful, the device moves to the Default group.
- If the validation is unsuccessful, the device moves to the Staging or Inactive group.

*NOTE:* While inventory validation is in progress, the device is disabled. To view the status of the device operation, move your mouse pointer on the device.

*NOTE:* The total count of devices in Site Inventory Validation table may not match with the total number of devices on the progress indicator. The device count on the progress indicator is assigned when periodic inventory validation begins or when SupportAssist Enterprise is upgraded to a newer version, whereas the device count in the Site Inventory Validation table is updated when:
  - Some associated devices are discovered as a part of the deep discovery process
  - New devices are added in SupportAssist Enterprise

Topics:
- View the Site Inventory Validation page
- Start inventory validation manually
- Schedule automatic inventory validation

Related links
  - Site Inventory Validation
  - View the Site Inventory Validation page
  - Start inventory validation manually
  - Schedule automatic inventory validation

**View the Site Inventory Validation page**

Point to **Devices** and click **Site Inventory Validation**.

The **Site Inventory Validation** page is displayed.
Related links
Validating device inventory
Site Inventory Validation

Start inventory validation manually

About this task
You can perform inventory validation on your devices to verify the status of the devices.

Steps
1. Point to **Devices** and click **View Devices**. The **Devices** page is displayed.
2. Select one or more devices and click **Validate Inventory**. SupportAssist Enterprise verifies the connectivity status of the devices.

**NOTE:** To view the count of devices that were successfully validated and the devices that failed validation, see the Site Inventory Validation page.

Related links
Validating device inventory
Site Inventory Validation

Schedule automatic inventory validation

About this task
By default, Inventory Validation is scheduled on a randomly determined day of every month at 11 PM. If necessary, you can change the schedule based on your requirement.

Steps
1. Point to **Settings** and click **Preferences**. The **Preferences** page is displayed.
2. In **Automatically start inventory validation**, depending upon your requirement, select the day on which you want to want to start inventory validation.
3. Click **Apply**.

Related links
Validating device inventory
Site Inventory Validation
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 Enable or disable 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 Edit Account Credentials.
- Install or upgrade dependent components such as Dell OpenManage Server Administrator (OMSA). See Install or upgrade OMSA by using SupportAssist Enterprise.
- Configure the SNMP settings of a device. See Configure SNMP settings by using SupportAssist Enterprise.
- Update the primary and secondary contact information, if there is a change in the contact details. See View and update the contact information.
- Update the parts dispatch preferences and shipping information to enable the dispatch of a replacement hardware component. View and update parts dispatch information.
- Update the proxy server settings in SupportAssist Enterprise, if applicable. See Configure proxy server settings.
- Update the SMTP server (email server) settings in SupportAssist Enterprise, if applicable. See Configure 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 Test the case creation capability.
- Clear the System Event Log of a server. See Clear 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 Delete a device.

Topics:
- Enable or disable monitoring of a device
- Perform deep discovery
- Install or upgrade OMSA by using SupportAssist Enterprise
- Configure SNMP settings by using SupportAssist Enterprise
- View and update the contact information
- View and update parts dispatch information
- Integrate SupportAssist Enterprise with your TechDirect account
- Configure proxy server settings
- Connectivity test
- Test the case creation capability
- Clear the System Event Log
- Automatic update
- Delete a device

Enable or disable monitoring of a device

**Prerequisite**

Ensure that you have completed the registration of SupportAssist Enterprise. See Register 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.

Figure 33. Enable or disable monitoring option

NOTE: If the registration of SupportAssist Enterprise is not completed, the Enable monitoring option is disabled.

NOTE: To allow SupportAssist Enterprise to monitor a device, in addition to enabling monitoring, the SNMP settings of the device must also be configured. For instructions to configure the SNMP settings of a device, see Configure SNMP settings by using SupportAssist Enterprise and Manually configure SNMP settings.

Perform deep discovery

Prerequisite
A Credential Profile must be assigned to the device.

About this task
Deep discovery enables you to discover a device and its associated device types. See Deep discovery.
Steps
1. Point to Devices and click View Devices. The Devices page is displayed.
2. Select the device for which you want to perform deep discovery. The device overview pane is displayed at the right side of the Devices page.
3. From the Tasks list, select Perform deep discovery. The Perform deep discovery window is displayed.

   NOTE: If deep discovery is not applicable for a device, the Perform deep discovery option is disabled.
4. Select a Credential Profile and click Next. The device is revalidated and the associated devices are discovered.

Related link
Deep discovery

Install or upgrade 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.
- You must have read-write access to the system drive of the target device.

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 2.0.21 Support Matrix at 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
   - Debian 7.x
   - Debian 8.x
   - Ubuntu 14.x
   - Ubuntu 16.x
   - Ubuntu 18.x

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 link
Support for automatically installing or upgrading OMSA

Configure 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.
- You must have read-write access to the system drive of the target device.

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

Figure 35. Configure SNMP option

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

Related link
Support for automatically configuring SNMP settings
View and update 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.

Prerequisite
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. Click Apply.

Related link
View and update parts dispatch information

View and update parts dispatch information

Prerequisite
You must be logged in to SupportAssist Enterprise with elevated or administrative privileges. See Granting elevated or administrative privileges to users.

About this task
Entering your dispatch preferences and shipping information enables Dell to dispatch a replacement hardware component to you. You can enter your dispatch preferences and shipping information during registration or later.

**NOTE:** Parts dispatch is supported only for systems that have an active ProSupport, ProSupport Plus, ProSupport One, or ProSupport Flex service entitlement.

Steps
1. Point to Settings and click Contact Information.
   The Contact Information page is displayed.
2. In the Parts Replacement Preferences for Dell Servers section, select I want Dell server replacement parts shipped automatically.
   **NOTE:** If you do not wish to set up parts replacement preferences, the shipment of Dell server replacement parts could be delayed.
3. To copy the contact information that you have provided on the Group and Contact Information page, click the appropriate link.
4. In the Primary Shipping Contact section, perform the following:
   **NOTE:** If you choose to use the already entered contact information, the first name, last name, phone number, and email address fields are populated with the contact information.
   a. Select the preferred contact hours during which Dell can contact you, if necessary.
   b. Select the time zone and type your shipping address in the appropriate fields.
   c. Type any specific dispatch related information in the Dispatch notes section.
NOTE: If a device is moved to a different location, ensure that the dispatch preferences and shipping information are updated.

5. If you want an onsite technician to replace the dispatched hardware component, select I want a technician to replace my parts onsite (if included in my service plan).

6. In the Secondary Shipping Contact section, type the first name, last name, phone number, and email address of the secondary contact, in the appropriate fields.

   NOTE: Contact details of the primary and secondary contact must be unique.

7. For Brazil only: Type the CNPJ and IE numbers.

8. Click Apply.

Related links
   - Register SupportAssist Enterprise
   - View and update the contact information
   - Registration
   - Contact Information

Integrate SupportAssist Enterprise with your TechDirect account

About this task
You can integrate SupportAssist Enterprise with specific TechDirect accounts, based on your preference.

Steps
1. Point to Settings and click TechDirect Login. The TechDirect Integration page is displayed.

2. Click Switch Account. The TechDirect Sign In page is displayed in a new web browser window.

3. Type the TechDirect username and password in the appropriate fields, and then click Sign In. The One-Time Password (OTP) is displayed.

4. In the TechDirect Integration page, enter the OTP in the appropriate field, and then click Apply. The user name of the integrated TechDirect account is displayed on the page.

5. In the TechDirect portal, log in to TechDirect by using the TechDirect username and password. The TechDirect Dashboard is displayed.

6. From the Services menu, click SupportAssist, and then in the SupportAssist Services page, click the Assets tab.

7. Click Manage Assets.
SupportAssist Enterprise is integrated with the TechDirect account. Also, after synchronization of the account is complete, the asset and alert information is displayed in the Manage Assets page in TechDirect. This synchronization operation may take up to 4 hours.

## Configure 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.

### Prerequisite

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 ranges or host name expressions 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, Storage SC Series 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.
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

### Figure 37. 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.

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.

### View 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.

### Perform 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.

### Test 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.

#### 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.
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.

### Clear the System Event Log

#### Prerequisite
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.

**Figure 39. 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. The application checks if any updates are available, every Monday at 11 p.m. (date and time as on the server where SupportAssist Enterprise is installed).

- **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. The application checks if any policy files updates are available, every Monday at 11:30 p.m. (date and time as on the server where SupportAssist Enterprise is installed).

- **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. The application checks if any product support files updates are available, every Monday at 11:30 p.m. (date and time as on the server where SupportAssist Enterprise is installed).

- **Adapter upgrade** — Enables support for more and newer versions of the OpenManage Essentials, System Center Operations Manager, or OpenManage Enterprise adapter. By upgrading the adapter, SupportAssist Enterprise can add and inventory more device types and device models from the systems management console. The application checks if any adapter upgrade updates are available, every Monday at 11:30 p.m. (date and time as on the server where SupportAssist Enterprise is installed).

**NOTE:** The adapter will be updated only if the update option is available.

By default, automatic update is enabled for the SupportAssist Enterprise application, policy files, product support files, and the adapter. 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 Enable or disable 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 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 — `<Drive where SupportAssist Enterprise is installed>:\Program Files\Dell\SupportAssist\logs`
- On Linux — `/opt/dell/supportassist/logs`

Enable or disable automatic updates

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

**Prerequisite**
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.
Delete a device

Prerequisite
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.

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

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 devices that you want to delete.
3. Click Delete.
   The Confirm Device Deletion window is displayed.
Figure 40. Delete option

4 Click Yes.

The devices are deleted from the Devices page.

**NOTE:** When a device is deleted, 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.
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. 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 Configure email notification settings.
- Configure SupportAssist Enterprise to send email notifications through the SMTP server (email server) utilized by your company. See Configure SMTP server settings.

**NOTE:** For information about the different types of SupportAssist Enterprise email notifications, see Types of email notifications.

### Configure email notification settings

**Prerequisite**
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 link**
Preferences
Configure SMTP server settings

**Prerequisite**
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**

> **NOTE:** Configuring the SMTP server settings is optional.

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.

**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 link**
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>
<thead>
<tr>
<th>Email notification type</th>
<th>When the email notification is sent</th>
<th>Origin of the email notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration confirmation and welcome email</td>
<td>After the registration of SupportAssist Enterprise is completed successfully.</td>
<td>SupportAssist server hosted by Dell</td>
</tr>
<tr>
<td>Case created</td>
<td>After a hardware issue is detected and a support case is created.</td>
<td>SupportAssist server hosted by Dell</td>
</tr>
<tr>
<td>Unable to create a case</td>
<td>After a hardware issue is detected, but a support case could not be created because of technical difficulties.</td>
<td>SupportAssist server hosted by Dell</td>
</tr>
<tr>
<td>Unable to collect system information</td>
<td>After a support case is created automatically for a device, but SupportAssist Enterprise is unable to collect system information from the device.</td>
<td>SupportAssist server hosted by Dell</td>
</tr>
<tr>
<td>Unable to send the collected system information to Dell</td>
<td>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.</td>
<td>SupportAssist server hosted by Dell</td>
</tr>
<tr>
<td>Email notification type</td>
<td>When the email notification is sent</td>
<td>Origin of the email notification</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inactive notification</td>
<td>If SupportAssist Enterprise is not monitoring any device and no device has been added in the past 30 days.</td>
<td>SupportAssist server hosted by Dell</td>
</tr>
<tr>
<td>Connectivity test alert</td>
<td>At 11 p.m. each day (date and time as on the server where SupportAssist Enterprise is installed).</td>
<td>SupportAssist Enterprise application</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The connectivity test alert notification is sent only if an issue is detected with connectivity to dependent resources.</td>
<td></td>
</tr>
<tr>
<td>Automatic maintenance mode</td>
<td>If an alert storm received from a device has resulted in SupportAssist Enterprise placing the device automatically in maintenance mode.</td>
<td>SupportAssist Enterprise application</td>
</tr>
<tr>
<td>Device status alert</td>
<td>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.</td>
<td>SupportAssist Enterprise application</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The device alert notification is sent only if an issue exists (warning or error status) with the setup or configuration of the devices.</td>
<td></td>
</tr>
</tbody>
</table>
| Issue with the adapter or Remote Collector | • Within 5 minutes after an adapter or Remote Collector connectivity issue is detected.  
• If the issue is not resolved, another email notification is sent 6 hours after the first email was sent. | SupportAssist Enterprise application                                  |
<p>| Resumed normal operations with the adapter or Remote Collector | If the issue is resolved within 6 hours, after the issue was detected. | SupportAssist Enterprise application                                  |
| Final message regarding unresolved issue with the adapter or Remote Collector | If the issue is not resolved within 6 hours, after the issue was detected. | SupportAssist Enterprise application                                  |
| Inventory validation summary             | After SupportAssist Enterprise has completed validating your device inventory for its automated support capabilities—support case/incident creation and collection of system information. | SupportAssist Enterprise application                                  |
| Alert from devices in Staging and Inactive group | If SupportAssist Enterprise has detected that the monitoring and automatic support request/incident creation capabilities are limited for some of your devices. | SupportAssist Enterprise application                                  |</p>
<table>
<thead>
<tr>
<th>Email notification type</th>
<th>When the email notification is sent</th>
<th>Origin of the email notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parts dispatch address validation</td>
<td>When SupportAssist Enterprise has detected a hardware issue on one of your devices and a part replacement is required to resolve the issue.</td>
<td>SupportAssist Enterprise application</td>
</tr>
<tr>
<td>Parts dispatch address confirmation</td>
<td>After the replacement part is ready to be dispatched.</td>
<td>SupportAssist Enterprise application</td>
</tr>
</tbody>
</table>

**NOTE:** Email notifications can be received only if the Receive email notification when a new support case is opened option is selected. See Configuring email notification 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 Enable or disable the automatic collection of system information on case creation.
- Disable the periodic collection of system information from all devices. See Enable or disable the periodic collection of system information from all devices.
- Disable the collection of identity information from all devices. See Enable or disable the collection of identity information.
- Disable the collection of software information and the system log from all devices. See Enable or disable the collection of software information and the system log.
- Enable or disable the automatic upload of collections. See Disable the automatic upload of collections.

Topics:
- Prerequisites for collecting system information
- Enable or disable the automatic collection of system information on case creation
- Enable or disable the periodic collection of system information from all devices
- Enable or disable the collection of identity information
- Enable or disable the collection of system information
- Enable or disable 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 about the hard drive space requirements, see Hardware requirements.
- For collecting system information from a remote device, the remote device 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 about the network port requirements, see Network requirements.
- If you have added a server in SupportAssist Enterprise by using the operating system IP address or hostname (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 that you have entered in SupportAssist Enterprise must have administrative privileges.
    - The device credentials must have privileges that are 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.
  - If the server is running a Linux operating system:
    - The device credentials that 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 Configure 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 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.
- Ensure that the system drive of the remote server running Windows operating system is accessible from the system on which SupportAssist Enterprise is installed.
- If your device is associated with a remote collector, ensure that the system drive of the device is reachable from the remote collector.

**Enable or disable the automatic collection of system information on case creation**

**Prerequisite**
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 link**
Preferences

**Enable or disable the periodic collection of system information from all devices**

**Prerequisite**
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 user-defined 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.

**Steps**
1. Point to **Settings** and click **Preferences**.
The Preferences page is displayed.

2 In Automatically collect system state information, select or clear the Starting from day N of every month at 11 PM option.

3 Click Apply.

Related link
Preferences

Enable or disable the collection of identity information

Prerequisite
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 details in the information that is sent to Dell option.

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

**NOTE:** If you clear the Include identification details in the information that is 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.
**Enable or disable the collection of system information**

**Prerequisite**
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:** When you select the collection purpose as Deployment, the following are collected by default:
   - Software and SMART logs from Server / Hypervisor
   - Logs from Fluid File System
   - Inter Array Connectivity Test logs from PeerStorage (PS) / EqualLogic

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

   **NOTE:** For information about the logs that are collected by SupportAssist Enterprise, see the SupportAssist Enterprise Version 2.0.21 Reportable Items document at Dell.com/ServiceabilityTools.
3. Click **Apply**.

**Enable or disable the automatic upload of collections**

**Prerequisite**
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**.

---

**NOTE:** If you have disabled the collection of identity information from devices, the identity information such as hostname, IP address, and so on, are replaced by tokenized values in the collected system information. The tokenized values are represented as TOKENn—for example, TOKEN0, TOKEN1, or TOKEN2.

3. Click **Apply**.

**Related link**
Preferences
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 Register 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 Start the collection of system information from multiple devices.

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 View 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.

**NOTE:** Collections tab will only display system information collected during the last 7 days. To view collections that are older than 7 days, use the date filter to display the list of collections.

Topics:

- View a collection from the Devices page
- View a collection from the Collections page
- Refine collections based on a date range
- Configuration Viewer
- Items reported in periodic collections from servers
- Download and view a multiple device collection

View 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.

Figure 41. 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.

View 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.
Steps
1. Point to Collections and click View Collections. The Collections page is displayed.
2. Select a collection that you want to view.

![Collection Overview Pane](image)

**Figure 42. 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 (for server collections) or Download (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.

Refine collections based on a date range

**Prerequisite**
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 Configuration Viewer displays information in a tabbed format. 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 Configuration Viewer comprises of the following:

- Top pane — Displays the various categories and sub categories of collection data in a menu format. You can move the mouse pointer over the menu to see subcategories. You can click Expand All or Collapse All to quickly expand or collapse all categories. In addition, the top pane also displays the Contacts tab and the Section Status tab.
  - Contacts — Displays case details, customer information that you have provided while registering SupportAssist Enterprise, collections details, and the application information. The Contacts tab is the default tab.
  - Section Status — Displays an overview of the section-level information of a collection. This tab displays the status and description of each section of the collection. The number of items that are displayed in Section Status is dependent on the configuration of the device. The Section Status section also displays the count and status of the collection. The available statuses are:
    - Success
    - Failed
    - Warning

- Bottom pane — Displays the collection details. The bottom pane also displays the information available for the category or subcategory that is selected in the top pane. To view more details of the collection, click one of the subcategories. When you click a category, the category is expanded, enabling you to view its sub categories. The bottom pane also includes a navigation trail, which you can click to navigate backwards on the current trail.

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
- Software — If the collection includes the system information from a software
- Virtual Machine — If the collection includes the system information from a virtual machine

![Figure 43. Device configuration viewer](image)

**NOTE:** If you have disabled the collection of identity information from devices, the identity information such as hostname, IP address, and so on, are replaced by tokenized values in the collected system information. The tokenized values are represented as TOKENn—for example, TOKEN0, TOKEN1, or TOKEN2.

**NOTE:** For a list of items that may be reported in collections from a server, see [Items reported in periodic collections from servers](#).
Log types

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

<table>
<thead>
<tr>
<th>Log types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structured logs</td>
<td>Contain application logs, Embedded Server Management (ESM) logs, smart logs, and event logs. When you click the Structured Logs 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.</td>
</tr>
<tr>
<td>Unstructured logs</td>
<td>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 Unstructured Logs category, the configuration viewer displays the list of available unstructured logs.</td>
</tr>
</tbody>
</table>

**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 2.0.21 Reportable Items document at 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>
<thead>
<tr>
<th>Items reported</th>
<th>Device added in SupportAssist Enterprise with Device Type as Server / Hypervisor</th>
<th>Device added in SupportAssist Enterprise with the Device Type as iDRAC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OMSA is installed on the device</td>
<td>OMSA is not installed on the device</td>
</tr>
<tr>
<td>Memory</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Memory Array</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Memory Operating Mode</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Memory Redundancy</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Slot</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Items reported</td>
<td>Device added in SupportAssist Enterprise with Device Type as Server / Hypervisor</td>
<td>Device added in SupportAssist Enterprise with the Device Type as iDRAC</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>OMSA is installed on the device</td>
<td>OMSA is not installed on the device</td>
</tr>
<tr>
<td>Controller</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Connector</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>PCIe-SSD-Extender</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Enclosure</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Array Disk</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Intrusion Switch</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Hardware Log</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Main Chassis</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Additional Information</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Modular Enclosure Information</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Firmware</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Processor</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Fan</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Fan Redundancy</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Temperature</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Voltage</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Power Supply</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Power Supply Redundancy</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Network</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>Items reported</td>
<td>Device added in SupportAssist Enterprise with Device Type as Server / Hypervisor</td>
<td>Device added in SupportAssist Enterprise with the Device Type as iDRAC</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Team Interface</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Interface Member</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Remote Access Device</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DRAC Information</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Serial Over LAN Configuration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IPv6 Detail</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>User Setting</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>User Information</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iDRAC User Privilege</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DRAC User Privilege</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Serial Port Configuration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NIC Configuration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Component Detail</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Controller TTY Log</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Operating System</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

**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.

# Download and view 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.

   VIEWING COLLECTIONS
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.
Using SupportAssist Enterprise to collect and send system information

SupportAssist Enterprise automates the collection of system information from your devices both periodically and on case creation. If required, you can also manually start the collection and upload of system information to Dell EMC at any time. You can choose to start the collection of 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 EMC, see the *SupportAssist Enterprise Version 2.0.21 Support Matrix* at [www.dell.com/serviceabilitytools](http://www.dell.com/serviceabilitytools).

**Topics:**
- Set up SupportAssist Enterprise for collecting and sending system information
- Start the collection of system information from a single device
- Start the collection of system information from multiple devices
- Upload a collection
- Upload a collection from a disconnected site

### Set 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 *Start 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 *Install SupportAssist Enterprise*.
2. (Optional) Register SupportAssist Enterprise. See *Register 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.
Start the collection of system information from a single device

**Prerequisites**

- Ensure that you have completed setting up SupportAssist Enterprise. See Set 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.
Figure 45. Starting a collection from a single device

3 Click **Start collection**.
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.

1. **NOTE:** If you want to cancel the collection of system information, click the \(\times\) icon that is displayed next to the progress bar.

2. **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.

3. **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.

**Start the collection of system information from multiple devices**

**Prerequisite**
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.

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

**Steps**

1. Point to Devices and click View Devices.
   
   The Devices page is displayed.

2. Select the devices from which you want to collect system information.
   
   The Start Collection link is disabled when you select more than one device.

3. From the Collection Purpose list, select a reason for the collection.
   
   The Start Collection link is enabled.

4. Click Start Collection.
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 Download and view 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.
Upload a collection

Prerequisite
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 5 GB.

Figure 49. Upload collection option

The Upload Status column displays the status of the upload.

Upload 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 Start the collection of system information from a single device.
2. If the collection was performed by SupportAssist Enterprise:
• For storage, networking, or multiple device collections only — On the Collections page, select the collection, and in the collection overview pane, click Download File.

• For other device collections, depending on the operating system, you can access the collection .zip file at the following location:
  – Windows — <Drive where SupportAssist Enterprise is installed>:\Program Files\Dell\SupportAssist\reports
  – Linux — /opt/dell/supportassist/scripts/reports

• If the collection was performed by a Remote Collector, log in to the server where the Remote Collector is installed. Depending on the operating system, you can access the collection .zip file at the following location:
  – Windows — <System drive of the remote system>:\Program Files\Dell\SupportAssist\reports
  – Linux — /opt/dell/supportassist/scripts/reports

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 Enable or disable 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 Enable or disable device-level maintenance mode.

- **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 Enable or disable 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:

- Enable or disable global-level maintenance mode
- Enable or disable device-level maintenance mode
Enable or disable global-level maintenance mode

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

**Prerequisite**
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 link**
- Preferences

Enable or disable device-level maintenance mode

**Prerequisite**
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 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.

**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.
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>
<thead>
<tr>
<th>Operating system where SupportAssist Enterprise is installed</th>
<th>SupportAssistAdmins</th>
<th>SupportAssistUsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>Local Administrators</td>
<td>Users</td>
</tr>
<tr>
<td>Windows domain controller</td>
<td>Domain Admins</td>
<td>Domain Users</td>
</tr>
<tr>
<td>Linux</td>
<td>root group</td>
<td>users group</td>
</tr>
</tbody>
</table>

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
- Add users to the SupportAssist Enterprise user groups – Windows
- Add 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>
<thead>
<tr>
<th>SupportAssist Enterprise functions</th>
<th>SupportAssistAdmins and users with elevated or administrative privileges</th>
<th>SupportAssistUsers and users with normal privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>View cases and check for cases</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>View the device inventory and device groups</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>View the collections page</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>View the collected system information</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Perform network connectivity tests</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Perform the case creation test</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Perform case management actions</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Create, manage, edit, or delete device groups</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Complete the registration of SupportAssist Enterprise</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Add devices</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Perform deep discovery</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Create device discovery rule</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Edit device credentials</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Delete devices</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Install/upgrade OMSA by using SupportAssist Enterprise</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Configure SNMP by using SupportAssist Enterprise</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Enable or disable global-level maintenance mode</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Enable or disable device-level maintenance mode</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Manually start the collection and upload of system information from a single device or multiple devices</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>View and configure SupportAssist Enterprise settings</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Perform automatic update</td>
<td>✓</td>
<td>x</td>
</tr>
</tbody>
</table>
SupportAssist Enterprise functions | SupportAssistAdmins and users with elevated or administrative privileges | SupportAssistUsers and users with normal privileges
--- | --- | ---
Clear System Event Log | ✔️ | ✗
Set up, edit, or delete an adapter | ✔️ | ✗
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 | ✔️ | ✗

| SupportAssist Enterprise user groups – Windows

**Prerequisite**
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.

Add users to the SupportAssist Enterprise user groups – Linux

**Prerequisite**
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:
   
   ```shell
   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:

   ```shell
   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 configure the alert destination of iDRAC by using the web interface
- Manually configure the alert destination of a chassis by using the web interface
- Manually configure 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 Configure SNMP settings by using SupportAssist Enterprise.

Related links
- Manually configuring the alert destination of a server by using the script file on server running Windows
- Manually configuring the alert destination of a server running Windows
- Manually configuring the alert destination of a server by using the script file on a server running Linux
- Manually configuring the alert destination of a server running Linux

Manually configuring the alert destination of a server by using the script file on server running 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:
- 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
- Windows Server 2019 Essentials and Datacenter
- Windows 2008 Small Business Server
- Windows 2011 Small Business Server
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016
- Windows Server Core 2019

Steps
1. On the server where SupportAssist Enterprise is installed, browse to the `<Drive where SupportAssist Enterprise is installed>\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 link
Manually configuring the alert destination of a server

Manually configuring the alert destination of a server running 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.
In the Services window, right-click SNMP Service and click Restart.

Related link
Manually configuring the alert destination of a server

Manually configuring the alert destination of a server by using the script file on a server running 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

Steps
1. On the server where SupportAssist Enterprise is installed, browse to the <Drive where SupportAssist Enterprise is installed>\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.
Open the terminal window and log in as a user with root privileges.

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 link**
Manually configuring the alert destination of a server

### Manually configuring the alert destination of a server running 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 link**
Manually configuring the alert destination of a server

### Manually configure 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 (public) and the SNMP alert port number (for example, 162) in the appropriate fields. For more information about the options, see *iDRAC Online Help*.
1. 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.

1. 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.

Manually configure the alert destination of a chassis by using the web interface

Prerequisite
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.

   1. 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 configure the alert destination of a networking device

About this task

1. 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.
Managing SupportAssist Enterprise alerts in TechDirect

Dell EMC TechDirect is a centralized support portal that enables administrators in your organization to manage alerts that are created by SupportAssist Enterprise. By default, SupportAssist Enterprise automatically forwards alerts that qualify for support case creation or parts dispatch to Dell EMC. TechDirect enables Administrators to set rules that allow them to review and determine if the alerts need to be forwarded to Dell EMC for case creation or parts dispatch.

Topics:
- Set up TechDirect to receive SupportAssist Enterprise alerts
- Configure alert rules in TechDirect
- View SupportAssist Enterprise alerts in TechDirect
- SupportAssist alerts
- SupportAssist alert actions

Set up TechDirect to receive SupportAssist Enterprise alerts

Prerequisite
The server where SupportAssist Enterprise is installed must have internet connectivity.

About this task
Setting up TechDirect to receive alerts from SupportAssist Enterprise enables you to view and manage alerts.

Steps
   The TechDirect home page is displayed.
2. Click Register and enter the following information on the Registration page:
   a. In the Contact Information section, type the first name, last name, email address, and company name, and select the country.
   b. In the Account Information section, select the preferred language and time zone.
   c. In the TechDirect Terms of Use section, read about the Dell TechDirect portal access and site terms of use, and then select Yes, I agree to the TechDirect Terms of Use.
   d. In the Security Check section, type the displayed text.
3. Click Submit.
   The Registration Complete page is displayed.
4. Click Sign In and type your TechDirect user name and password.
   The TechDirect Dashboard is displayed.
5. From the Services menu, click SupportAssist.
   The SupportAssist page is displayed.
6. Read about the SupportAssist terms of use and select I have read and understood these terms and conditions, and I am authorized to accept these terms.
7. If you have multiple accounts, select an account from the Select Account list.
8. In the Manage Devices gadget, click Manage.
   The Manage Devices page is displayed.
TechDirect is set up to receive alerts from SupportAssist Enterprise.

## Configure alert rules in TechDirect

**About this task**

Administrators in your organization can configure rules to determine how alerts created by SupportAssist are handled by the TechDirect portal. For example, you can choose to automatically forward all alerts to technical support or have the alerts placed in your SupportAssist alert queue for your support team to review and determine if the alert should be forwarded to Dell.

### Steps

1. Go to [TechDirect.com](#).
   
   The TechDirect home page is displayed.

2. Click **Sign In** and type your TechDirect user name and password.
   
   The TechDirect **Dashboard** is displayed.

3. From the **Services** menu, click **SupportAssist**.
   
   The **SupportAssist** page is displayed.

4. In the **Configure Rules** gadget, click **Configure**.
   
   The **Configure SupportAssist Alert Rules** page is displayed.

5. In the **Inactivity notification alert period** field, type the desired duration.

6. For the **Automated technical support case requests?** option, select one of the following:
   
   - Select **Yes** to directly forward all technical support alerts to Dell.
   - Select **No** to send all technical support alerts to your company’s SupportAssist Enterprise alerts queue for review by your support team to determine if the alert should be forwarded to Dell.

7. For the **Auto-forward all Dispatch alerts to Dell?** option, select one of the following:
   
   - Select **Yes** to directly forward all parts dispatch alerts to Dell.
   - Select **No** to send all parts dispatch alerts to your company’s SupportAssist Enterprise alerts queue for review by your support team to determine if the alert should be forwarded to Dell.

   The **Group Management** section is displayed if you have chosen to forward all parts dispatch alerts to Dell.

8. Click **Add Group Rule**.
   
   The group rules are used to identify the address where dispatched parts should be sent. Whenever a SupportAssist Enterprise alert is forwarded to Dell EMC for parts dispatch, the address in the alert is compared with the addresses defined in the group rules. If there is a match, the address information associated with that group rule is used to identify the address where the dispatched parts should be sent.

9. On the **Add Group Rule** page, select one of the following options:
   
   - **By Country** — Select this option if you want to route all auto-dispatches from a country to a specific address.
   - **By State/Province** — Select this option if you want to route all auto-dispatches from a state or province to a specific address.
   - **By City** — Select this option if you want to route all auto-dispatches from a city to a specific address.
   - **By ZIP/Postal Code** — Select this option if you want to route all auto-dispatches with a ZIP/Postal Code to a specific address.

10. Enter the required details based on the option that you have selected in Step 8 and click **Save Rule**.

11. Click **Save Alert Rules**.

## View SupportAssist Enterprise alerts in TechDirect

**About this task**

You can view SupportAssist Enterprise alerts in TechDirect after you set up TechDirect to receive alerts.

### Steps

1. Go to [TechDirect.com](#).

164  Managing SupportAssist Enterprise alerts in TechDirect
The TechDirect home page is displayed.

2. Click **Sign In** and type your TechDirect user name and password. The TechDirect **Dashboard** is displayed.

3. From the **Services** menu, click **SupportAssist**. The **SupportAssist** page is displayed.

4. In the **Manage SupportAssist Alerts** tile, click **Manage**. The **SupportAssist Alerts** page is displayed.

### SupportAssist alerts

You can view details about the alerts generated by SupportAssist Enterprise through the TechDirect portal. The following table describes the details displayed on the **SupportAssist Alerts** page.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Tag</strong></td>
<td>Displays the unique identifier of the system which reported an issue.</td>
</tr>
<tr>
<td><strong>Alert Number</strong></td>
<td>Displays the unique support request number assigned to the alert that you can reference while communicating with technical support.</td>
</tr>
<tr>
<td><strong>Alert Type</strong></td>
<td>Displays the type of alert:</td>
</tr>
<tr>
<td></td>
<td>• Technical Support</td>
</tr>
<tr>
<td></td>
<td>• Dispatch</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>Displays details about the issue that was detected and error information for investigation.</td>
</tr>
<tr>
<td><strong>Create Timestamp</strong></td>
<td>Displays the date and time that the alert was created in TechDirect.</td>
</tr>
<tr>
<td><strong>Last Activity Time</strong></td>
<td>Displays the date and time of the last action taken by the customer Administrator or Technician User.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Displays the status of the alert:</td>
</tr>
<tr>
<td></td>
<td>• Unassigned — No customer Technician User has ownership</td>
</tr>
<tr>
<td></td>
<td>• Assigned — A customer Technician User has ownership</td>
</tr>
<tr>
<td></td>
<td>• Submit Failed — Attempt to forward to Dell failed</td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td>Click to view actions available for the alert.</td>
</tr>
<tr>
<td></td>
<td>Technician Users may:</td>
</tr>
<tr>
<td></td>
<td>• Take ownership of the alert</td>
</tr>
<tr>
<td></td>
<td>• Update the alert details</td>
</tr>
<tr>
<td></td>
<td>• Close the alert</td>
</tr>
<tr>
<td></td>
<td>• Forward the alert to Dell</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>Displays the Technician User who is currently the owner of an alert.</td>
</tr>
</tbody>
</table>

Managing SupportAssist Enterprise alerts in TechDirect
SupportAssist alert actions

You can take action on the alerts created by SupportAssist through the TechDirect portal. The following table describes the actions available for alerts created by SupportAssist.

Table 27. Alert actions

<table>
<thead>
<tr>
<th>TechDirect account type</th>
<th>Available actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator and Technician Users</td>
<td>Take Ownership</td>
<td>Individual Technician Users under a TechDirect account can see all SupportAssist Enterprise alerts as they arrive. A Technician User may take ownership of an alert. Technician Users may not reassign alerts, only the TechDirect Administrator for the account may reassign alerts.</td>
</tr>
<tr>
<td></td>
<td>Update</td>
<td>Displays the Details page that allows you to add a note or an attachment about the alert.</td>
</tr>
<tr>
<td></td>
<td>Close Alert</td>
<td>Closes the alert. Both you and Dell will not be able to take any further action on the alert.</td>
</tr>
<tr>
<td></td>
<td>Forward To Dell</td>
<td>Forwards the support request to technical support. You can continue to monitor progress from either your Technical Support or Dispatch Summary pages in TechDirect.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Assign Ownership</td>
<td>Assigns a Technician User as the owner of an alert. May also be used to reassign to another Technician User.</td>
</tr>
</tbody>
</table>
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
- Installing patch for SupportAssist Enterprise
- Enable or disable API interface settings
- Signing in to TechDirect
- Deep discovery
- Device correlation
- Association view
- Detection of hardware issues in attached storage devices
- Support for Dell OEM servers
- Install Net-SNMP on a server running Linux
- Configure sudo access for SupportAssist Enterprise on a server running 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
- View 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 2.0.21 Support Matrix** at [Dell.com/ServiceabilityTools](https://www.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.

**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 2.0.21 Support Matrix at 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 ✔️ Success.

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 link
Install or upgrade 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 link
Configure SNMP settings by using SupportAssist Enterprise

Installing patch for SupportAssist Enterprise

Occasionally, a patch may be available for SupportAssist Enterprise to address certain issues and potential security vulnerabilities.

SupportAssist Enterprise checks if any patch updates are available, every Monday at 10.30 p.m. (date and time as on the server where SupportAssist Enterprise is installed).

When a patch is available, a Patch for SupportAssist Enterprise (Optional Patch) banner is displayed with the following options:

- **Update now** — To enable SupportAssist Enterprise to download and install the update.
- **Skip this version** — To skip the update. The update available banner is not displayed again until the next version of the update is available.
- **Remind me later** — To close the Update Available banner. The Update Available banner is not displayed until you log in to SupportAssist Enterprise again.
- **More Info** — Provides details about the patch version and the fixes available in the patch update.
Enable or disable API interface settings

Prerequisite
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
Enabling REST API interfaces enables you to programmatically integrate SupportAssist Enterprise with your data center tools and applications. For more information, see the REST API Guide — SupportAssist Enterprise at Dell.com/ServiceabilityTools.

NOTE: You can perform a maximum of 10 operations such as adding devices and collecting system information, in parallel. Before you query the operation status and operation ID, ensure that there is a minimum delay of 5 seconds.

Steps
1. Point to Settings and click Preferences. The Preferences page is displayed.
2. In API Interface Collection Data Settings, depending on your requirement, select or clear the Enable API Interfaces for SupportAssist Enterprise option.
3. Click Apply.

Signing in to TechDirect

Signing in to your company's TechDirect account from SupportAssist Enterprise enables you to integrate automated parts dispatch with your company's TechDirect account. For more information, see Integrate parts dispatch with your TechDirect account.

You can sign in to your TechDirect account through one of the following methods:

• During the registration of SupportAssist Enterprise
• On the TechDirect Login page

When you try to sign in to your TechDirect account in SupportAssist Enterprise:

1. The TechDirect Sign In page is displayed.
2. After you enter the credentials and click Sign In, the OTP is displayed.
3. Enter the OTP and click Submit.

NOTE:
• When you sign in to your TechDirect account in SupportAssist Enterprise, you are automatically signed in with the same TechDirect account to Dell portals that you may open on any other window or tab of the same web browser.
• If you had already signed in to any Dell portal on the web browser, and then try to sign in to TechDirect in SupportAssist Enterprise, the OTP related to the signed in account is displayed. To continue signing in to the same account, enter the OTP and click Submit. If you want to use a different account to sign in, then sign out from the Dell portal and then try again.

Related link
TechDirect Login
Deep discovery

The deep discovery feature enables you to discover and add other devices that are associated with a primary device. To perform deep discovery, you must assign a credential profile to the discovery task. You can choose to perform deep discovery while discovering the primary device or after the primary device is discovered.

**NOTE:** Deep discovery may result in an increase in the duration of the overall discovery process.

The following table lists the primary device and its associated devices that are discovered by deep discovery.

<table>
<thead>
<tr>
<th>Primary Device</th>
<th>Associated devices discovered by deep discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server running Windows</td>
<td>• vCenter</td>
</tr>
<tr>
<td></td>
<td>• SCVMM</td>
</tr>
<tr>
<td></td>
<td>• SAN-HQ</td>
</tr>
<tr>
<td>Chassis</td>
<td>iDRAC*</td>
</tr>
<tr>
<td></td>
<td>Networking switches</td>
</tr>
<tr>
<td>Storage PS Series group</td>
<td>• Storage PS Series members</td>
</tr>
<tr>
<td></td>
<td>• Storage PS Series FluidFS</td>
</tr>
<tr>
<td>Storage MD Series Enclosure</td>
<td>JBODs</td>
</tr>
<tr>
<td>Networking - management switch</td>
<td>Member switches</td>
</tr>
<tr>
<td>Web-scale converged appliances</td>
<td>• Controller VM</td>
</tr>
<tr>
<td></td>
<td>• Node (iDRAC / ESX)</td>
</tr>
</tbody>
</table>

* On deep discovery of chassis, discovery of the iDRAC (modular servers) is supported only for iDRAC7 or later.

**NOTE:** On deep discovery of a chassis, networking devices associated with the chassis are also discovered. However, you can collect system information only from networking devices that are supported by SupportAssist Enterprise. For the list of supported networking devices, see the SupportAssist Enterprise Version 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

**Related links**
- Add a server or hypervisor
- Add a chassis
- Add a Networking device
- Add a solution
- Perform deep discovery
- Association view

**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.

**Association view**

The Devices page supports two types of views for displaying the list of devices:

- Default view — Displays all available devices as a list
- Association view — Displays all available devices as groups based on their association. This view enables you to view a primary device and its associated devices as a group

The following table lists how the devices are grouped in the association view.

### Table 29. Device grouping in association view

<table>
<thead>
<tr>
<th>Primary Device</th>
<th>Associated devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>• iDRAC</td>
</tr>
<tr>
<td></td>
<td>• vCenter</td>
</tr>
<tr>
<td></td>
<td>• SCVMM</td>
</tr>
<tr>
<td></td>
<td>• SAN-HQ</td>
</tr>
<tr>
<td>Chassis</td>
<td>• iDRAC*</td>
</tr>
<tr>
<td></td>
<td>• Networking switches</td>
</tr>
<tr>
<td>Storage PS Series group</td>
<td>• Storage PS Series members</td>
</tr>
<tr>
<td></td>
<td>• Storage PS Series FluidFS</td>
</tr>
<tr>
<td>Storage MD Series Enclosure</td>
<td>JBODs</td>
</tr>
<tr>
<td>Networking - management switch</td>
<td>Member switches</td>
</tr>
<tr>
<td>Web-scale converged appliances</td>
<td>• Controller VM</td>
</tr>
<tr>
<td></td>
<td>• iDRAC</td>
</tr>
</tbody>
</table>

* Only iDRAC7 or later is displayed under the Chassis node.

**NOTE:** Starting the collection of system information is not supported for the following devices that may be displayed in the Association view:

- JBODs
- Storage PS Series members
- Stacked switches
- Devices that are listed in SupportAssist Enterprise with an IP address as 0.0.0.0

**Related link**

Deep discovery
Detection of hardware issues in attached storage devices

In addition to monitoring PowerEdge servers, SupportAssist Enterprise can also process alerts received from Dell EMC Storage MD Series 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 EMC 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 Technical Support and not available for other support case service request management systems.

As with any system that is modified for custom solutions, it is recommended that you verify all SupportAssist Enterprise features to ensure proper operation with those modifications.

Install Net-SNMP on a server running Linux

**Prerequisite**
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:
     2. `zypper refresh`
     3. `zypper install net-snmp`

Configure sudo access for SupportAssist Enterprise on a server running 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.

**Prerequisite**
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://is.us.dell.com/*` — the file upload server and related services.
  - `https://downloads.dell.com/*` — For downloading Dell OpenManage Server Administrator (OMSA) and receiving new SupportAssist Enterprise release information, policy files, and product support files.
  - 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: `is.us.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 Configure 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 (`<Drive where SupportAssist Enterprise is installed>\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`
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. 20171101
- application.log. 20171102.zip
- application.log. 20171103.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 <Drive where SupportAssist Enterprise is installed>:
\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.

### View 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.

**NOTE:** During the uninstallation of SupportAssist Enterprise, all adapters and Remote Collectors that you have set up are also uninstalled, provided the systems hosting the adapters and Remote Collectors are reachable.
Uninstall SupportAssist Enterprise - Windows

Prerequisite
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.
   • On Windows Server Core 2016 or 2019, open the terminal emulator and run the following commands:
     1. wmic get product name
     2. wmic product get
     3. wmic product get IdentifyingNumber
     The unique identification number is displayed.
     4. MsiExec.exe /<unique identification number>
     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 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.

Uninstall SupportAssist Enterprise - Linux

Prerequisite
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.

Uninstall SupportAssist Enterprise in silent mode - Linux

Prerequisite
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 30. PowerEdge server examples

<table>
<thead>
<tr>
<th>PowerEdge server generation</th>
<th>Representation of the server model</th>
<th>Examples of server models</th>
</tr>
</thead>
<tbody>
<tr>
<td>9th</td>
<td>PowerEdge x9xx</td>
<td>PowerEdge 2900</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power Edge 6950</td>
</tr>
<tr>
<td>10th</td>
<td>PowerEdge yx0x</td>
<td>PowerEdge M600</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge R300</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge T105</td>
</tr>
<tr>
<td>11th</td>
<td>PowerEdge yx1x</td>
<td>PowerEdge M610</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge R310</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge T110</td>
</tr>
<tr>
<td>12th</td>
<td>PowerEdge yx2x</td>
<td>PowerEdge M620</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge R620</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge T620</td>
</tr>
<tr>
<td>13th</td>
<td>PowerEdge yx3x</td>
<td>PowerEdge M630</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge R630</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge R730</td>
</tr>
</tbody>
</table>

Other useful information
<table>
<thead>
<tr>
<th>PowerEdge server generation</th>
<th>Representation of the server model</th>
<th>Examples of server models</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PowerEdge FC630</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge T320</td>
</tr>
<tr>
<td>14th</td>
<td>PowerEdge yx4x</td>
<td>PowerEdge R740</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge T640</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge M640</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerEdge R7415</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DSS 9620</td>
</tr>
</tbody>
</table>

**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
- 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
- Tool tips
- Other services
- Security
- Logs

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 Perform 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 <Drive where SupportAssist Enterprise is installed>:\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](image) status:

° If the device is an iDRAC, ensure that the iDRAC has an Enterprise or Express license installed. For information on purchasing and installing an Enterprise or Express license, see "Managing Licenses" section in the iDRAC User's Guide at Dell.com/idracmanuals.
° If the device is a Storage SC Series 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.
° 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.

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 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.
° Ensure that the prerequisites for adding the device are met. For information on the prerequisites for adding a device, see Adding devices.
° Verify if the device is reachable from the server where SupportAssist Enterprise is installed.
° Verify if the device credentials (user name and password) you provided are correct.
° If the error message states that the device could not be added within the predefined time limit, retry adding the device.
° If the device encryption level is greater than 128 bits, perform one of the following:
  – Reduce the encryption level to 128 bits.
  – On the server running SupportAssist Enterprise, the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files must be installed in the Java Development Kit (JDK) or Java Runtime Environment (JRE). For more information on the JCE Unlimited file, visit Oracle.com.

**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.
° 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 Configure 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.
- 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: `<Drive where SupportAssist Enterprise is installed>\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 a Storage PS Series 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 Storage 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.

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 SAN Headquarters device from the registry entry: HKLM\SOFTWARES\PerformanceMonitor.
  - Ensure that the value of the install type attribute is "Full" and logdir attribute has a value.
Ensure that the WMI and EQLPerfX services are running on the device.

**Solution**

- Ensure that you are logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- Ensure that the device is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that port 443 is open on the device.
- Ensure that firmware version 4.x or later is installed on the device for the collection of system information.
- Verify if the assigned Account Credentials (user name and password) you provided are correct.

**Virtual machine**

- Ensure that you are logged in to SupportAssist Enterprise with elevated or administrative privileges. See [Granting elevated or administrative privileges to users](#).
- Ensure that the system hosting the virtual machine is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that the required ports and protocols are enabled on the network. See [Network port requirements](#).

**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 2.5 or later.
- 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 4.5 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.
- Locate the **appconfig.properties file** in the **config** folder, and then increase the timeout value for **adapter.websocket.timeout**. The default time is 5 seconds and maximum time is 1 minute.
- Ensure that **SupportAssist_RestError.xml** file is not present at **C:\ProgramData** on the system where OpenManage Essentials is installed.

**Unable to add Remote Collector**

If the **Remote Collectors** page displays a **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 the 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 the 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.
- For OpenManage Essentials adapter, if you have added the adapter by using your service account, try deleting the `REST_Error.xml` file available at `<System drive>\ProgramData`, and then manually synchronize the adapter.

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 Install or upgrade 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 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

SNMP not configured

If a device displays an **SNMP not configured** status:

- Configure the SNMP settings on the device by using the **Configure SNMP** option. See Configure 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 configure the alert destination of a server.
  - For a server that you added in SupportAssist Enterprise by using the iDRAC IP address: Manually configure 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 Install or upgrade 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 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.
Unable to configure SNMP

If a device displays an Unable to configure SNMP status:

- Ensure that the network settings are correct.
- Ensure that the SNMP port (162) is open.
- Ensure that the firewall settings are correct.
- Configure the SNMP settings of the device by using the Configure SNMP option. See Configure 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 configure the alert destination of a server.
- For a server that you added in SupportAssist Enterprise by using the iDRAC IP address: Manually configure 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 Configure 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 <System drive>\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 Configure sudo access for SupportAssist Enterprise (Linux).
  - Ensure that the device has all the required OMSA dependencies installed. For more information about OMSA dependencies, see the "Remote Enablement Requirements" section in the Dell OpenManage Server Administrator Installation Guide at DellTechCenter.com/OMSA.
• Retry the installation of OMSA. See Install or upgrade 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 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

**NOTE:** Upgrade from a 32-bit version of OMSA to a 64-bit version of OMSA is not supported. In this scenario, you must uninstall the existing version of OMSA, and install OMSA by using SupportAssist Enterprise. For instructions to install OMSA by using SupportAssist Enterprise, see Install or upgrade 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 Perform the connectivity test.
• Ensure that the OMSA services are running on the device.
• Retry the installation of OMSA. See Install or upgrade 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 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.

**OMSA not supported**

If a device displays the OMSA not supported status:

• Log in to the device and uninstall the existing version of OMSA.
• Install OMSA on the device by using the Install / Upgrade OMSA option. See Install or upgrade 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 Delete 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.

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 Configure 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.

If the error message states that SupportAssist Enterprise is unable to gather system information from the device because the SSL encryption level of the device is set to 256 bit or higher:

a. Download the Zulu Cryptographic Extension Kit available at the Azul Systems website.

b. Extract the downloaded file.

c. Copy the local_policy.jar and US_export_policy.jar files and paste them at the following location on the system where SupportAssist Enterprise is installed:

   - On Windows: `<Drive where SupportAssist Enterprise is installed>\Program Files\Dell\SupportAssist\jre\lib\security`
   - On Linux: `/opt/dell/supportassist/jre/lib/security`

d. Restart the SupportAssist service and retry the operation.

After resolving the underlying issue, manually initiate the collection and upload of system information. See Start 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:

  a. Disable WBEM on your device: `esxcli system wbem set --enable false`.
b. 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 a Storage PS Series 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 Storage SC Series array:

- Ensure that the REST service is running on the device.
- Ensure that SupportAssist is enabled in Enterprise Manager. For information on enabling SupportAssist in Enterprise Manager, see the *Dell Enterprise Manager Administrator's Guide* at [Dell.com/storagemanuals](https://Dell.com/storagemanuals).

If the device is a FluidFS NAS device, ensure that SSH service is running on the device.

**Networking**

- Ensure that Secure Shell (SSH) and SNMP service are running on the device.
- If the enable password is configured on the device, ensure that you provide the enable password in SupportAssist Enterprise.

**Chassis**

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

**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 SAN Headquarters device from the registry entry: `HKLM\SOFTWARE\Dell\SAN\PerformanceMonitor`
  - Ensure that the value of the install type attribute is "Full" and logdir attribute has a value.
  - Ensure that the WMI and EQLPerfX services are running on the device.

**Solution**

- Ensure that the device is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that port 443 is open on the device.
- Ensure that firmware version 4.x or later is installed on the device for the collection of system information.
Virtual machine

- Ensure that you are logged in to SupportAssist Enterprise with elevated or administrative privileges. See Granting elevated or administrative privileges to users.
- Ensure that the system hosting the virtual machine is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that the required ports and protocols are enabled on the network. See Network port requirements.

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 Start 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 Configure proxy server settings.
- Perform the network connectivity test and ensure that connectivity to the Dell upload server is successful. See Perform 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.
- Ensure that the collection file does not contain any potential threats such as viruses or malware.

After resolving the underlying issue, manually initiate the collection and upload of system information. See Start 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.
**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.

- 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 Configure 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 a Storage PS Series 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 Storage SC Series 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.

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 SAN Headquarters device from the registry entry: HKLM\SOFTWARES\PerformanceMonitor.

Ensure that the value of the install type attribute is "Full" and logdir attribute has a value.

Ensure that the WMI and EQLPerfX services are running on the device.

Solution

- Ensure that the device is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that port 443 is open on the device.
- Ensure that firmware version 4.x or later is installed on the device for the collection of system information.
- Verify if the assigned Account Credentials (user name and password) you provided are correct.

Virtual machine

- Ensure that you are logged in to SupportAssist Enterprise with elevated or administrative privileges. See Granting elevated or administrative privileges to users.
- Ensure that the system hosting the virtual machine is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that the required ports and protocols are enabled on the network. See Network port requirements.

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:

- Clear the System Event Log by using IDRAC
- Clear the System Event Log by using OMSA

Clear the System Event Log by using iDRAC

Prerequisite

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 clrsel
Steps
1. In the iDRAC web console, click **Overview > Server > Logs Page**.
2. Click **Clear Log**.

Clear the System Event Log by using OMSA

**Prerequisite**
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.

1. **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`

2. **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 **Enable or disable device-level maintenance mode**.
- If required, you may place SupportAssist Enterprise in maintenance mode. See **Enable or disable 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 **Perform 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.

- 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 Configure 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: <Drive where SupportAssist Enterprise is installed>:\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 a Storage PS Series 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 Storage SC Series 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.

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 SAN Headquarters device from the registry entry: HKLM\SOFTWARES\\PerformanceMonitor.
  - Ensure that the value of the install type attribute is "Full" and logdir attribute has a value.
  - Ensure that the WMI and EQLPerfX services are running on the device.

Solution

- Ensure that the device is reachable from the server where SupportAssist Enterprise is installed.
- Verify if the assigned Account Credentials (user name and password) you provided are correct.

Virtual machine

- Ensure that you are logged in to SupportAssist Enterprise with elevated or administrative privileges. See Granting elevated or administrative privileges to users.
- Ensure that the system hosting the virtual machine is reachable from the server where SupportAssist Enterprise is installed.
- Ensure that the required ports and protocols are enabled on the network. See Network port requirements.

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 Enable or disable 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 Perform the connectivity test.
- Perform the case creation test and ensure that the Ready to Create Cases status is displayed. See Test the case creation capability.
- Check the application.log file available at <Drive where SupportAssist Enterprise is installed>\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
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 [Verify the status of SupportAssist Enterprise services (Windows)](#) or [Verify 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 — `<Drive where SupportAssist Enterprise is installed>\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 [Perform 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.

**Verify the status of SupportAssist Enterprise services on 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.
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.

### Verify the status of SupportAssist Enterprise services on 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.

### Verify the status of SupportAssist Enterprise services on Ubuntu and Debian

To verify the status of the SupportAssist Enterprise services on Ubuntu and Debian operating systems:

1. Open the terminal window on the system where SupportAssist Enterprise is installed.
2. Type `systemctl status supportassist.service` and press Enter.
   
   The status of the Dell EMC SupportAssist Enterprise service is displayed.
3. Type `systemctl status supportassistdatabase.service` and press Enter.
   
   The status of the Dell EMC SupportAssist Enterprise DB service is displayed.

   **NOTE:** If your system is running the Systemd service, the Dell EMC SupportAssist Enterprise service and the Dell EMC SupportAssist Enterprise DB service may not display the correct status.
4. If the services are not running, type `systemctl start <service name>.service` and press Enter.
5. To stop the services, type `systemctl stop <service name>.service` and press Enter.
6. To restart the services, type `systemctl restart <service name>.service` and press Enter.

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

### Tool tips

If tool tips are not displayed in Mozilla Firefox:

1. Open Mozilla Firefox, and type `about:config` in the address bar.
2. If a warning is displayed, click Accept.
3. Verify if the `browser.chrome.toolbar_tips` value is set to True.
4. If the `browser.chrome.toolbar_tips` value is False, double-click the value to set it to True.

### 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

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.

Logs

If you notice that the size of the SupportAssist Enterprise application logs file increases intermittently, then:

1. Stop the SupportAssist Enterprise services.
2. Back up the application.log file.
3. Delete the application.log file.
4. Restart the SupportAssist Enterprise services.
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 Rules for Device Discovery** — Enables you to create device discovery rules.
  - **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 31. Links in the SupportAssist Enterprise header area

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SupportAssist Enterprise Community</td>
<td>Opens the SupportAssist Enterprise community website in a new browser window.</td>
</tr>
</tbody>
</table>

**User name**

The user name of the currently logged in user. Point to the **user name** link to view a drop-down list that contains the following links:

- **Network Connectivity Test** — Opens the Network Connectivity Test page.
- **SupportAssist Enterprise Test** — Opens the SupportAssist Enterprise Test page.
- **Logout** — Allows you to log out of SupportAssist Enterprise.

**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.
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 32. Banners in the SupportAssist Enterprise header area

<table>
<thead>
<tr>
<th>Banner</th>
<th>Description</th>
</tr>
</thead>
</table>
| Not registered                | This banner is displayed if you have not completed the registration of SupportAssist Enterprise. The not registered banner displays the following options:  
  - Register now — To register SupportAssist Enterprise.  
  - Remind me later — To close the 'not registered' banner. The 'not registered' banner is not displayed until you log in to SupportAssist Enterprise again.  
  - Why register — To learn about the importance of registering SupportAssist Enterprise. |
| Update available              | The types of banners displayed are:  
  - SupportAssist Enterprise  
  - Patch Update  
  - Product Support  
  - Policy Update  
  - OpenManage Essentials Adapter update  
  - System Center Operations Manager Adapter update  
  - OpenManage Enterprise Adapter update  
  This banner is displayed in the following scenarios:  
  - If an update is available, but you have disabled the automatic update of the SupportAssist Enterprise application, policy files, and product support files.  
  - If an error occurred during the update of SupportAssist Enterprise.  
  The update available banner displays the following options:  
  - Update now — To enable SupportAssist Enterprise to download and install the update.  
  - Skip this version — To skip the update. The update available banner is not displayed again until the next version of the update is available.  
  - Remind me later — To close the 'update available' banner. The 'update available' banner is not displayed until you log in to SupportAssist Enterprise again.  

1 **NOTE:** The update available banner is displayed only if you are logged in to SupportAssist Enterprise with administrative or elevated privileges.  

Also, one of the following banners may be displayed on the SupportAssist Enterprise user interface:  
  - Dispatch preference is a new feature in the upgraded application banner — This banner is displayed when you have upgraded to SupportAssist Enterprise without providing the dispatch address in the previous instance.  
  - Update your secondary shipping contact details for replacement parts dispatch to ensure a timely delivery banner — This banner is displayed when you have already provided the dispatch address in the previous instance and then upgraded to SupportAssist Enterprise. |
| Dispatch preferences          | This banner is displayed after you upgrade from SupportAssist Enterprise 1.1, 1.2, or later. |
| Maintenance Mode              | This banner is displayed when you place SupportAssist Enterprise in maintenance mode. For more information about maintenance mode, see Understanding maintenance mode. |
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.

**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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use proxy settings</td>
<td>Select this option to enable configuring the proxy server settings.</td>
</tr>
<tr>
<td>Proxy Server Address or Name</td>
<td>The proxy server address or name.</td>
</tr>
<tr>
<td>Proxy Port Number</td>
<td>The proxy server port number.</td>
</tr>
<tr>
<td>Proxy requires authentication</td>
<td>Select this option if the proxy server requires authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name required to connect to the proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password required to connect to the proxy server.</td>
</tr>
</tbody>
</table>

**Registration**

The *Registration* page enables you to provide your contact information and register SupportAssist Enterprise.

The fields that are displayed in the *Registration* page are described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Information</td>
<td></td>
</tr>
<tr>
<td>Company Name</td>
<td>The name of the company.</td>
</tr>
<tr>
<td>Country/Territory</td>
<td>The location of the company.</td>
</tr>
<tr>
<td>IT Administrator Contact Information</td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the primary contact.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the primary contact.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the primary contact.</td>
</tr>
<tr>
<td>Alternate phone number</td>
<td>The alternate phone number of the primary contact.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the primary contact. SupportAssist Enterprise email</td>
</tr>
<tr>
<td></td>
<td>notifications are sent to this email address.</td>
</tr>
<tr>
<td>Time zone</td>
<td>The time zone of the primary contact.</td>
</tr>
<tr>
<td>Parts Replacement Preferences for Dell Servers</td>
<td>Select this check box if you agree to have Dell contact your company and send replacement parts.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Primary Shipping Contact</strong></td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td><strong>Secondary Shipping Contact</strong></td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td><strong>Shipping Address</strong></td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone of the primary or secondary contact.</td>
</tr>
<tr>
<td>Preferred contact hours</td>
<td>The preferred hours when Technical Support can contact the person who is responsible for receiving the dispatched part, if there are any issues.</td>
</tr>
<tr>
<td>Country / Territory</td>
<td>Select the country.</td>
</tr>
<tr>
<td>Shipping Address</td>
<td>The address where a replacement component must be dispatched.</td>
</tr>
<tr>
<td>City / Town</td>
<td></td>
</tr>
<tr>
<td>State / Province / Region</td>
<td></td>
</tr>
<tr>
<td>Zip / Postal code</td>
<td></td>
</tr>
<tr>
<td>Dispatch Notes</td>
<td>Type any specific dispatch related information.</td>
</tr>
<tr>
<td>CNPJ</td>
<td>For Brazil only: The CNPJ and IE number of your contact.</td>
</tr>
<tr>
<td>IE</td>
<td></td>
</tr>
<tr>
<td>I want a technician to replace my parts onsite (if included in my service plan)</td>
<td>Select this option if you want an onsite technician to replace the dispatched hardware component.</td>
</tr>
<tr>
<td><strong>TechDirect Integration</strong></td>
<td></td>
</tr>
<tr>
<td>Sign In</td>
<td>Click to sign in to your company’s TechDirect Administrator account to get the One-Time Password (OTP).</td>
</tr>
<tr>
<td>OTP</td>
<td>Enter the OTP to verify your TechDirect account.</td>
</tr>
</tbody>
</table>

**Related link**
View and update parts dispatch information
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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>User name required to log in to SupportAssist Enterprise.</td>
</tr>
<tr>
<td>Password</td>
<td>Password required to log in to SupportAssist Enterprise.</td>
</tr>
<tr>
<td>Login</td>
<td>Click to log in to SupportAssist Enterprise.</td>
</tr>
</tbody>
</table>

Site Health

The following table describes the information displayed on the Site Health page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current SupportAssist Enterprise (Hostname) Details</td>
<td>Displays information about the devices managed by SupportAssist Enterprise.</td>
</tr>
<tr>
<td>Current SupportAssist Overview</td>
<td>Displays the number of devices monitored by SupportAssist Enterprise. It also displays the number of support cases that are open.</td>
</tr>
<tr>
<td>Sitewide Inventory Validations</td>
<td>Displays the site-wide inventory validation results.</td>
</tr>
<tr>
<td>Network Connectivity</td>
<td>Displays the status of SupportAssist Enterprise connectivity to the dependent network resources.</td>
</tr>
<tr>
<td>Extensions Tree View</td>
<td>Displays the adapter and remote collectors that have been set up in SupportAssist Enterprise.</td>
</tr>
</tbody>
</table>

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.

**NOTE:** You must enter a minimum of 3 characters to perform the search.

- **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.

- **TechDirect** — Opens the Dell EMC TechDirect home page in a new web browser window.

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 37. Cases page

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box</td>
<td>Use to select a support case for performing case management actions.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The check box is displayed only for cases that were automatically created by SupportAssist Enterprise.</td>
<td></td>
</tr>
<tr>
<td>Name/IP Address</td>
<td>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 Devices page.</td>
</tr>
<tr>
<td>Number</td>
<td>The numeric identifier assigned to the support case.</td>
</tr>
<tr>
<td>Status</td>
<td>The current state of the support case. The status of a support case may be:</td>
</tr>
<tr>
<td></td>
<td>• Submitted — SupportAssist Enterprise has submitted the support case.</td>
</tr>
<tr>
<td></td>
<td>• Open — Technical Support has opened the submitted support case.</td>
</tr>
<tr>
<td></td>
<td>• In Progress — Technical Support is working on the support case.</td>
</tr>
<tr>
<td></td>
<td>• Customer Deferred — Technical Support has deferred the support case at the customer’s request.</td>
</tr>
<tr>
<td></td>
<td>• Reopened — The support case was previously closed, and has been reopened.</td>
</tr>
<tr>
<td></td>
<td>• Suspended — Technical Support has suspended activities related to the support case for 24 hours based on your request.</td>
</tr>
<tr>
<td></td>
<td>• Closure Requested — You have requested Technical Support to close the support case.</td>
</tr>
<tr>
<td></td>
<td>• Closed — The support case is closed.</td>
</tr>
<tr>
<td>Column name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|             | - Not Applicable — 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.  
- Unavailable — The support case status could not be retrieved from Dell.  
- Unknown — SupportAssist Enterprise is unable to determine the status of the support case. |
| Title       | The support case name, which identifies:  
- Support case generation method  
- Device model  
- Device operating system  
- Alert ID, if available  
- Alert description, if available  
- Warranty status  
- Resolution description |
| Date Opened | The date and time when the support case was opened. |
| Service Contract | The Dell service contract level under which the device is covered. The Service Contract column may display:  
- Unknown — SupportAssist Enterprise cannot determine the service contract.  
- Invalid Service Tag — The Service Tag of the device is invalid.  
- No Service Contract — This device is not covered under a Dell service contract.  
- Expired Service Contract — The service contract of the device has expired.  
- Basic Support — The device is covered under a Dell Basic Hardware service contract.  
- ProSupport — The device is covered under a Dell ProSupport service contract.  
- ProSupport Plus — The device is covered under a Dell ProSupport Plus service contract.  
- ProSupport Flex for Data Center — The device is covered under a ProSupport Flex for Data Center service contract.  
- ProSupport One for Data Center Or ProSupport Flex for Data Center — The device is covered under a ProSupport One for Data Center Or ProSupport Flex for Data Center service contract. |
| Service Tag | A unique, alphanumeric identifier that allows Dell to individually recognize each Dell device. |

**NOTE:** When you check for support cases of a specific device, the support cases of that device are displayed at the top of the Cases page with a blue border for the appropriate rows. See Checking for support cases.

You can choose to refine the displayed devices based on the device type, case status, service contract type, case source, or other criteria. The following are the available options for refining the displayed data:

- **Device Type**  
  - Server  
  - Storage  
  - Networking  
  - Chassis  
- **Case Status**  
  - Open  
  - Submitted  
  - In Progress  
  - Suspended  
  - Requested for Closure  
- **Service Contract**  
  - Basic
– ProSupport
– ProSupport Plus
– ProSupport Flex for Data Center
– ProSupport One for Data Center Or ProSupport Flex for Data Center

• Source Type
  – Email
  – Phone
  – Chat
  – SupportAssist
  – Help Desk
  – TechDirect
  – Others

Related links
  Case management options
  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.

  ☞ | **NOTE:** You must enter a minimum of 3 characters to perform the search.

- **Add Device** — To add a device.
- **Start Collection** — To initiate a single device or multiple device collections.
- **Edit** — To update the name and account credentials of the device.
- **Delete** — To delete a device from SupportAssist Enterprise.
- **Collection Purpose** — To select a reason for performing a multiple device collection.
- **Assign Credential Profile** — To assign credentials for devices.
- **Validate Inventory** — To perform device inventory validation.
- **Refresh** — To refresh the device inventory view.
- **View by** — Enables you to view the devices in a (list) view or (association) view.

The following table describes the automatically generated inventory information for your supported Dell devices, as displayed in the **Devices** page.

**Table 38. Devices page**

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box</td>
<td>You can use the check box to:</td>
</tr>
<tr>
<td>Column name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Select a device</td>
<td>Select a device for viewing the devices overview pane.</td>
</tr>
<tr>
<td></td>
<td>Select one or more devices for performing certain tasks on the device.</td>
</tr>
</tbody>
</table>

**NOTE:** The check box is disabled while the following SupportAssist Enterprise initiated tasks are in progress:
- SNMP configuration
- Installation or upgrade of OMSA
- Clear System Event Log
- Collection of system information immediately after an automatic support case creation and also during a manually initiated collection
- Inventory validation

<table>
<thead>
<tr>
<th>Name/IP Address</th>
<th>Displays the following information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Device name — Displays the name, host name, or IP address depending on the information you have provided for the device.</td>
</tr>
</tbody>
</table>
|                  | - 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:
  - For a collection that you manually initiate:
    - **NOTE:** When a manually initiated collection is in progress, a icon is displayed next to the progress bar. Click the icon to cancel the collection, if necessary.
    - **NOTE:** 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.
    - Starting collection
    - Collection in progress
    - Sending collection
    - Canceling collection
  - For an automated collection that is initiated because a support case was created for a detected hardware issue:
    - Starting collection for support case
    - Collection for support case in progress
    - Sending collection for support case
    - **NOTE:** If a hardware issue is detected on a device with a Dell Basic Service contract, the automated collection is initiated. However, a support case is not created for that device.
  - For an automated periodic collection based on the default or configured collection schedule:
    - Starting periodic collection
    - Periodic collection in progress
    - Sending periodic collection
    - **NOTE:** In some instances, when a collection is in progress (manual) on a device another collection (periodic) may be initiated. In such scenarios, the collection status is displayed in the following order of priority:
      - Manual collection
      - Support case collection
      - Periodic collection
  - Maintenance mode — If the device is placed in maintenance mode, the maintenance mode icon is displayed.
<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Model of the device. For example, PowerEdge M820.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of inventory validation. The status can be categorized as follows:</td>
</tr>
<tr>
<td></td>
<td>• Success — Inventory validation of the device is successfully complete.</td>
</tr>
<tr>
<td></td>
<td>• Failed — Inventory validation of the device is unsuccessful.</td>
</tr>
<tr>
<td></td>
<td>• In progress — Inventory validation of the device is in progress.</td>
</tr>
<tr>
<td></td>
<td>• No status — The inventory validation is yet to be initiated on the device.</td>
</tr>
</tbody>
</table>

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
  - Virtual Machine

- **Need Attention**
  - Staging — Displays a status icon and a rollup count of number of devices that are present in the Staging group.
  - Inactive — Displays a status icon and a rollup count of number of devices that are present in the Inactive group.

- **Inventory Validation**
  - Success — Displays a status icon and the rollup count of number of devices that were validated successfully.
  - Failed — Displays a status icon and the rollup count of number of devices that were not validated successfully.

- **Groups**
  - Default — Displays all devices.
  - Staging — Displays devices in the staging group.
  - Inactive — Displays devices that are not reachable.

- **Adapter**
- **Remote Collector**
- **Collection Host**
  - SupportAssist Enterprise
- **Devices Added**
  - SupportAssist Enterprise
  - Adapters

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**.
- **Multiple Device Collection** pane — When a multiple device collections is in progress. See **Multiple Device Collection pane**.

**Related links**
- Adding devices
- Delete a device
- Enable or disable device-level maintenance mode
- Install or upgrade OMSA by using SupportAssist Enterprise
- View support cases for a specific device
- Sorting the displayed data
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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Type</strong></td>
<td>Displays a list of device types that you can add. The available device types are:</td>
</tr>
<tr>
<td></td>
<td>• Chassis</td>
</tr>
<tr>
<td></td>
<td>• Fluid File System (FluidFS)</td>
</tr>
<tr>
<td></td>
<td>• iDRAC</td>
</tr>
<tr>
<td></td>
<td>• Networking</td>
</tr>
<tr>
<td></td>
<td>• Peer Storage (PS) / EqualLogic</td>
</tr>
<tr>
<td></td>
<td>• PowerVault</td>
</tr>
<tr>
<td></td>
<td>• Server / Hypervisor</td>
</tr>
<tr>
<td></td>
<td>• Software</td>
</tr>
<tr>
<td></td>
<td>• Solution</td>
</tr>
<tr>
<td></td>
<td>• Storage Center (SC) / Compellent</td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine</td>
</tr>
<tr>
<td><strong>Host Name / IP Address</strong></td>
<td>IP address or host name of the device that you want to add.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: For adding a Storage PS Series storage array, enter the management IP address.</td>
</tr>
<tr>
<td><strong>Perform deep discovery</strong></td>
<td>To discover devices and their associated device types.</td>
</tr>
<tr>
<td><strong>Name (Optional)</strong></td>
<td>An optional name you want to use for identifying the device. If provided, this name is used to identify the device in SupportAssist Enterprise.</td>
</tr>
<tr>
<td><strong>Account Credentials</strong></td>
<td>Use to select or create an Account Credentials that contains the credentials of a device.</td>
</tr>
<tr>
<td><strong>Credential Profile</strong></td>
<td>Use to select or create a Credential Profile that contains the Account Credentials for the device types within the discovery ranges.</td>
</tr>
<tr>
<td><strong>Enable monitoring</strong></td>
<td>To allow SupportAssist Enterprise to monitor the device for hardware issues.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: The Enable monitoring option is displayed only for the following Device Types: Server / Hypervisor, iDRAC, Chassis, and Networking.</td>
</tr>
<tr>
<td><strong>Configure SNMP settings</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
NOTE: The Configure SNMP settings option is displayed only for the following Device Types: Server, iDRAC, and Hypervisor.

Install or upgrade OMSA

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.

NOTE: The Install, or upgrade OMSA option is displayed only for the following Device Types: Server and Hypervisor.

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

- Add a server or hypervisor
- Add a chassis
- Add a Networking device
- Add a solution
- Add an iDRAC
- Add a PowerVault storage array
- Add an EqualLogic PS Series storage solution
- Add a Compellent SC Series storage solution
- Add a Fluid File System NAS device
- Add a software
- Add a virtual machine

Assign Device Group

The Assign Device Group (Optional) page enables you to assign the device to a custom device group.

The following table describes the fields displayed on the Assign Device Group (Optional) page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name you have provided for the device.</td>
</tr>
<tr>
<td>Current Group</td>
<td>The device group the device is assigned to.</td>
</tr>
<tr>
<td>Assign Other Group</td>
<td>The available device groups to which you can assign the device.</td>
</tr>
</tbody>
</table>
Summary page

The Summary page displays the status and details of the device addition.

Table 41. Summary page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name that you have provided for the device.</td>
</tr>
<tr>
<td>IP Address / Host name</td>
<td>The IP address or host name that you have provided for the device.</td>
</tr>
<tr>
<td>Service Tag</td>
<td>A unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of the device.</td>
</tr>
<tr>
<td>Model</td>
<td>The model of the device.</td>
</tr>
<tr>
<td>OS Type</td>
<td>The operating system installed on the device.</td>
</tr>
<tr>
<td>Group</td>
<td>The device group to which the device is assigned.</td>
</tr>
</tbody>
</table>

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 42. Device overview pane

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Tasks               | • **Clear System Event Log** — To clear the System Event Log (SEL) or Embedded System Management (ESM) log.  
|                     | • **Check for Cases** — To check for support cases that are present for a device.  
|                     | • **Perform deep discovery** — To discover a device and its associated device types.  
|                     | • **Maintenance Mode**  
|                     | — **Enable** — To place the device in maintenance mode.  
|                     | — **Disable** — To place the device in normal mode.  
|                     | • **Dependencies**  
|                     | — **Install / Upgrade OMSA** — To install or upgrade OMSA on the device.  
<p>|                     | — <strong>Configure SNMP</strong> — To configure the SNMP settings of the device.       |
| Hostname / IP address | Displays the IP address or host name of the device.                        |
| Model               | Displays the model information of the device. For example, PowerEdge M820. |
| Service Tag         | Displays a unique, alphanumeric identifier that allows Dell to individually recognize the device. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Monitoring                   | • **Enable** — To enable monitoring hardware issues that may occur the device.  
• **Disable** — To disable monitoring hardware issues that may occur the device. |
| Software Version             | Displays the version of the firmware installed on the device.                                                                                |
| Display Name                 | Displays the name that you have provided for the device.                                                                                   |
| Device Type                  | Displays the type of the device. For example, Server.                                                                                       |
| Collections                  | Displays a list that contains the collection history. You can select a date and time from the list to view the system information that was collected. |
|                              | **NOTE:** 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 |
<p>| Next Scheduled Collection    | Displays the date and time of the next scheduled collection.                                                                                |
| Last Device Job Status       | 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: |
|                              | <strong>Informational status</strong>                                                                                                                   |
|                              | • ✓ OK — The device is configured correctly for SupportAssist Enterprise functionality.                                                   |
|                              | • <img src="https://example.com" alt="Installing" /> OMSA — Installation or upgrade of Dell OpenManage Server Administrator (OMSA) is in progress.                |
|                              | • <img src="https://example.com" alt="Configuring" /> SNMP — Configuring the SNMP settings of the device is in progress.                                     |
|                              | • <img src="https://example.com" alt="Clearing System Event Log" /> — Clearing of the System Event Log is in progress.                                     |
|                              | • ✓ System Event Log cleared — System Event Log has been cleared successfully.                                                              |
|                              | • <img src="https://example.com" alt="Revalidating" /> device — SupportAssist Enterprise is validating the prerequisites and the credentials of the device.  |
|                              | <strong>Warning status</strong>                                                                                                                         |
|                              | • <img src="https://example.com" alt="OMSA not installed" /> — OMSA is not installed on the device.                                                        |
|                              | • <img src="https://example.com" alt="SNMP not configured; OMSA not latest" /> — 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. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>SNMP not configured</strong> — SNMP settings of the device is not configured.</td>
<td></td>
</tr>
<tr>
<td>• <strong>New version of OMSA available</strong> — A newer version of OMSA is available for installation on the device.</td>
<td></td>
</tr>
<tr>
<td>• <strong>OMSA installed, reboot the added device</strong> — Installation of OMSA is complete on the device. Restart the device for the changes to take effect.</td>
<td></td>
</tr>
</tbody>
</table>

**Error status**

- **Unable to add device** — SupportAssist Enterprise has placed the device in the Staging group because the device did not meet certain prerequisites. For more information on the Staging group, see Predefined device groups.
- **Unable to configure SNMP** — SupportAssist Enterprise is unable to configure the SNMP trap destination of the device.
- **Unable to verify SNMP configuration** — SupportAssist Enterprise is unable to verify the SNMP configuration of the iDRAC.
- **Unable to install OMSA** — Installation of OMSA could not be completed.
- **OMSA not supported** — Installation of OMSA is not supported.
- **Unable to reach device** — SupportAssist Enterprise is unable to communicate with the device.
- **Authentication failed** — SupportAssist Enterprise cannot log in to the device.
- **Unable to gather system information** — SupportAssist Enterprise is unable to collect system information from the device.
- **Insufficient storage space to gather system information** — The server where SupportAssist Enterprise is installed does not have sufficient space to gather system information from the device.
- **Unable to export collection** — SupportAssist Enterprise is unable to process the collected system information.
- **Unable to send system information** — SupportAssist Enterprise is unable to send the collected system information to Dell.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearing System Event Log failed — SupportAssist Enterprise is unable to clear the System Event Log or Embedded System Management logs on the device.</td>
<td></td>
</tr>
<tr>
<td>Maintenance Mode — 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 Understanding maintenance mode.</td>
<td></td>
</tr>
<tr>
<td>Credentials not provided — The username and password of the device has not been provided.</td>
<td></td>
</tr>
<tr>
<td>Credentials not correct — The username and password provided for the device is incorrect.</td>
<td></td>
</tr>
<tr>
<td>Unable to start collection — Unable to start the collection as the Remote SupportAssist Collector is down.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** The error status may be displayed as a link that you can click to view a description of the issue and the possible resolution steps.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Displays the operating system installed on the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software (for Chassis, networking, and other devices)</td>
<td>Displays the firmware version installed on the device.</td>
</tr>
<tr>
<td>iSM (for iDRAC)</td>
<td>Displays the iSM version installed on the device.</td>
</tr>
<tr>
<td>OMSA (for servers)</td>
<td>Displays the OMSA version installed on the device.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Click to add a device that is of the same type as a device that you have already added.</td>
</tr>
</tbody>
</table>

**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 43. Multiple Device Collection window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Name (Optional)</td>
<td>The name that you want to assign to the collection.</td>
</tr>
<tr>
<td>Dell EMC Support Request/case number (Optional)</td>
<td>The case identifier that you want to associate with the collection.</td>
</tr>
<tr>
<td>Dell EMC Technician Email (Optional)</td>
<td>The email address or name of the Technical Support contact.</td>
</tr>
<tr>
<td>Project ID (Optional)</td>
<td>The project identification information.</td>
</tr>
<tr>
<td>Upload collection</td>
<td>• Select this option to upload the collection to Dell after the collection is completed.  &lt;br&gt; • Clear this option to only save the collection on the local system (server where SupportAssist Enterprise is installed).</td>
</tr>
</tbody>
</table>

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.

Site Inventory Validation

The Site Inventory Validation page displays the following sections:

- Validation test status — Displays the type of tests performed during inventory validation.
- Progress indicator — Indicates the status of the inventory validation.
- History — Displays the inventory validation test history.

Related links
- Validating device inventory
- View the Site Inventory Validation page
- Start inventory validation manually
- Schedule automatic inventory validation

Validation test status

The following table provides information about the items displayed in the Validation test section on the Site Inventory Validation page.
### Table 44. Validation test status

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation test</td>
<td>Displays a type of tests performed during inventory validation.</td>
</tr>
<tr>
<td>Success</td>
<td>Displays a status icon and the rollup count of number of devices that were validated successfully.</td>
</tr>
<tr>
<td>Failed</td>
<td>Displays a status icon and the rollup count of number of devices that were not validated successfully.</td>
</tr>
<tr>
<td>Others</td>
<td>Displays a status icon and the rollup count of number of:</td>
</tr>
<tr>
<td></td>
<td>• Devices that may not be supported or monitored by SupportAssist Enterprise</td>
</tr>
<tr>
<td></td>
<td>• Devices added or discovered in SupportAssist Enterprise through the adapter</td>
</tr>
<tr>
<td></td>
<td>• Devices for which the connectivity test has failed</td>
</tr>
<tr>
<td></td>
<td>• Devices for which you have disabled monitoring</td>
</tr>
</tbody>
</table>

### History of inventory validation

The following table provides information about the items displayed in the history section on the Site Inventory Validation page.

#### Table 45. History of inventory validation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Started</td>
<td>Date and time when the periodic inventory validation was started.</td>
</tr>
<tr>
<td>Completed</td>
<td>Date and time when the periodic inventory validation was completed.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you are running periodic inventory validation for the first time, the Completed value will be NA.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Date and time when the periodic inventory validation was last performed.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you are running periodic inventory validation for the first time, the Last Updated value will be blank.</td>
</tr>
</tbody>
</table>

### 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 46. Device Groups**

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

**Related links**

- Manage Devices
- Create or Edit 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 47. Manage Devices**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device group.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of device as discovered by OpenManage Essentials:</td>
</tr>
<tr>
<td></td>
<td>- <strong>PowerVault Storage Device</strong> — The device is a Storage MD Series array.</td>
</tr>
<tr>
<td></td>
<td>- <strong>PowerVault Server</strong> — The device is a Storage NX Network Attached Storage (NAS) device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>EqualLogic Storage</strong> — The device is a Storage PS Series array.</td>
</tr>
<tr>
<td></td>
<td>- <strong>PowerEdge Server Device</strong> — The device is a Dell PowerEdge, PowerEdge VRTX, iDRAC, or CMC device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>PowerEdge Direct Attached Storage</strong> — The device is a Storage MD Series or NX Direct Attached Storage (DAS) device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Dell Networking</strong> — The device is a Dell Networking switch.</td>
</tr>
<tr>
<td>Model</td>
<td>Model of the device. For example, PowerEdge M820.</td>
</tr>
<tr>
<td>Service Tag</td>
<td>A unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.</td>
</tr>
<tr>
<td>Save</td>
<td>Click to save the changes you have made.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to discard the changes you have made.</td>
</tr>
</tbody>
</table>

**NOTE:** You can use the filter icon displayed in the column titles to filter the displayed data.
Create or Edit Device Group

The Create or Edit Device Group window allows you to edit the device group details of a group.

The following table provides information about the fields displayed in the Create or Edit Device Group window.

**Table 48. Create or Edit Device Group**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group and Contact Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the device group.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the device group.</td>
</tr>
<tr>
<td>IT Administrator Contact Information</td>
<td>Select this check box to enter the contact information of the IT Administrator.</td>
</tr>
<tr>
<td>Primary</td>
<td>Select this option to view or edit the primary contact information.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Select this option to view or edit the secondary contact information.</td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the primary or secondary contact.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the primary or secondary contact.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the primary or secondary contact.</td>
</tr>
<tr>
<td>Alternate phone number</td>
<td>The alternate phone number of the primary or secondary contact.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the primary or secondary contact.</td>
</tr>
<tr>
<td>Preferred contact method</td>
<td>Select the preferred contact method. The available options are:</td>
</tr>
<tr>
<td></td>
<td>- Phone</td>
</tr>
<tr>
<td></td>
<td>- Email</td>
</tr>
<tr>
<td>Preferred contact hours</td>
<td>The preferred hours when Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone of the primary or secondary contact.</td>
</tr>
<tr>
<td><strong>Parts Replacement Preferences for Dell Servers</strong></td>
<td></td>
</tr>
<tr>
<td>I want Dell server replacement parts shipped automatically</td>
<td>Select this check box if you agree to have Dell contact your company and send replacement parts.</td>
</tr>
<tr>
<td><strong>Primary Shipping Contact</strong></td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Secondary Shipping Contact</strong></td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td><strong>Shipping Address</strong></td>
<td></td>
</tr>
<tr>
<td>Preferred Contact Hours</td>
<td>The preferred hours when Technical Support can contact the person who is responsible for receiving the dispatched part, if there are any issues.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone of the primary or secondary contact.</td>
</tr>
<tr>
<td>Country / Territory</td>
<td>Select the country.</td>
</tr>
<tr>
<td>Shipping Address</td>
<td>The address where a replacement component must be dispatched.</td>
</tr>
<tr>
<td>City / Town</td>
<td></td>
</tr>
<tr>
<td>State / Province / Region</td>
<td></td>
</tr>
<tr>
<td>Zip / Postal code</td>
<td></td>
</tr>
<tr>
<td>Dispatch Notes</td>
<td>Type and specific dispatch related information.</td>
</tr>
<tr>
<td>CNPJ IE</td>
<td>For Brazil only: The CNPJ and IE number of your contact.</td>
</tr>
<tr>
<td>I want a technician to replace my parts onsite (if included in my service plan)</td>
<td>Select this option if you want an onsite technician to replace the dispatched hardware component.</td>
</tr>
</tbody>
</table>

**Related links**
- Device Groups page
- View and update device group information

**Manage Device Discovery Rule**

The [Manage Device Discovery Rule](#) page enables you to discover and add devices based on IP address ranges or comma separated hostname expressions or IP addresses. The following table provides information about the options in the Manage Device Discovery Rule section.

**Table 49. Manage Device Discovery Rule**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Discovery Rule</td>
<td>Click to create a discovery rule.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click to edit the discovery rule.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click to delete the discovery rule.</td>
</tr>
<tr>
<td>Run now</td>
<td>Click to discover devices immediately.</td>
</tr>
<tr>
<td>Name</td>
<td>The name that you have provided for the discovery rule.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of a discovery rule.</td>
</tr>
</tbody>
</table>

### Related links
- Create device discovery rule
- View the device discovery rule overview pane
- Edit device discovery rule
- Delete device discovery rule
- Run the discovery rule

## Create or Edit Device Discovery Rule

The **Create or Edit Device Discovery Rule** window enables you to create a device discovery rule. The following table provides information about the options in the **Create or Edit Device Discovery Rule** section.

### Table 50. Create or Edit Device Discovery Rule

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Rule Name</td>
<td>Type a name for the discovery rule.</td>
</tr>
<tr>
<td>Credential Profile</td>
<td>Use to select or create a Credential Profile that contains the Account Credentials for the device types within the discovery ranges.</td>
</tr>
<tr>
<td>IP address / range</td>
<td>Select to enter an IP address range to discover devices by using IP address ranges.</td>
</tr>
<tr>
<td>IP Address / Range Address</td>
<td>The IP address or IP range address of the devices that you want to discover.</td>
</tr>
<tr>
<td>Subnet mask (Optional)</td>
<td>A subnet mask that is associated with the IP address. By default, the subnet mask value is 255.255.255.0.</td>
</tr>
<tr>
<td>Add another range</td>
<td>Click to open an additional IP address or IP address range fields.</td>
</tr>
<tr>
<td>Devices</td>
<td>Select to discover devices by using the hostname or IP addresses.</td>
</tr>
<tr>
<td>Enter hostname or IP address as comma-separated values</td>
<td>Enter the hostname or IP address of devices as comma-separated values.</td>
</tr>
<tr>
<td>Run now</td>
<td>Select to discover the devices immediately.</td>
</tr>
<tr>
<td>Run once</td>
<td>Select to discover the devices at a specific date and time.</td>
</tr>
<tr>
<td>Recur</td>
<td>Select to schedule the discovery of devices at periodic intervals.</td>
</tr>
<tr>
<td>Device type</td>
<td>The device types for which credentials are included in the Credential Profile and PowerVault are selected. The available device types are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Chassis</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Fluid File System (FluidFS)</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>iDRAC</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Networking</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Peer Storage (PS) / EqualLogic</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>PowerVault</strong></td>
</tr>
</tbody>
</table>
Perform deep discovery
To discover devices and their associated device types.

Enable Monitoring (may require additional SNMP settings)
To allow SupportAssist Enterprise to monitor the device for hardware issues.

Configure SNMP to receive alerts from this device
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.

Install latest version of OMSA (This will generate alerts and allow the collection of System State Information)
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.

### Related links
- Create device discovery rule
- Edit device discovery rule

## Discovery Rule Details

You can view details of a discovery rule such as the IP range, schedule, status of discovery, and the last run date and time in the Discovery Rule Details pane. The following table provides information about the attributes displayed in the Discovery Rule Details pane.

### Table 51. Discovery Rule Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td>The IP address or IP range address of the devices that are discovered.</td>
</tr>
<tr>
<td>Schedule</td>
<td>The schedule of a discovery rule.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of a discovery rule.</td>
</tr>
<tr>
<td>Last Run</td>
<td>The date and time of when the discovery rule was last run.</td>
</tr>
</tbody>
</table>

### Related link
- View the device discovery rule overview pane
Discovery Rule Current Iteration Status

You can view details of a discovery rule such as the number of devices added, number of devices moved to staging group, and so on, in the Discovery Rule Current Iteration Status pane. The following table provides information about the attributes displayed in the Discovery Rule Current Iteration Status pane.

Table 52. Discovery Rule Current Iteration Status

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the discovery rule. The following are the available statuses:</td>
</tr>
<tr>
<td></td>
<td>• Success—Number of devices added successfully.</td>
</tr>
<tr>
<td></td>
<td>• Staging—Number of devices moved to the staging group.</td>
</tr>
<tr>
<td></td>
<td>• Inactive—Number of inactive devices.</td>
</tr>
<tr>
<td></td>
<td>• Failed—Number of failed devices.</td>
</tr>
<tr>
<td>Devices</td>
<td>The device count.</td>
</tr>
<tr>
<td>Export CSV</td>
<td>Click to export the list of devices that were not discovered as a CSV file.</td>
</tr>
</tbody>
</table>

Recent Activity

You can view details of a discovery rule such as the IP Address, date, and the timestamp of devices for which discovery is in progress in the Recent Activity (Latest 10) pane. The following table provides information about the attributes displayed in the Recent Activity (Latest 10) pane.

Table 53. Recent Activity (Latest 10)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The IP address or IP address range for which discovery is in progress.</td>
</tr>
<tr>
<td>Result</td>
<td>The result of a discovery rule.</td>
</tr>
<tr>
<td>Time</td>
<td>The date and timestamp of a discovery rule that is in progress.</td>
</tr>
</tbody>
</table>

Current versus Previous Discovery Rule Status

You can view details of a discovery rule such as the number of devices that were added, number of devices moved to the staging group, number of inactive devices, and the number of devices that were deleted from the discovery rule in the Current v/s Previous Discovery...
Rule Status pane. The following table provides information about the attributes displayed in the Current v/s Previous Discovery Rule Status pane.

### Table 54. Current versus Previous Discovery Rule Status

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added</td>
<td>Number of added devices.</td>
</tr>
<tr>
<td>Staging</td>
<td>Number of devices moved to the staging group.</td>
</tr>
<tr>
<td>Inactive</td>
<td>Number of inactive devices.</td>
</tr>
<tr>
<td>Deleted</td>
<td>Number of deleted devices.</td>
</tr>
<tr>
<td>Devices</td>
<td>The status of the devices.</td>
</tr>
<tr>
<td>Number</td>
<td>The device count.</td>
</tr>
</tbody>
</table>

**Related link**
View the device discovery rule overview pane

### Manage Account Credentials

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

### Table 55. Manage Account Credentials

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

**Related links**
Account Credentials  
Add Account Credentials  
Reassign Account Credentials  
Edit Account Credentials  
Delete 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the Account Credentials.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The list of device types that you can add. The available device types are:</td>
</tr>
<tr>
<td></td>
<td>• Chassis</td>
</tr>
<tr>
<td></td>
<td>• Fluid File System (FluidFS)</td>
</tr>
<tr>
<td></td>
<td>• iDRAC</td>
</tr>
<tr>
<td></td>
<td>• Networking</td>
</tr>
<tr>
<td></td>
<td>• Peer Storage (PS) / EqualLogic</td>
</tr>
<tr>
<td></td>
<td>• Server / Hypervisor</td>
</tr>
<tr>
<td></td>
<td>• Software</td>
</tr>
<tr>
<td></td>
<td>• Solution</td>
</tr>
<tr>
<td></td>
<td>• Storage Center (SC) / Compellent</td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine</td>
</tr>
<tr>
<td>Username*</td>
<td>The user name required to connect to the device type.</td>
</tr>
<tr>
<td>Password*</td>
<td>The password required to connect to the device type.</td>
</tr>
<tr>
<td>Community String</td>
<td>The community string assigned to the device.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Community String option is displayed only for the Networking</td>
</tr>
<tr>
<td></td>
<td>and Peer Storage (PS) / EqualLogic device types.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>The enable password configured on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Enable Password option is displayed only for the Networking</td>
</tr>
<tr>
<td></td>
<td>device type.</td>
</tr>
<tr>
<td>Operating system type</td>
<td>The list of operating system types. The available operating system types are:</td>
</tr>
<tr>
<td></td>
<td>• Windows (displayed only if SupportAssist Enterprise is installed on a</td>
</tr>
<tr>
<td></td>
<td>server running Windows)</td>
</tr>
<tr>
<td></td>
<td>• Linux</td>
</tr>
<tr>
<td></td>
<td>• ESX</td>
</tr>
<tr>
<td></td>
<td>• ESXi</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Operating system type option is displayed only for the Server</td>
</tr>
<tr>
<td></td>
<td>/ Hypervisor device type.</td>
</tr>
<tr>
<td>Software Type</td>
<td>The list of software types. The available software types are:</td>
</tr>
<tr>
<td></td>
<td>• SCVMM</td>
</tr>
<tr>
<td></td>
<td>• vCenter</td>
</tr>
<tr>
<td></td>
<td>• SAN HQ</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
• HIT Kit / VSM for VMware
| NOTE: The Software Type option is displayed only for the Software device type.
| NOTE: If SupportAssist Enterprise is installed on a Linux operating system, adding SCVMM and SAN HQ is not supported.

**Solution Type**
The type of solution. The available type of solution is **Web Scale**.
| NOTE: The Solution Type option is displayed only for the Solution device type.

* For Solution device type, you must enter the SSH and REST user name and password.

**Related link**
Add 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Type a name for the Account Credentials.</td>
</tr>
</tbody>
</table>
| **Device Type** | The list of device types that you can add. The available device types are:  
• Chassis  
• Fluid File System (FluidFS)  
• iDRAC  
• Networking  
• Peer Storage (PS) / EqualLogic  
• Server / Hypervisor  
• Software  
• Solution  
• Storage Center (SC) / Compellent  
• Virtual Machines |
| **Username** | The user name required to connect to the device type. |
| **Password** | The password required to connect to the device type. |
| **Community String** | The community string assigned to the device.  
| NOTE: The Community String option is displayed only for the Networking and Peer Storage (PS) / EqualLogic device types. |
| **Enable Password** | The enable password configured on the device. |
## Operating system type

The list of operating system types. The available operating system types are:

- Windows
- Linux
- ESX
- ESXi

**NOTE:** The Operating system type option is displayed only for the Server / Hypervisor device type.

## Software Type

The list of software types. The available software types are:

- SCVMM
- vCenter
- SAN HQ
- HIT Kit / VSM for VMware

**NOTE:** The Software Type option is displayed only for the Software device type.

**NOTE:** If SupportAssist Enterprise is installed on a Linux operating system, adding SCVMM and SAN HQ is not supported.

## Solution Type

The type of solution. The available type of solution is **Web Scale**.

**NOTE:** The Solution Type option is displayed only for the Solution device type.

* For Solution device type, you must enter the SSH and REST user name and password.

### 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Profile</td>
<td>Click to add a Credential Profile.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click to edit a Credential Profile.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click to delete a Credential Profile.</td>
</tr>
<tr>
<td>Name</td>
<td>The name that you have provided for the Credential Profile.</td>
</tr>
</tbody>
</table>
Related links
Credential Profiles
Create Credential Profile
Assign Credential Profile
Edit Credential Profile
Delete 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 59. Add Credential Profile

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the Credential Profile.</td>
</tr>
<tr>
<td>Check box</td>
<td>Use to select a device type.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The list of device types that you can select. The available device types are:</td>
</tr>
<tr>
<td></td>
<td>• Chassis</td>
</tr>
<tr>
<td></td>
<td>• Fluid File System (FluidFS)</td>
</tr>
<tr>
<td></td>
<td>• iDRAC</td>
</tr>
<tr>
<td></td>
<td>• Networking</td>
</tr>
<tr>
<td></td>
<td>• Peer Storage (PS) / EqualLogic</td>
</tr>
<tr>
<td></td>
<td>• PowerVault</td>
</tr>
<tr>
<td></td>
<td>• Server / Hypervisor</td>
</tr>
<tr>
<td></td>
<td>• Software</td>
</tr>
<tr>
<td></td>
<td>• Solution</td>
</tr>
<tr>
<td></td>
<td>• Storage Center (SC) / Compellent</td>
</tr>
<tr>
<td>Account Credentials</td>
<td>The Account Credentials that you have created for the specific device type.</td>
</tr>
<tr>
<td>Add Account Credentials</td>
<td>Click to add new account credentials.</td>
</tr>
</tbody>
</table>

Related link
Create 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 60. Edit Credential Profile

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Credential Profile.</td>
</tr>
<tr>
<td>Check box</td>
<td>Use to select a device type.</td>
</tr>
<tr>
<td><strong>Device Type</strong></td>
<td>The list of device types that you can select. The available device types are:</td>
</tr>
<tr>
<td></td>
<td>• Chassis</td>
</tr>
<tr>
<td></td>
<td>• Fluid File System (FluidFS)</td>
</tr>
<tr>
<td></td>
<td>• iDRAC</td>
</tr>
<tr>
<td></td>
<td>• Networking</td>
</tr>
<tr>
<td></td>
<td>• Peer Storage (PS) / EqualLogic</td>
</tr>
<tr>
<td></td>
<td>• PowerVault</td>
</tr>
<tr>
<td></td>
<td>• Server / Hypervisor</td>
</tr>
<tr>
<td></td>
<td>• Software</td>
</tr>
<tr>
<td></td>
<td>• Solution</td>
</tr>
<tr>
<td></td>
<td>• Storage Center (SC) / Compellent</td>
</tr>
<tr>
<td><strong>Account Credentials</strong></td>
<td>The Account Credentials that you have created for the specific device type.</td>
</tr>
</tbody>
</table>

**Related link**

Edit 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.

**NOTE:** You must enter a minimum of 3 characters to perform the search.

- **Upload** — To upload a collection to Dell.

The following table describes the information displayed in the Collections page.
<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box</td>
<td>Use to select a collection for viewing the collection overview pane and to upload a collection.</td>
</tr>
<tr>
<td>Information icon</td>
<td>Displayed when some attributes or sections were not collected from the device.</td>
</tr>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Collection Date</td>
<td>The date when the collection was started.</td>
</tr>
<tr>
<td>Collection Purpose</td>
<td>The reason selected while performing a multiple device collection.</td>
</tr>
<tr>
<td>Case Number</td>
<td>The numeric support case identifier.</td>
</tr>
<tr>
<td>Upload Status</td>
<td>The upload status of the collection.</td>
</tr>
</tbody>
</table>

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
- **Collection Purpose**
  - Technical Support
  - Deployment
  - System Maintenance
  - Consulting
  - Others
- **Device Type**
  - Server
  - Storage
  - Networking
  - Chassis
  - Software
  - Solution
- **Collection Host**
  - SupportAssist Enterprise
  - Remote Collector
- **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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned of the collection.</td>
</tr>
<tr>
<td>Upload status</td>
<td>The status of the collection upload.</td>
</tr>
<tr>
<td>Date</td>
<td>The date and time when the collection was started.</td>
</tr>
<tr>
<td>IP Address / Host name</td>
<td>The IP address of host name of the device.</td>
</tr>
<tr>
<td>Service Tag</td>
<td>A unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.</td>
</tr>
<tr>
<td>Collection status</td>
<td>The status of the collection from the device.</td>
</tr>
<tr>
<td>View Collection (for server collections only)</td>
<td>Click to open a collection from a server in the Configuration Viewer.</td>
</tr>
<tr>
<td>Download Collection (for collections from all other device types and multiple device collections)</td>
<td>Click to download the collection as a .zip file.</td>
</tr>
</tbody>
</table>

**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, Microsoft System Center Operations Manager, or OpenManage Enterprise.

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 overview
Remote Collectors overview

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 63. Adapters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Up Adapter</td>
<td>Click to set up an adapter.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click to edit the details of an adapter.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click to delete an adapter.</td>
</tr>
<tr>
<td>Check box</td>
<td>Use to select an adapter that you have set up.</td>
</tr>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Type</td>
<td>The adapter type.</td>
</tr>
<tr>
<td>Managed Devices</td>
<td>The total number of devices that are added through the adapter.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the adapter application.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the adapter. The status of an adapter may be:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Connected</strong> — SupportAssist Enterprise is able to connect successfully to the adapter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disconnected</strong> — SupportAssist Enterprise is unable to connect to the adapter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Initial Synchronization</strong> — Initial inventory of devices in progress.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Periodic Synchronization</strong> — Automatic periodic inventory of devices is in progress.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Manual Synchronization</strong> — Manually-initiated inventory of devices is in progress.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Connection lost</strong> — The server running SupportAssist Enterprise is unable to connect to the server where the adapter is set up.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Copy in progress</strong> — The adapter installer package is being copied to the system.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Installation in progress</strong> — Installation of the adapter is in progress.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Validation in progress</strong> — SupportAssist Enterprise is verifying if the adapter meets the prerequisites for setting up the adapter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Configuration in progress</strong> — SupportAssist Enterprise is configuring the settings of the adapter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Starting service</strong> — SupportAssist Enterprise had installed the adapter and the adapter service is started.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Awaiting connection</strong> — SupportAssist Enterprise is waiting for the adapter service to start.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Connection in progress</strong> — SupportAssist Enterprise is trying to connect to the adapter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Assigning Profile</strong> — 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.</td>
</tr>
</tbody>
</table>
Related links
- Set up OpenManage Essentials adapter
- Set up the Microsoft System Center Operations Manager adapter
- View the adapter overview pane
- View devices inventoried by the adapter
- Synchronize adapter
- Edit adapter
- Delete adapter

Set Up OpenManage Essentials Adapter

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 64. Set Up Adapter (OpenManage Essentials)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adapter type</strong></td>
<td>Use to select the type of adapter that you want to set up. The available adapter types are:</td>
</tr>
<tr>
<td></td>
<td>- OpenManage Essentials — Select to set up the Open Manage Essentials adapter.</td>
</tr>
<tr>
<td></td>
<td>- System Center Operations Manager — Select to set up the System Center Operations Manager adapter.</td>
</tr>
<tr>
<td></td>
<td>- OpenManage Enterprise — Select to set up the OpenManage Enterprise adapter.</td>
</tr>
<tr>
<td><strong>Host name / IP address</strong></td>
<td>The host name or IP address of the server where OpenManage Essentials is installed.</td>
</tr>
<tr>
<td><strong>Name (Optional)</strong></td>
<td>An optional name that you want to use for identifying the adapter in SupportAssist Enterprise.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The user name required to connect to the server where OpenManage Essentials is installed.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password required to connect to the server where OpenManage Essentials is installed.</td>
</tr>
<tr>
<td><strong>Credential Profile</strong></td>
<td>Use to select a Credential Profile that is required to add the devices that are inventoried by the adapter.</td>
</tr>
<tr>
<td><strong>Update device inventory</strong></td>
<td>Use to select the frequency at which the adapter must inventory devices from the adapter. The available options are:</td>
</tr>
<tr>
<td></td>
<td>- Every 12 hours</td>
</tr>
<tr>
<td></td>
<td>- Daily</td>
</tr>
<tr>
<td></td>
<td>- Weekly</td>
</tr>
<tr>
<td></td>
<td>- Every two weeks</td>
</tr>
<tr>
<td></td>
<td>- Monthly</td>
</tr>
</tbody>
</table>

Related link
- Set up OpenManage Essentials adapter
Set Up Microsoft System Center Operations Manager Adapter

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 65. Set Up Adapter (Microsoft System Center Operations Manager)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adapter type</strong></td>
<td>Use to select the type of adapter that you want to set up. The available adapter types are:</td>
</tr>
<tr>
<td></td>
<td>• OpenManage Essentials — Select to set up the OpenManage Essentials adapter.</td>
</tr>
<tr>
<td></td>
<td>• System Center Operations Manager — Select to set up the System Center Operations Manager adapter.</td>
</tr>
<tr>
<td></td>
<td>• OpenManage Enterprise — Select to set up the OpenManage Enterprise adapter.</td>
</tr>
<tr>
<td><strong>Name</strong> (Optional)</td>
<td>An optional name that you want to use for identifying the adapter in SupportAssist Enterprise.</td>
</tr>
<tr>
<td><strong>Establish a remote connection with the management group</strong></td>
<td>Select this option if you are setting up the adapter on the server hosting the Remote Console.</td>
</tr>
<tr>
<td><strong>Management group Host name / IP address</strong></td>
<td>The host name or IP address of the server that hosts the management group.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>The user name required to connect to the server that hosts the management group.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password required to connect to the server that hosts the management group.</td>
</tr>
<tr>
<td><strong>Remote Console Host name / IP address</strong></td>
<td>The host name or IP address of the server that hosts the Remote Console.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>The user name required to connect to the server that hosts the Remote Console.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password required to connect to the server that hosts the Remote Console.</td>
</tr>
<tr>
<td><strong>Credential Profile</strong></td>
<td>Use to select a Credential Profile that is required to add the devices that are inventoried by the adapter.</td>
</tr>
<tr>
<td><strong>Update device inventory</strong></td>
<td>Use to select the frequency at which the adapter must inventory devices from the adapter. The available options are:</td>
</tr>
<tr>
<td></td>
<td>• Every 12 hours</td>
</tr>
<tr>
<td></td>
<td>• Daily</td>
</tr>
<tr>
<td></td>
<td>• Weekly</td>
</tr>
<tr>
<td></td>
<td>• Every two weeks</td>
</tr>
<tr>
<td></td>
<td>• Monthly</td>
</tr>
</tbody>
</table>

**Related link**

Set up the Microsoft System Center Operations Manager adapter
Set Up OpenManage Enterprise adapter

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

### Table 66. Set Up Adapter (OpenManage Enterprise)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adapter type</strong></td>
<td>Use to select the type of adapter that you want to set up. The available adapter types are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenManage Essentials</strong> — Select to set up the Open Manage Essentials adapter.</td>
</tr>
<tr>
<td></td>
<td>• <strong>System Center Operations Manager</strong> — Select to set up the System Center Operations Manager adapter.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenManage Enterprise</strong> — Select to set up the OpenManage Enterprise adapter.</td>
</tr>
<tr>
<td><strong>Host name / IP address</strong></td>
<td>The host name or IP address of the server where OpenManage Enterprise – Tech Release or OpenManage Enterprise Version 3.0 is installed.</td>
</tr>
<tr>
<td><strong>Name (Optional)</strong></td>
<td>An optional name that you want to use for identifying the adapter in SupportAssist Enterprise.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The user name required to connect to the server where OpenManage Enterprise – Tech Release or OpenManage Enterprise Version 3.0 is installed.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password required to connect to the server where OpenManage Enterprise – Tech Release or OpenManage Enterprise Version 3.0 is installed.</td>
</tr>
<tr>
<td><strong>Credential Profile</strong></td>
<td>Use to select a Credential Profile that is required to add the devices that are inventoried by the adapter.</td>
</tr>
<tr>
<td><strong>Update device inventory</strong></td>
<td>Use to select the frequency at which the adapter must inventory devices from the adapter. The available options are:</td>
</tr>
<tr>
<td></td>
<td>• Every 12 hours</td>
</tr>
<tr>
<td></td>
<td>• Daily</td>
</tr>
<tr>
<td></td>
<td>• Weekly</td>
</tr>
<tr>
<td></td>
<td>• Every two weeks</td>
</tr>
<tr>
<td></td>
<td>• Monthly</td>
</tr>
</tbody>
</table>

**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 67. Adapter overview pane

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name that you have provided for the adapter.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address or host name of the server where the adapter is set up.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the adapter.</td>
</tr>
<tr>
<td>Sync now</td>
<td>Click to inventory devices from the systems management console.</td>
</tr>
<tr>
<td>Last sync</td>
<td>The date and time when the devices were last inventoried.</td>
</tr>
<tr>
<td>Adapter type</td>
<td>The type of adapter.</td>
</tr>
<tr>
<td>OS Type</td>
<td>The operating system running on the server where the adapter is set up.</td>
</tr>
<tr>
<td>Assigned devices</td>
<td>The total number of devices that are added successfully through the adapter.</td>
</tr>
<tr>
<td>Staging devices</td>
<td>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.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the adapter application.</td>
</tr>
</tbody>
</table>

**Related link**

View the 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 68. Remote Collectors

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Up Remote Collector</td>
<td>Click to set up a Remote Collector.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click to edit the details of a Remote Collector.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click to delete a Remote Collector.</td>
</tr>
<tr>
<td>Check box</td>
<td>Use to select a Remote Collector that you have set up.</td>
</tr>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Managed Devices</td>
<td>The total number of devices that are associated with the Remote Collector.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the Remote Collector application.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the Remote Collector.</td>
</tr>
</tbody>
</table>
The status of a Remote Collector may be:

- **Connected** — The server where SupportAssist Enterprise is installed is able to connect to the server where the Remote Collector is set up.
- **Disconnected** — The server where SupportAssist Enterprise is installed is not able to connect to the server where the Remote Collector is set up.
- **Connection failed** — Displayed when a connection fails while connecting to the SupportAssist server.
- **Registration failed** — Displayed when a Remote Collector fails to connect to SupportAssist Enterprise.
- **Registration initiated** — Displayed when the Remote Collector connects to SupportAssist Enterprise.
- **Copy in progress** — The Remote Collector installer package is being copied to the remote system.
- **Validation in progress** — SupportAssist Enterprise is verifying if the remote server meets the prerequisites for setting up the Remote Collector.
- **Configuration in progress** — SupportAssist Enterprise is configuring the settings of the Remote Collector.
- **Registration in progress** — The server running SupportAssist Enterprise is communicating with the Remote Collector after the configuration is complete.
- **Installation in progress** — Installation of the Remote Collector application is in progress.
- **Installer not found** — The Remote Collector installer file is corrupted or deleted manually from the server running SupportAssist Enterprise.
- **Copy failed** — The Remote Collector could not be copied to the remote server.
- **Installation failed** — Installation of the Remote Collector could not be completed successfully.
- **Configuration failed** — SupportAssist Enterprise could not complete the configuring the settings of the Remote Collector.
- **Validation failed** — SupportAssist Enterprise could not verify if the remote server meets the prerequisites for setting up the Remote Collector.
- **Low disk space** — The free hard-drive space on the server where the Remote Collector is set up is less than 500 MB.
- **Connection initiated** — Displayed when a connection is initiated while connecting to the SupportAssist server.

**Upload Connectivity**

Displays the status of the internet connectivity from the remote system to Dell.

**Related links**

- Set up Remote Collector
- View collections for devices associated with a Remote Collector
- View the Remote Collector overview pane
- View devices associated with a Remote Collector
- Edit Remote Collector
- Delete 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host name / IP address</strong></td>
<td>The host name or IP address of the server where you want to set up the Remote Collector.</td>
</tr>
<tr>
<td><strong>Name (Optional)</strong></td>
<td>An optional name that you want to use for identifying the Remote Collector in SupportAssist Enterprise.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The user name required to connect to the server where you want to set up the Remote Collector.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password required to connect to the server where you want to set up the Remote Collector.</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>Select to enter a hostname expression for assigning devices to the Remote Collector.</td>
</tr>
<tr>
<td><strong>Expression</strong></td>
<td>The hostname expression for assigning devices to the Remote Collector.</td>
</tr>
<tr>
<td><strong>IP address / range</strong></td>
<td>Select to enter an IP address range for assigning devices to the Remote Collector.</td>
</tr>
<tr>
<td><strong>Add another hostname</strong></td>
<td>Click to open an additional hostname expression field.</td>
</tr>
<tr>
<td><strong>IP address / range</strong></td>
<td>The IP address or IP address range of the devices that you want to associate with the Remote Collector.</td>
</tr>
<tr>
<td><strong>Add another expression</strong></td>
<td>Click to open an additional hostname expression field.</td>
</tr>
<tr>
<td><strong>The remote system connects to the internet through a proxy server</strong></td>
<td>Select to enter details of the proxy server through which the remote server connects to the internet.</td>
</tr>
<tr>
<td><strong>Host name / IP address</strong></td>
<td>The host name or IP address of the proxy server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port number used by the proxy server.</td>
</tr>
<tr>
<td><strong>Requires authentication</strong></td>
<td>Select this option if a user name and password are required to connect to the proxy server.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>The user name required to connect to the proxy server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password required to connect to the proxy server.</td>
</tr>
<tr>
<td><strong>Proxy Exclusion List</strong></td>
<td>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, Storage SC Series arrays, VMware ESX and ESXi, and XC Series of Web-scale Hyper-converged appliances.</td>
</tr>
</tbody>
</table>

SupportAssist Enterprise user interface 237
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 70. Remote Collector overview pane

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name that you have provided for the Remote Collector.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address or host name of the server where the Remote Collector is set up.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the Remote Collector.</td>
</tr>
<tr>
<td>Collector Type</td>
<td>The type of the collector.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the Remote Collector application.</td>
</tr>
<tr>
<td>OS</td>
<td>The operating system running on the server where the Remote Collector is set up.</td>
</tr>
<tr>
<td>Managed devices</td>
<td>The total number of devices associated with the Remote Collector.</td>
</tr>
<tr>
<td>Collection Range</td>
<td>The IP address ranges that are assigned to the Remote Collector.</td>
</tr>
<tr>
<td>View all devices</td>
<td>Click to open the Devices page where all devices that are associated with the Remote Collector are displayed.</td>
</tr>
</tbody>
</table>

Related link
View 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.
- **TechDirect Login** — To view your Dell EMC asset information from your company's TechDirect account.
- **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.
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 71. Proxy Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use proxy server</td>
<td>Select this option to enable configuring the proxy server settings.</td>
</tr>
<tr>
<td>Host Name / IP Address</td>
<td>The host name or IP address of the proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used by the proxy server.</td>
</tr>
<tr>
<td>Requires authentication</td>
<td>Select this option if a user name and password are required to connect to the proxy server.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name required to connect to the proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password required to connect to the proxy server.</td>
</tr>
<tr>
<td>Proxy exclusion list</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related link**

Configure 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 72. Preferences**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Tasks</td>
<td>Displays options to automatically download and install the latest updates, when they are available. The download and installation of</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>SupportAssist Enterprise application</strong></td>
<td>Select this option to automatically download and install the SupportAssist Enterprise application update whenever it is available.</td>
</tr>
<tr>
<td><strong>Policy files</strong></td>
<td>Select this option to automatically download and install the policy files update whenever it is available.</td>
</tr>
<tr>
<td><strong>Product support files</strong></td>
<td>Select this option to automatically download and install the device support update whenever it is available.</td>
</tr>
<tr>
<td><strong>Adapter Upgrade</strong></td>
<td>Select this option to automatically download and install the adapter update whenever it is available.</td>
</tr>
<tr>
<td><strong>Automatically collect system state information:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Starting from day N of every month at 11 PM</strong></td>
<td>Select this option to automatically collect system state information from each device type on a randomly determined day of every month at 11 PM.</td>
</tr>
<tr>
<td><strong>When a new support case is created</strong></td>
<td>Select this option to automatically start a system log collection when a new support case is generated.</td>
</tr>
<tr>
<td><strong>Automatically upload:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>System state information collected from devices to Dell EMC</strong></td>
<td>Select to automatically upload collections to Dell EMC.</td>
</tr>
<tr>
<td><strong>Automatically start inventory validation:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Starting from day N of every month at 11 PM</strong></td>
<td>Select this option to automatically get the validation information from each device type on a randomly determined day of every month at 11 PM.</td>
</tr>
<tr>
<td><strong>API Interface</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enable API interfaces for SupportAssist Enterprise</strong></td>
<td>Select this option to enable API interfaces for SupportAssist Enterprise.</td>
</tr>
<tr>
<td><strong>Email Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Receive email notification when a new support case is opened</strong></td>
<td>Select this option to receive an email notification when a new support case is opened.</td>
</tr>
<tr>
<td><strong>Preferred email Language</strong></td>
<td>Select the preferred language for email notifications.</td>
</tr>
<tr>
<td><strong>Email Notifications</strong></td>
<td>Click to expand the email notifications list:</td>
</tr>
<tr>
<td></td>
<td>• Remote Collector Connectivity Status</td>
</tr>
<tr>
<td></td>
<td>• Adapter Connectivity Status</td>
</tr>
<tr>
<td></td>
<td>• Remote Collector Upload Connectivity Status</td>
</tr>
<tr>
<td></td>
<td>• Connectivity Test</td>
</tr>
<tr>
<td></td>
<td>• Maintenance Mode</td>
</tr>
<tr>
<td></td>
<td>• Device Validation Status</td>
</tr>
<tr>
<td></td>
<td>• Periodic Inventory Validation</td>
</tr>
</tbody>
</table>

**NOTE:** Dell recommends that you select automatic updates to ensure that SupportAssist Enterprise is up-to-date with the latest features and enhancements.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommendation Report Settings</strong></td>
<td>To access the interactive recommendations report, log in to TechDirect.com</td>
</tr>
<tr>
<td></td>
<td>and click Services &gt; SupportAssist &gt; ProSupport Plus Reporting.</td>
</tr>
<tr>
<td><strong>Collection Data Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Server / Hypervisor</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Software</strong> to collect software-related information from the device.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>System Logs</strong> to collect logs from the device.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Smart Logs</strong> to collect smart CTL logs from the device.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: For information about the logs that are collected by SupportAssist</td>
</tr>
<tr>
<td></td>
<td>Enterprise, see the SupportAssist Enterprise Version 2.0.21 Reportable Item</td>
</tr>
<tr>
<td></td>
<td>s document at Dell.com/ServiceabilityTools.</td>
</tr>
<tr>
<td><strong>Storage: Fluid File System (FluidFS)</strong></td>
<td>Select <strong>Logs</strong> to collect logs from the device.</td>
</tr>
<tr>
<td><strong>Storage: Peer Storage (PS) / EqualLogic</strong></td>
<td>• Select <strong>Diagnostic Data (Diags collection)</strong> to collect diagnostic</td>
</tr>
<tr>
<td></td>
<td>information from the device.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Inter Array Connectivity Test (Ping Test)</strong> to collect the</td>
</tr>
<tr>
<td></td>
<td>ping test result from the device.</td>
</tr>
<tr>
<td><strong>Storage: PowerVault</strong></td>
<td>Select <strong>Support Data</strong> to collect support data from the device.</td>
</tr>
<tr>
<td><strong>Software: HIT Kit/VSM for VMware</strong></td>
<td>Select <strong>Advanced Logs</strong> to collect logs from the device.</td>
</tr>
<tr>
<td><strong>Solution: Nutanix</strong></td>
<td>Select <strong>Logs</strong> to collect logs from the device.</td>
</tr>
<tr>
<td><strong>Virtual Machine</strong></td>
<td>Select <strong>System Logs</strong> to collect logs from the device.</td>
</tr>
<tr>
<td><strong>Device Identification Information Settings</strong></td>
<td>Select this option to allow sending identity information to Dell.</td>
</tr>
<tr>
<td><strong>Include device identification details in</strong></td>
<td><strong>NOTE</strong>: If you clear this option, settings for the collection of logs</td>
</tr>
<tr>
<td>the information that is sent to Dell</td>
<td>and diagnostic data under Collection Data Settings are automatically</td>
</tr>
<tr>
<td></td>
<td>disabled.</td>
</tr>
<tr>
<td><strong>Maintenance Mode</strong></td>
<td>Select this option to set all devices to maintenance mode. While in</td>
</tr>
<tr>
<td></td>
<td>maintenance mode, no new support cases are opened.</td>
</tr>
</tbody>
</table>

**Related links**
- Enable or disable automatic updates
- Configure email notification settings
- Enable or disable the automatic collection of system information on case creation
- Enable or disable the periodic collection of system information from all devices
- Enable or disable the collection of identity information
- Enable or disable 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 that are 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 73. Contact Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company name</td>
<td>The name of your company.</td>
</tr>
<tr>
<td>Primary</td>
<td>Select this option to view or edit the primary contact information.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Select this option to view or edit the secondary contact information.</td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the primary or secondary contact.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the primary or secondary contact.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the primary or secondary contact.</td>
</tr>
<tr>
<td>Alternate phone number</td>
<td>The alternate phone number of the primary or secondary contact.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the primary or secondary contact.</td>
</tr>
<tr>
<td>Preferred contact method</td>
<td>Select the preferred contact method. The available options are:</td>
</tr>
<tr>
<td></td>
<td>• Phone</td>
</tr>
<tr>
<td></td>
<td>• Email</td>
</tr>
<tr>
<td>Preferred contact hours</td>
<td>The preferred hours when Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone of the primary or secondary contact.</td>
</tr>
<tr>
<td>Parts Replacement Preferences for Dell Servers</td>
<td></td>
</tr>
<tr>
<td>I want Dell server replacement parts shipped automatically</td>
<td>Select this check box if you agree to have Dell contact your company and send replacement parts.</td>
</tr>
<tr>
<td>Primary Shipping Contact</td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the primary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Preferred contact hours</td>
<td>The preferred hours when Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.</td>
</tr>
<tr>
<td>Country / Territory</td>
<td>Select the country.</td>
</tr>
<tr>
<td>Shipping address</td>
<td>The address where a replacement component must be dispatched.</td>
</tr>
<tr>
<td>City / Town</td>
<td></td>
</tr>
<tr>
<td>State / Province / Region</td>
<td></td>
</tr>
<tr>
<td>Zip / Postal code</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone of the primary or secondary contact.</td>
</tr>
<tr>
<td>Dispatch Notes</td>
<td>Type and specific dispatch related information.</td>
</tr>
<tr>
<td>I want a technician to replace my parts onsite (if included in my service plan)</td>
<td>Select this option if you want an onsite technician to replace the dispatched hardware component.</td>
</tr>
<tr>
<td>CNPJ</td>
<td>For Brazil only: The CNPJ and IE number of your contact.</td>
</tr>
<tr>
<td>IE</td>
<td></td>
</tr>
<tr>
<td>Secondary Shipping Contact</td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The first name of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Last name</td>
<td>The last name of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the secondary contact who will be responsible for receiving the dispatched part.</td>
</tr>
</tbody>
</table>

**Related links**
- View and update the contact information
- View and update parts dispatch information

**TechDirect Login**

The **TechDirect Integration** page allows you to access reports and manage SupportAssist alerts in TechDirect. The following table provides information about the items displayed in the **TechDirect Integration** page.

At the top of the **TechDirect Integration** page, the navigation trail is displayed.
Table 74. TechDirect Login

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about TechDirect</td>
<td>Opens the TechDirect website in a new web browser window.</td>
</tr>
<tr>
<td>Sign In</td>
<td>Click to sign in to TechDirect.</td>
</tr>
<tr>
<td>OTP</td>
<td>The one-time password required to verify the TechDirect account.</td>
</tr>
</tbody>
</table>

Related link
Sign in to TechDirect

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.

The following table provides information about the items displayed in the SMTP Settings page.

Table 75. SMTP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use SMTP server</td>
<td>Select this option to enable configuring the email server settings.</td>
</tr>
<tr>
<td>Host Name / IP Address</td>
<td>The host name or IP address of the email server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used by the email server.</td>
</tr>
<tr>
<td>Requires authentication</td>
<td>Select this option if a user name and password are required to connect to the email server.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name required to connect to the email server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password required to connect to the email server.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option to use secure communication for sending emails.</td>
</tr>
</tbody>
</table>

Related link
Configure 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 76. Connectivity Test

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box</td>
<td>Select the appropriate check boxes to test the connectivity status you want to verify.</td>
</tr>
<tr>
<td>Test</td>
<td>The dependent network resources that you can test. The available options are:</td>
</tr>
<tr>
<td></td>
<td>• Internet Connectivity</td>
</tr>
<tr>
<td></td>
<td>• SMTP Server</td>
</tr>
<tr>
<td></td>
<td>• Dell EMC FTP Server</td>
</tr>
<tr>
<td></td>
<td>• Dell EMC Upload Server</td>
</tr>
<tr>
<td></td>
<td>• SupportAssist Enterprise Server</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the purpose of each test.</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Displays an icon and a message that indicates the connectivity status. The possible statuses are:</td>
</tr>
<tr>
<td></td>
<td>• Not Configured (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 SMTP Settings in SupportAssist Enterprise.</td>
</tr>
<tr>
<td></td>
<td>• In Progress — The connectivity test is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Connected — The connectivity test is successful.</td>
</tr>
<tr>
<td></td>
<td>• Error — The connectivity test is unsuccessful.</td>
</tr>
<tr>
<td>NOTE</td>
<td>The Error status is displayed as a link that you can click to view a description of the issue and the possible resolution steps.</td>
</tr>
</tbody>
</table>

| Last Verified | The date and time the connectivity status was last verified. |
| Test Connectivity | Click to perform the selected connectivity tests. |

Related link

Perform 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 77. SupportAssist Enterprise test

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box</td>
<td>Select the appropriate check box to test the task that you want to verify.</td>
</tr>
<tr>
<td>Test</td>
<td>The feature that you can test. The available option is Case Creation, which enables you to verify the ability of SupportAssist Enterprise to create a support case with Technical Support.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the purpose of the test.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Status** | Displays an icon and a message that indicates the test status. The possible statuses are:
- **Not validated** — The support case creation task has not been tested.
- **In Progress** — The support case creation test is in progress.
- **Ready to Create Cases** — SupportAssist Enterprise can create cases successfully.
- **Unable to Create Case** — SupportAssist Enterprise cannot create support cases because of a possible issue with the support case creation workflow.

**Last Verified** | The date and time the status was last verified.

**Run Tests** | Click to perform the selected test.

**Related link**
*Test the case creation capability*
The following table lists the error codes, error messages, and possible resolutions.

Table 78. Error code appendix

<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000_1</td>
<td>An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on device_name.</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td>3000_2</td>
<td></td>
<td>- Select the device in the <strong>Devices</strong> page, and in the device overview pane, select <strong>Install / Upgrade OMSA</strong> from the <strong>Tasks</strong> list.</td>
</tr>
<tr>
<td>3000_3</td>
<td></td>
<td>- Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <strong>SupportAssist Enterprise Version 2.0.21 Support Matrix</strong> at Dell.com/ServiceabilityTools.</td>
</tr>
<tr>
<td>3000_4</td>
<td></td>
<td>If the problem persists, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>3000_5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_6</td>
<td>A component required for installing Dell OpenManage Server Administrator (OMSA) could not be downloaded.</td>
<td>1 Make sure that the system has internet connectivity.</td>
</tr>
<tr>
<td>3000_9</td>
<td></td>
<td>2 Perform the Connectivity Test and ensure that the system has connectivity to the dependent resources.</td>
</tr>
<tr>
<td>3000_11</td>
<td></td>
<td>3 Select the device in the <strong>Devices</strong> page, and in the device overview pane, select <strong>Install / Upgrade OMSA</strong> from the <strong>Tasks</strong> list.</td>
</tr>
<tr>
<td>3000_7</td>
<td>Installation of Dell OpenManage Server Administrator (OMSA) is not supported on the operating system running on device_name.</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td>3000_8</td>
<td>An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on device_name.</td>
<td>Try to repair the SupportAssist Enterprise installation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Open <strong>Control Panel</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 In <strong>Programs</strong>, click <strong>Uninstall a Program</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 In the <strong>Programs and Features</strong> window, select <strong>Dell SupportAssist</strong> and click <strong>Change</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 In the <strong>Welcome to Dell SupportAssist Enterprise Installer</strong> window, click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 Click <strong>Repair</strong> and then click <strong>Install</strong>.</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3000_10</td>
<td>An unexpected error occurred during the installation of Dell OMSA on device.</td>
<td>If the problem persists, contact Technical Support for further assistance.</td>
</tr>
<tr>
<td>3000_12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_15</td>
<td>An unexpected error occurred during the installation of Dell OMSA on device.</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td>3000_16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_18</td>
<td>A service required for the installation of Dell OMSA is either not running or not enabled on device.</td>
<td>Make sure that the device is reachable and the configured device credentials have Administrator rights, and then do one of the following:</td>
</tr>
<tr>
<td>3000_19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3000_36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| 3000_37    | An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on device_name. | Make sure that port 22 is open and SSH is enabled on the system, and then do one of the following:  
- Select the device in the Devices page, and in the device overview pane, select Install / Upgrade OMSA from the Tasks list.  
- Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the SupportAssist Enterprise version 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.  
If the problem persists, contact Technical Support for assistance. |
| 3000_38    |                         |                     |
| 3000_39    |                         |                     |
| 3000_40    |                         |                     |
| 3000_41    |                         |                     |
| 3000_42    |                         |                     |
| 3000_43    |                         |                     |
| 3000_44    |                         |                     |
| 3000_45    |                         |                     |
| 3000_46    |                         |                     |
| 3000_49    |                         |                     |
| 3000_51    |                         |                     |
| 3000_52    |                         |                     |
| 3000_53    |                         |                     |
| 3000_54    |                         |                     |
| 3000_55    |                         |                     |
| 3000_57    |                         |                     |
| 3000_58    |                         |                     |
| 3000_59    |                         |                     |
| 3000_60    | An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on device_name. | - Verify if the device is reachable.  
- Verify if the configured device credentials have Administrator rights.  
- Select the device in the Devices page, and in the device overview pane, select Install / Upgrade OMSA from the Tasks list.  
- Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the SupportAssist Enterprise version 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.  
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 Install / Upgrade OMSA from the Tasks 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. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000_1</td>
<td>SNMP settings of the device could not be configured because of an unexpected error.</td>
<td>You must either try to configure the SNMP settings through the <strong>Tasks &gt; Configure SNMP</strong> option or manually configure the SNMP settings. For instructions to manually configure the SNMP settings, see Configuring the alert destination of an iDRAC by using the web interface.</td>
</tr>
<tr>
<td>5000_2</td>
<td>SNMP settings of the device could not be configured because the integrated Dell Remote Access Controller (iDRAC) does not have the required license installed.</td>
<td>Make sure that iDRAC has an Enterprise or Express license installed, and then try to configure the SNMP settings through the <strong>Tasks &gt; Configure SNMP</strong> option.</td>
</tr>
<tr>
<td>5000_3</td>
<td>SNMP settings of the device could not be configured because all configurable fields of the integrated Dell Remote Access Controller (iDRAC) are occupied.</td>
<td>You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see Configuring the alert destination of an iDRAC using the web interface.</td>
</tr>
<tr>
<td>5000_4</td>
<td>SNMP settings of the device could not be configured because the credentials you have entered do not have the required privileges.</td>
<td>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 <strong>Tasks &gt; Configure SNMP</strong> option on the device overview pane.</td>
</tr>
<tr>
<td>5000_5</td>
<td>SNMP settings of the device could not be configured because an attempt to connect to the integrated Dell Remote Access Controller (iDRAC) was unsuccessful.</td>
<td>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 <strong>Tasks &gt; Configure SNMP</strong> option on the device overview pane.</td>
</tr>
<tr>
<td>5000_6</td>
<td>SNMP settings of the device could not be configured because the credentials you have entered are invalid.</td>
<td>Make sure that the credentials are valid, and then try to configure the SNMP settings through the <strong>Tasks &gt; Configure SNMP</strong> option on the device overview pane. If the problem persists, contact your system administrator for assistance.</td>
</tr>
<tr>
<td>5000_7</td>
<td>SNMP settings of the device could not be configured because of an unexpected error.</td>
<td>You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see Configuring the alert destination of an iDRAC using the web interface.</td>
</tr>
<tr>
<td>5000_8</td>
<td>SNMP settings of the device could not be configured because of an unexpected error.</td>
<td>You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see Manually configuring the alert destination (Windows) or Manually configuring the alert destination (Linux).</td>
</tr>
<tr>
<td>5000_9</td>
<td>SNMP settings of the device could not be configured because the user account does not have the sufficient privileges on the device.</td>
<td>You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see Manually configuring the alert destination (Windows) or Manually configuring the alert destination (Linux).</td>
</tr>
<tr>
<td>5000_10</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>5000_11</td>
<td>SNMP settings of the device could not be configured because the SNMP service is not installed on the device.</td>
<td>Manually install the SNMP service on the device, and then try to configure the SNMP settings through the <strong>Tasks &gt; Configure SNMP</strong> option on the device overview pane.</td>
</tr>
<tr>
<td>5000_12</td>
<td>SNMP settings of the device could not be configured because SupportAssist Enterprise does not support the operating system running on the device.</td>
<td>For information on the operating systems supported by SupportAssist Enterprise, see the SupportAssist Enterprise documentation.</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5000_13</td>
<td>SNMP settings of the device could not be configured because the SNMP service has not started.</td>
<td>Manually start the SNMP service on the device, and then try to configure the SNMP settings through the Tasks &gt; Configure SNMP option.</td>
</tr>
<tr>
<td>5000_14</td>
<td>SNMP settings of the device could not be configured because the WMI service is disabled.</td>
<td>Manually start the WMI service on the device, and then try to configure the SNMP settings through the Tasks &gt; Configure SNMP option on the device overview pane.</td>
</tr>
<tr>
<td>5000_15</td>
<td>SupportAssist Enterprise has configured the SNMP settings successfully, but the automated test to verify that the SNMP settings was unsuccessful.</td>
<td>To resolve the issue, verify the network settings and make sure that the SNMP port (162) is open.</td>
</tr>
<tr>
<td>6000_01</td>
<td>SupportAssist Enterprise is unable to clear System Event Log from device_name because of a technical error.</td>
<td>To resolve this issue, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>6000_02</td>
<td>SupportAssist Enterprise is unable to clear System Event Log from device_name because the device is not reachable.</td>
<td>Make sure that the device is reachable from the server running SupportAssist Enterprise and then retry the operation.</td>
</tr>
<tr>
<td>6000_03</td>
<td>SupportAssist Enterprise is unable to clear System Event Log from device_name because the host name of the device could not be resolved to an IP address.</td>
<td>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.</td>
</tr>
<tr>
<td>6000_4</td>
<td>SupportAssist Enterprise is unable to clear System Event Log from device_name because of an internal error.</td>
<td>To resolve this issue, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>6000_6</td>
<td>SupportAssist Enterprise is unable to clear System Event Log from device_name because an attempt to connect to the device is unsuccessful.</td>
<td>Make sure that WMI service is running on the device and then retry the operation.</td>
</tr>
</tbody>
</table>
| 6000_7     | SupportAssist Enterprise is unable to clear System Event Log from device_name because the credentials of the device are either incorrect or do not have the required privileges. | • Make sure that SupportAssist Enterprise is updated with the correct user name and password of the device.  
• Make sure that the user account has administrator or root privileges on the device. |
<p>| 6000_10    | SupportAssist Enterprise is unable to clear System Event Log from device_name 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 device_name 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 device_name because the device does not support this operation. | Not applicable. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>6000_18</td>
<td>SupportAssist Enterprise is unable to clear System Event Log from <code>device_name</code> because an attempt to connect to the device is unsuccessful.</td>
<td>Make sure that the SSH service is running on the device and then retry the operation.</td>
</tr>
<tr>
<td>6000_20</td>
<td>SupportAssist Enterprise is unable to import devices because the device count is more than 300.</td>
<td>Make sure that the device count is below 300 and then retry the operation.</td>
</tr>
<tr>
<td>6000_22</td>
<td>The device import operation is canceled.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>SA-0001</td>
<td>SupportAssist Enterprise is unable to add the devices because the entered host name or IP address, and device type are incorrect.</td>
<td>Retry adding the device with the correct host name or IP address, and device type.</td>
</tr>
<tr>
<td>SA-0005</td>
<td>SupportAssist Enterprise is unable to add the <code>device_name</code> because an attempt to connect to the device is unsuccessful.</td>
<td>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.</td>
</tr>
<tr>
<td>SA-0010</td>
<td>SupportAssist Enterprise is unable to add the <code>device_name</code> because the entered host name or IP address is incorrect.</td>
<td>Retry adding the device with the correct host name or IP address.</td>
</tr>
</tbody>
</table>
| SA-0012    | SupportAssist Enterprise is unable to add the `device_name` because an unknown error occurred while discovering the device. | Verify the following and then retry adding the device:  
  • Make sure that the device is supported by SupportAssist Enterprise. For the list of supported device models, see the `SupportAssist Enterprise Version 2.0.21 Support Matrix` at `Dell.com/ServiceabilityTools`.  
  • Make sure that the user account has administrator/root privileges. |
<p>| SA-0020    | SupportAssist Enterprise is unable to add the <code>device_name</code> because the device is already added. | Not applicable. |
| SA-0025    | SupportAssist Enterprise is unable to add the <code>device_name</code> because of an unknown error. | Verify if the device is supported by SupportAssist Enterprise. For the list of supported device models, see the <code>SupportAssist Enterprise Version 2.0.21 Support Matrix</code> at <code>Dell.com/ServiceabilityTools</code>. If the problem persists, contact Technical Support for assistance. |
| SA-0030    | SupportAssist Enterprise is unable to add the <code>device_name</code> 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 <code>device_name</code> 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 <code>device_name</code> because the name 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 <code>device_name</code> because of an unknown error. | Verify if the device is supported by SupportAssist Enterprise. For the list of supported device models, see the <code>SupportAssist Enterprise Version 2.0.21 Support Matrix</code> at <code>Dell.com/ServiceabilityTools</code>. If the problem persists, contact Technical Support for assistance. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-0055</td>
<td>SupportAssist Enterprise is unable to add the device_name because the device is not supported.</td>
<td>For the list of supported device models, see the SupportAssist Enterprise Version 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.</td>
</tr>
<tr>
<td>SA-0060</td>
<td>SupportAssist Enterprise is unable to add the device_name because a required file has either been deleted or moved.</td>
<td>Restart the Dell SupportAssist service on the system running SupportAssist Enterprise, and then retry adding the device.</td>
</tr>
<tr>
<td>SA-0065</td>
<td>SupportAssist Enterprise is unable to add the device_name because the entered credentials do not have superuser privileges.</td>
<td>Enter the credentials that have superuser privileges, and then retry adding the device.</td>
</tr>
<tr>
<td>SA-0070</td>
<td>Installation of Dell OpenManage Server Administrator (OMSA) is not supported on this device.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>SA-0075</td>
<td>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.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>SA-0080</td>
<td>SupportAssist Enterprise has detected that the Dell OpenManage Server Administrator (OMSA) services are not running on the device.</td>
<td>For optimal SupportAssist Enterprise capability, you must restart the OMSA services.</td>
</tr>
<tr>
<td>SA-0085</td>
<td>SupportAssist Enterprise has detected that Dell OpenManage Server Administrator (OMSA) version x.x is installed on the device.</td>
<td>For optimal SupportAssist Enterprise capability, Dell recommends that you upgrade OMSA to version x.x.</td>
</tr>
<tr>
<td>SA-0090</td>
<td>SupportAssist Enterprise has detected that Dell OpenManage Server Administrator (OMSA) version x.x is installed on the device.</td>
<td>It is recommended that you download and install OMSA version x.x on the device.</td>
</tr>
<tr>
<td>SA-0095</td>
<td>SupportAssist Enterprise is unable to verify the OMSA version installed on the device.</td>
<td>To resolve the issue, see Unable to verify OMSA version.</td>
</tr>
<tr>
<td>SA-0100</td>
<td>The recommended version of Dell OpenManage Server Administrator (OMSA) is already installed on the device.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>SA-0105</td>
<td>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.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>SA-0110</td>
<td>SupportAssist Enterprise is unable to add the device_name because it does not have a valid license.</td>
<td>Make sure that the iDRAC has a valid Enterprise or Express license, and then retry the operation.</td>
</tr>
<tr>
<td>SA-0115</td>
<td>SupportAssist Enterprise is unable to add the device_name because the operating system is not supported.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>SA-0120</td>
<td>SupportAssist Enterprise is unable to add the device because a required service is disabled on the device_name.</td>
<td>Make sure that the required service is running on the device, and then retry adding the device. For information on the required service, see Other services.</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>SA-0125</td>
<td>SupportAssist Enterprise is unable to add the device_name because a response was not received within the predefined time limit.</td>
<td>Try adding the device again. For additional troubleshooting information, see Unable to add the device.</td>
</tr>
<tr>
<td>SA-0130</td>
<td>SupportAssist Enterprise is unable to add the device_name because the SSL encryption level of the device is set to 256 bit or higher.</td>
<td>For troubleshooting steps, see Unable to add the device.</td>
</tr>
<tr>
<td>SA-0135</td>
<td>SupportAssist Enterprise is unable to add the device_name because the device type that you selected is incorrect.</td>
<td>Ensure that you select the correct device type and then try again.</td>
</tr>
</tbody>
</table>
| SA-0140    | SupportAssist Enterprise is unable to add the device_name because a connection to the device was unsuccessful. | Perform the following:  
  - Ensure that the required ports are open on the device. For information on the required ports, see the SupportAssist Enterprise Version 2.0.21 User’s Guide at Dell.com/ServiceabilityTools.  
  - 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 SupportAssist Enterprise Version 2.0.21 Support Matrix at Dell.com/ServiceabilityTools. |
| SA-0145    | SupportAssist Enterprise is unable to add the device_name because the device credentials were not provided. | Enter the device credentials and then try again. |
| SA-0150    | SupportAssist Enterprise is unable to add the device_name because the device credentials were either not provided or incorrectly provided. | 1. Enter the device credentials.  
  2. Ensure that the device credentials are correct. |
| SA-0155    | SupportAssist Enterprise is unable to add the device_name because it is a Storage PS Series member IP address. | Try adding the device again with the Peer Storage PS Series group IP address. |
| SA-0160    | The IP address that you have entered is a Dell Peer Storage/Storage PS Series 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 device_name because an attempt to connect to the device is unsuccessful. | Make sure that both the system running SupportAssist Enterprise and the device are connected to the network, and then retry the operation. |
| SA-1010    | SupportAssist Enterprise is unable to edit the credentials of the device_name because of an unexpected error. | Verify the following and then retry editing the device credentials:  
  - Make sure that the required services are running on the device. For information on the required services, see the Online Help.  
  - Make sure that the entered credentials have administrator or root privileges. |
<p>| SA-1015    | SupportAssist Enterprise is unable to edit the credentials of the device_name 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 device_name because the entered it is already in use by another device. | Enter any other name, and then retry editing the device credentials. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-1030</td>
<td>SupportAssist Enterprise is unable to edit the device credentials because the entered credentials do not have superuser rights.</td>
<td>Enter the credentials that have superuser rights, and then retry saving the device credentials.</td>
</tr>
<tr>
<td>SA-1035</td>
<td>SupportAssist Enterprise is unable to update the device credentials because a required service is disabled on the device.</td>
<td>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 Other services.</td>
</tr>
<tr>
<td>SA-1040</td>
<td>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.</td>
<td>For troubleshooting steps, see Unable to edit device credentials.</td>
</tr>
<tr>
<td>SA-0165</td>
<td>SupportAssist Enterprise is unable to edit the credentials of the device because an attempt to connect to the device is unsuccessful.</td>
<td>Perform the following:</td>
</tr>
<tr>
<td>SA-1045</td>
<td>SupportAssist Enterprise is unable to edit the credentials of the device because an attempt to connect to the device is unsuccessful.</td>
<td>1 Ensure that the FTP port is open.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Enter the correct device credentials.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 If the problem persists, contact your network administrator for assistance.</td>
</tr>
<tr>
<td>SA-2000</td>
<td>SupportAssist Enterprise is unable to establish connections required to auto create cases with Technical Support.</td>
<td>Perform the connectivity test and ensure that the internet connectivity is successful.</td>
</tr>
<tr>
<td>SA-2001</td>
<td>SupportAssist Enterprise is unable to establish connections required to auto create cases with Technical Support.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>SA-4015</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td>To retry collecting the system information, select the device and click Start Collection. If the problem persists, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>SA-4020</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4025</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4030</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4035</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4040</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4045</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4050</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4055</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4060</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4065</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4070</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4071</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4072</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4073</td>
<td>SupportAssist Enterprise is unable to package the system information collected from the device because of an unknown error.</td>
<td>To retry collecting the system information, select the device and click Start Collection. If the problem persists, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>SA-4074</td>
<td>SupportAssist Enterprise is unable to package the system information collected from the device because of an unknown error.</td>
<td></td>
</tr>
<tr>
<td>SA-4075</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because an attempt to connect to the device is unsuccessful.</td>
<td>• Make sure that WMI service is running on the device.</td>
</tr>
<tr>
<td>SA-4080</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because an attempt to connect to the device is unsuccessful.</td>
<td>• To retry collecting the system information, select the device and click Start Collection.</td>
</tr>
<tr>
<td>SA-4085</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because an attempt to connect to the device is unsuccessful.</td>
<td>• Make sure that WS-Man service is running on the device.</td>
</tr>
<tr>
<td>SA-4090</td>
<td>SupportAssist Enterprise is unable to collect system information from the device because an attempt to connect to the device is unsuccessful.</td>
<td></td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SA-4110</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td>• To retry collecting the system information, select the device and click <strong>Start Collection</strong>. If the problem persists, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>SA-4115</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td></td>
</tr>
<tr>
<td>SA-4120</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td>• Make sure that SNMP service is running on the device.</td>
</tr>
<tr>
<td>SA-4125</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td>• To retry collecting the system information, select the device and click <strong>Start Collection</strong>. If the problem persists, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>SA-4130</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td></td>
</tr>
<tr>
<td>SA-4135</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td>• Make sure that vSphere SDK service is running on the device.</td>
</tr>
<tr>
<td>SA-4140</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td>• To retry collecting the system information, select the device and click <strong>Start Collection</strong>. If the problem persists, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>SA-4145</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td></td>
</tr>
<tr>
<td>SA-4150</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because an attempt to connect to the device is unsuccessful.</td>
<td>• Make sure that REST API service is running on the device.</td>
</tr>
<tr>
<td>SA-4155</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because the device is not reachable.</td>
<td>• To retry collecting the system information, select the device and click <strong>Start Collection</strong>.</td>
</tr>
<tr>
<td>SA-4160</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because the IP address of the device is invalid.</td>
<td>• Make sure that SupportAssist Enterprise is updated with the correct IP address of the device.</td>
</tr>
<tr>
<td>SA-4165</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because the download of a certificate file could not be completed successfully.</td>
<td>• Verify the firewall and network settings to make sure that download of the certificate file is not blocked.</td>
</tr>
<tr>
<td>SA-4170</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because the credentials of the device are either incorrect or do not have the required privileges.</td>
<td>• Make sure that SupportAssist Enterprise is updated with the correct user name and password of the device.</td>
</tr>
<tr>
<td>SA-4175</td>
<td>SupportAssist Enterprise is unable to collect system information from the \device_name\ because the credentials of the device are either incorrect or do not have the required privileges.</td>
<td>• Make sure that the user account has administrator or root privileges on the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To retry collecting the system information, select the device and click <strong>Start Collection</strong>.</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>SA-4180</td>
<td>SupportAssist Enterprise is unable to collect system information from the <code>device_name</code> because the device is not supported.</td>
<td>For the list of supported device models, see the SupportAssist Enterprise Version 2.0.21 Support Matrix at Dell.com/ServiceabilityTools.</td>
</tr>
</tbody>
</table>
| SA-4185    | SupportAssist Enterprise is unable to collect system information from the `device_name` because of an attempt to connect to the device is unsuccessful. | - Make sure SupportAssist Enterprise is updated with the credentials of a user account that has root privileges. See Configuring sudo access for SupportAssist Enterprise (Linux).  
- To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4190    | SupportAssist Enterprise is unable to gather system information from the `device_name` because the SSL encryption level of the device is set to 256 bit or higher. | For troubleshooting steps, see Unable to gather system information. |
| SA-4500    | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because the receiving server hosted by Dell is unreachable. | To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact Technical Support for assistance. |
| SA-4501    | SupportAssist Enterprise is unable to collect system information from the `device_name` because of an unknown error. | To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact Technical Support for assistance. |
| SA-4502    | SupportAssist Enterprise is unable to collect system information from the `device_name` because of an unknown error. | To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact Technical Support for assistance. |
| SA-4511    | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because of an unknown error. | - Perform **Network Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful.  
- To retry collecting the system information, select the device and click **Start Collection**. |
| SA-15000   | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because of an unknown error. | - Perform **Network Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful.  
- To retry collecting the system information, select the device and click **Start Collection**. |
| SA-15001   | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because of an unknown error. | - Perform **Network Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful.  
- To retry collecting the system information, select the device and click **Start Collection**. |
| SA-15002   | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because of an unknown error. | - Perform **Network Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful.  
- To retry collecting the system information, select the device and click **Start Collection**. |
| SA-15011   | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because of an unknown error. | - Perform **Network Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful.  
- To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact Technical Support for assistance. |
| SA-15012   | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because of an unknown error. | - Perform **Network Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful.  
- To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact Technical Support for assistance. |
| SA-15013   | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because of an invalid file token. | - Perform **Network Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful.  
- To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact Technical Support for assistance. |
| SA-15014   | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because the collection file is corrupted. | - Perform **Network Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful.  
- To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact Technical Support for assistance. |
| SA-15021   | SupportAssist Enterprise is unable to send the collected system information from the `device_name` because the proxy server is not reachable. | - Verify the proxy server settings in SupportAssist Enterprise.  
- Make sure that the proxy server is reachable.  
- To retry collecting the system information, select the device and click **Start Collection**. |
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-4522</td>
<td>SupportAssist Enterprise is unable to send the collected system information from the <em>device_name</em> because an attempt to connect to proxy server is unsuccessful.</td>
<td>If the problem persists, contact your network administrator for assistance.</td>
</tr>
<tr>
<td>SA-15022</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| SA-4523    | SupportAssist Enterprise is unable to send the collected system information from the *device_name* because the proxy server user name or password is incorrect. | *Verify the proxy server settings in SupportAssist Enterprise.*  
*Make sure that the proxy server is reachable.*  
To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact your network administrator for assistance. |
| SA-15023   | | |
| SA-4524    | SupportAssist Enterprise is unable to send the collected system information from the *device_name* because of an unknown error with reaching the proxy server. | *Verify the proxy server settings in SupportAssist Enterprise.*  
*Make sure that the proxy server is reachable.*  
To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact your network administrator for assistance. |
<p>| SA-15024   | | |
| SA-4550    | SupportAssist Enterprise is unable to collect system information from the device <em>device_name</em> 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 <strong>Hardware requirements</strong>. |
| SA-30130   | SupportAssist Enterprise has placed the device <em>device_name</em> in the <strong>Staging</strong> group because a required verification could not be completed. | To add the device, revalidate the device later. |
| SA-30180   | SupportAssist Enterprise has placed the device <em>device_name</em> in the <strong>Staging</strong> 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 <em>device_name</em> in the <strong>Staging</strong> 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 <em>adapter_name</em> 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 <em>adapter_name</em> because the name 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 <em>adapter_name</em> because of an unknown error. | Retry adding the adapter. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-20020</td>
<td>SupportAssist is unable to set up the adapter <code>adapter_name</code> because the Management Group credentials are incorrect.</td>
<td>Enter the correct Management Group credentials and retry.</td>
</tr>
</tbody>
</table>
| 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:  
  - The adapter is reachable from the server where SupportAssist Enterprise is installed.  
  - Port 5700 is open on the server where SupportAssist Enterprise is installed.  
  - SupportAssist Enterprise Adapter service is running. |
| SA-20030   | SupportAssist Enterprise is unable to reach the system where the adapter is installed. | Verify the following and then retry:  
  - Management Group credentials are correct.  
  - Adapter is connected to the Management Group.  
  - SupportAssist Enterprise Adapter service is running. |
| SA-20035   | SupportAssist Enterprise is unable to set up the adapter `adapter_name` 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 `adapter_name` 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:  
  - Microsoft System Center Operations Manager instance is available.  
  - Microsoft System Center Operations Manager Service is running. |
<p>| SA-20045   | SupportAssist Enterprise is unable to reach the adapter <code>adapter_name</code> because the Management Group credentials are incorrect or does not have sufficient privileges. | Enter the correct Management Group credentials and retry. |
| SA-20050   | SupportAssist Enterprise is unable to reach the adapter <code>adapter_name</code> because of an unknown error. | Not applicable. |
| SA-20055   | SupportAssist Enterprise is unable to reach the adapter <code>adapter_name</code> because of an unknown error. | Not applicable. |
| SA-20065   | SupportAssist Enterprise is unable to reach the adapter <code>adapter_name</code> because of an unknown error. | Not applicable. |
| SA-20080   | SupportAssist Enterprise is unable to reach the adapter <code>adapter_name</code> because of an unknown error. | Not applicable. |
| SA-20085   | SupportAssist Enterprise is unable to reach the adapter <code>adapter_name</code> because of an unknown error. | Not applicable. |
| SA-20404   | SupportAssist Enterprise is unable to set up the adapter <code>adapter_name</code> 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 <code>adapter_name</code> because the name 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 <code>adapter_name</code> 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 <code>adapter_name</code> 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 <code>adapter_name</code> because the adapter is not reachable. | Ensure that the details of the adapter are correct and then retry. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-20095</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because a connection could not be established with the system.</td>
<td>Ensure the following and retry the operation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ensure that the credentials are valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ensure that you have administrator privileges.</td>
</tr>
<tr>
<td>SA-20100</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because a connection could not be established with the system.</td>
<td>Ensure that the remote system has sufficient free hard-drive space required for installing the adapter and retry the operation.</td>
</tr>
<tr>
<td>SA-20105</td>
<td>SupportAssist Enterprise is unable to copy installer file to the system.</td>
<td>Ensure that the system is reachable and the installer file is present at the required location.</td>
</tr>
<tr>
<td>SA-20110</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because the installation of the adapter could not be completed successfully.</td>
<td>Retry setting up the adapter.</td>
</tr>
<tr>
<td>SA-20115</td>
<td>SupportAssist Enterprise is unable to start the adapter service on the system.</td>
<td>Ensure that the installation of the adapter is successful and the configuration file has the correct values.</td>
</tr>
<tr>
<td>SA-20120</td>
<td>SupportAssist Enterprise is unable to copy the configuration file.</td>
<td>Ensure that the configuration file that is generated is not empty and the system is reachable.</td>
</tr>
<tr>
<td>SA-20125</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because the OpenManage Essentials adapter is already installed on the system.</td>
<td>Ensure that the OpenManage Essentials adapter is not installed on the system and then retry the operation.</td>
</tr>
<tr>
<td>SA-20130</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because the status of the required network port could not be verified.</td>
<td>Ensure that the system is running a Windows operating system and the WMI port (135) is open on the system.</td>
</tr>
<tr>
<td>SA-20135</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because the OpenManage Essentials services are not running on the remote system.</td>
<td>Ensure that OpenManage Essentials services are running and retry the operation.</td>
</tr>
<tr>
<td>SA-20140</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name on the system device_name because of one of the following:</td>
<td>Ensure that OpenManage Essentials version 2.3 or later is installed on the system and then retry the operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- OpenManage Essentials is not installed on the system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The adapter is not compatible with the version of OpenManage Essentials installed on the system</td>
</tr>
<tr>
<td>SA-20145</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because the installer for OpenManage Essentials adapter is not present at the required location.</td>
<td>Reinstall SupportAssist Enterprise and then retry the operation.</td>
</tr>
<tr>
<td>SA-20150</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because the operating system installed on the remote system is not of 64-bit architecture.</td>
<td>Ensure that the remote system is running a 64-bit Windows Operating System and retry the operation.</td>
</tr>
<tr>
<td>SA-20155</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because the version of OpenManage Essentials installed on the system is not compatible with the OpenManage Essentials adapter.</td>
<td>Ensure that the OpenManage Essentials version 2.3 or later is installed on the system and then retry the operation.</td>
</tr>
<tr>
<td>SA-20160</td>
<td>SupportAssist Enterprise is unable to set up the adapter adapter_name because the Microsoft .NET package is not installed on the system.</td>
<td>Ensure that the Microsoft .NET package is installed on the remote system and then retry the operation.</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>SA-20165</td>
<td>SupportAssist Enterprise is unable to set up the adapter <code>adapter_name</code> because the version of the Microsoft .NET package installed on the remote system is not compatible with the OpenManage Essentials adapter.</td>
<td>Ensure that the Microsoft .NET package version 4.0 or later is installed on the remote system and then retry the operation.</td>
</tr>
<tr>
<td>SA-20170</td>
<td>SupportAssist Enterprise is unable to set up the adapter <code>adapter_name</code> because Microsoft System Center Operations Manager is not installed on the remote system.</td>
<td>Ensure that the Microsoft System Center Operations Manager is installed on the remote system and then retry the operation.</td>
</tr>
<tr>
<td>SA-20175</td>
<td>SupportAssist Enterprise is unable to set up the adapter <code>adapter_name</code> because the version of Microsoft System Center Operations Manager installed on the remote system is not compatible with Microsoft System Center Operations Manager adapter.</td>
<td>Ensure that the Microsoft System Center Operations Manager version 7.0 or later is installed on the remote system and then retry the operation.</td>
</tr>
<tr>
<td>SA-20180</td>
<td>SupportAssist Enterprise is unable to set up the adapter <code>adapter_name</code> because the Microsoft System Center Operations Manager service is not running on the remote system.</td>
<td>Ensure that the Microsoft System Center Operations Manager service is running and then retry the operation.</td>
</tr>
<tr>
<td>SA-20185</td>
<td>SupportAssist Enterprise is unable to set up the adapter <code>adapter_name</code> because the Microsoft System Center Operations Manager adapter is already installed on the remote system.</td>
<td>Ensure that the Microsoft System Center Operations Manager adapter is not previously installed on the remote system and then retry the operation.</td>
</tr>
</tbody>
</table>
| SA-20190   | SupportAssist Enterprise is unable to edit the adapter `adapter_name` because a connection could not be established with the remote system. | Ensure the following and retry the operation:  
• Ensure that the credentials are valid.  
• Ensure that you have administrator privileges. |
<p>| SA-20200   | SupportAssist Enterprise is unable to edit the adapter <code>adapter_name</code> because the adapter is uninstalled on the remote system. | Not applicable. |
| SA-20205   | SupportAssist Enterprise is unable to set up the adapter <code>adapter_name</code> 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 <code>adapter_name</code>. | Select the adapter and then perform a manual device synchronization. |
| SA-20215   | SupportAssist Enterprise is unable to delete the adapter <code>adapter_name</code> because the adapter is not present on the system. | Not applicable. |
| SA-30005   | SupportAssist Enterprise is unable to set up the Remote Collector <code>Remote Collector_name</code> 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 <code>Remote Collector_name</code> because the provided name 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 <code>Remote Collector_name</code> because the provided IP address range <code>IP address_range</code> overlaps with the IP address range of another Remote Collector. | Provide a mutually exclusive IP address range and retry. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-30020</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector <code>Remote Collector_name</code> because another operation is in progress.</td>
<td>Retry the operation after some time.</td>
</tr>
<tr>
<td>SA-30025</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector <code>Remote Collector_name</code> because the credentials provided for the remote system are incorrect.</td>
<td>Provide the correct credentials and retry.</td>
</tr>
<tr>
<td>SA-30404</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector <code>Remote Collector_name</code> because the Remote Collector is either not valid or not reachable.</td>
<td>Verify the details of the Remote Collector and retry.</td>
</tr>
<tr>
<td>SA-30405</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector <code>Remote Collector_name</code> because Start IP Address is greater than the End IP Address.</td>
<td>Provide the correct IP address range and retry.</td>
</tr>
<tr>
<td>SA-30406</td>
<td>SupportAssist Enterprise is unable to delete the Remote Collector <code>Remote Collector_name</code> because another operation is currently in progress.</td>
<td>Retry the operation after some time.</td>
</tr>
<tr>
<td>SA-30408</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <code>Remote Collector_name</code> because the name is already in use by another Remote Collector.</td>
<td>Provide any other name and retry.</td>
</tr>
<tr>
<td>SA-30409</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <code>Remote Collector_name</code> because the credentials of the Remote Collector are incorrect.</td>
<td>Verify the credentials of the Remote Collector and retry.</td>
</tr>
<tr>
<td>SA-30410</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <code>Remote Collector_name</code> because Remote Collector is either not valid or not reachable.</td>
<td>Verify the details of the Remote Collector and retry.</td>
</tr>
<tr>
<td>SA-30411</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <code>Remote Collector_name</code> because the provided IP address range <code>IP address_range</code> overlaps with the IP address range of another Remote Collector.</td>
<td>Provide a mutually exclusive IP address range and retry.</td>
</tr>
<tr>
<td>SA-30412</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <code>Remote Collector_name</code> because the Start IP Address is greater than the End IP Address.</td>
<td>Provide the correct IP address range and retry.</td>
</tr>
<tr>
<td>SA-30413</td>
<td>SupportAssist Enterprise is unable to update the Remote Collector <code>Remote Collector_name</code> because another operation is in progress.</td>
<td>Retry the operation after some time.</td>
</tr>
<tr>
<td>SA-30414</td>
<td>SupportAssist Enterprise is unable to connect to the Remote Collector <code>Remote Collector_name</code> because of an internal error.</td>
<td>Ensure that the Remote Collector application is running and then retry the operation.</td>
</tr>
<tr>
<td>SA-30415</td>
<td>SupportAssist Enterprise is unable to connect to the Remote Collector <code>Remote Collector_name</code> because of an internal error.</td>
<td>Update the credentials of the Remote Collector, ensure that the Remote Collector application is running, and then retry.</td>
</tr>
<tr>
<td>SA-30416</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector <code>Remote Collector_name</code> because the provided IP address range <code>IP address_range</code> overlaps with the IP address range of same Remote Collector.</td>
<td>Provide a mutually exclusive IP address range and retry.</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SA-30417</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the installer for Remote Collector could not be found at the required location.</td>
<td>Reinstall SupportAssist Enterprise and then retry the operation.</td>
</tr>
<tr>
<td>SA-30418</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because a connection could not be established with the remote system.</td>
<td>Ensure the following and retry the operation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the credentials are valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that you have administrator privileges.</td>
</tr>
<tr>
<td>SA-30419</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the Remote Collector installer could not be copied to the remote system.</td>
<td>Ensure that the remote system is reachable. Verify the credentials of the remote system and then retry the operation.</td>
</tr>
<tr>
<td>SA-30420</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the Remote Collector installation on the remote system was unsuccessful.</td>
<td>Ensure that the remote system is compatible with the hardware and software requirements for setting up a Remote Collector.</td>
</tr>
<tr>
<td>SA-30421</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the Remote Collector installation was not successful.</td>
<td>Ensure that the remote system is compatible with the hardware and software requirements for setting up a Remote Collector.</td>
</tr>
<tr>
<td>SA-30422</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the installation of the Remote Collector was unsuccessful.</td>
<td>Reinstall SupportAssist Enterprise and then retry the operation.</td>
</tr>
<tr>
<td>SA-30423</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the Remote Collector configuration was unsuccessful.</td>
<td>Reinstall SupportAssist Enterprise and then retry the operation.</td>
</tr>
<tr>
<td>SA-30424</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the remote system does not have sufficient free hard-drive space.</td>
<td>Ensure that the remote system has at least 500 MB of free hard-drive space.</td>
</tr>
<tr>
<td>SA-30425</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because SupportAssist Enterprise is already installed on the remote system.</td>
<td>Uninstall SupportAssist Enterprise from the remote system and then retry the operation.</td>
</tr>
<tr>
<td>SA-30426</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the IP address or hostname that has been provided is of the local system.</td>
<td>Provide the correct IP address or hostname of a remote system and retry the operation.</td>
</tr>
<tr>
<td>SA-30427</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the remote system is not reachable.</td>
<td>Ensure that the remote system is reachable and then retry the operation.</td>
</tr>
<tr>
<td>SA-30428</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because the Remote Collector is not supported on a non-Windows operating system.</td>
<td>Ensure you provide the details of a remote system that is running a Windows operating system and then retry the operation.</td>
</tr>
<tr>
<td>SA-30429</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector Remote Collector_name because the provided IP address range IP address_range overlaps</td>
<td>Provide a mutually exclusive IP address range and retry.</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>SA-30430</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <strong>Remote Collector_name</strong> because the credentials of the Remote Collector are incorrect.</td>
<td>Verify the credentials of the Remote Collector and retry the operation.</td>
</tr>
<tr>
<td>SA-30431</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <strong>Remote Collector_name</strong> because the Remote Collector configuration on the remote system was not successful.</td>
<td>Ensure that the remote system is reachable. Verify the credentials of the remote system and then retry the operation.</td>
</tr>
<tr>
<td>SA-30432</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <strong>Remote Collector_name</strong> because the SupportAssist Enterprise service is not running on the remote system.</td>
<td>Start the SupportAssist Enterprise service on the remote system and then retry the operation.</td>
</tr>
<tr>
<td>SA-30433</td>
<td>SupportAssist Enterprise is unable to update the details of the Remote Collector <strong>Remote Collector_name</strong> because the Remote Collector application is not installed on the remote system.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>SA-30434</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector <strong>Remote Collector_name</strong> because the operating system installed on the remote system is not of 64-bit architecture.</td>
<td>Ensure that you provide the details of a remote system that is running a 64-bit Windows operating system and then retry the operation.</td>
</tr>
<tr>
<td>SA-30435</td>
<td>SupportAssist Enterprise is unable to set up the Remote Collector <strong>Remote Collector_name</strong> because the validation of the Remote Collector was unsuccessful.</td>
<td>Ensure that the remote system is compatible with the hardware and software requirements for setting up a Remote Collector.</td>
</tr>
<tr>
<td>SA-4525</td>
<td>Uploaded collection file from <strong>device_name</strong> was deleted because a potential security risk was detected.</td>
<td>For information on security risks, see the SupportAssist Enterprise Version 2.0.21 User’s Guide at Dell.com/ServiceabilityTools.</td>
</tr>
<tr>
<td>SA-4530</td>
<td>Upload of the system information collected from <strong>device_name</strong> was unsuccessful because the upload process exceeded the defined time limit.</td>
<td>To retry the upload, select the collection from the Collections page and click Upload. If the problem persists, contact Dell Technical Support for assistance.</td>
</tr>
<tr>
<td>SA-4531</td>
<td>Upload of the system information collected from <strong>device_name</strong> was unsuccessful because of an issue with the upload server hosted by Dell.</td>
<td>To retry the upload, select the collection from the Collections page and click Upload. If the problem persists, contact Dell Technical Support for assistance.</td>
</tr>
<tr>
<td>SA-4040</td>
<td>SupportAssist Enterprise is unable to package the system information collected from the device <strong>device_name</strong> because of an unknown error.</td>
<td>To retry collecting the system information, select the device and click Start Collection. If the problem persists, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>SA-4073</td>
<td>SupportAssist Enterprise is unable to collect system information from the device <strong>device_name</strong> because an attempt to connect to the device is unsuccessful.</td>
<td>• Make sure that WMI service is running on the device. • To retry collecting the system information, select the device and click Start Collection.</td>
</tr>
<tr>
<td>SA-4080</td>
<td>SupportAssist Enterprise is unable to collect system information from the device <strong>device_name</strong> because an attempt to connect to the device is unsuccessful.</td>
<td>To retry collecting the system information, select the device and click Start Collection. If the problem persists, contact Technical Support for assistance.</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Possible resolution</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| SA-4095    | SupportAssist Enterprise is unable to collect system information from the device `device_name` because an attempt to connect to the device is unsuccessful. | • Make sure that the SSH service is running on the device.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4100    | SupportAssist Enterprise is unable to collect system information from the device `device_name` because the device is not reachable. | • Make sure the device you are trying to add is reachable from the server running SupportAssist Enterprise.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4105    | SupportAssist Enterprise is unable to collect system information from the device `device_name` because the IP address of the device is invalid. | • Make sure that SupportAssist Enterprise is updated with the correct IP address of the device.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4155    | SupportAssist Enterprise is unable to collect system information from the device `device_name` because the download of a certificate file could not be completed successfully. | • Verify the firewall and network settings to make sure that download of the certificate file is not blocked.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4170    | SupportAssist Enterprise is unable to collect system information from the device `device_name` because the credentials of the device are either incorrect or do not have the required privileges. | • Make sure that SupportAssist Enterprise is updated with the correct user name and password of the device.  
• Make sure that the user account has administrator/root privileges on the device.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4185    | SupportAssist Enterprise is unable to collect system information from the device `device_name` because of an attempt to connect to the device is unsuccessful. | • Make sure SupportAssist Enterprise is updated with the credentials of a user account that has root privileges. For instructions to add a user account to the root group, see the "Adding a user to the root user group" section in the SupportAssist Enterprise Version 2.0.21 User’s Guide at Dell.com/ServiceabilityTools.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4500    | SupportAssist Enterprise is unable to send the collected system information from the device `device_name` because the receiving server hosted by Dell is unreachable. | To retry collecting the system information, select the device and click **Start Collection**. If the problem persists, contact Technical Support for assistance. |
| SA-4513    | SupportAssist Enterprise is unable to send the collected system information from the device `device_name` because of an invalid file token. | • Perform the Connectivity Test and make sure that connectivity to the Dell Upload Server is successful.  
• To retry collecting the system information, select the device and click **Start Collection**. |
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
</table>
| SA-4514    | SupportAssist Enterprise is unable to send the collected system information from the device device_name because the collection file is corrupted. | If the problem persists, contact Dell Technical Support for assistance.  
• Perform the Connectivity Test and make sure that connectivity to the Dell Upload Server is successful.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4521    | SupportAssist Enterprise is unable to send the collected system information from the device device_name because the proxy server is not reachable. | If the problem persists, contact Dell Technical Support for assistance.  
• Verify the proxy server settings in SupportAssist Enterprise.  
• Make sure that the proxy server is reachable.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4522    | SupportAssist Enterprise is unable to send the collected system information from the device device_name because the proxy server is not reachable. | If the problem persists, contact Dell Technical Support for assistance.  
• Verify the proxy server settings in SupportAssist Enterprise.  
• Make sure that the proxy server is reachable.  
• To retry collecting the system information, select the device and click **Start Collection**. |
| SA-4523    | SupportAssist Enterprise is unable to send the collected system information from the device device_name because the proxy server username or password is incorrect. | If the problem persists, contact Dell Technical Support for assistance.  
• Make sure that the proxy server user name and password you have entered in SupportAssist Enterprise are correct.  
• To retry collecting the system information, select the device and click **Start Collection**. |
<p>| SA-30265   | SupportAssist Enterprise has placed the device device_name in the Staging group because the Software service is not running on the device. | To add the device, ensure that the software service is running and then revalidate the device. |
| SA-0170    | SupportAssist Enterprise is unable to add the device device_name because you have entered the hostname/IP address of a Web-Scale Cluster VM. | Try adding the device by entering the hostname/IP address of Web-Scale Cluster. |
| SA-0136    | SupportAssist Enterprise is unable to add the device device_name because the device sub type that you have selected is incorrect. | Ensure that you select the correct device sub type and try again. |
| SA-30428   | SupportAssist Enterprise is unable to set up the Remote Collector Remote Collector_name because setting up a Remote Collector on a Windows system is not supported. | Ensure that the remote system has Linux operating system installed and retry the operation. |
| SA-30438   | SupportAssist Enterprise is unable to add the Remote Collector Remote Collector_name because the provided hostname expression hostname_expression matches with the hostname expression of another Remote Collector. | Provide a mutually exclusive hostname expression and retry. |
| SA-30442   | SupportAssist Enterprise is unable to add the Remote Collector Remote Collector_name because the provided hostname expression hostname_expression is duplicated within the same Remote Collector. | Provide a mutually exclusive hostname expression and retry. |
| SA-30439   | SupportAssist Enterprise is unable to add the Remote Collector Remote Collector_name because the pre-check operation. | Ensure that the remote system is reachable. Also verify the credentials of the Remote Collector and retry the operation. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-30443</td>
<td>SupportAssist Enterprise is unable to edit the Remote Collector Remote Collector_name because the Remote Collector configuration is corrupted on the remote system.</td>
<td>To resolve the issue, delete the Remote collector, and retry setting up the Remote Collector again.</td>
</tr>
<tr>
<td>SA-30444</td>
<td>SupportAssist Enterprise is unable to add the Remote Collector Remote Collector_name because download of Remote Collector installer was unsuccessful.</td>
<td>Run the Connectivity Test to ensure that connectivity to the Dell EMC FTP server is successful and then retry.</td>
</tr>
</tbody>
</table>
| SA-20620   | SupportAssist Enterprise is unable to update the details of the host adapter_name, because a connection could not be established between the host and management console. | Verify the following and then retry the operation:  
  - The host running the management console must be reachable.  
  - The credentials of the host must be valid and must also have administrator rights.  
  - The adapter service must be running on the host. |
| SA-20550   | SupportAssist Enterprise is unable to connect to Adapter adapter_name because the adapter service may not be running. | Ensure that the adapter service is running on the host. |
| SA-20666   | SupportAssist Enterprise is unable to connect to Adapter adapter_name, because a connection could not be established between the host and management console. | Verify the following and then retry the operation:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise.  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise. |
| SA-20070   | SupportAssist Enterprise is unable to connect to the adapter adapter_name because the adapter credentials are either incorrect or do not have the required privileges. | Ensure the following and then retry:  
  - The adapter credentials must be correct.  
  - The adapter credentials must have administrator privileges. |
| SA-20075   | SupportAssist Enterprise is unable to connect to the adapter adapter_name because of an unknown error. | Ensure the following and then retry:  
  - If the credentials of the system where the adapter is set up have changed, update the adapter credentials in SupportAssist Enterprise.  
  - The adapter services must be running on the system where the adapter is set up.  
  - OpenManage Essentials services must be running on the system where the adapter is set up. |
| SA-20090   | SupportAssist Enterprise is unable to connect to the adapter adapter_name because the OpenManage Essentials services are not running. | Ensure that OpenManage Essentials services are running on the system where the adapter is setup and then retry. |
| SA-30414   | SupportAssist Enterprise is unable to reach the Remote Collector Remote Collector_name. | Ensure the following:  
  - The server hosting the remote collector must be reachable from the server where SupportAssist Enterprise is installed.  
  - The Remote Collector services must be running on the server hosting the Remote Collector. |
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-20605</td>
<td>SupportAssist Enterprise is unable to set up the adapter because the hostname/IP address hostname/IP address is either invalid or unreachable.</td>
<td>Ensure that the hostname/IP address is valid and reachable, and then try setting up the adapter.</td>
</tr>
<tr>
<td>SA-20610</td>
<td>SupportAssist Enterprise is unable to set up the adapter for the host hostname/IP address because the credentials are incorrect.</td>
<td>Ensure that the credentials of the host are correct and then try setting up the adapter.</td>
</tr>
</tbody>
</table>
| SA-20615   | SupportAssist Enterprise is unable to inventory devices through the adapter because a connection could not be established with the host/management console. | Ensure the following and then retry the operation:  
  - The host running the management console must be reachable.  
  - The credentials of the host must be valid and must also have administrator rights.  
  - The systems management console services must be running on the host. |
| SA-20620   | SupportAssist Enterprise is unable to set up the adapter on the host hostname/IP address because the operating system is not supported. | For information on the operating systems that support setting up the adapter_name, see the Online Help. |
| SA-20625   | SupportAssist Enterprise is unable to set up the adapter on the host hostname/IP address because the operating system is not supported. | Ensure the following and then try setting up the adapter:  
  - The host running the management console must be reachable and must also have more than 500 MB free hard-drive space.  
  - Port x must be open on the host.  
  - The systems management console must be installed on the host.  
  - The systems management console services must be running on the host. |
| SA-20634   | SupportAssist Enterprise is unable to set up the adapter_name adapter on the host hostname/IP address because it does not meet certain requirements. | Ensure that the systems management console services are running on the host and then try setting up the adapter. |
| SA-20644   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the adapter installer file is not available at the default location. | Reinstall SupportAssist Enterprise and then try setting up the adapter. |
| SA-20646   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Try setting up the adapter after the installation of the other adapter is complete. |
| SA-20648   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Ensure the following:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise |
| SA-20650   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Ensure the following:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise |
| SA-20652   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Ensure the following:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise |
| SA-20654   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Ensure the following:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise |
| SA-20658   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Ensure the following:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise |
| SA-20660   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Ensure the following:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise |
| SA-20662   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Ensure the following:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise |
| SA-20664   | SupportAssist Enterprise is unable to set up the adapter_name adapter because the installation of another adapter is in progress. | Ensure the following:  
  - The system where the management console is set up must be reachable from the server running SupportAssist Enterprise  
  - If the credentials of the management console have changed, update the credentials of the adapter in SupportAssist Enterprise |
<p>| SA-20666   | SupportAssist Enterprise is unable to connect to Adapter adapter_name. | None |
| SA-9000    | Inventory Validation capabilities have not been verified for the device. | None |
| SA-9015    | The monitoring capability is disabled for the device. | Ensure that the monitoring capability is enabled for the device. |</p>
<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Possible resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-9020</td>
<td>SNMP settings of the device could not be configured because the SNMP service or Net-SNMP service is not installed on your system.</td>
<td>Ensure that you install the SNMP service or Net-SNMP service on your system.</td>
</tr>
</tbody>
</table>
| SA-9025    | SupportAssist Enterprise is unable to run the script file because of one of the following:  
1. You may not have superuser privileges on the system.  
2. You have not entered the Management Server IP address.  
3. Network sharing might be disabled. | Perform the following:  
1. Ensure that you have superuser privileges on the system.  
2. Enter the Management Server IP address. |
| SA-9030    | SNMP service is not running on the device. | Manually start the SNMP service on the device. |
| SA-9035    | The SNMP trap destination is not configured on the device. | You must either try to configure the SNMP settings through the Tasks > Configure SNMP option or manually configure the SNMP settings. For instructions to manually configure the SNMP settings, see "Manually configuring SNMP settings" in the Online Help or User's Guide. |
| SA-9040    | SupportAssist Enterprise has detected that Dell OpenManage Server Administrator (OMSA) is not installed on the device. | Select the device in the Devices page, and in the device overview pane, select Install/Upgrade OMSA from the Tasks list. |
| SA-9045    | The system hosting the Remote Collector is not reachable or the Remote Collector service is not running on the system. | Make sure that the system hosting the Remote Collector is reachable and the Remote Collector service is running on the system. |
| SA-9050    | SupportAssist Enterprise has detected that the OpenManage Server Administrator (OMSA) services are not running on the system. | Make sure that the OpenManage Server Administrator (OMSA) services are running on the system. |
| SA-9055    | Collection of system information is not supported on the device because it is assigned to a Remote Collector hosted on a Linux operating system. | Assign the device to a Remote Collector hosted on a Windows operating system. |
Related documents and resources

In addition to this guide you can access the following documents that provide more information on SupportAssist Enterprise and the other related products.

Table 79. Related documents

<table>
<thead>
<tr>
<th>Document title</th>
<th>How to access the document</th>
</tr>
</thead>
<tbody>
<tr>
<td>SupportAssist Enterprise Version 2.0.21 Online Help</td>
<td>Click the help icon in the SupportAssist Enterprise user interface.</td>
</tr>
<tr>
<td>SupportAssist Enterprise Version 2.0.21 Reportable Items</td>
<td>3 Click Manuals.</td>
</tr>
<tr>
<td>SupportAssist Enterprise Version 2.0.21 Release Notes</td>
<td></td>
</tr>
<tr>
<td>OpenManage Server Administrator Installation Guide</td>
<td>Visit Dell.com/OpenManageManuals and click OpenManage Server Administrator.</td>
</tr>
<tr>
<td>OpenManage Server Administrator User’s Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 Click ProSupport Plus Reporting.</td>
</tr>
<tr>
<td></td>
<td>3 Click Manuals.</td>
</tr>
</tbody>
</table>

Video tutorials

You can access the following video tutorials to learn about the features of SupportAssist Enterprise. To access the video tutorials, visit the Dell TechCenter Channel.

- SupportAssist Enterprise: Installing and Registering (Windows)
- SupportAssist Enterprise: Installing and Registering (Linux)
- SupportAssist Enterprise: Checking for Cases
- SupportAssist Enterprise: Testing Case Creation
- SupportAssist Enterprise: Monitoring the Local System
- SupportAssist Enterprise: Adding Devices
- SupportAssist Enterprise: Case Management
- SupportAssist Enterprise: Managing Device Groups
- 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 Enterprise: Creating Device Discovery Rule
- SupportAssist Enterprise: Managing SupportAssist Enterprise Alerts in TechDirect
- SupportAssist Enterprise: Performing Deep Discovery
- SupportAssist Enterprise: Setting up Automated Dispatch

SupportAssist community

You can ask peer-to-peer questions on the Dell SupportAssist Enterprise community forum.

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 — www.dell.com/esmmanuals
- For Dell EMC OpenManage documents — www.dell.com/openmanagemanuals
- For Dell EMC Remote Enterprise Systems Management documents — www.dell.com/esmmanuals
- For iDRAC and Dell Lifecycle Controller documents — www.dell.com/idracmanuals
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — www.dell.com/esmmanuals
- For Dell EMC Serviceability Tools documents — www.dell.com/serviceabilitytools
- Go to www.dell.com/support.
- Click Browse all products.
- From All products page, click Software, and then click the required link from the following:
  - Analytics
  - Client Systems Management
  - Enterprise Applications
  - Enterprise Systems Management
  - Public Sector Solutions
  - Utilities
  - Mainframe
  - Serviceability Tools
  - Virtualization Solutions
  - Operating Systems
  - Support
- To view a document, click the required product and then click the required version.
- Using search engines:
  - Type the name and version of the document in the search box.

Contacting Dell

Prerequisite

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.