

# Dell SupportAssist Version 1.0.1 for Servers User's Guide



# Notes, cautions, and warnings

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

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

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

**Copyright © 2015 Dell Inc. All rights reserved.** This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2015 - 04

Rev. A00

# Contents

<b>1 Overview.....</b>	<b>7</b>
What is new in this release.....	7
How SupportAssist works.....	8
SupportAssist capabilities available with Dell service contracts.....	8
Data collected by SupportAssist.....	9
Event storm handling.....	10
<b>2 Getting started with SupportAssist.....</b>	<b>11</b>
Basic setup.....	11
Advanced setup.....	11
Trying out SupportAssist.....	11
Downloading the SupportAssist installation package.....	12
Minimum requirements for installing SupportAssist.....	12
Hardware requirements.....	12
Software requirements.....	13
Network requirements.....	13
Installing SupportAssist.....	14
Setting up SupportAssist.....	15
Upgrading SupportAssist.....	17
Opening the SupportAssist user interface.....	17
Logging on to SupportAssist.....	18
Logging out of SupportAssist.....	18
<b>3 Adding devices for monitoring.....</b>	<b>19</b>
Adding a device (agent-based monitoring).....	19
Configuring the alert (SNMP trap) destination.....	21
Adding a device (agentless monitoring).....	24
Manually configuring the alert destination of an iDRAC using the web interface.....	25
<b>4 Viewing cases and devices.....</b>	<b>27</b>
Viewing the cases.....	27
Viewing the device inventory.....	27
Filtering the displayed data.....	28
Clearing the data filter.....	28
Sorting the displayed data.....	28
<b>5 Understanding maintenance mode.....</b>	<b>29</b>
Global-level maintenance mode.....	29

Device-level maintenance mode.....	29
Enabling or disabling global-level maintenance mode.....	30
Enabling or disabling device-level maintenance mode.....	30
<b>6 Maintaining SupportAssist capability.....</b>	<b>32</b>
Editing device credentials.....	32
Installing or upgrading OMSA using SupportAssist.....	33
Configuring SNMP settings using SupportAssist.....	33
Viewing and updating the contact information.....	34
Configuring proxy server settings.....	34
Connectivity test.....	35
Viewing the connectivity status.....	35
Performing the connectivity test.....	36
Auto update.....	36
Enabling auto update.....	37
Deleting a device.....	37
<b>7 Configuring email notifications.....</b>	<b>38</b>
Configuring email notification settings.....	38
Configuring SMTP server settings.....	39
<b>8 Configuring data collection settings.....</b>	<b>40</b>
Enabling or disabling the automatic collection of system information.....	40
Enabling or disabling the periodic collection of system information from all devices.....	41
Customizing the schedule for periodic collection of system information.....	41
Disabling the periodic collection of system information from specific devices.....	42
Filtering the collection of system information.....	43
<b>9 Accessing the collected data and log files.....</b>	<b>45</b>
Accessing and viewing the collected system information.....	45
Accessing and viewing the logs.....	45
<b>10 Other useful information.....</b>	<b>47</b>
Sending the system information manually.....	47
SupportAssist user groups.....	47
Support for automatically installing or upgrading OMSA.....	49
Support for automatically configuring SNMP settings.....	50
Detection of hardware issues in attached storage devices.....	50
Support for Dell OEM servers.....	50
Default schedule for collection of system information.....	51
Types of email notifications.....	51


Ensuring successful communication between the SupportAssist application and the SupportAssist server.....	53
Verifying the server certificate.....	53
Verifying the installation of the SupportAssist component.....	54
Accessing the context-sensitive help.....	54
Viewing SupportAssist product information.....	54
Uninstalling SupportAssist.....	54
Identifying the generation of a Dell PowerEdge server.....	55
Known issues.....	56
<b>11 Troubleshooting.....</b>	<b>57</b>
Installing SupportAssist.....	57
SupportAssist registration.....	57
Opening the SupportAssist user interface.....	57
Logging on to SupportAssist.....	58
Unable to add device.....	58
OMSA not installed.....	59
SNMP not configured.....	59
New version of OMSA available.....	60
Device configuration not supported by OMSA.....	60
Unable to configure SNMP.....	60
Unable to verify SNMP configuration.....	61
Unable to install OMSA.....	61
Unable to verify OMSA version.....	62
Unsupported operating system.....	62
Unexpected error occurred.....	62
Unable to reach device.....	64
Enterprise license required.....	64
Authentication failed.....	64
Unable to gather system information.....	65
Insufficient storage space to gather system information.....	65
Unable to reach Dell upload server.....	66
Timed out sending system information.....	66
SupportAssist component is not available.....	66
Maintenance mode.....	67
Auto update.....	67
Unable to edit device credentials.....	67
Automatic case creation.....	68
Scheduled tasks.....	68
SupportAssist services.....	68
Other services.....	69
WMI service.....	69

SSH service.....	69
Security.....	70
Troubleshooting SSL connection failure.....	70
Exporting the root certificate.....	70
Installing the root certificate.....	71
<b>12 Error code appendix.....</b>	<b>73</b>
<b>13 Dell SupportAssist user interface.....</b>	<b>80</b>
Setup Wizard.....	81
Welcome.....	81
Proxy Settings.....	81
Registration.....	82
Summary.....	82
Login.....	82
Cases.....	82
Device inventory.....	84
Add Device.....	86
Settings.....	87
System logs.....	87
Proxy settings.....	88
Preferences.....	89
Contact information.....	90
SMTP settings.....	91
Connectivity test.....	91
<b>14 Related documents and resources.....</b>	<b>93</b>
Video tutorials.....	93
SupportAssist community.....	93
Dell Remote Consulting Service.....	94
Accessing Documents From Dell Support Site.....	94
Contacting Dell.....	94


# Overview


Dell SupportAssist for Servers is an application that enables automated support from Dell by proactively identifying hardware issues in Dell servers. When an issue is detected, SupportAssist automatically opens a support case with Dell Technical Support and sends you an email notification. Data required for troubleshooting the issue is automatically collected and sent securely to Dell. The collected data helps Dell to provide you an enhanced, personalized, and efficient support experience. SupportAssist capability also includes proactive contact from Dell Technical Support to help you resolve the issue.

Installing and using SupportAssist is voluntary, and results in improved support, products, and services designed to meet your needs.

 **NOTE:** SupportAssist capabilities supported on a monitored Dell server may vary based on the Dell service contract. For more information about the capabilities of SupportAssist, see [SupportAssist capabilities available with Dell service contracts](#).

SupportAssist Version 1.0.1 for Servers provides automated support capabilities for Dell's 9th to 13th generation of PowerEdge servers. SupportAssist also supports monitoring of Dell's 12th and 13th generation of PowerEdge servers through the Integrated Dell Remote Access Controller (iDRAC).

 **NOTE:** SupportAssist for Servers can discover and monitor devices independently. It does not depend on systems management consoles such as Dell OpenManage Essentials or Microsoft System Center Operations Manager for discovering and monitoring devices.

 **NOTE:** SupportAssist Version 1.0.1 for Servers supports monitoring of up to 20 Dell PowerEdge servers. For a list of supported server models, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

## Related References

- [Data collected by SupportAssist](#)
- [Identifying the generation of a Dell PowerEdge server](#)


## What is new in this release


- Support for additional models of Dell's 13th generation of PowerEdge servers.
- Support for Dell OEM servers. See [Support for Dell OEM servers](#).
- Ability to detect hardware issues that may occur on attached storage devices. See [Detection of hardware issues in attached storage devices](#).
- Ability to automatically configure the SNMP settings of a device. See [Support for automatically configuring SNMP settings](#).
- Addition of Red Hat Enterprise Linux 7 as a supported operating system for SupportAssist on Dell's 11th and 12th generation of PowerEdge servers.
- Addition of support for Simple Network Management Protocol (SNMP) version 2.

- Support for installing SupportAssist on a domain controller.
- Support for upgrading from SupportAssist version 1.0 to version 1.0.1. See [Upgrading SupportAssist](#).

## How SupportAssist works

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










 **NOTE:** For more information about how SupportAssist processes alerts and automatically creates support cases, see the *Dell SupportAssist: Alert Policy* technical document at [Dell.com/SupportAssistGroup](http://Dell.com/SupportAssistGroup).













 **NOTE:** SupportAssist 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 capabilities available with Dell service contracts

The primary benefits of SupportAssist are available only for devices that have an active Dell ProSupport or Dell ProSupport Plus service contract. SupportAssist also detects potential hardware issues in devices that have a Dell Basic Hardware service contract, and sends an automatic email notification, but a support case is not created automatically.

The following table provides a comparison of the SupportAssist capabilities supported with the Basic Hardware, ProSupport, and ProSupport Plus service contracts.

SupportAssist capability	Description	Dell service contract type		
		Basic Hardware	ProSupport	ProSupport Plus
Proactive detection of potential hardware issues	SupportAssist receives alerts for hardware events in monitored devices and proactively determines if the event can result in a potential hardware issue.			
Automated data collection	Data required for troubleshooting the issue is automatically collected from the device and sent securely to Dell.			
Automated email notification	An email notification about the support case or issue is			

SupportAssist capability	Description	Dell service contract type		
		Basic Hardware	ProSupport	ProSupport Plus
	automatically sent to your primary and secondary SupportAssist contacts.			
Automated support case creation	When a critical alert is received from a monitored device, the alert information is sent securely to Dell and a service request is automatically created.			
Proactive contact from Dell Technical Support	A Dell technical support agent contacts you proactively about the support case and helps you resolve the issue.			
Proactive parts dispatch	Based on examination of the collected data, if the Dell Technical Support agent determines that a part needs to be replaced to resolve the issue, a replacement part is dispatched to you with your consent.			
ProSupport Plus reporting	Data collected periodically by SupportAssist enables Dell to provide you an insight into the as-maintained environment configuration with proactive firmware recommendations and other reports.			

## Data collected by SupportAssist



SupportAssist continually monitors the configuration data and usage information of managed Dell hardware and software. While Dell does not anticipate accessing or collecting personal information, such as your personal files, web-browsing history, or cookies in connection with this program, any personal data inadvertently collected or viewed will be treated in accordance with the Dell Privacy Policy available for review at [Dell.com/privacy](https://www.dell.com/privacy).

The information encrypted in the data log sent to Dell includes 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.
- **Network identity information** – Computer name, domain name, and IP address.
- **Event data** – Windows event logs, core dump, and debug logs.

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

By default, SupportAssist collects data from all monitored devices, irrespective of the service contract type of the devices, and sends the data securely to Dell. The collection of data is staggered, and the data is collected from 5 devices at a time. For information about the default frequency of data collection, see [Default schedule for collection of system information](#).

-  **NOTE:** If the security policy of your company restricts sending some of the collected data outside of your company network, you can configure SupportAssist to filter the data that is collected from monitored devices. For information about filtering the data that is collected, see [Filtering the collection of system information](#).
-  **NOTE:** For more information about the data collected by SupportAssist and how the collected data is used by Dell, see the *Dell SupportAssist: Security Considerations* technical document at [Dell.com/SupportAssistGroup](https://Dell.com/SupportAssistGroup).

## Event storm handling

SupportAssist intelligently handles event storm conditions, allowing up to nine separate alerts from a monitored device in a 60-minute time span. However, if it receives 10 or more separate alerts, SupportAssist automatically places the device in maintenance mode. Maintenance mode suspends 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 automatically removes the device from maintenance mode and resumes normal alert processing. For more information on maintenance mode, see [Understanding maintenance mode](#).

# Getting started with SupportAssist

SupportAssist provides automated support capabilities for Dell PowerEdge servers running Microsoft Windows or Linux operating systems. You can use SupportAssist to monitor one or more servers.

This chapter provides the information required to get started with monitoring devices using SupportAssist.

## Basic setup

The basic setup enables SupportAssist to monitor the device on which it is installed. If you only have a single device that you want to monitor, you must complete the basic setup, which includes the installation and registration of SupportAssist.

To complete the basic setup:

1. Download the SupportAssist installation package. See [Downloading the SupportAssist installation package](#).
2. Review the minimum requirements for installing SupportAssist. See [Minimum requirements for installing SupportAssist](#).
3. Install SupportAssist. See [Installing SupportAssist](#).
4. Complete the steps in the SupportAssist setup wizard. See [Setting up SupportAssist](#).
5. (Optional) Update the contact information to include a secondary SupportAssist contact. See [Viewing and updating the contact information](#).

## Advanced setup

The advanced setup enables SupportAssist to monitor multiple devices, and includes adding each device you want to monitor in SupportAssist.

To complete the advanced setup:

1. Ensure that you have completed the steps listed in the "Basic setup" section.
2. Add each server you want to monitor in SupportAssist. See [Adding devices for monitoring](#).
3. (Optional) If your company utilizes an SMTP server (email server), configure the SMTP server settings in SupportAssist. See [Configuring the SMTP server settings](#).

## Trying out SupportAssist

If you have concerns about the security and data collected by SupportAssist, you can disable certain configuration options and try out SupportAssist. By default, SupportAssist automatically collects system information from monitored devices at periodic intervals, and also when a support case is created. The collected system information is then sent securely to Dell. For information about the data collected by SupportAssist from monitored devices, see [Data collected by SupportAssist](#).

You can also view the data that is collected by SupportAssist. For information about viewing the collected data, see [Accessing and viewing the collected system information](#).

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

- You can prevent the collection of certain personally identifiable information (PII) from the monitored devices. See [Filtering the collection of system information](#).
- You can disable the periodic collection of system information from all monitored devices. See [Enabling or disabling the periodic collection of system information from all devices](#).
- You can disable the periodic collection of system information for specific devices. See [Disabling the periodic collection of system information from specific devices](#).
- You can disable the automatic collection of system information when a support case is created. See [Enabling or disabling the automatic collection of system information](#).

In most cases, part or all of the data collected by SupportAssist is required to properly diagnose issues and provide an appropriate solution. To receive the full benefits of SupportAssist, you must enable all the data collection options.

## Downloading the SupportAssist installation package



1. Visit [Dell.com/SupportAssistGroup](https://Dell.com/SupportAssistGroup).  
The SupportAssist community page is displayed.
2. In the **SupportAssist for Enterprise** section, click the **Download** link for **PowerEdge - for managing up to 20 servers**.  
The Dell **Driver Details** page is displayed.
3. In the **Available formats** section, click the **Download** link that is displayed under **File Format: Application**.

## Minimum requirements for installing SupportAssist




You can install SupportAssist on a Dell PowerEdge server that meets the minimum requirements specified in the following sections.

### Hardware requirements


Hardware	Requirement
Type	Dell PowerEdge server (9th to 13th generation)
Processor	2 cores (2 GHz)
Memory (RAM)	4 GB
Hard drive	8 GB free space on the C:\ drive or on the primary partition where SupportAssist is installed.

Hardware	Requirement
 <b>NOTE:</b> If SupportAssist is configured to collect the system information at regular intervals, additional hard-drive space is required. The hard-drive space required may be determined as 10 MB x number of monitored devices.	 <b>NOTE:</b> The hard-drive space required may vary based on the number of monitored devices.

## Software requirements

- Operating system — The server on which you want to install SupportAssist must be running one of the following operating systems.
  -  **NOTE:** SupportAssist can be installed only on 64-bit operating systems.
  -  **NOTE:** SupportAssist can also be installed on a domain controller.
    - Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise, and Datacenter
    - Windows Server 2008 SP2 Standard, Enterprise, and Datacenter
    - Windows Server 2012 R2 Standard and Datacenter
    - Windows Server 2012 Standard, Essentials, and Datacenter
    - Small Business Server 2008 Essentials and Standard
    - Small Business Server 2011 Essentials and Standard
- Web browser — To view the SupportAssist user interface, one of the following web browsers is required.
  -  **NOTE:** Transport Layer Security (TLS) version 1.0 or later must be enabled on the web browser.
    - Internet Explorer 8, 9, 10, or 11
    - Mozilla Firefox 22 or 23

## Network requirements

- Internet connection — standard Gbe network.
- The server on which SupportAssist is installed must be able to communicate with the SupportAssist server hosted by Dell over the HTTPS protocol.
- The server on which SupportAssist is installed must be able to connect to the following destinations:
  - <https://api.dell.com/support/case/v2/WebCase> — end point for the SupportAssist server.
  - <https://ddldropbox.us.dell.com/upload.ashx/> — the file upload server where the collected system information is uploaded.
  - <https://ftp.dell.com/> — for getting new SupportAssist release information.
  - <https://downloads.dell.com/> — for downloading Dell OpenManage Server Administrator (OMSA).
  -  **NOTE:** To verify if the destinations are reachable, follow the instructions in [Ensuring successful communication between the SupportAssist application and the SupportAssist server.](#)

The following table lists the ports that must be open on the server on which SupportAssist is installed.

Port	Usage
2607	For opening SupportAssist securely (HTTPS) from a remote system.
9090	For opening SupportAssist from the system on which SupportAssist is installed.
162	For receiving alerts (SNMP traps) from monitored devices.
27015	For receiving forwarded alerts.
443	For Secure Socket Layer (SSL) communication and for verifying SupportAssist update information.

## Installing SupportAssist

Installing SupportAssist enables monitoring of Dell PowerEdge servers, and automates support case creation when issues arise on the monitored servers.

### Prerequisites

- Ensure that you have downloaded the SupportAssist installation package. See [Downloading the SupportAssist installation package](#).
- Ensure that the system meets the minimum requirements for installing SupportAssist. See [Minimum requirements for installing SupportAssist](#).

### Steps

1. Right-click the SupportAssist 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 on to system as an Administrator, double-click the installer package to install SupportAssist. However, make sure 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 Dell SupportAssist Installer** page is displayed.

2. Click **Next**.

The **License Agreement** page is displayed.



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

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

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

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

The **SupportAssist Login** page opens in a web browser window.



**NOTE:** If the system is a member of a 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.

6. Type the Microsoft Windows operating system user name and password, and then click **Log In**.

The **Dell SupportAssist Setup Wizard** is displayed.

### Next steps

Follow the instructions in the **Dell SupportAssist Setup Wizard** to complete the registration of SupportAssist.


## Setting up SupportAssist


### Prerequisites

- If the system on which you have installed SupportAssist 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.

### About this task

The **Dell SupportAssist Setup Wizard** guides you through configuring the proxy server settings (if applicable) and completing the registration. The setup wizard is displayed when you log on to SupportAssist for the first-time.

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

 **NOTE:** It is mandatory to complete all applicable steps displayed on the setup wizard before you can use SupportAssist. If you do not complete all applicable steps in the setup wizard, whenever you log on to SupportAssist, the **SupportAssist Setup Incomplete** page is displayed. On this page, you can click **Setup** to open the setup wizard and complete the applicable steps.

### Steps

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

SupportAssist verifies connectivity to the Internet.

- If SupportAssist is able to connect to the Internet, the **Registration** page is displayed.
- If SupportAssist 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 proxy server IP address or host name.
  - b. In the **Port** field, type the proxy server port number.
  - c. If a user name and password is required to connect to the proxy server, select **Requires authentication**.
  - d. Type the user name and password in the appropriate fields.
  - e. Click **Next**.

SupportAssist 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:
  - **Company Name** — The company name must contain one or more printable characters, and must not exceed 256 characters.

- **Country/Territory** — Select your country or territory.
- **First Name** — The first name can contain letters, quotation marks [ ' ], periods [ . ], spaces, and must not exceed 50 characters.
- **Last Name** — The last name can contain letters, quotation marks [ ' ], periods [ . ], spaces, and must not exceed 50 characters.
- **Phone Number** — The phone number must contain a minimum of 10 characters and must not exceed 50 characters. The phone number can be provided in the international format, including special characters such as ( , ) , + , and –.
- **Alternate Phone Number** — Optional, with the same requirements as the **Phone Number**.
- **Email Address** — Provide the email address in the name@company.com format. It must contain a minimum of five characters and not exceed 50 characters.

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

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




4. Click **Next**.

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


5. Click **Finish**.


The SupportAssist **Cases** page is displayed.

SupportAssist performs the following tasks automatically in the background:

- A SupportAssist component required for collecting system information from devices to be monitored is downloaded and installed on the host server. If the component is already installed on the server, it may be migrated to a version that is compatible with SupportAssist.
- SupportAssist verifies if Dell OpenManage Server Administrator (OMSA) is installed on the host server:
  - If OMSA is either not installed or requires an upgrade, the recommended version of OMSA is downloaded and installed automatically. The host server is listed on the **Device Inventory** page with an  **Installing OMSA** status. After the installation of OMSA is completed, the status changes to  **OK**.
  - If the recommended version of OMSA is already installed, the host server is listed on the **Device Inventory** page with an  **OK** status.

 **CAUTION:** Without OMSA, SupportAssist will not be able to monitor the host server.

 **NOTE:** The SupportAssist recommended version of OMSA may vary based on the generation of the PowerEdge server and the operating system running on the server. For information on the recommended versions of OMSA, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

 **NOTE:** If an issue occurs during the installation of OMSA, an appropriate status is displayed on the **Device Inventory** page. To try installing OMSA again, you can use the **Install/Upgrade OMSA** option available in SupportAssist. See [Installing or upgrading OMSA](#).

#### Next steps

- Add the devices that you want to monitor in SupportAssist. For more information, see [Adding devices for monitoring](#).
- (Optional) If your company utilizes an SMTP server (email server), configure the SMTP server settings in SupportAssist. This enables SupportAssist to utilize the SMTP server to send you device status and connectivity status email notifications. For more information, see [Configuring the SMTP server settings](#).
- (Optional) Update the contact details of the primary and secondary SupportAssist contacts. See [Viewing and updating the contact information](#).

## Upgrading SupportAssist


You can upgrade from SupportAssist version 1.0 to version 1.0.1.

#### Prerequisites

Ensure that you have downloaded the latest version of SupportAssist. See [Downloading the SupportAssist installation package](#).

#### Steps

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

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

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

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

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

3. Click **Upgrade**.

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

4. Click **Finish**.

The **SupportAssist Login** page opens in a web browser window.

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

The SupportAssist **Cases** page is displayed.


## Opening the SupportAssist user interface

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

- On the server on which SupportAssist is installed:


- Double-click the Dell SupportAssist desktop icon.
- If the server is running Windows Server 2008 or Windows Small Business Server 2011 — Click **Start**→ **All Programs**→ **Dell**→ **SupportAssist**→ **SupportAssist**.
- If the server is running Windows Server 2012 — Move the mouse pointer to the bottom-left corner, and then click the **Start** icon. On the **Start** screen, click the **SupportAssist** tile.
- Open a web browser and type the address in the following format: `http://localhost:9090/SupportAssist/resx/login.jsp`.
- On a remote system, open a web browser and type the address in the following format: `https://<IP address or host name of server on which SupportAssist is installed>:2607/SupportAssist/resx/login.jsp`. For example, `https://10.25.35.1:2607/SupportAssist/resx/login.jsp`.
  - If you are using Internet Explorer, the following message is displayed: **There is a problem with this website's security certificate**. To open SupportAssist, click **Continue to this website (not recommended)**.
  - If you are using Mozilla Firefox, the following message is displayed: **This Connection is Untrusted**. To open SupportAssist, click **I Understand the Risks**, and then click **Add Exception**. In the **Add Security Exception** window, click **Confirm Security Exception**.


The SupportAssist **Login** window is displayed on the web browser.

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

## Logging on to SupportAssist


1. On the SupportAssist **Login** window, type the user name and password in the appropriate fields.

 **NOTE:** You must provide the user name and password of a user account that is a member of either the **SupportAssistAdmins** or **SupportAssistUsers** user group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

 **NOTE:** If the system on which SupportAssist is installed is a member of a 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 **Log In**.

The SupportAssist **Cases** page is displayed.

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


## Logging out of SupportAssist

1. Move the mouse pointer over the currently logged in **user name** displayed at the top-right of the SupportAssist header area.  
The **Connectivity Test** and **Logout** options are displayed.
2. Click **Logout**.


## Adding devices for monitoring

To enable SupportAssist to monitor devices and automatically create a support case if an issue occurs, you must add the devices in SupportAssist. SupportAssist can monitor a device through one of the following methods:

- **Agent-based monitoring** — In this method, an agent acts as an interface between the device and SupportAssist. 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 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 on which it is installed. Whenever a hardware event occurs on the device, the OMSA agent generates an alert. SupportAssist 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 device \(agent-based monitoring\)](#).

 **NOTE:** Without OMSA, SupportAssist will not be able to monitor a device through the agent-based monitoring method.

- **Agentless monitoring** — In this method, the Integrated Dell Remote Access Controller (iDRAC) available on the device acts as an interface between the device and SupportAssist. Whenever a hardware event occurs on the device, the iDRAC generates an alert. SupportAssist processes the alert to determine if the alert qualifies for creating a support case. For instructions to add device for agentless monitoring, see [Adding a device \(agentless monitoring\)](#).

 **NOTE:** Agentless monitoring is supported only for Dell's 12th and 13th generation of PowerEdge servers.

Even though Dell's 12th and 13th generation of PowerEdge servers can be monitored through the agentless (iDRAC) method, agent-based (OMSA) method has the following benefits:

- Alert generation capabilities of OMSA and iDRAC are not the same. In Dell's 13th generation of PowerEdge servers, the alert generation capabilities of OMSA and iDRAC are almost similar. However, alerts from chipset and software RAID are available only through OMSA.
- For devices with a ProSupport Plus service contract, Dell's recommendations for operating system and software component versions are available only if the device is monitored through OMSA.
- OMSA is the only option available for monitoring Dell's 9th to 11th generation of PowerEdge servers.

## Adding a device (agent-based monitoring)

### Prerequisites

- Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** user group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).
- Ensure that the device is reachable from the server on which SupportAssist is installed.
- Ensure that you have the host name or IP address, user name, and password of the device.
- 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).
- Port 1311 must be open on the device for OMSA communication.
- Review the requirements for installing OMSA on the device. For more information, see the “Installation Requirements” section in the *Dell OpenManage Server Administrator Installation Guide* at [Dell.com/OpenManageManuals](http://Dell.com/OpenManageManuals).

#### About this task

Adding a device enables SupportAssist to receive alerts and collect system information from the device. To discover and add a device for agent-based monitoring, SupportAssist requires you to provide the details of the device. While discovering and adding the device, you are prompted to allow SupportAssist to perform the following tasks that are required for monitoring the device:

- Install or upgrade OMSA – OMSA is required to generate alerts for hardware events that occur on the device.
- Configure SNMP – Configuration of SNMP settings is required to forward alerts from the device to SupportAssist.

#### Steps

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

The **Device Inventory** page is displayed.

**2. Click **Add**.**

The **Add Device** window is displayed.

**3. Type the host name or IP address of the device, display name (optional), user name, and password in the appropriate fields.**



**NOTE:** It is recommended that you provide the host name of the device. If the host name is not available, you may provide the IP address of the device.



**NOTE:** SupportAssist requires the user name and password to log on to the device and run a component that collects the device information and uploads it to Dell. Therefore, the user name and password you provide must have:

- Local administrator or domain administrator rights and WMI access on the device (if the device is running a Windows operating system)
- Root, super user, or sudo user rights (if the device is running a Linux operating system). If you are providing the user name and password of a sudo user, ensure that the user is added to the root group. To add the user to the root group, include the following in the sudoers file:

```
%root ALL=(ALL) NOPASSWD: ALL — To provide permission to all users in the root group
<User> ALL=(ALL) NOPASSWD: ALL — To provide permission only to a specific user
```





**NOTE:** If the system 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


**4. Click **Add**.**


The **Add Device** window is displayed, prompting you to allow SupportAssist to configure SNMP and install/upgrade OMSA on the device (if applicable).

 **NOTE:** By default, the **Configure SNMP** option is selected on the **Add Device** window. If SupportAssist has detected that OMSA is either not installed or requires an upgrade, the **Install/Upgrade OMSA** option is selected on the **Add Device** window.

 **NOTE:** The **Install/Upgrade OMSA** option is disabled on the **Add Device** window in the following scenarios:



- SupportAssist has detected that OMSA is installed on the device, but is unable to identify the version of OMSA.
- SupportAssist has detected that the recommended version of OMSA is already installed on the device.

 **NOTE:** Configuring SNMP sets the alert destination of a device, and ensures that alerts from the device are forwarded to the server running SupportAssist. The alert destination of the device is set to the IP address of the server running SupportAssist.



 **CAUTION:** Without OMSA and SNMP configuration, SupportAssist will not be able to identify hardware issues that may occur on the device.

5. Click **OK**.

The device is listed on the **Device Inventory** page with an appropriate status:

- While SupportAssist configures the SNMP settings, the device displays a  **Configuring SNMP** status.
- While SupportAssist installs or upgrades OMSA, the device displays an  **Installing OMSA** status.

After the installation of OMSA and configuration of SNMP are completed, the device status changes

to  **OK**. If the device displays an  error status, you click the error link to see a description of the issue and the possible resolution steps.

 **NOTE:** If an issue occurs during the SNMP configuration or OMSA installation, the device displays an appropriate status on the **Device Inventory** page. To retry the OMSA installation or SNMP configuration, you can use the **More Tasks** list available on the **Device Inventory** page.

#### Related References

[Add Device](#)

## Configuring the alert (SNMP trap) destination

Configuring the alert destination of a device ensures that SupportAssist receives alerts from the device. By default, when you add a device, SupportAssist allows you to automatically configure the alert destination of the device. If the automatic SNMP configuration is unsuccessful, you can configure the SNMP settings of a device using the following methods:

- Running a script file — The SupportAssist 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 monitored device.
- Manually configure the SNMP settings — You can configure settings by accessing the SNMP trap service.

The following sections provide information required to configure the alert destination of a device.

### Related Tasks

[Configuring the alert destination using the script file \(Windows\)](#)

[Manually configuring the alert destination \(Windows\)](#)

[Configuring the alert destination using the script file \(Linux\)](#)

[Manually configuring the alert destination \(Linux\)](#)

## Configuring the alert destination using the script file (Windows)

### Prerequisites

- Microsoft Windows PowerShell version 1.0 or later must be installed on the device.



**NOTE:** The script file is supported only on Windows PowerShell. It is not supported on Windows PowerShell (x86), Windows PowerShell ISE, or Windows PowerShell ISE (x86).

- Ensure that you have Administrator rights on the device to run the PowerShell script file.
- Ensure that you have write permissions on the **C:\** drive of the device.
- If the device is running Windows 2003, ensure that the SNMP service is installed. On all other supported operating systems, the script file installs the SNMP service if it is not installed already.

The script file is supported only on devices running the following operating systems:

- Windows Server 2003
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2008 SP2 (64-bit)
- Windows Server 2008 SP2 (32-bit)
- Windows Small Business Server 2011
- Windows Server 2012
- Windows Server 2012 R2

### Steps

1. On the server where SupportAssist is installed, browse to the **C:\Program Files (x86)\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 based 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 on which SupportAssist 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 Concepts

[Configuring the alert \(SNMP trap\) destination](#)

## Manually configuring the alert destination (Windows)

You can perform the following steps to manually configure the alert destination of a monitored device 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** dialog box 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. Under **Trap destinations**, click **Add**. The **SNMP Service Configuration** dialog box is displayed.
  - c. In the **Host name, IP or IPX address** field, type the host name or IP address of the server on which SupportAssist is installed, and click **Add**.
5. Click **Apply**.
6. In the **Services** window, right-click **SNMP Service** and click **Restart**.

### Related Concepts

[Configuring the alert \(SNMP trap\) destination](#)

## Configuring the alert destination using the script file (Linux)

### Prerequisites

- Ensure that Net-SNMP is installed on the device. For information on downloading and installing Net-SNMP, visit [net-snmp.org](http://net-snmp.org).
- 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 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 7.0 (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)

## Steps

1. On the server on which SupportAssist is installed, browse to the **C:\Program Files (x86)\Dell\SupportAssist\scripts** folder.
2. Copy the script file (**LinuxSNMPConfig.sh**) located in the folder and paste the file at a desired location (for example, **\root**) on the device.
3. Open the terminal and log in as a user with root privileges.
4. Run the script file on the device using the following syntax: `sh LinuxSNMPConfig.sh -d <IP address of the server on which SupportAssist is installed>`. For example, `sh LinuxSNMPConfig.sh -d 10.10.10.10`.

## Related Concepts

[Configuring the alert \(SNMP trap\) destination](#)

## Manually configuring the alert destination (Linux)

You can perform the following steps to manually configure the alert destination of a monitored device 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 on which SupportAssist is installed> <community string>` For example, `trapsink 10.94.174.190 public`.
6. Restart the SNMP services (`service snmpd restart`).

## Related Concepts

[Configuring the alert \(SNMP trap\) destination](#)

# Adding a device (agentless monitoring)

## Prerequisites

- Ensure that you are logged on as a member of the **SupportAssistAdmins** user group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).
- Ensure that the device is a 12th or 13th generation Dell PowerEdge server. For information about identifying the generation of a PowerEdge server, see [Identifying the generation of a PowerEdge server](#).
- Ensure that the device is reachable from the server on which SupportAssist is installed.
- Ensure that you have the IP address, user name, and password of the iDRAC.
- Ensure that an Enterprise or Express license is 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/ESMmanuals](http://Dell.com/ESMmanuals).

## About this task

Adding a device enables SupportAssist to receive alerts and collect system information from the device. To add a device for agentless monitoring, SupportAssist requires you to provide the details of the iDRAC available on the device.

## Steps

1. Click **Devices**.

The **Device Inventory** page is displayed.

2. Click **Add**.

The **Add Device** window is displayed.

3. Type the iDRAC IP address, display name (optional), user name, and password in the appropriate fields.



**NOTE:** SupportAssist requires the user name and password to log on to the iDRAC and run a component that collects the system information from the device and sends it securely to Dell. Therefore, the user name and password you provide must have Administrator, Operator, or Read Only rights on the iDRAC.

4. Click **Add**.

The **Add Device** window is displayed, prompting you to allow SupportAssist to configure the SNMP settings of the iDRAC.






**NOTE:** By default, the **Configure SNMP** option is selected on the **Add Device** window. The **Install/Upgrade OMSA** option is disabled because OMSA is not required for monitoring through the agentless method.



**NOTE:** Configuring SNMP sets the alert destination of a device, and ensures that alerts from the device are forwarded to the server running SupportAssist. The alert destination of the device is set to the IP address of the server running SupportAssist.

5. Click **OK**.

The device is listed on the **Device Inventory** page with a  **Configuring SNMP** status. After configuring the SNMP settings, SupportAssist automatically verifies if the iDRAC can forward alerts successfully. If the verification of the SNMP configuration is successful, the status changes to 

**OK.** If the device displays an  error status, you click the error link to see a description of the issue and the possible resolution steps.

## Next steps

If you provided the Read Only credentials for adding the device or if SupportAssist is unable to configure the iDRAC to forward alerts (SNMP traps), you must manually configure the iDRAC to forward alerts to the server on which SupportAssist is installed.


## Related References

[Add Device](#)


## Manually configuring the alert destination of an iDRAC using the web interface

You can perform the following steps to manually configure the alert destination of an iDRAC.

1. Log on 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 under 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 on which SupportAssist is installed.
  9. Type the iDRAC SNMP community string (for example, public) and the SNMP alert port number (for example, 162) in the appropriate fields.  
For more information about the options, see the *iDRAC Online Help*.  
 **NOTE:** The community string value indicates the community string to use 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**.

The iDRAC is now configured to forward alerts to the server running SupportAssist.

-  **NOTE:** For information on configuring alert destination of an iDRAC using other methods, see the “Configuring IP Alert Destinations” section in the *iDRAC User’s Guide* at [Dell.com/ESMmanuals](http://Dell.com/ESMmanuals).


## Viewing cases and devices

The SupportAssist user interface displays the automatically created cases and the devices you have added for monitoring. You can filter and sort the displayed data based on your preferences.


### Viewing the cases

To view the cases, click the **Cases** tab on the SupportAssist user interface. A progress indicator may appear at the bottom of the report to indicate that SupportAssist is in the process of updating the cache of open support cases.

 **NOTE:** By default, the case list is sorted by **Date Opened**, in descending order.

 **NOTE:** Support cases opened prior to SupportAssist installation, and cases opened by contacting Dell Technical Support, are not displayed on the **Cases** page.


Support case information is automatically available, for supported devices with valid Service Tags when SupportAssist connects to the Dell support case and service contract databases over the Internet. The 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.

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

### Viewing the device inventory

To view the device inventory, click the **Devices** tab on the SupportAssist user interface.

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

 **NOTE:** By default, the device inventory is sorted by **Device Name**, in ascending order.

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

## Filtering the displayed data

You can filter the data displayed on the **Device Inventory** and **Cases** pages based on your preferences.


1. Click the filter icon  displayed in the column header.
2. Type or select the filtering criteria.
3. Click **Filter**.

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



## Clearing the data filter

The data filter you applied on the **Cases** and **Device Inventory** pages can be cleared to view all the available data.

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

## Sorting the displayed data

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

## Understanding maintenance mode




The maintenance mode functionality suspends the alert processing and automatic case creation capability of SupportAssist, thereby preventing the creation of unnecessary support cases during an alert storm or a planned maintenance activity. If an alert storm is received from a monitored device, SupportAssist automatically places the device in maintenance mode. You can also manually enable the maintenance mode functionality before a planned maintenance activity to suspend the automatic case creation capability. The following sections provide information required to understand and use 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 displays a yellow **Maintenance Mode** banner at the top of the page. You can enable global-level maintenance mode to prevent the creation of unnecessary support cases during downtime or a routine maintenance activity. For instructions to enable global-level maintenance mode, see [Enabling or disabling global-level maintenance mode](#).

### Device-level maintenance mode

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

- Automated device-level maintenance mode** — By default, if SupportAssist receives 10 or more valid hardware alerts within 60 minutes from a specific device, SupportAssist automatically places that device in maintenance mode. The device remains in maintenance mode for 30 minutes, 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 **Device Inventory** user interface. After 30 minutes, the device is automatically removed from maintenance mode, enabling SupportAssist to resume normal alert processing for the device. If required, you can retain the device in maintenance mode until you resolve the issue, by manually enabling maintenance mode. You can also remove a device from automated maintenance mode before the 30-minute period. For instructions to enable or disable the device-level maintenance mode, see [Enabling or disabling device-level maintenance mode](#).
  -  **NOTE:** The email notification for automated device-level maintenance mode can be received only if the SMTP server (email server) settings are configured in SupportAssist. See [Configuring SMTP server settings](#).
- Manual device-level maintenance mode** — If you have a planned maintenance activity on a device, and do not want SupportAssist 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 **Device Inventory** page. After the maintenance activity is completed, you can remove the device from maintenance mode, enabling SupportAssist to resume processing alerts from the device

normally. For instructions to enable device-level maintenance mode, see [Enabling or disabling device-level maintenance mode](#).

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

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

## Enabling or disabling global-level maintenance mode

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

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **Preferences**.  
The **Preferences** page is displayed.
3. Under **Maintenance Mode**, select or clear the **Temporarily suspend case generation activity (for example, for purposes of downtime, external troubleshooting, etc.)** option to toggle the maintenance mode status.
  - If you select this option, SupportAssist is placed in global-level maintenance mode.
  - If you clear this option, SupportAssist is taken out of global-level maintenance mode.
4. Click **Apply**.  
A yellow banner appears along the top of the SupportAssist user interface displaying **Maintenance Mode**. Once manually placed in global-level maintenance mode, SupportAssist remains in that state unless you clear the option as in step 3.

### Related References

[Preferences](#)

## Enabling or disabling device-level maintenance mode

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

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### Steps

1. Click **Devices**.  
The **Devices Inventory** page is displayed.
2. Select a device in the **Device Inventory** page.
3. Click **More Tasks** and select one of the following:
  - **Enable** — Places the device in maintenance mode.
  - **Disable** — Removes the device from maintenance mode.

If maintenance mode is enabled for a specific device, the maintenance mode icon  is displayed on the **Device Inventory** page. If you disable maintenance mode for a device, the maintenance mode icon is not displayed on the **Device Inventory** page.

## Maintaining SupportAssist capability

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

- Edit the credentials (user name and password) of a monitored device, if the device credentials were changed due to the company security policy or other reasons. See [Editing device credentials](#).
- Install or upgrade dependent components such as Dell OpenManage Server Administrator (OMSA). See [Installing or upgrading OMSA using SupportAssist](#).
- Configure the SNMP settings of a device. See [Configuring SNMP settings using SupportAssist](#).
- Update the primary and secondary contact information, if there is a change in the contact details. See [Viewing and updating the contact information](#).
- Update the proxy server settings in SupportAssist, if applicable. See [Configuring proxy server settings](#).
- Update the SMTP server (email server) settings in SupportAssist, if applicable. See [Configuring the SMTP server settings](#).
- Perform the connectivity test to ensure that SupportAssist is able to connect to all dependent network resources. See [Connectivity test](#).
- Upgrade or update SupportAssist. See [Auto update](#).

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

## Editing device credentials

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

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### Steps

1. Click the **Devices** tab.  
The **Device Inventory** page is displayed.
2. Select a device in the **Device Inventory** page.  
The **Edit Credentials** link is enabled.
3. Click **Edit Credentials**.  
The **Edit Credentials** dialog box is displayed with the existing user name and password.
4. Edit the display name, user name, and password as required.
5. Click **Save**.



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

## Installing or upgrading OMSA using SupportAssist

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### About this task

For monitoring a device using the agent-based method, the Dell OpenManage Server Administrator (OMSA) agent must be installed and running on the device. If OMSA is either not installed or requires an upgrade on a device, the **Status** column on the **Device Inventory** page displays an appropriate message. You can use the **Install/Upgrade** option to automatically download and install the recommended version of OMSA on a device.



**NOTE:** The SupportAssist recommended version of OMSA may vary based on the generation of the PowerEdge server and the operating system running on the server. For information on the recommended versions of OMSA, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

### Steps

1. Click **Devices**.  
The **Devices Inventory** page is displayed.
2. Select the device on which you want to install or upgrade OMSA.
3. Click **More Tasks** → **Install/Upgrade OMSA**.  
The **Status** column on the **Device Inventory** page displays the status of the OMSA installation or upgrade.

## Configuring SNMP settings using SupportAssist

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### 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 running SupportAssist. If the SNMP settings of a device is not configured, the status column on the **Device Inventory** page displays an appropriate message. You can use the **Configure SNMP** option to automatically configure the SNMP settings of a device.

### Steps

1. Click **Devices**.  
The **Devices Inventory** page is displayed.
2. Select the device on which you want to configure the SNMP settings.
3. Click **More Tasks** → **Configure SNMP**.  
The **Status** column on the **Device Inventory** page displays the status of the SNMP configuration.

## Viewing and updating the contact information

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

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **Contact Information**.  
The **Contact Information** page is displayed.
3. Select the type of contact:
  - **Primary**
  - **Secondary**
4. Make the required changes to any of the following fields:
  - **First Name** — The first name can contain letters, quotation marks [ ' ], periods [ . ], spaces, and not exceed 50 characters.
  - **Last Name** — The last name can contain letters, quotation marks [ ' ], periods [ . ], spaces, and not exceed 50 characters.
  - **Phone Number** — In 123-456-7890 format, or in 123-456-7890 x 123 format (to include an extension). It must contain a minimum of 10 characters, and not exceed 50 characters.
  - **Alternate Phone Number** — Optional, with the same format and character requirements as the Phone Number.
  - **Email Address** — Provide the e-mail address in the name@company.com format. It must contain a minimum of five characters, and not exceed 50 characters.
  - **Country** — Select the country.
5. Click **Apply**.

## Configuring proxy server settings

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

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).


### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **Proxy Settings**.  
The **Proxy Settings** page is displayed.

3. Select **Use Proxy Settings**.

 **NOTE:** SupportAssist supports Windows NT LAN Manager (NTLM) authentication protocol only.

4. Type the proxy server IP address or name and port number in the appropriate fields.


 **NOTE:** If the user name and password required to connect to the proxy server are not provided, SupportAssist connects to the proxy server as an anonymous user.

5. If a user name and password is required to connect to the proxy server, select **Proxy requires authentication**, and then provide the following information in the corresponding fields:

- **User Name** — The user name must contain one or more printable characters, and not exceed 104 characters.
- **Password** — The user password must contain one or more printable characters, and not exceed 127 characters.

6. Click **Apply**.

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

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

#### Related References


[Proxy settings](#)

## Connectivity test

The **Connectivity Test** page enables you to verify and test SupportAssist connectivity status to the following dependent resources:

- Internet (including the proxy server, if the system on which SupportAssist is installed connects to the Internet through a proxy server)
- The SMTP server (email server) utilized by your company
- Dell File Transfer Protocol (FTP) server
- File upload server hosted by Dell
- SupportAssist server hosted by Dell


By default, SupportAssist automatically tests the connectivity to the dependent resources every day at 11 pm (management server time), and displays the result in the **Connectivity Status** column. If there is an issue with connectivity to a dependent resource, a status e-mail is sent to your primary and secondary SupportAssist contacts.

 **NOTE:** The status email is only sent if you have configured the details of the SMTP server (email server) utilized by your company in SupportAssist. See [Configuring the SMTP server settings](#).

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


### Viewing the connectivity status

Move the mouse pointer over the **user name** link that is displayed beside the **Help** link, and then click **Connectivity Test**.


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

## Performing the connectivity test


1. Move the mouse pointer over the **user name** link that is displayed beside the **Help** link, and then click **Connectivity Test**.  
The **Connectivity Test** page is displayed.
2. Select the tests that you want to perform.
3. Click **Test Connectivity**.

The **Connectivity 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.


## Auto update


 **NOTE:** It is recommended that you enable auto update to ensure that SupportAssist is up-to-date with the latest features and enhancements.

The auto update feature, when enabled, ensures that SupportAssist and the associated collection component are automatically updated, when an update is available. By default, the SupportAssist application checks if any updates are available, every Monday at 11 am (date and time as on the server on which SupportAssist is installed).


- If updates are available and auto update is enabled, the updates are downloaded and automatically installed in the background.
- If updates are available, but auto update is disabled, the **An upgrade to SupportAssist is available** notification window is displayed. You can click **Install** to download and install the latest updates. If you select the **Do not remind me again about the upgrade** check box and click **Cancel**, SupportAssist does not display the  **Update Available** notification until a newer upgrade is available.

For instructions to enable auto update, see [Enabling auto update](#).

The  **Update Available** notification is displayed in the SupportAssist header, if you click **Cancel** in the **An upgrade to SupportAssist is available** notification window or an error occurs during the update process. You can click the **Update Available** notification to download and install the updates at a later time.

 **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 interface.

Information related to the SupportAssist update is logged in the log file located at **C:\Program Files (x86)\Dell\SupportAssist\logs**.

 **NOTE:** If you disable auto update, you must manually download the install the latest updates from [Dell.com/SupportAssistGroup](http://Dell.com/SupportAssistGroup).

## Enabling auto update

Enabling auto update ensures that SupportAssist is automatically updated when an update is available.

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **Preferences**.  
The **Preferences** page is displayed.
3. Under **Auto Update**, select **Enable auto update**.
4. Click **Apply**.

### Related References

[Preferences](#)

## Deleting a device

You can delete a device from SupportAssist, if you do not want to monitor a device or for other reasons. Deleting a device only removes the device from the SupportAssist user interface, it does not affect the functionality of the device.

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).


### Steps

1. Click **Devices**.  
The **Devices Inventory** page is displayed.
2. Select the device that you want to delete.
3. Click **Delete**.  
The **Confirm Device Deletion** dialog box is displayed.
4. Click **Yes**.  
The device is deleted from the **Device Inventory** page.

# Configuring email notifications

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

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

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



## Configuring email notification settings

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

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **Preferences**.  
The **Preferences** page is displayed.
3. To receive email notifications when a new support case is opened, under **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
4. 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.
5. Click **Apply**.

## Related References

[Preferences](#)


# Configuring SMTP server settings

## Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

## About this task

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

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

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

## Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **SMTP Settings**.  
The **SMTP Settings** page is displayed.
3. Select **Enable Email Notifications**.
4. Provide the following information in the corresponding fields:
  - **Host Name/IP address** — The name or the IP address of the email server.
  - **Port**— The port number of the email server.
5. If the SMTP server requires authentication for sending emails, select **Requires authentication**.
6. Provide the following information in the corresponding fields:
  - **User Name** — The user name must contain one or more printable characters, and not exceed 104 characters.
  - **Password** — The user password must contain one or more printable characters, and not exceed 127 characters
7. To send email notifications securely, select **Use SSL**.
8. Click **Apply**.

## Related References

[SMTP settings](#)

# Configuring data collection settings

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

- Disable the automatic collection of system information from monitored a devices when a support case is created or updated. See [Enabling or disabling the automatic collection of system information](#).
- Disable the periodic collection of system information from all monitored device. See [Enabling or disabling the periodic collection of system information from all devices](#).
- Customize the schedule for periodic collection of system information. See [Customizing the schedule for periodic collection of system information](#)
- Disable the periodic collection of system information from specific devices. See [Enabling or disabling the periodic collection of system information from specific devices](#).
- Filter the collection of system information from all monitored devices. See [Filtering the collection of system information](#).


## Enabling or disabling the automatic collection of system information

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).


### About this task

By default, when a support case is created, SupportAssist 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 based on your preferences.

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

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **Preferences**.  
The **Preferences** page is displayed.
3. Under **Support Collection**, select or clear the **Automatically start a log collection when a new support case is generated** option to toggle the automatic collection of system information.
  - If you select this option, the automatic collection of system information is enabled.
  - If you clear this option, the automatic collection of system information is disabled.

 **NOTE:** By default, the **Automatically start a log collection when a new support case is generated** option is selected.

4. Click **Apply**.

#### Related References

[Preferences](#)


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

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### About this task

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

 **NOTE:** Selecting the **Enable system log collection scheduling** option enables the collection and upload of system information at periodic intervals from all monitored device types. If you do not want SupportAssist to collect the system information for a specific device type, you can disable scheduling for that specific device through the **System Logs** tab. For more information, see [Disabling the periodic collection of system information from specific devices](#).

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **Preferences**.  
The **Preferences** page is displayed.
3. Under **Support Collection**, select or clear the **Enable system log collection scheduling** option to toggle the scheduling of collecting system information.
  - If the option is selected, scheduling of collecting system information is enabled.
  - If the option is cleared, scheduling of collecting system information is disabled.

 **NOTE:** By default, the **Enable system log collection scheduling** option is selected.

4. Click **Apply**.

#### Related References

[Preferences](#)

## Customizing the schedule for periodic collection of system information


### Prerequisites

- Make sure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).
- Make sure that the **Enable system log collection scheduling** option is enabled in the **Preferences** page.

### About this task

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

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Select the **Credential Type** from the list.  
The options available are:
  - **Windows**
  - **Linux**
  - **iDRAC**
3. Under **System Log Collection Schedule**, set the **Frequency** to **Weekly** or **Monthly**.  
 **NOTE:** If you want to disable the scheduling of system information for a specific **Device Type** and **Credential Type**, set the **Frequency** to **None**.
4. In the **Specify date and time** fields, select an appropriate schedule. The options available vary based on the selected **Frequency**.
5. Repeat step 2 and step 3 until you have scheduled the periodic collection of system information for all device types.
6. Click **Apply**.

### Related References

[System logs](#)


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

### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

### About this task

By default, SupportAssist collects system information from all monitored devices at periodic intervals and sends it securely to Dell. If required, you can disable the periodically collection of system information from devices of a specific type based on your preferences. For example, you can disable the periodic collection of system information from all servers running the Windows operating system.

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

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Select the **Credential Type** for which you want to disable scheduling.
3. In **System Log Collection Schedule** section, set the **Frequency** to **None**.

4. Click **Apply**.

The following message is displayed in the **System Log Collection Schedule** section: System Log Collection scheduling is turned off for the current Device Type and Credential Type.

## Filtering the collection of system information

### Prerequisites


Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).


### About this task

The system information collected by SupportAssist includes personally identifiable information (PII) such as the complete configuration snapshot of systems, hosts, and network devices which 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 certain data outside of the company network, you can configure SupportAssist to filter such data from being collected and sent to Dell.

The following is the list of network identity information that you can filter 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

 **NOTE:** When the **Send network identification information to Dell** option is cleared, some of the data about your company network is not transmitted to Dell. This may impede Dell technical support from resolving issues that may occur on monitored devices.

 **NOTE:** If your devices are covered under the Dell ProSupport Plus service contract, when the **Send network identification information to Dell** option is disabled, you will not receive some reporting information about your devices.

### Steps

1. Click the **Settings** tab.  
The **System Logs** page is displayed.
2. Click **Preferences**.  
The **Preferences** page is displayed.
3. Under **System Log Collection Details**, clear the **Send network identification information to Dell** option.



**NOTE:** By default, the **Send network identification information to Dell** option is selected.

4. Click **Apply**.

#### **Related References**

[Preferences](#)

## Accessing the collected data and log files

The collected system information and log files are saved in the SupportAssist installation folder on the server on which SupportAssist is installed. You can access and view the collected system information and the log file.


### Accessing and viewing the collected system information

When a support case is created by SupportAssist, system information required to troubleshoot the issue is automatically collected and sent to Dell Technical Support. The collected system information is compressed and stored at **C:\Program Files (x86)\Dell\SupportAssist\reports\Dset** on the server on which SupportAssist is installed.

The file name includes the device's IP address, Dell Service Tag, and the date/time when the file was created. For example:

- **DSET\_Report\_for[ 192.168.1.254\_SvcTag\_AL12G26\_2014-10-07T132648 ].zip**
- **Periodic\_DSET\_Report\_for[ 192.168.1.254\_SvcTag\_AL12G26\_2014-10-07T132648 ].zip**

The report file is encrypted with the password, dell (all lowercase). The report information can then be viewed by opening the dsetreport.hta file using a web browser.

 **NOTE:** You should open the reports only when asked to do so by Dell Technical Support. Your report will not be reviewed unless you have an open support case.

### Accessing and viewing the logs

SupportAssist stores Windows events and log messages in two locations:

- The Windows Event Log
- The installation logs folder (**C:\Program Files (x86)\Dell\SupportAssist\logs**).

A new log is created daily at 11:59 PM as per the time zone configured on the system, and is stored in the logs folder. The **application.log** file contains log information for the current day. At the end of each day, the log file is renamed as **application.log<date format in yyyyymmdd>**. If the log file is older than two days, the log file is zipped automatically. This enables you to identify the exact log file stored for a given date when alerts occur. For example, log files similar to the following can be seen:

- **application.log**
- **application.log.20141126**
- **application.log.20141127.zip**

- **application.log.20141128.zip**

The log files are purged from storage after 30 days.

In the SupportAssist installation folder, you can view one log file per day. The current log file is named **application.log**, and 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 located at **C:\Program Files (x86)\Dell\SupportAssist\config**. A value of ERROR in the **log4j.xml** file results in logs messages of FATAL, and ERROR, since FATAL is a higher level than ERROR.

## Other useful information

This chapter provides additional information that you may require while using SupportAssist.

### Sending the system information manually

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

#### Prerequisites

Ensure that you are logged on to SupportAssist as a member of the **SupportAssistAdmins** group. For information about the SupportAssist user groups, see [SupportAssist user groups](#).

#### Steps

1. Click the **Devices** tab.  
The **Device Inventory** page is displayed.
2. Select a device in the **Device Inventory** page.  
The **Send System Information** link is enabled.
3. Click **Send System Information**.  
The **Status** column on the **Device Inventory** page displays the status of the collection and upload of the system information.

### SupportAssist user groups

SupportAssist maintains security through the following user groups that are created during the installation of SupportAssist:

- **SupportAssistAdmins**
- **SupportAssistUsers**

After the installation of SupportAssist, by default, members of the Microsoft Windows:

- Local Administrators group are added to the **SupportAssistAdmins** group
- Users group are added to the **SupportAssistUsers** group

If SupportAssist is installed on a domain controller, by default, members of the Windows:

- Domain Admins group are added to the **SupportAssistAdmins** group

- Domain Users group are added to the **SupportAssist Users** group

If you have Administrator rights on the system, you can add user accounts to the appropriate SupportAssist user group based on the privileges you want to grant to a user account. The following table provides a comparison of the privileges of the SupportAssist user groups.

Privilege	SupportAssistAdmins	SupportAssistUsers
View cases	✓	✓
View the device inventory	✓	✓
Perform the connectivity tests	✓	✓
Setup SupportAssist and complete registration through the setup wizard	✓	✗
Add devices	✓	✗
Edit device credentials	✓	✗
Delete devices	✓	✗
Install/Upgrade OMSA using the <b>More Tasks</b> option	✓	✗
Configure SNMP using the <b>More Tasks</b> option	✓	✗
Enable or disable global-level maintenance mode	✓	✗
Enable or disable device-level maintenance mode	✓	✗
Send system information manually	✓	✗
View and configure SupportAssist settings	✓	✗
Perform auto update	✓	✗
Uninstall SupportAssist	✓	✗


## Support for automatically installing or upgrading OMSA

To monitor a device through the agent-based method, SupportAssist 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 on which 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 receives the alert from the device and processes the alert to identify if the alert indicates a hardware issue. For more information on OMSA, visit [Delltechcenter.com/OMSA](http://Delltechcenter.com/OMSA).

 **NOTE:** The SupportAssist recommended version of OMSA may vary based on the generation of the PowerEdge server and the operating system running on the server. For information on the recommended versions of OMSA, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).


SupportAssist has the capability to automatically download and install the recommended version of OMSA on monitored devices. By default, when a device is added for agent-based monitoring, SupportAssist verifies if the recommended version of OMSA is installed on the device.


- If OMSA is not installed on the device, SupportAssist prompts for your confirmation to download and install the recommended version of OMSA on the device. On confirmation, SupportAssist downloads and installs OMSA in the background. The OMSA installation status is displayed in the **Status** column on the **Device Inventory** 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 **More Tasks** → **Install/Upgrade OMSA** option on the **Device Inventory** page.


- If OMSA is already installed on the device, SupportAssist verifies if the version of OMSA matches with the recommended OMSA version for SupportAssist. If the existing version of OMSA is not the recommended version, but supports direct upgrade to the recommended version of OMSA, SupportAssist prompts for your confirmation to download and upgrade OMSA on the device. The OMSA upgrade status is displayed in the **Status** column on the **Device Inventory** 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, you can use the **More Tasks** → **Install/Upgrade OMSA** option on the **Device Inventory** page.

 **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 Inventory** page or you can manually download and upgrade to OMSA version 7.4.


 **NOTE:** When you allow or use SupportAssist to install or upgrade OMSA, the downloaded packages of OMSA are retained in the SupportAssist installation folder. If a compatible version of OMSA was already downloaded during an earlier operation, SupportAssist does not download OMSA again. In this scenario, SupportAssist only installs or upgrades OMSA on the device using the already downloaded version of OMSA.


 **NOTE:** The time taken to download OMSA is dependent on the Internet download speed and network bandwidth.

If the recommended version of OMSA is installed and running on the device, the status of the device is displayed as  **OK**.

## Support for automatically configuring SNMP settings

To enable SupportAssist to monitor a device, the device must be configured to forward alerts (SNMP traps) to the server on which SupportAssist 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 running SupportAssist. SupportAssist has the capability to automatically configure the SNMP settings of a device, such that the device forwards alerts to the server on which SupportAssist is installed. By default, when you add a device, SupportAssist prompts for your confirmation to automatically configure the SNMP settings of the device. The status of the SNMP configuration is displayed in the **Status** column on the **Device Inventory** page. While SupportAssist configures the SNMP settings of a device, the device displays

a  **Configuring SNMP** status. You can also use the **More Tasks** → **Configure SNMP** option on the **Device Inventory** page to automatically configure the SNMP settings of a device at any time.

 **NOTE:** When you allow or use SupportAssist to automatically configure the SNMP settings of a device, the alert destination of the device is set to the IP address of the server running SupportAssist.

## Detection of hardware issues in attached storage devices

In addition to monitoring PowerEdge servers, SupportAssist can also process alerts received from Dell PowerVault MD series storage arrays that may be attached to a server. Alert generation from an attached storage device occurs through the Dell OpenManage Storage Services (OMSS) application installed on the server. When you allow SupportAssist 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 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 automatically creates a support case for the associated server.

## Support for Dell OEM servers

Dell OEM-ready devices (either re-branded or de-branded Dell hardware), when added, are classified under the re-branded name and not the original Dell hardware name. All of the functionality available for Dell standard devices, such as alerts handling, automatic case creation (when the support level has been validated at the time of the support incident as ProSupport or ProSupport Plus), and ProSupport Plus reports are available for OEM-ready devices. OEM-ready devices are classified in the SupportAssist user interface and ProSupport Plus reports under the re-branded name.

Automatic case creation is supported through Dell Enterprise Technical Support and not available for other support case service request management systems.

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

## Default schedule for collection of system information



By default, SupportAssist collects system information from monitored devices periodically and also when a support case is created. The following table provides the default schedule for the collection of system information from monitored devices.


Device type	Operating system or component	Schedule
Server	Windows	Monthly; Monday of the first week at 12:00 AM
	Linux	Monthly; Monday of the first week at 12:00 AM
	iDRAC	Monthly; Monday of the first week at 12:00 AM

## Types of email notifications

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

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

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

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

# Ensuring successful communication between the SupportAssist application and the SupportAssist server

The server on which SupportAssist 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 generated system log collection to Dell.


To ensure that the SupportAssist application is able to successfully communicate with the SupportAssist server:

- The server on which the SupportAssist application is installed must be able to connect to the following destinations:
  - **https://api.dell.com/support/case/v2/WebCase** — end point for the SupportAssist server. On the server on which SupportAssist is installed, verify if you can access the following location using the web browser: **https://api.dell.com/support/case/v2/WebCase?wsdl**.
  - **https://ddldropbox.us.dell.com/upload.ashx/** — the file upload server where the diagnostic test results are uploaded.
  - **https://downloads.dell.com/** — for downloading Dell OpenManage Server Administrator (OMSA). On the server on which SupportAssist is installed, verify if you can access the following location using the web browser: **https://downloads.dell.com/**
  - On the server on which SupportAssist is installed, verify if port 443 is open for **ddldropbox.us.dell.com**, **ftp.dell.com**, and **downloads.dell.com**. You can use a telnet client to test the connection. For example, use the following command: `o ddldropbox.us.dell.com 443`
  - **https://ftp.dell.com/** — for getting new SupportAssist release information. On the server on which SupportAssist is installed, verify if you can access the following location using the web browser: **https://ftp.dell.com/**.
- Verify if the server certificate on **ddldropbox.us.dell.com** is valid. For more information, see [Verifying the server certificate](#).
- On the server on which SupportAssist is installed, verify if the network settings are correct.
- If the server on which SupportAssist is installed connects the Internet through a proxy server, configure the proxy settings in SupportAssist. See [Configuring proxy server settings](#).

If the communication problem persists, contact your network administrator for further assistance.

## Verifying the server certificate

You can perform the following steps to verify if the server certificate on **ddldropbox.us.dell.com** is valid.

1. Open **https://ddldropbox.us.dell.com** on a web browser.  
A **404 — File or directory not found** error may be displayed.
2. On the address bar, click the **Security Report** icon , and then click **View Certificates**.  
The **Certificate** is displayed.

3. In the **General** tab, verify if the certificate displays a valid date.
4. Click the **Certification Path** tab, and verify if the **GTE CyberTrust Global** root certificate is listed.

## Verifying the installation of the SupportAssist component

### About this task

SupportAssist utilizes an associated collection component to collect system information from monitored devices. The SupportAssist component is automatically downloaded and installed in the background after the installation of SupportAssist. To successfully collect the system information, the component must be of a version that is compatible with SupportAssist.

### Steps


1. On the server on which SupportAssist is installed, open the **Control Panel**.
2. Click **Programs** → **Programs and Features**.  
The **Uninstall or change a program** window is displayed.
3. In the list of installed applications, verify if Dell System E-Support Tool (DSET) is installed.



**NOTE:** For information on the version of DSET that is compatible with SupportAssist, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

## Accessing the context-sensitive help

The 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 help system.

To access the context-sensitive help, click the  icon that appears in the user interface. The context-sensitive help is displayed in a new browser window.

## Viewing SupportAssist product information

1. Move the mouse pointer over the **Help** link at the top-right corner of the SupportAssist user interface, and then click **About**.  
The **About** window is displayed, where you can view the SupportAssist product version and the registration ID.
2. Click **Close** to return to the SupportAssist user interface.

## Uninstalling SupportAssist

1. Perform one of the following based on the operating system:
  - On Windows Server 2012 — Move the mouse pointer to the bottom-left corner, and then click the **Start** icon. On the **Start** screen, click the **Control Panel** tile. On the **Control Panel**, click **Uninstall a program**.
  - On Windows Server 2008 or Windows Small Business Server 2011 — Click **Start** → **Control Panel** → **Programs and Features**.


- The **Uninstall or change a program** window is displayed.
2. Select **Dell SupportAssist** and click **Change**.  
The **Welcome to Dell SupportAssist Installer** window is displayed.
  3. Click **Next**.  
The **Dell SupportAssist Maintenance** window is displayed.
  4. Select **Remove**, and click **Next**.  
The **Feedback** window is displayed.
  5. Select an appropriate reason from the **Select an option** drop-down list, provide your comments, and click **Remove**.  
The **Remove the Program** window is displayed.
  6. Click **Remove**.  
The **Uninstallation Completed** window is displayed.
  7. Click **Finish**.  
SupportAssist is now uninstalled.

## 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.

PowerEdge server generation	Representation of the server model	Examples of server models
9th	PowerEdge x9xx	PowerEdge 2900 Power Edge 6950
10th	PowerEdge yx0x	PowerEdge M600 PowerEdge R300 Power Edge T105
11th	PowerEdge yx1x	PowerEdge M610 PowerEdge R310 PowerEdge T110
12th	PowerEdge yx2x	PowerEdge M620 PowerEdge R620 PowerEdge T620
13th	PowerEdge yx3x	PowerEdge M630 PowerEdge R630

PowerEdge server generation	Representation of the server model	Examples of server models
		PowerEdge R730

 **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.

## Known issues

The following are some of the known issues with SupportAssist for Servers.

Issue	Workaround
The status of a device displayed in the <b>Device Inventory</b> page does not change if an error or warning status of a device is resolved manually. For example, if OMSA is not installed on a device, and you log on to the device and manually install the recommended version of OMSA, the status of the device is not updated automatically.	Manually send the system information to Dell — Select the device in the <b>Device Inventory</b> page and click <b>Send System Information</b> . The status of the device is updated automatically.
Pressing the <Enter> key does not start a new line on the comments field that is displayed while uninstalling SupportAssist.	To start a new line, press <Ctrl><Enter>.
If the calendar settings of the server on which SupportAssist is installed is changed to certain non-English formats (for example, Thailand), the <b>Status</b> column in SupportAssist may display an incorrect date.	Reset the calendar settings to use an English format.
After editing the contact information, if you select either <b>Primary</b> or <b>Secondary</b> on the <b>Contact Information</b> page, the changes are not saved.	After editing the contact information, click <b>Apply</b> , and then select <b>Primary</b> or <b>Secondary</b> based on your preference.
On devices running Windows Server 2003 or 2008 x86, if Windows PowerShell is not installed, automatic configuration of SNMP settings through SupportAssist results in an unexpected error.	Ensure that PowerShell is installed on the device, and try configuring the SNMP settings again. If the problem persists, manually configure the SNMP settings of the device.
If auto update of SupportAssist occurs during the collection of system information from a device, after the update is installed: <ul style="list-style-type: none"> <li>The collection of system information from the device is not restarted automatically.</li> <li>The device displays an unexpected error status.</li> </ul>	Manually send the system information to Dell — Select the device in the <b>Device Inventory</b> page and click <b>Send System Information</b> . The status of the device is updated automatically.

# Troubleshooting

The following sections provide information required to troubleshoot issues that may occur while installing and using SupportAssist.

## Installing SupportAssist

If you experience any issues while installing SupportAssist:

- Ensure that you right-click the installer package and select **Run as administrator** to start the installation.
- 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 on which you are installing SupportAssist for Servers does not have any other SupportAssist application installed already.

## SupportAssist registration

If the **SupportAssist Setup Wizard** is unable to complete the registration, an appropriate error message is displayed. If you experience any issues with the registration of SupportAssist:

- Verify if the server on which SupportAssist is installed can connect to the Internet.
- If the server on which SupportAssist is installed connects to the Internet through a proxy server, provide the proxy server details in the SupportAssist setup wizard.
- Verify if the network settings of the server on which SupportAssist is installed are correct.
- Ensure that the registration details such as first name, last name, email address, and phone number you provided are valid.
- Verify if port 443 is open on the firewall to access <https://api.dell.com/support/case/v2/WebCase>.
- Perform the connectivity test and ensure that connectivity to the SupportAssist server is successful. See [Performing the connectivity test](#). If the test is successful, close the web browser, open the SupportAssist user interface again and retry the registration.
- The registration request may have timed out. Retry the registration after some time.

## Opening the SupportAssist user interface

If a `Problem starting the SupportAssistService` error is displayed when you open the SupportAssist user interface:

- Ensure that you are logged with a user account that has the required privileges to start system services.

- Try to restart the **Dell SupportAssist Service**. See [SupportAssist services](#).
- Check the log file, **application.log**, available at **C:\Program Files (x86)\Dell\SupportAssist\logs** to identify the component that failed to load.

## Logging on to SupportAssist

If you experience any issues while logging on to SupportAssist:

- Verify if the user account you are using to log on 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 under the **SupportAssistAdmins** or **SupportAssistUsers** group, add the user account to one of the SupportAssist user groups.
  - If you want to add users to the SupportAssist 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 user groups, and then add users to the groups:
  - To create the SupportAssist 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 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. See [SupportAssist services](#).

## Unable to add device

If an error message is displayed stating that SupportAssist 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 Version 1.0.1 for Services Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

- Verify if the device is reachable from the server on which SupportAssist is installed.
- Verify if the device credentials (user name and password) you provided are correct.
- If you are adding a device by providing the server 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 the “Handling Remote Connections Under UAC” section of the “User Account Control and WMI” knowledge base article at [Microsoft.com](https://Microsoft.com).
- If you are adding a device by providing the server 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 are providing the user name and password of a sudo user, ensure that the user is added to the root group. To add the user to the root group, add the following in the sudoers file:
 

```
%root ALL=(ALL) NOPASSWD: ALL — To provide permission to all users in the root group
<User> ALL=(ALL) NOPASSWD: ALL — To provide permission only to a specific user
```
  - 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 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 “Managing Licenses” section in the *iDRAC User’s Guide* at [Dell.com/ESMmanuals](https://Dell.com/ESMmanuals).

## OMSA not installed

If a device displays an  **OMSA not installed** status:

- Install OMSA on the device using the **Install/Upgrade OMSA** option. See [Installing or upgrading OMSA](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log on to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](https://Dell.com/ServiceabilityTools).

## SNMP not configured

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

- Configure the SNMP settings on the device using the **Configure SNMP** option. See [Configuring SNMP settings](#).
- If the SNMP configuration cannot be completed successfully even after repeated attempts, log on to the device and manually configure SNMP settings. For instructions to manually configure the SNMP settings:
  - Agent-based monitoring: [Configuring the alert \(SNMP trap\) destination](#).
  - Agentless monitoring: [Manually configuring the alert destination of an iDRAC using the web interface](#).


## New version of OMSA available

If a device displays an  **New version of OMSA available** status:

- Install OMSA on the device using the **Install/Upgrade OMSA** option. See [Installing or upgrading OMSA](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log on to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

## Device configuration not supported by OMSA

A  **Device configuration not supported by OMSA** status indicates that SupportAssist cannot receive alerts from the device through the agent-based monitoring method. If the device is a Dell 12th or 13th generation PowerEdge server, you may perform the following:

 **NOTE:** For information on identifying the generation of a PowerEdge server, see [Identifying the generation of a PowerEdge server](#).

1. Delete the device from SupportAssist. See [Deleting a device](#).
2. Add the device by providing the iDRAC details. See [Adding a device \(agentless method\)](#).

## 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 using the Configure SNMP option. See [Configuring SNMP settings](#).

If the SNMP configuration is still unsuccessful you can manually configure the SNMP using the web interface. For instructions to manually configure the SNMP settings:

- Agent-based monitoring: [Configuring the alert \(SNMP trap\) destination](#).
- Agentless monitoring: [Manually configuring the alert destination of an iDRAC 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 using the Configure SNMP option. See [Configuring SNMP settings](#).

## Unable to install OMSA

If an error message is displayed stating that SupportAssist is unable to install OMSA on the device:

- Verify if the device is reachable from the server on which SupportAssist 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 on which SupportAssist is installed and the device.
  - Delete any files available in the **C:\Windows\temp** folder on the server on which SupportAssist 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 have provided the user name and password of a sudo user, ensure that the user is added to the root group. To add the user to the root group, add the following in the sudoers file:

```
%root ALL=(ALL) NOPASSWD: ALL – To provide permission to all users in the root group
<User> ALL=(ALL) NOPASSWD: ALL – To provide permission only to a specific user
```
  - Ensure that the device has all the required OMSA dependencies installed. For more information about OMSA dependencies, see the “Remote Enablement Requirements” section in the *Dell OpenManage Server Administrator Installation Guide* at [DellTechCenter.com/OMSA](http://DellTechCenter.com/OMSA).
- Retry the installation of OMSA. See [Installing or upgrading OMSA](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log on to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).


 **NOTE:** Upgrade from a 32-bit version of OMSA to a 64-bit version of OMSA is not supported. In this case, you must uninstall the existing version of OMSA, and install OMSA through SupportAssist. [Installing or upgrading OMSA](#).

## Unable to verify OMSA version

If an error message is displayed stating that SupportAssist is unable to verify the OMSA version installed on the device:


- Click the error status link in the **Status** column on the **Device Inventory** page to view the possible resolution steps.
- Perform the connectivity test and ensure that connectivity to the Dell FTP server is successful. See [Performing the connectivity test](#).
- Ensure that the OMSA services are running on the device.
- Retry the installation of OMSA. See [Installing or upgrading OMSA](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log on to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

## Unsupported operating system

An  **Unsupported operating system** status indicates that SupportAssist cannot receive alerts from the device through the agent-based monitoring method. If the device is a Dell 12th or 13th generation PowerEdge server, you may perform the following:

1. Click the error status link in the **Status** column on the **Device Inventory** page to view the possible resolution steps.
2. Delete the device from SupportAssist. See [Deleting a device](#).
3. Add the device by providing the iDRAC details. See [Adding a device \(agentless method\)](#).

## Unexpected error occurred

An  **Unexpected error occurred** status may be displayed during either the installation of OMSA or the collection of system information from a device, because of a technical issue.

If the issue occurred during the installation or upgrade of OMSA, you may try the following:


- Verify if the device is reachable from the server on which SupportAssist 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 on which SupportAssist is installed and the device.
  - Delete any files available in the **C:\Windows\temp** folder on the server on which SupportAssist 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 have provided the user name and password of a sudo user, ensure that the user is added to the root group. To add the user to the root group, add the following in the sudoers file:

```
%root ALL=(ALL) NOPASSWD: ALL — To provide permission to all users in the root group
```

```
<User> ALL=(ALL) NOPASSWD: ALL — To provide permission only to a specific user
```

- Ensure that the device has all the required OMSA dependencies installed. For more information about OMSA dependencies, see the “Remote Enablement Requirements” section in the *Dell OpenManage Server Administrator Installation Guide* at [DellTechCenter.com/OMSA](http://DellTechCenter.com/OMSA).
- Retry the installation of OMSA. See [Installing or upgrading OMSA](#).
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log on to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.0.1 for Servers Support Matrix* at [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools).

 **NOTE:** Upgrade from a 32-bit version of OMSA to a 64-bit version of OMSA is not supported. In this case, you must uninstall the existing version of OMSA, and install OMSA through SupportAssist. [Installing or upgrading OMSA](#).

If the issue occurred during the collection of system information from a device, you may try the following:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Verify if the device is reachable from the server on which SupportAssist 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.
- If you have added the device by providing the server 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 you have added the device by providing the server 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 are providing the user name and password of a sudo user, make sure that the user is added to the root group. To add the user to the root group, add the following in the sudoers file:

```
%root ALL=(ALL) NOPASSWD: ALL — To provide permission to all the users in the root group
```

```
<User> ALL=(ALL) NOPASSWD: ALL — To provide permission only to a specific user
```

  - Verify if the SSH service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).
- If you have added the device by providing the iDRAC details (agentless monitoring), ensure that the iDRAC has an Enterprise license installed. For information on purchasing and installing an Enterprise license, see the “Managing Licenses” section in the *iDRAC User’s Guide* at [Dell.com/ESMmanuals](http://Dell.com/ESMmanuals).


After resolving the underlying issue, manually initiate the collection and upload of system information. See [Sending the system information manually](#).

If the **Unexpected error occurred** status persists, contact Dell Technical Support for assistance.


## 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 **Device Inventory** page to view the possible resolution steps.
- Verify if the device is turned on and connected to the network.
- Verify if ports 22, 23, 80, 135, 443, 1311, 2463, and 5989 are open on the device.
- If you added the device in SupportAssist by providing the server IP address, verify if the IP address of the server has changed. The IP address changes each time the server is restarted, if the server is configured to obtain a dynamic IP address.
- If the IP address of the device has changed:
  - Delete the device from SupportAssist. See [Deleting a device](#).
  - Add the device again. See [Adding a device \(agent-based monitoring\)](#).

 **NOTE:** To avoid deleting and adding a device each time the IP address of the device changes, it is recommended that you provide the host name of the device (instead of the IP address) while adding the device.

## Enterprise license required

If a device displays an  **Enterprise license required** status, ensure that the iDRAC on the device has an Enterprise license installed. For information on purchasing and installing an Enterprise license, see the “Managing Licenses” section in the *iDRAC User’s Guide* at [Dell.com/ESMmanuals](http://Dell.com/ESMmanuals).

## Authentication failed

If a device displays an  **Authentication failed** status:

- Click the error status link in the **Status** column on the **Device Inventory** page to view the possible resolution steps.
- Verify if the device credentials (user name and password) you provided are correct. If the credentials have changed, update the credentials of the device. See [Editing device credentials](#).
- If you added the device by providing the server 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 the “Handling Remote Connections Under UAC” section of the “User Account Control and WMI” knowledge base article at [Microsoft.com](http://Microsoft.com).
- If you added the device by providing the server 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 have provided the user name and password of a sudo user, ensure that the user is added to the root group. To add the user to the root group, add the following in the sudoers file:
 

```
%root ALL=(ALL) NOPASSWD: ALL — To provide permission to all the users in the root group
<User> ALL=(ALL) NOPASSWD: ALL — To provide permission only to a specific user
```
- Verify if the SSH service is running on the device.
- Verify if SSH password authentication is enabled (enabled by default).

## 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 on which SupportAssist 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.
- If you have added the device by providing the server 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 you have added the device by providing the server 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 are providing the user name and password of a sudo user, make sure that the user is added to the root group. To add the user to the root group, add the following in the sudoers file:
 


```
%root ALL=(ALL) NOPASSWD: ALL — To provide permission to all the users in the root group
<User> ALL=(ALL) NOPASSWD: ALL — To provide permission only to a specific user
```
  - Verify if the SSH service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).
- If you have added the device by providing the iDRAC details (agentless monitoring), ensure that the iDRAC has an Enterprise license installed. For information on purchasing and installing an Enterprise license, see the “Managing Licenses” section in the *iDRAC User’s Guide* at [Dell.com/ESMmanuals](http://Dell.com/ESMmanuals).

After resolving the underlying issue, manually initiate the collection and upload of system information. See [Sending the system information manually](#).

## Insufficient storage space to gather system information

If a device displays an  **Insufficient storage space to gather system information** status, ensure that the server on which SupportAssist is installed has sufficient free space on the C:\drive. The minimum hard-drive space required for installing and using SupportAssist is 8 GB.

## Unable to reach Dell upload server

If a device displays an  **Unable to reach Dell upload server** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Verify if the server on which SupportAssist is installed is able to connect to the Internet.
- If the server on which SupportAssist is installed connects to the Internet through a proxy server, ensure that the proxy settings are configured in SupportAssist. See [Configuring proxy server settings](#).
- Perform the connectivity test and ensure that connectivity to the Dell upload server is successful. See [Performing the connectivity test](#).

After resolving the underlying issue, manually initiate the collection and upload of system information. See [Sending the system information manually](#).

## Timed out sending system information


If a device displays a  **Timed out sending system information** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Verify if the server on which SupportAssist is installed is able to connect to the Internet.
- If the server on which SupportAssist is installed connects to the Internet through a proxy server, ensure that the proxy settings are configured in SupportAssist. See [Configuring proxy server settings](#).
- Perform the connectivity test and ensure that connectivity to the Dell upload server is successful. See [Performing the connectivity test](#).

After resolving the underlying issue, manually initiate the collection and upload of system information. See [Sending the system information manually](#).

## SupportAssist component is not available

If a device displays the  **SupportAssist component is not available** status:

 **NOTE:** SupportAssist periodically verifies if the required component is installed on the server on which SupportAssist is installed. If the component is not installed, SupportAssist automatically downloads and installs the component.

- Verify if the SupportAssist component is installed on the server on which SupportAssist is installed. See [Verifying the installation of the SupportAssist component](#).
- If the automatic installation of the SupportAssist component is not successful, manually download and install the appropriate version of Dell System E-Support Tool (DSET). You can download DSET from [Dell.com/support/tools](#).


## Maintenance mode

If a device displays the  **Maintenance Mode** status:

- Ensure that the issue with the device is resolved.
- If more time is required to resolve the issue, you may place the device in manual maintenance mode. See [Enabling or disabling device-level maintenance mode](#).
- If required, you may place SupportAssist in maintenance mode. See [Enabling or disabling global-level maintenance mode](#).

## Auto update

If the auto update is unsuccessful:

1. Perform the connectivity test and ensure that connectivity to the Dell FTP server is successful. See [Performing the connectivity test](#).
2. Click the  **Update Available** notification to try installing the update again.

## Unable to edit device credentials


If an error message is displayed stating that SupportAssist is unable to edit the credentials of a device:

- Verify if the device is reachable from the server on which SupportAssist is installed.
- Verify if the device credentials (user name and password) you provided are correct.
- 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 the “Handling Remote Connections Under UAC” section of the “User Account Control and WMI” knowledge base article at [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 are providing the user name and password of a sudo user, ensure that the user is added to the root group. To add the user to the root group, add the following in the sudoers file:

```
%root ALL=(ALL) NOPASSWD: ALL — To provide permission to all users in the root group
<User> ALL=(ALL) NOPASSWD: ALL — To provide permission only to a specific user
```
  - Verify if the Secure Shell (SSH) service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).

## Automatic case creation

If an issue occurs on a device, but a support case is not created automatically:

-  **NOTE:** SupportAssist 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 predefined criteria for support case creation.
- Ensure that the device is configured to forward alerts to the server on which SupportAssist is installed. See [Configuring the SNMP trap destination](#).
  - Restart the **Dell SupportAssist Trap Listener** service on the server on which SupportAssist is installed. See [SupportAssist services](#).
  - Ensure that the **Dell SupportAssist Trap Listener** service is running.
  - Perform the connectivity test and ensure that the connectivity to the SupportAssist server is successful. See [Performing the connectivity test](#).
  - Check the **application.log** file available at **C:\Program Files (x86)\Dell\SupportAssist\logs** to identify if the alert was received successfully by SupportAssist.

## Scheduled tasks

If the time or time zone of the system on which SupportAssist is installed is changed, all built-in and user-defined schedule tasks do not work as expected. Examples of scheduled tasks include the following:

- Periodic collection of system information from monitored devices
- Upload of device inventory information to Dell
- Connectivity test email notifications

To resolve this issue, restart the **Dell SupportAssist Service**.

## SupportAssist services


If the SupportAssist application does not seem to connect to the SupportAssist server or respond appropriately, ensure that the SupportAssist Windows services are running:

1. On the server on which SupportAssist is installed, click **Start** → **Run**.  
The **Run** dialog box is displayed.
2. Type `services.msc`, and then click **OK**.  
The **Services** Microsoft Management Console (MMC) is displayed.
3. Verify if the **Dell SupportAssist Service** and **Dell SupportAssist Trap Listener** display the status as **Running**.
4. If the service is not running, right-click the service and select **Start**.
5. If the service cannot or does not start, open the most recent log file (**application.txt**), and then search for text with a timestamp of when you tried to start the service. The log file may contain a message indicating any user interface startup errors and a possible problem diagnosis.
6. To verify that the SupportAssist application can connect to the SupportAssist server hosted by Dell, perform the connectivity test. See [Performing the connectivity test](#).

- If the server is responding, a success message is displayed in the user interface. If not, the server may be unreachable. If this occurs, check the **application.txt** file available at **C:\Program Files (x86)\Dell\SupportAssist\logs** to find details. If there are no discernible details in the log file, and the server is not reachable, contact Dell Technical Support.
- If communication is successful, but no data updates occur, the SupportAssist application may be identifying itself with an ID that is unknown to the server. If this occurs, check the **application.txt** file available at **C:\Program Files (x86)\Dell\SupportAssist\logs** to find details. The log file may contain a message stating that the SupportAssist application was not recognized. If the SupportAssist application is not recognized by the SupportAssist server, uninstall and reinstall the SupportAssist application.

The **Dell SupportAssist Trap Listener** service is dependent on the Windows **SNMP Trap** service. For receiving alerts from monitored devices, SupportAssist requires the **SNMP Trap** service and **Dell SupportAssist Trap Listener** to be running.

- If the **SNMP Trap** service is stopped, the **Dell SupportAssist Trap Listener** service is also stopped automatically.
- If the **SNMP Trap** service is stopped and you restart the **Dell SupportAssist Trap Listener** service, both the **Dell SupportAssist Trap Listener** service and **SNMP Trap** service are started automatically.

 **NOTE:** Restarting the **SNMP Trap** service does not start the **Dell SupportAssist Trap Listener** service.

## Other services

To add a device and perform other operations on the device, SupportAssist requires the following services to be installed and running on the device:

- WMI service (on devices running a Windows operating system)
- SSH service (on devices running a Linux operating system)

If the services are either not installed or not running, an error message is displayed in SupportAssist. The following sections provide information about verifying the status of the service and restarting the service (if required).

### WMI service

To verify the status of the WMI service and to start the service (if required):

1. Click **Start** → **Run**. The **Run** dialog box is displayed.
2. Type `services.msc`, and then click **OK**. The **Services** Microsoft Management Console (MMC) is displayed.
3. In the list of services, verify the status of the **Windows Management Instrumentation** service. If the service is running, the status is displayed as **Running**.
4. If the service does not display a **Running** status, right-click **Windows Management Instrumentation** → **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 **Send System Information** links remain disabled even after selecting a device in the **Device Inventory**, ensure that you are logged on as a member of **SupportAssistAdmins** group.

## Troubleshooting SSL connection failure

SSL connection failure may occur if the system does not have the required certificate installed from the issuing root certificate authority – GTE CyberTrust Global Root. All Dell certificates are issued from this certificate authority.

### Steps


1. Click **Tools** → **Internet Options**.  
The **Internet Options** dialog box is displayed.
2. Click the **Content** tab, and then click **Certificates**.  
The **Certificates** dialog box is displayed.
3. Click the **Trusted Root Certification Authorities** tab.
4. Scroll to verify if **GTE CyberTrust Global Root** is listed in the **Issued To** and **Issued By** columns.

### Next steps

If **GTE CyberTrust Global Root** is not listed, you must install the required certificates. See [Exporting the root certificate](#) and [Installing the root certificate](#).

## Exporting the root certificate

You can perform the following steps to export the root certificate from **Dell.com**.

1. In Internet Explorer, go to **https://dell.com**.
2. If the **Certificate Error: Navigation Blocked** page is displayed, click **Continue to this website (not recommended)**.
3. At the **Do you want to view only the webpage content that was delivered securely?** prompt, click **Yes**.
4. On the address bar, click the **Security Report** icon .
5. Click **View certificates**.  
The **Certificate** window is displayed.
6. Click **Details**.
7. Click **Copy to File**.  
The **Certificate Export Wizard** is displayed.
8. Click **Next**.
9. In the **Export File Format** page, click **Next**.
10. In the **File to Export** page, click **Browse**.  
The **Save As** window is displayed.
11. Navigate to the location you want to save the certificate file.

12. Type a file name and click **Save**.
13. In the **Export File Format** page, click **Next**.
14. Click **Finish**.  
The status of the export is displayed.
15. Click **OK**.

## Installing the root certificate

You can perform the following steps to install the root certificate on the server on which SupportAssist is installed.

### Prerequisites

- Ensure that you are logged on using the user account with which SupportAssist was installed.
- Ensure that you have administrator privileges.
- Ensure that the SupportAssist service is running.
- Ensure that you have exported the certificate file. See [Exporting the root certificate](#).

### About this task

To resolve SSL connection issues, you must install the following root certificates in the appropriate folders of the current user and local computer.

Certificate Files	Installation Folder
Dell_Inc_Enterprise_Issuing_CA1.cer Dell_Inc_Enterprise_CA.cer	Intermediate Certification Authorities
GTE_CyberTrust Global Root.cer	Trusted Root Certification Authorities

### Steps

1. On the server on which SupportAssist is installed, click **Start** → **Run**.  
The **Run** dialog box is displayed.
2. In the **Open** box, type `mmc`, and click **OK**.  
The **Console 1 – [Console Root]** window is displayed.
3. Click **File** → **Add/Remove Snap-in**.  
The **Add or Remove Snap-ins** dialog box is displayed.
4. Under **Available snap-ins**, select **Certificates**, and click **Add >**.  
The **Certificates snap-in** dialog box is displayed.
5. Ensure that **My user account** is selected, and then click **Finish**.
6. In the **Add or Remove snap-ins** dialog box, click **Add >**.  
The **Certificates snap-in** dialog box is displayed.
7. Select **Computer account** and click **Next**.  
The **Select Computer** dialog box is displayed.
8. Ensure that **Local computer (the computer this console is running on)** is selected, and click **Finish**.
9. In the **Add or Remove snap-ins** dialog box, click **OK**.
10. Under the **Console Root**, click **Certificates – Current User**.
11. Right-click **Trusted Root Certification Authority** → **All Tasks** → **Import**.  
The **Certificate Import Wizard** is displayed.

12. Click **Next**.  
The **File to Import** dialog box is displayed.
13. Browse to select the location of the certificate files, select a certificate file and click **Next**.  
The **Certificate Store** information is displayed.
14. Click **Next**.
15. Click **Finish**.
16. Perform step 11 to step 15 until all three certificate files are imported.
17. Right-click **Intermediate Certification Authorities** → **All Tasks** → **Import**.  
The **Certificate Import Wizard** is displayed.
18. Perform step 12 to step 15 until all three certificate files are imported.
19. Under the **Console Root**, click **Certificates – Local Computer**.
20. Right-click **Trusted Root Certification Authority** → **All Tasks** → **Import**.  
The **Certificate Import Wizard** is displayed.
21. Perform step 12 to step 15 until all three certificate files are imported.
22. Right-click **Intermediate Certification Authorities** → **All Tasks** → **Import**.  
The **Certificate Import Wizard** is displayed.
23. Perform step 12 to step 15 until all three certificate files are imported.

## Error code appendix

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

Error code	Error message	Possible resolution
1000_1 1000_2	An unexpected error has happened while collecting system information from the <device name>.	If the problem persists, contact Dell Technical Support for assistance. For more information about unexpected errors, see <a href="#">Unexpected error occurred</a> .
1000_3	SupportAssist is having a problem communicating with <device name>.	Please verify if the device can be reached from the host where SupportAssist is installed and that port 22, 23, 80, 135, 443, 1311, 2463, and 5989 are open on the device. For information about resolving the issue, see <a href="#">Unable to reach device</a> .
1000_4	SupportAssist is unable to collect system information from <device name> because the iDRAC does not have an Enterprise license.	For information about purchasing and upgrading to an Enterprise license, see the <i>iDRAC User's Guide</i> at <a href="#">Dell.com/ESMmanuals</a> .
1000_5 1000_7 1000_40	SupportAssist was unable to log on to <device name> to collect system information.	Please update the user name and password for this device in SupportAssist and verify the user permissions on the remote device.
1000_6 1000_8 1000_9	SupportAssist is unable to collect system information from <device name>.	Ensure the following: <ul style="list-style-type: none"> <li>• Provide the Administrator credentials for the device in SupportAssist.</li> <li>• iDRAC firmware is updated, if applicable.</li> </ul>
1000_10 1000_11	SupportAssist can no longer communicate with <device name>.	Either the WMI service is having a problem (for Windows device) or the port is no longer accessible from the host where SupportAssist is installed. For more information about this error, see <a href="#">Other services</a> .
1000_12 1000_14 1000_18 1000_19 1000_41 1000_42	An unexpected error has happened while collecting system information from <device name>.	If the problem persists, contact Dell Technical Support for assistance. For more information about this error, see <a href="#">Unexpected error occurred</a> .

Error code	Error message	Possible resolution
1000_13	SupportAssist is unable to collect system information from the <device name>, because the space available on the C:\ drive of the host where SupportAssist is installed has become critically low.	For information about the hard-disk space requirements for a SupportAssist environment, see "Hardware requirements" in <a href="#">Minimum requirements for installing SupportAssist</a> .
1000_20 1000_21 1000_23 1000_24 1000_25 1000_26 1000_28	SupportAssist is unable to send the system information file from <device name>.	<ul style="list-style-type: none"> <li>Perform the Connectivity Test and make sure that the connectivity to the Dell upload server is successful.</li> <li>Select the device and click Send System Information.</li> </ul> <p>If the problem persists, contact Dell technical support for assistance.</p>
1000_22	SupportAssist is unable to send the system information file from <device name> because the system information file size exceeds the predefined upload file size limit.	If the problem persists, contact Dell Technical Support for assistance.
1000_27	The time allowed to send the system information file from <device name> has expired. This is usually caused by a disruption in the connection to the receiving server.	To generate and send the system information manually, select the device and click Send system information. For more information about verifying your Internet connection, see <a href="#">Connectivity Test</a> .
1000_29	SupportAssist is unable to send the system information file from <device name>.	Ensure that the proxy server is reachable. For more information about verifying the proxy server connection, see <a href="#">Connectivity Test</a> .
1000_30	The authentication protocol used to communicate with the proxy server is not supported. SupportAssist supports Basic and NTLM methods. The proxy server is rejecting the authentication attempts.	Please verify if the proxy will allow the methods being used by SupportAssist. For more information about proxy settings, see <a href="#">Configuring proxy server settings</a> .
1000_31	SupportAssist is unable to log on to the proxy server.	Please update the proxy server user name and password in SupportAssist. For more information about verifying the proxy server connection, see <a href="#">Connectivity Test</a> .
3000_1 3000_2 3000_3 3000_4 3000_5	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <device name>.	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Select the device in the <b>Devices Inventory</b>, and then click <b>Actions</b> → <b>Install/Upgrade OMSA</b>.</li> <li>Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell SupportAssist Version 1.0.1 for Servers Support Matrix</i> at <a href="#">Dell.com/ServiceabilityTools</a>.</li> </ul>

Error code	Error message	Possible resolution
		If the problem persists, contact Dell Technical Support for assistance.
3000_6 3000_9 3000_11	A component required for installing Dell OpenManage Server Administrator (OMSA) could not be downloaded.	<ol style="list-style-type: none"> <li>1. Make sure that the system has Internet connectivity.</li> <li>2. Perform the Connectivity Test to make sure that the system has connectivity to the dependent resources.</li> <li>3. Select the device in the <b>Devices Inventory</b>, and then click <b>Actions</b> → <b>Install OMSA</b></li> </ol> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_7	Installation of Dell OpenManage Server Administrator (OMSA) is not supported on the operating system running on <device name>.	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Select the device in the <b>Devices Inventory</b>, and then click <b>Actions</b> → <b>Install OMSA</b>.</li> <li>• Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell SupportAssist Version 1.0.1 for Servers Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_8	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <device name>.	Try to repair the SupportAssist installation from the Control Panel. If the problem persists, contact Dell Technical Support for further assistance.
3000_10 3000_12 3000_13 3000_14	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <device name>.	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Select the device in the <b>Devices Inventory</b>, and then click <b>Actions</b> → <b>Install OMSA</b>.</li> <li>• Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell SupportAssist Version 1.0.1 for Servers Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_15 3000_16 3000_17	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <device name>.	<ul style="list-style-type: none"> <li>• Make sure that the device is reachable and the configured device credentials have Administrator rights, and then do one of the following:</li> </ul>

Error code	Error message	Possible resolution
3000_22 3000_23 3000_29 3000_47 3000_48 3000_50 3000_56 3000_61		<ul style="list-style-type: none"> <li>Select the device in the <b>Devices Inventory</b>, and then click <b>Actions</b> → <b>Install OMSA</b></li> <li>Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell SupportAssist Version 1.0.1 for Servers Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a></li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_18	A service required for the installation of Dell OpenManage Server Administrator (OMSA) is either not running or not enabled on <device name>.	<ul style="list-style-type: none"> <li>If the device is running Microsoft Windows, make sure that the WMI service is running.</li> <li>If the device is running Linux, make sure that SSH is enabled.</li> </ul> <p>For more information, see <a href="#">Other services</a>.</p>
3000_19	A service required for the installation of Dell OpenManage Server Administrator (OMSA) is not running on <device name>.	Make sure that the WMI service is running on the device. For more information, see <a href="#">Other services</a> .
3000_20 3000_21 3000_24 3000_25 3000_26 3000_27 3000_28 3000_30 3000_31 3000_32 3000_33 3000_34 3000_35 3000_36 3000_37 3000_38 3000_39 3000_40 3000_41 3000_42 3000_43 3000_44 3000_45 3000_46 3000_49	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <device name>.	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Select the device in the <b>Devices Inventory</b>, and then click <b>Actions</b> → <b>Install OMSA</b>.</li> <li>Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell SupportAssist Version 1.0.1 for Servers Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>




Error code	Error message	Possible resolution
3000_51 3000_54 3000_55 3000_57 3000_58 3000_59		
3000_52 3000_53	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <device name>.	<p>Make sure that port 22 is open and SSH is enabled on the system, and then do one of the following:</p> <ul style="list-style-type: none"> <li>• Select the device in the <b>Devices Inventory</b>, and then click <b>Actions</b> → <b>Install OMSA</b>.</li> <li>• Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell SupportAssist Version 1.0.1 for Servers Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_60	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on <device name>.	<ul style="list-style-type: none"> <li>• Verify if the device is reachable.</li> <li>• Verify if the configured device credentials have Administrator rights.</li> <li>• Select the device in the <b>Devices Inventory</b>, and then click <b>Actions</b> → <b>Install OMSA</b>.</li> <li>• Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the <i>Dell SupportAssist Version 1.0.1 for Servers Support Matrix</i> at <a href="http://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a>.</li> </ul> <p>If the problem persists, contact Dell Technical Support for assistance.</p>
3000_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 click <b>More Tasks</b> → <b>Install/Upgrade OMSA</b> . If the problem persists, contact Dell Technical Support for assistance.
4000_500	This device has generated an unusual number of alerts exceeding the set threshold limit. SupportAssist has temporarily placed it under maintenance mode. During this period, SupportAssist will not process any alerts from this device.	Ensure the health of this device is restored for optimal SupportAssist operations.

Error code	Error message	Possible resolution
4000_501	SupportAssist component is not available.	If the problem persists, it may require log files to further troubleshoot. Contact Dell Technical Support for assistance.
4000_502	SupportAssist is unable to configure the SNMP settings on this device.	To manually configure the SNMP settings, see <a href="#">Configuring the alert destination of an iDRAC using the web interface</a> .
5000_2	SNMP settings of the device could not be configured because the integrated Dell Remote Access Controller (iDRAC) does not have the required license installed.	Make sure that the iDRAC has an Enterprise or Express license installed, and then try to configure the SNMP settings through the <b>More Tasks</b> → <b>Configure SNMP</b> option.
5000_3	SNMP settings of the device could not be configured because all configurable fields of the integrated Dell Remote Access Controller (iDRAC) are occupied.	You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see <a href="#">Configuring the alert destination of an iDRAC using the web interface</a> .
5000_4	SNMP settings of the device could not be configured because the credentials you have entered do not have the required privileges.	Make sure that the credentials have either Administrator or Operator privileges on the integrated Dell Remote Access Controller (iDRAC), and then try to configure the SNMP settings through the <b>More Tasks</b> → <b>Configure SNMP</b> option.
5000_5	SNMP settings of the device could not be configured because an attempt to connect to the integrated Dell Remote Access Controller (iDRAC) was unsuccessful.	Make sure that the iDRAC is reachable from the system on which SupportAssist is installed, and then try to configure the SNMP settings through the <b>More Tasks</b> → <b>Configure SNMP</b> option.
5000_6	SNMP settings of the device could not be configured because the credentials you have entered are invalid.	Make sure that the credentials are valid, and then try to configure the SNMP settings through the <b>More Tasks</b> → <b>Configure SNMP</b> option. If the problem persists, contact your system administrator for assistance.
5000_7	SNMP settings of the device could not be configured because of an unexpected error.	You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see <a href="#">Configuring the alert destination of an iDRAC using the web interface</a> .
5000_8	SNMP settings of the device could not be configured because of an unexpected error.	You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see <a href="#">Configuring the alert (SNMP trap) destination</a> .


Error code	Error message	Possible resolution
5000_9	SNMP settings of the device could not be configured because the user account does not have the sufficient privileges on the device.	You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see <a href="#">Manually configuring the alert destination (Windows)</a> or <a href="#">Manually configuring the alert destination (Linux)</a> .
5000_10	SNMP settings of the device could not be configured because the hostname/IP address of the system on which SupportAssist is installed was not provided.	If you ran the script file to configure the SNMP settings, make sure that you type the IP address of the system on which SupportAssist is installed as an argument.
5000_11	SNMP settings of the device could not be configured because the SNMP service is not installed on the device.	Manually install the SNMP service on the device, and then try to configure the SNMP settings through the <b>More Tasks</b> → <b>Configure SNMP</b> option.
5000_12	SNMP settings of the device could not be configured because SupportAssist does not support the operating system running on the device.	For information on the operating systems supported by SupportAssist, see the <i>SupportAssist Version 1.0.1 for Servers Support Matrix</i> at <a href="#">Dell.com/ServiceabilityTools</a> .
5000_13	SNMP settings of the device could not be configured because the SNMP service has not started.	Manually start the SNMP service on the device, and then try to configure the SNMP settings through the <b>More Tasks</b> → <b>Configure SNMP</b> option.
5000_14	SNMP settings of the device could not be configured because the WMI service is disabled.	Manually start the WMI service on the device, and then try to configure the SNMP settings through the <b>More Tasks</b> → <b>Configure SNMP</b> option.
5000_15	SupportAssist has configured the SNMP settings successfully, but the automated test to verify the SNMP settings was unsuccessful	To resolve the issue, verify the network settings and make sure that the SNMP port (162) is open.

## Dell SupportAssist user interface

The top-right corner of the SupportAssist user interface displays links that you can use to navigate the interface. The following table describes the links that are displayed.

Link	Description
<b>SupportAssist Community</b>	Opens the SupportAssist community website in a new browser window.
<b>Help</b>	<p>Move the mouse pointer over the link to display a drop-down that provides the following options:</p> <ul style="list-style-type: none"> <li>• <b>Help</b> – Opens the <b>Help</b> window that provides links to Dell technical support and product manuals.</li> <li>• <b>About</b> – Opens the <b>About</b> window that provides information about the SupportAssist version, copyright information, and also notifies if a newer version of SupportAssist is available.</li> </ul>
<b>User name</b>	<p>Displays the user name of the currently logged in user. Move the mouse pointer over the <i>user name</i> link to display a drop-down that contains the following links:</p> <ul style="list-style-type: none"> <li>• <b>Connectivity Test</b> – Opens the connectivity test page.</li> <li>• <b>Logout</b> – Enables you to log out of SupportAssist.</li> </ul> <p> <b>NOTE:</b> The <b>Connectivity Test</b> link is enabled only if you are logged in as a member of the <b>SupportAssistAdmins</b> group.</p>
 <b>Update Available</b>	<p>Displays in the SupportAssist header area in the following situations:</p> <ul style="list-style-type: none"> <li>• If an error occurred during the update of SupportAssist.</li> <li>• If the <b>Settings</b> → <b>Preferences</b> → <b>Enable auto update option</b> is not selected, and you cancel the <b>SupportAssist Update</b> notification that is displayed.</li> </ul> <p>You can click the link to download and install the SupportAssist update.</p> <p> <b>NOTE:</b> The <b>Update Available</b> link is displayed only if you are logged in as a member of the <b>SupportAssistAdmins</b> group.</p>

By default, the **Cases** tab is displayed when SupportAssist is launched. The **Devices** tab displays the supported devices you have added. The **Settings** tab enables you to configure SupportAssist.

 **NOTE:** The **Settings** tab is accessible only if you are logged on as a member of the **SupportAssistAdmins** group.

### Related References

[Setup Wizard](#)

[Login](#)

[Cases](#)

[Device inventory](#)

[Settings](#)  
[Connectivity test](#)

## Setup Wizard

The **Setup Wizard** guides you through the setup and registration of SupportAssist. The fields displayed in the pages of the **Setup Wizard** are described in the following sections.

### Related References

[Welcome](#)  
[Proxy Settings](#)  
[Registration](#)  
[Summary](#)

### Related Tasks


[Setting up SupportAssist](#)

## Welcome

The **Welcome** page enables you to start the SupportAssist setup. Click **Next** to start setting up SupportAssist.

## Proxy Settings

The **Proxy Settings** page enables 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.

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

## Registration

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

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

Field	Description
<b>Company Information</b>	
<b>Company Name</b>	The name of the company.
<b>Country/Territory</b>	The location of the company.
<b>Primary Contact Information</b>	
<b>First Name</b>	The first name of the primary contact.
<b>Last Name</b>	The last name of the primary contact.
<b>Phone Number</b>	The phone number of the primary contact.
<b>Alternate Phone Number</b>	The alternate phone number of the primary contact.
<b>Email Address</b>	The email address of the primary contact. SupportAssist email notifications will be sent to this email address.

## Summary

The **Summary** page enables you to complete the setup. Click **Finish** to open the SupportAssist **Cases** page.

## Login


The following table describes the fields displayed in the **Login** window.

Field	Description
<b>User Name</b>	User name required to log in to SupportAssist.
<b>Password</b>	Password required to log in to SupportAssist.
<b>Log In</b>	Click to log on to SupportAssist.

### Related Tasks

[Logging on to SupportAssist](#)

## Cases

The **Cases** page is the default SupportAssist view. You can use the  **Refresh** link to refresh the case list.

The following table describes the automatically-generated support case information for your supported Dell devices, as displayed in the **Cases** page.

Column	Description
<b>Status</b>	The current state of the support case. The status of a case may be: <ul style="list-style-type: none"> <li>• <b>Open</b> – Dell technical support has opened the submitted case.</li> <li>• <b>In Progress</b> – The case is currently being worked by Dell technical support.</li> <li>• <b>Customer Deferred</b> – Dell technical support has deferred the case at the customer's request.</li> <li>• <b>Submitted</b> – SupportAssist has submitted the case.</li> <li>• <b>No Case</b> – No case exists for this device.</li> <li>• <b>Reopened</b> – The case was previously closed, and has been reopened.</li> </ul>
<b>Number</b>	The numeric identifier assigned to the support case.
<b>Title</b>	The case name, which identifies: <ul style="list-style-type: none"> <li>• Case generation method</li> <li>• Device model</li> <li>• Device operating system</li> <li>• Alert ID, if available</li> <li>• Alert description, if available</li> <li>• Warranty status</li> <li>• Resolution description</li> </ul>
<b>Service Contract</b>	The Dell service contract level under which the device is covered. The service contract column may display: <ul style="list-style-type: none"> <li>• <b>Unknown</b> – SupportAssist cannot determine the service contract.</li> <li>• <b>Invalid Service Tag</b> – The service tag of the device is invalid.</li> <li>• <b>No Service Contract</b> – This device is not covered under a Dell service contract.</li> <li>• <b>Expired Service Contract</b> – The service contract of the device has expired.</li> <li>• <b>Basic Support</b> – This device is covered under a Dell Basic Hardware service contract.</li> <li>• <b>ProSupport</b> – This device is covered under a Dell ProSupport service contract.</li> <li>• <b>ProSupport Plus</b> – This device is covered under a Dell ProSupport Plus service contract.</li> </ul>
<b>Device Type</b>	Indicates the type of device.
<b>Service Tag</b>	A unique, alphanumeric identifier that enables Dell to individually recognize each Dell device.
<b>Date Opened</b>	The date and time when the support case was opened.

#### Related Tasks


[Filtering the displayed data](#)

[Clearing the data filter](#)







[Sorting the displayed data](#)



















## Device inventory






The **Device Inventory** page displays the devices you have added. The following are the options available on the **Devices** tab.

- **Add** — To add a device for monitoring.
- **Edit Credentials** — To edit the user name and password required to log in to a device and collect system information.
- **Delete** — To delete a device from SupportAssist.
- **Send System Information** — To initiate the collection and upload of system information.
- **More Tasks** — To access the following options:
  - **Maintenance** — To enable or disable a device from maintenance.
  - **Dependencies** — To install or upgrade OMSA and to configure SNMP settings.
-  **Refresh** — To refresh the device inventory view.

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

Column	Description
<b>Name</b>	Displays either the display name, host name, or IP address that was provided when adding the device. If the device is placed in maintenance mode, the maintenance mode icon  is also displayed.
<b>Model</b>	Model of the device. For example, PowerEdge M820.
<b>Status</b>	<p>Displays the status of the SupportAssist functionality on the device, and the date and time the status was generated. The status can be categorized as follows:</p> <p><b>Informational status</b></p> <ul style="list-style-type: none"> <li>•  <b>OK</b> — The device is configured correctly for SupportAssist functionality. If the device was added for monitoring through agent-based method (OMSA), you must ensure that the device is configured to forward alerts to the host server.</li> <li>•  <b>Installing OMSA</b> — Installation or upgrade of Dell OpenManage Server Administrator (OMSA) is in progress.</li> <li>•  <b>Configuring SNMP</b> — Configuring the SNMP settings of the device is in progress.</li> <li>•  <b>Installing required components</b> — Installation or upgrade of a required SupportAssist component is in progress.</li> <li>•  <b>Gathering system information</b> — SupportAssist is collecting system information from the device.</li> </ul>

Column	Description
	<ul style="list-style-type: none"> <li data-bbox="486 243 1267 323">•  <b>System information sent</b> – System information has been sent successfully to Dell.</li> </ul> <p data-bbox="486 348 659 373"><b>Warning status</b></p> <ul style="list-style-type: none"> <li data-bbox="486 390 1225 443">•  <b>OMSA not installed</b> – OMSA is not installed on the device.</li> <li data-bbox="486 453 1366 506">•  <b>SNMP not configured</b> – SNMP settings of the device is not configured.</li> <li data-bbox="486 516 1369 596">•  <b>New version of OMSA available</b> – A newer version of OMSA is available for installation on the device.</li> <li data-bbox="486 606 1315 686">•  <b>Device configuration not supported by OMSA</b> – OMSA cannot be installed on the device.</li> </ul> <p data-bbox="486 711 619 737"><b>Error status</b></p> <ul style="list-style-type: none"> <li data-bbox="486 747 1362 793">•  <b>Unable to install OMSA</b> – Installation of OMSA could not be completed.</li> <li data-bbox="486 804 1337 863">•  <b>Unable to configure SNMP</b> – SupportAssist is unable to configure the SNMP trap destination of the device.</li> <li data-bbox="486 873 1362 932">•  <b>Unable to verify SNMP configuration</b> – SupportAssist is unable to verify the SNMP configuration of the iDRAC.</li> <li data-bbox="486 942 1362 1022">•  <b>Unsupported operating system</b> – Installation of OMSA is not supported on the operating system running on the device.</li> <li data-bbox="486 1033 1315 1092">•  <b>Unexpected error occurred</b> – An unexpected error occurred when installing OMSA on the device.</li> <li data-bbox="486 1102 1362 1161">•  <b>Unable to reach device</b> – SupportAssist is unable to communicate with the device.</li> <li data-bbox="486 1171 1362 1268">•  <b>Enterprise license required</b> – SupportAssist cannot collect system information from the device because the iDRAC does not have an Enterprise license installed.</li> <li data-bbox="486 1278 1289 1325">•  <b>Authentication failed</b> – SupportAssist cannot login to the device.</li> <li data-bbox="486 1335 1378 1394">•  <b>Unable to gather system information</b> – SupportAssist is unable to gather system information from the device.</li> <li data-bbox="486 1404 1388 1501">•  <b>Insufficient storage space to gather system information</b> – The system on which SupportAssist is installed does not have sufficient space to gather system information from the device.</li> <li data-bbox="486 1512 1385 1591">•  <b>Timed out sending system information</b> – SupportAssist is unable to send the system information file to Dell because the time limit for uploading the file has expired.</li> <li data-bbox="486 1602 1385 1719">•  <b>Proxy authentication method not supported</b> – SupportAssist is unable to send the system information to Dell because SupportAssist does not support the authentication method of the proxy server. Only Basic and NTLM authentication methods are supported.</li> <li data-bbox="486 1730 1378 1810">•  <b>Unable to reach Dell upload server</b> – SupportAssist is unable to send the system information file because of a disruption in the connection to the receiving server hosted by Dell.</li> </ul>

Column	Description
	<ul style="list-style-type: none"> <li> <b>SupportAssist component is not available</b> — A SupportAssist component required for collecting system information is not installed.</li> <li> <b>Unable to configure SNMP</b> — SupportAssist is unable to configure the SNMP trap destination of the iDRAC.</li> <li> <b>Maintenance Mode</b> — SupportAssist has placed the device in automatic maintenance mode because of an alert storm. No new support cases will be created while the device is in maintenance. For more information, see <a href="#">Understanding maintenance mode</a>.</li> </ul> <p> <b>NOTE:</b> The <b>Error</b>  status is displayed as a link that you can click to view a description of the issue and the possible resolution steps.</p>

### Related Tasks

- [Adding a device \(agent-based monitoring\)](#)
- [Editing device credentials](#)
- [Deleting a device](#)
- [Sending the system information manually](#)
- [Enabling or disabling device-level maintenance mode](#)
- [Installing or upgrading OMSA using SupportAssist](#)
- [Filtering the displayed data](#)
- [Clearing the data filter](#)
- [Sorting the displayed data](#)

## Add Device

The **Add Device** window enables you to add devices that you want SupportAssist to monitor.

The following table provides information about the items displayed in the **Add Devices** window.

Field	Description
<b>Host Name / IP Address</b>	Host name or IP address of the device you want to add.
<b>Display Name</b> (Optional)	An optional name you want to use for identifying the device. This name is displayed in the <b>Device Inventory</b> .
<b>User Name</b>	User name required to login to the device.
<b>Password</b>	Password required to login to the device.
<b>Add</b>	Click to initiate device discovery and then add the device.
<b>Cancel</b>	Click to close the <b>Add Device</b> window.

### Related Tasks

- [Adding a device \(agent-based monitoring\)](#)
- [Adding a device \(agentless monitoring\)](#)

# Settings

The **Settings** tab enables you to configure SupportAssist. By default, the **System Logs** page is displayed when the **Settings** tab is opened. The **Settings** tab includes the following pages:

- **System Logs**
- **Proxy Settings**
- **Preferences**
- **Contact Information**
- **Email Settings**

## Related References

[System logs](#)

[Proxy settings](#)


[Preferences](#)


[Contact information](#)

[SMTP settings](#)

## System logs

The **System Logs** page enables you to schedule the collection of system information from devices monitored by SupportAssist. The following table provides information about the fields displayed in the **System Log Collection Schedule** page.

 **NOTE:** The **System Log Collection Schedule** options are only enabled if the **Enable system log collection scheduling** option is selected in the **Preferences** page.

 **NOTE:** If your devices are covered under the Dell ProSupport Plus service contract, when the **Enable system log collection scheduling** option is not selected, you will not receive some reporting information about your devices.

Field	Description
<b>Device Type</b>	The available device type is <b>Server</b> .
<b>Credential Type</b>	Select the specific device for which you want to schedule the collection of system information. The available options are: <ul style="list-style-type: none"><li>• <b>Windows</b></li><li>• <b>Linux</b></li><li>• <b>iDRAC</b></li></ul>
<b>Frequency</b>	Enables selecting the frequency at which system information is collected. The available options are: <ul style="list-style-type: none"><li>• <b>None</b></li><li>• <b>Weekly</b></li><li>• <b>Monthly</b></li></ul>

Field	Description
<b>Specify day and time</b>	<p>Enables selecting the day and time when you want to collect system information.</p> <ul style="list-style-type: none"> <li>If the <b>Frequency</b> is set to <b>None</b>, the periodic collection of system logs is disabled for the selected <b>Device Type</b> and <b>Credential Type</b>.</li> <li>If the <b>Frequency</b> is set to <b>Weekly</b>, the available options are: weeks (<b>1</b> or <b>2</b>), day of the week (<b>sunday, monday, tuesday, wednesday, thursday, friday,</b> and <b>saturday</b>), hour (in hh:mm format), and <b>AM/PM</b>.</li> <li>If the <b>Frequency</b> is set to <b>Monthly</b>, the available options are: week of the month (<b>first, second, third, fourth,</b> and <b>last</b>), day of the week (<b>sunday, monday, tuesday, wednesday, thursday, friday,</b> and <b>saturday</b>), hour (in hh:mm format), <b>AM/PM</b>, and months (<b>1</b> or <b>3</b>).</li> </ul>
<b>Start Date</b>	Displays the date and time at which the system information will be collected next.
<b>Apply</b>	Click to save the settings.
<b>Cancel</b>	Click to cancel the changes.

#### Related Tasks

[Customizing the schedule for periodic collection of system information](#)

## Proxy settings

The **Proxy Settings** page enables you to configure the proxy server settings.

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


Field	Description
<b>Use Proxy Settings</b>	Select this option to enable configuring the proxy server settings.
<b>Host Name / IP Address</b>	View or edit the proxy server address or name.
<b>Port</b>	View or edit the proxy server port number.
<b>Proxy requires authentication</b>	Select this option if a user name and password are required to login to the proxy server.
<b>User Name</b>	View or edit the user name required to connect to the proxy server.
<b>Password</b>	Edit the password required to login to the proxy server.
<b>Apply</b>	Click to save the settings.
<b>Cancel</b>	Click to cancel the changes.

#### Related Tasks

[Configuring proxy server settings](#)

## Preferences

The **Preferences** page enables you to configure **Auto Update**, **Email Settings**, **Support Collection**, and **Maintenance Mode**. The following table provides information about the options displayed in the **Preferences** page.

Field	Description
<b>Auto Update</b>	
<b>Enable auto update</b>	Select this option to automatically download and install the latest SupportAssist and collection tool updates, when they are available. The download and installation of the updates occur in the background. A message will be displayed if problems occur during the update process.   <b>NOTE:</b> It is recommended that you select the <b>Enable auto update</b> option, to ensure that SupportAssist is up-to-date with the latest features and enhancements.
<b>Email Settings</b>	
<b>Receive email notification when a new support case is opened</b>	Select this option to receive an email notification when a new support case is opened.
<b>Preferred email Language</b>	Select the preferred language for email notifications.
<b>Support Collection</b>	
<b>Automatically start a log collection when a new support case is generated</b>	Select this option to automatically start a system log collection when a new support case is generated.
<b>Enable system log collection scheduling</b>	Select this option to enable scheduling of the system log collection. To schedule the system log collection, configure the <b>System Log Collection Schedule</b> in the <b>System Logs</b> tab.
<b>Send network identification information to Dell</b>	Select this option to allow sending network identification information to Dell.
<b>Maintenance Mode</b>	
<b>Temporarily suspend case generation activity (e.g., for purposes of downtime, external troubleshooting, etc.)</b>	Select this option to set all devices to maintenance mode. While in maintenance mode, no new support cases are opened.
<b>Apply</b>	Click to save the settings.
<b>Cancel</b>	Click to cancel the changes.


### Related Tasks

[Enabling auto update](#)

- [Configuring email notification settings](#)
- [Enabling or disabling the automatic collection of system information](#)
- [Enabling or disabling the periodic collection of system information from all devices](#)
- [Filtering the collection of system information](#)
- [Enabling or disabling global-level maintenance mode](#)

## Contact information

The **Contact Information** page enables you to view and edit the primary and secondary contact information. The following table provides information about the items displayed in the **Contact Information** page.

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


Field	Description
<b>Company</b>	View or edit the company name.
<b>Primary</b>	Select this option to view the primary contact information.
<b>Secondary</b>	Select this option to view the secondary contact information.
<b>First Name</b>	View or edit the first name of the primary or secondary contact.
<b>Last Name</b>	View or edit the last name of the primary or secondary contact.
<b>Phone</b>	View or edit the phone number of the primary or secondary contact.
<b>Alternate Phone</b>	View or edit the alternate phone number of the primary or secondary contact.
<b>Email</b>	View or edit the email address of the primary or secondary contact.
<b>Country</b>	Enables you to select the country.
<b>Apply</b>	Click to save the information.
<b>Cancel</b>	Click to cancel the changes.

### Related Tasks

- [Viewing and updating the contact information](#)

## SMTP settings

The **SMTP Settings** page enables you to configure the SMTP server (email server) settings. If your company utilizes an SMTP server, it is recommended that you configure the SMTP server settings.

 **NOTE:** SupportAssist utilizes the SMTP server to send you device status and connectivity status email notifications. You will not receive those email notifications if:

- Your company does not utilize an SMTP server
- Your company utilizes an SMTP server, but the SMTP server settings are either not configured or configured incorrectly.

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

Field	Description
<b>Enable Email Notification</b>	Select this option to enable configuring the email server settings.
<b>Host Name / IP Address</b>	View or edit the email server address or name.
<b>Port</b>	View or edit the email server port number.
<b>Requires Authentication</b>	Select this option if the email server requires authentication.
<b>User Name</b>	View or edit the user name required to connect to the email server.
<b>Password</b>	Edit the password required to connect to the email server.
<b>Use SSL</b>	Select this option to use secure communication for sending emails.
<b>Apply</b>	Click to save the settings.
<b>Cancel</b>	Click to cancel the changes.






### Related Tasks

[Configuring SMTP server settings](#)

## Connectivity test

The **Connectivity Test** page enables you to test SupportAssist connectivity to the dependent network resources.

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

Field	Description
Check box	Select the appropriate check boxes to test the connectivity status you want to verify.
<b>Test</b>	<p>Displays the dependent network resources that you can test. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Internet Connectivity</b></li> <li>• <b>SMTP Server</b></li> <li>• <b>Dell FTP Server</b></li> <li>• <b>Dell Upload Server</b></li> <li>• <b>SupportAssist Server</b></li> </ul>
<b>Description</b>	Provides a description of the test.
<b>Connectivity Status</b>	<p>Displays an icon and a message that indicates the connectivity status. The possible statuses are:</p> <ul style="list-style-type: none"> <li>•  <b>Not Configured</b> (applicable only for the SMTP Server test) — The SMTP server settings are not configured in SupportAssist. If your company utilizes an SMTP server (email server), it is recommended that you configure the <b>SMTP Settings</b> in SupportAssist.</li> <li>•  <b>In Progress</b> — The connectivity test is in progress.</li> <li>•  <b>Connected</b> — The connectivity test is successful.</li> <li>•  <b>Error</b> — The connectivity test is unsuccessful.</li> </ul> <p> <b>NOTE:</b> The <b>Error</b> status is displayed as a link that you can click to view a description of the issue and the possible resolution steps.</p>
<b>Last Verified</b>	Displays the date and time the connectivity status was last verified.
<b>Test Connectivity</b>	Click to perform the selected connectivity tests.

## Related documents and resources

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

Document title	How to access the document
<i>Dell SupportAssist Version 1.0.1 for Servers Quick Setup Guide</i>	Visit <a href="https://Dell.com/ServiceabilityTools">Dell.com/ServiceabilityTools</a> .
<i>Dell SupportAssist Version 1.0.1 for Servers Support Matrix</i>	
<i>Dell SupportAssist Version 1.0.1 for Servers Release Notes</i>	
<i>Dell System E-Support Tool User's Guide</i>	
<i>Dell OpenManage Server Administrator Installation Guide</i>	Visit <a href="https://Dell.com/OpenManageManuals">Dell.com/OpenManageManuals</a> and click <b>OpenManage Server Administrator</b> .
<i>Dell OpenManage Server Administrator User's Guide</i>	
<i>iDRAC User's Guide</i>	Visit <a href="https://Dell.com/ESMmanuals">Dell.com/ESMmanuals</a> and click <b>Remote Access Controller</b> .
<i>Dell SupportAssist: Alert Policy</i>	Visit <a href="https://Dell.com/SupportAssistGroup">Dell.com/SupportAssistGroup</a> .
<i>Managing Windows Device Credentials in SupportAssist Using Service Account</i>	

## Video tutorials

You can access the following video tutorials related to SupportAssist for Servers.

Video title	How to access the videos
Monitoring Local System	Visit the <b>Dell TechCenter</b> channel on YouTube, and click <b>Playlist</b> . On the playlist, click <b>SupportAssist for Servers</b> .
Adding Devices	
Configuring Alert Destination (Windows)	
Configuring Alert Destination (Linux)	
Auto Installation or Upgrade of OMSA	

## SupportAssist community

You can also find video tutorials, peer-to-peer questions, user's guides, and other useful information on the Dell SupportAssist community forum at [Dell.com/SupportAssistGroup](https://Dell.com/SupportAssistGroup).

# Dell Remote Consulting Service

You can use your existing Dell Remote Consulting Service contract or place an order and schedule time with a systems management deployment expert for SupportAssist installation, set up, and configuration from start to finish. For more information, see the [Remote Consulting Services service description](#) document.

## Accessing Documents From Dell Support Site

You can access the required documents in one of the following ways:

- Using the following links:
  - For all Enterprise Systems Management documents — [dell.com/softwaresecuritymanuals](https://dell.com/softwaresecuritymanuals)
  - For OpenManage documents — [dell.com/openmanagemanuals](https://dell.com/openmanagemanuals)
  - For Remote Enterprise Systems Management documents — [dell.com/esmmanuals](https://dell.com/esmmanuals)
  - For OpenManage Connections Enterprise Systems Management documents — [dell.com/OMConnectionsEnterpriseSystemsManagement](https://dell.com/OMConnectionsEnterpriseSystemsManagement)
  - For Serviceability Tools documents — [dell.com/serviceabilitytools](https://dell.com/serviceabilitytools)
  - For Client Systems Management documents — [dell.com/clientsystemsmanagement](https://dell.com/clientsystemsmanagement)
  - For OpenManage Connections Client Systems Management documents — [dell.com/dellclientcommandsuite manuals](https://dell.com/dellclientcommandsuite manuals)
- From the Dell Support site:
  - a. Go to [dell.com/support/home](https://dell.com/support/home).
  - b. Under **Select a product** section, click **Software & Security**.
  - c. In the **Software & Security** group box, click the required link from the following:
    - **Enterprise Systems Management**
    - **Remote Enterprise Systems Management**
    - **Serviceability Tools**
    - **Client Systems Management**
    - **Connections Client Systems Management**
  - d. To view a document, click the required product version.
- Using search engines:
  - Type the name and version of the document in the search box.

## Contacting Dell

### Prerequisites

 **NOTE:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

**About this task**

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

**Steps**

1. Go to **dell.com/support**.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.