Dell SupportAssist Version 1.3 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.

2017 - 02

Rev. A01

Contents

1

Overview

Dell SupportAssist for Servers is an application that enables automated support from Dell by proactively identifying hardware issues in Dell devices. 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 Technical Support. The collected data helps Dell Technical Support to provide you an enhanced, personalized, and efficient support experience. SupportAssist capability also includes a proactive response from Dell Technical Support to help you resolve the issue.

NOTE: SupportAssist capabilities supported on a monitored Dell device may vary based on the Dell service contract. For more information about the capabilities of SupportAssist, see SupportAssist capabilities available with Dell service contracts.

Installing and using SupportAssist is optional, and results in improved support, products, and services designed to meet your needs. SupportAssist Version 1.3 for Servers automates support from Dell Technical Support for:

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

For the complete list of supported device models, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.

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.

This document provides the information required for installing and using SupportAssist to monitor devices for hardware issues, collect system information, and automatically create a support case when an issue is detected.

NOTE: In this document, the term *local system* refers to the system on which you install SupportAssist; *remote device* refers to any other device that you want SupportAssist to monitor for hardware issues. By default, SupportAssist automatically monitors hardware issues that may occur on the local system. To allow SupportAssist to monitor hardware issues that may occur on remote devices, you must add each remote device in SupportAssist.

Related links

Data collected by SupportAssist
Identifying the generation of a Dell PowerEdge server

What is new in this release

- Display of support case status and source irrespective of the case creation method for Service Tags with a ProSupport or ProSupport Plus entitlement that are monitored by SupportAssist. See Cases.
- Ability to quickly view the support cases for a specific device. See Checking for support cases.
- Ability to test the support case creation capability. See Testing the case creation capability.
- Ability to request Dell Technical Support to suspend, resume, or close activities related to a support case. See Case management options.

- Ability to transpose the data displayed in the configuration viewer. See Data views.
- Ability to cancel a manually-initiated collection. See Sending the system information manually.
- Support for Dell Datacenter Scalable Solutions. For the complete list of supported device models, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.
- Support for collection of the following data:
  - Dell Lifecycle Controller log from Dell's 12th and 13th generation of PowerEdge servers.
  - TTY log from PowerEdge servers that have iDRAC firmware version 2.00.00.00 or later installed.
- Support for installing SupportAssist on additional Linux operating systems. See Minimum requirements for installing and using SupportAssist.

How SupportAssist works

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

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.

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. However, a support case is not created automatically for devices with a Basic Hardware service contract.

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

Table 1. SupportAssist capabilities

SupportAssist capability	Description	Dell service contract type		
		Basic Hardware	ProSupport	ProSupport Plus
Proactive detection of hardware failures	SupportAssist receives alerts for hardware events that occur in monitored devices and proactively determines if the alerts indicate a hardware failure.	✓	✓	✓
Predictive detection of hardware failures*	Intelligent analysis of data collected from a monitored device is used to predict hardware failures that may occur in future.	✗	✗	✓
Automated data collection	Data required for troubleshooting a hardware failure is automatically collected from the monitored device and sent securely to Dell.	✓	✓	✓
Automated support case creation	When a hardware failure is detected either proactively or predictively, a Service Request is automatically created with Dell Technical Support.	✗	✓	✓

SupportAssist capability	Description	Dell service contract type		
		Basic Hardware	ProSupport	ProSupport Plus
Automated email notification	An email notification about the support case or issue is automatically sent to your company's primary and secondary SupportAssist contacts.	✗	✓	✓
Proactive response from Dell Technical Support	A Dell Technical Support agent contacts you proactively about the support case and helps you resolve the issue.	✗	✓	✓
Proactive parts dispatch	Based on examination of the collected system information, if the Dell Technical Support agent determines that a part needs to be replaced to resolve the issue, a replacement part is dispatched to you with your consent.	✗	✓	✓
ProSupport Plus reporting	Data collected periodically by SupportAssist enables Dell to provide you an insight into your company's as-maintained environment configuration with proactive firmware recommendations and other reports.	✗	✗	✓

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

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.

The information encrypted in the data log sent to Dell contains the following categories of data:

- **Hardware and software inventory** — Installed devices, processors, memory, network devices, usage, and Service Tag
- **Software configuration for servers** — Operating system and installed applications
- **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 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 10 devices at a time. For information about the default frequency of data collection, see Default schedule for collection of system information.

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

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

2

Getting started with SupportAssist

SupportAssist automates support from Dell Technical Support for Dell devices. You can use SupportAssist to monitor one or more devices.

Basic setup

The basic setup enables SupportAssist to monitor the local system (the server on which SupportAssist is installed). If you only have a single device that you want to monitor, only the basic setup is required. For monitoring more than one device, you must complete the basic and advanced setup.

To complete the basic setup:

1. Download the SupportAssist installation package. See Downloading the SupportAssist installation package.
2. Review the requirements for installing SupportAssist. See Minimum requirements for installing and using SupportAssist.
3. Install SupportAssist. See Installing SupportAssist.
4. Complete the registration of SupportAssist. See Registering SupportAssist.
5. (Optional) Update the contact information to include a secondary SupportAssist contact and a parts dispatch address. See Viewing and updating the contact information.

Advanced setup

The advanced setup enables SupportAssist to monitor multiple devices, and includes adding each device that 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 device that 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.
4. (Optional) If you want to manage a set of devices as a group, create one or more device groups based on your preference. See Device grouping.

Evaluating 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 on the data collected by SupportAssist from monitored devices, see Data collected by SupportAssist. If you have concerns about the security and data collected by SupportAssist, you can disable certain configuration options and evaluate SupportAssist.

You can also view the data that is collected by SupportAssist. For information on viewing the collected data, see Viewing the collected system information.

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

- You can disable the collection of identity information from all monitored devices. See Enabling or disabling the collection of identity information.

- You can disable the collection of software information and the system log from all monitored devices. See Enabling or disabling the collection of software information and the system log.
- You can disable the periodic collection of system information from all 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 by Dell Technical Support 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/SupportAssist.
   The SupportAssist portal is displayed.
2. In the **Available Versions** section, click the **Learn More** link that is displayed under **SupportAssist for servers, storage and networking**.
   The **SupportAssist for servers, storage and networking** page is displayed.
3. In the **Downloads** section, under **SupportAssist for Servers**, do one of the following based on the installation package that you want to download:
   - For the Windows installation package, click the **SupportAssist for servers (Windows)** link.
   - For the Linux installation package, click the **SupportAssist for servers (Linux)** link.

   The **Drivers Details** page is displayed in a new web browser window.
4. In the **Available formats** section, click the **Download File** link that is displayed under **File Format: Application**.

Minimum requirements for installing and using SupportAssist

You can install SupportAssist on any Dell PowerEdge server (9th to 13th generation) that meets the minimum requirements specified in the following sections.

Hardware requirements

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

Table 2. Hardware requirements

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

NOTE: For monitoring a large number of devices in your environment, Dell recommends that you install SupportAssist on a dedicated server. Periodic collections (required for ProSupport Plus reporting) from a large number of devices may result in a high processor or memory utilization on the monitoring server. The high resource utilization may affect other applications that are running on the monitoring server, if the resources are shared with other applications.

Operating system requirements for installing SupportAssist

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

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

NOTE: Installation of SupportAssist is not supported on Server Core.

The server on which you want to install SupportAssist must be running one of the following Windows or Linux operating systems.

- Windows operating systems:
  - Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise, and Datacenter
  - Windows Server 2008 SP2 Standard, Enterprise, and Datacenter
  - Windows Server 2012 R2 Standard and Datacenter
  - Windows Server 2012 Standard, Essentials, and Datacenter
  - Small Business Server 2008 Essentials and Standard
  - Small Business Server 2011 Essentials and Standard
- Linux operating systems:
  - Red Hat Enterprise Linux 7.*x*
  - Red Hat Enterprise Linux 6.*x*
  - Red Hat Enterprise Linux 5.*x*
  - CentOS 7.*x*
  - CentOS 6.*x*
  - Novell SUSE Linux Enterprise Server 12 SP1
  - SUSE Linux Enterprise Server 12
  - SUSE Linux Enterprise Server 11 SP4
  - SUSE Linux Enterprise Server 10 SP4
  - Oracle Linux 7.*x*
  - Oracle Linux 6.*x*

Web browser requirements

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 10 or 11
- Mozilla Firefox 31 or later

NOTE: On supported Linux operating systems, SupportAssist can also be accessed using the native web browser version.

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 local system (the server on which SupportAssist is installed) must be able to connect to the following destinations:
  - **https://apidp.dell.com** and **https://api.dell.com** — end point for the SupportAssist server.
  - **https://is.us.dell.com/FUS/api/2.0/uploadfile** — the file upload server where the collected system information is uploaded.
  - **https://downloads.dell.com/** — for downloading Dell OpenManage Server Administrator (OMSA) and receiving new SupportAssist release information.

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 local system.

Table 3. Network port requirements on the local system

Port	Usage
22	For adding the local system running a Linux operating system and for collecting system information
25	For SMTP communication (required for SupportAssist to send certain email notifications through the SMTP server utilized by your company)
80	For HTTP communication
135	For Windows Management Instrumentation (WMI) communication
162	For receiving alerts (SNMP traps) from remote devices
443	For Secure Socket Layer (SSL) communication, WS-Man communication, and verifying SupportAssist update information
1311	For OMSA communication
2607	For opening SupportAssist securely (HTTPS) from a remote system
9090	For opening SupportAssist from the local system
61616	For processing SupportAssist tasks

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

Table 4. Network port requirements on remote devices

Port	Usage
22	For adding a remote device that is running a Linux operating system and to collect system information from the device
135	For WMI communication
161	For forwarding alerts (SNMP traps) to the local system
443	For Secure Socket Layer (SSL) communication and WS-Man communication
1311	For OMSA communication

Installing SupportAssist

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

NOTE: For SupportAssist installation on Linux operating systems only: When SupportAssist is installed on a server running a Linux operating system, SupportAssist can monitor the local system and the remote devices running the supported Linux operating system. Monitoring remote devices running any other operating system is only possible if the devices are added in SupportAssist for agentless monitoring. For information on adding a device for agentless monitoring, see Adding a device (agentless monitoring).

Installing SupportAssist (Windows)

Prerequisites

- Ensure that you have downloaded the SupportAssist installation package for Windows operating systems. See Downloading the SupportAssist installation package.
- Ensure that the system meets the requirements for installing SupportAssist. See Minimum requirements for installing and using 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 in to the system as an administrator, double-click the installer package to install SupportAssist. However, ensure that you acknowledge the Open File - Security Warning dialog box to proceed.

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

Figure 1. Login page

NOTE: If the initialization of the SupportAssist service takes longer than expected, an error message is displayed. If this issue occurs, close the web browser and try accessing SupportAssist later. For instructions to access SupportAssist, see Opening the SupportAssist user interface.

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.

Installing SupportAssist (Linux)

Prerequisites

- Ensure that you have downloaded the SupportAssist installation package for Linux operating systems.
- Ensure that you are logged in to the system with root privileges.
- Ensure that Net-SNMP is installed on the system. For information on installing Net-SNMP, see Installing Net-SNMP (Linux only).

  NOTE: If you choose to install Net-SNMP after installing SupportAssist, ensure that you run the script file, snmptrapdServiceConfiguration.sh, after installing Net-SNMP. The script file will be available at /opt/dell/supportassist/scripts after the installation of SupportAssist is completed.
- Ensure that the system meets the requirements for installing SupportAssist. See Minimum requirements for installing and using SupportAssist.

Steps

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

   The **Welcome to the Dell SupportAssist Installer** message is displayed.
5. To continue, type `c`.

   The **SupportAssist License Agreement** is displayed.
6. Read the license agreement and type `y` to start the installation.

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

Figure 2. Login page

NOTE: If the initialization of the SupportAssist service takes longer than expected, an error message is displayed. If this issue occurs, close the web browser and try accessing SupportAssist later. For instructions to access SupportAssist, see Opening the SupportAssist user interface.

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

- Log in to a remote system and access the following web address by using a web browser:
  `https://<IP address or host name of server on which SupportAssist is installed>:2607/SupportAssist`

  NOTE: You can access SupportAssist from a remote system only if port 2607 is open on the system where SupportAssist is installed.
- Log in to the local system and access the following web address by using a web browser:
  `http://localhost:9090/SupportAssist`

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

Installing SupportAssist in silent mode (Linux)

Prerequisites

- Ensure that you have downloaded the SupportAssist installation package for Linux operating systems.
- Ensure that you are logged in to the system with root privileges.
- Ensure that Net-SNMP is installed on the system. For information on installing Net-SNMP, see Installing Net-SNMP (Linux only).

  NOTE: If you choose to install Net-SNMP after installing SupportAssist, ensure that you run the script file, snmptrapdServiceConfiguration.sh, after installing Net-SNMP. The script file will be available at /opt/dell/supportassist/scripts after the installation of SupportAssist is completed.
- Ensure that the system meets the requirements for installing SupportAssist. See Minimum requirements for installing and using SupportAssist.

Steps

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

Next steps

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

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

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

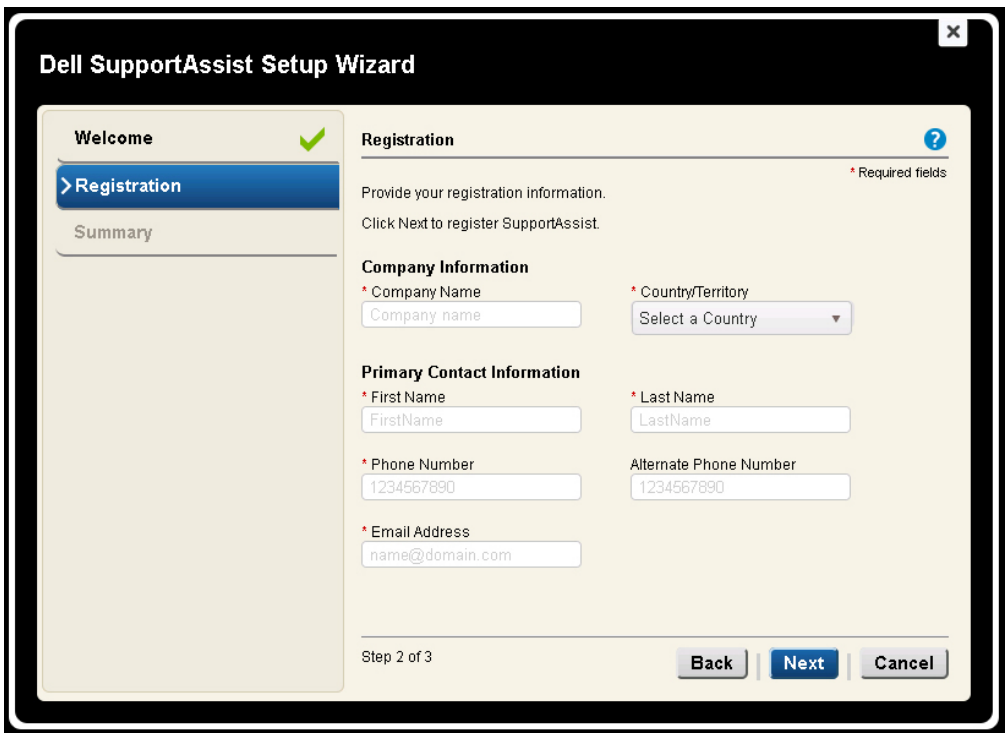

Figure 3. Registration page

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

NOTE: After registering 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:

- SupportAssist verifies if Dell OpenManage Server Administrator (OMSA) is installed on the local system:
  - If OMSA is either not installed or requires an upgrade, the recommended version of OMSA is downloaded and installed automatically. The local system 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 local system is listed on the **Device Inventory** page with an **OK** status.

CAUTION: Without OMSA, SupportAssist will not be able to monitor the local system.

NOTE: The SupportAssist recommended version of OMSA may vary depending on the generation of the PowerEdge server and the operating system running on the server. For information on the recommended versions of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at 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

- If you have installed SupportAssist on a server running a Linux operating system that has Security Enhanced Linux (SELinux) enabled, set up the device to receive alerts from remote devices. For more information, see Setting up an SELinux enabled system to receive alerts.
- 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 and provide a parts dispatch address. See Viewing and updating the contact information.
- (Optional) If you want to manage a set of devices as a group, create one or more device groups based on your preference. See Device grouping.

Setting up an SELinux enabled system to receive alerts

About this task

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

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

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

Steps

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

```
module supportassistpolicy 1.0;

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

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

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

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

Upgrading SupportAssist (Windows)

If SupportAssist is installed on a Windows operating system, you can upgrade from SupportAssist version 1.0.1 or 1.2 to version 1.3.

Prerequisites

Ensure that you have downloaded the latest version of SupportAssist. See Downloading the SupportAssist installation package.

Steps

1. Right-click the 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 in to the system as an administrator, double-click the installer package to install SupportAssist. However, ensure 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. Devices that you added in the previous version of SupportAssist are displayed in the **Device Inventory** page.

Upgrading SupportAssist (Linux)

If SupportAssist is installed on a Linux operating system, you can upgrade from SupportAssist version 1.2 to version 1.3.

Prerequisites

Ensure that you have downloaded the latest version of SupportAssist. See Downloading the SupportAssist installation package.

Steps

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

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

   The **Welcome to the Dell SupportAssist Installer** message is displayed.
5. To continue, type `c`.
   The **SupportAssist License Agreement** is displayed.
6. Read the license agreement and type `y` to start the installation.
   After the installation is completed, the **SupportAssist Login** page opens in a web browser window.

   NOTE: If the initialization of the SupportAssist service takes longer than expected, an error message is displayed. If this issue occurs, close the web browser and try accessing SupportAssist later. For instructions to access SupportAssist, see Opening the SupportAssist user interface.

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

   - Log in to a remote system and access the following web address by using a web browser:
     `https://<IP address or host name of server on which SupportAssist is installed>:2607/SupportAssist`

     NOTE: You can access SupportAssist from a remote system only if port 2607 is open on the system where SupportAssist is installed.
   - Log in to the local system and access the following web address by using a web browser:
     `http://localhost:9090/SupportAssist`
7. Type the user name and password of a user with root privileges on the system where SupportAssist is installed, and then click **Log In**.
   The **Cases** page is displayed.

Opening the SupportAssist user interface

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

- If you are logged in to the server on which SupportAssist is installed:

- If the server is running a Windows operating system, 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, point to the bottom-left corner of the screen, and then click the **Start** icon. On the **Start** screen, click the **SupportAssist** tile.
- If the server is running a Linux operating system, click **Applications** → **System Tools** → **Dell SupportAssist**.
- Open a web browser and type the address in the following format:
  `http://localhost:9090/SupportAssist`

  .

- To access SupportAssist from 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`.

  For example, https://10.25.35.1:2607/SupportAssist.
  - 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** page is displayed in the web browser.

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

Logging in to SupportAssist

1. In 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 the SupportAssistAdmins, SupportAssistUsers user group. If SupportAssist is installed on a Linux operating system, you can also provide the user name and password of a user account that is a member of the root or users user group. For information on the SupportAssist user groups, see SupportAssist user groups.

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

2. Click **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. Point to the ***user name*** link that is displayed at the top-right of the SupportAssist header area.
   The **Connectivity Test** and **Logout** options are displayed.
2. Click **Logout**.

3

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 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.

  NOTE: Installation of OMSA may not be supported on certain operating systems. SupportAssist may be able to monitor devices running such operating systems only through the agent-based monitoring method. For information on the operating system requirements for agent-based monitoring, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.

- **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 a 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 (iDRAC 7 and iDRAC 8).

  NOTE: The iDRAC can be configured to send alerts through SNMP and IPMI. However, SupportAssist can only receive alerts sent through SNMP. To ensure that SupportAssist receives alerts sent from an iDRAC, you must ensure that all SNMP Trap options are selected in the Alerts and Remote System Log Configuration section of the iDRAC web console.

Benefits of agent-based monitoring

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

- Alert generation capabilities of OMSA and iDRAC are not the same. In Dell's 13th generation of PowerEdge servers, the alert generation capabilities of OMSA and iDRAC are almost similar. However, alerts from chipset and software RAID are available only through OMSA.
- For devices with a ProSupport Plus 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 in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.
- 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).
  - Unzip package must be installed on the device.
- If the device is running VMware ESXi, SSH service must be running on the device.
- Port 1311 must be open on the device for OMSA communication.
- If the device connects to the internet through a proxy server, ensure that the following ports are open on the proxy server firewall: 161, 22 (for adding devices running Linux), 135 (for adding devices running Windows), and 1311.
- Review the requirements for installing OMSA on the device. For more information, see the "Installation Requirements" section in the *Dell OpenManage Server Administrator Installation Guide* at Dell.com/OpenManageManuals.

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.

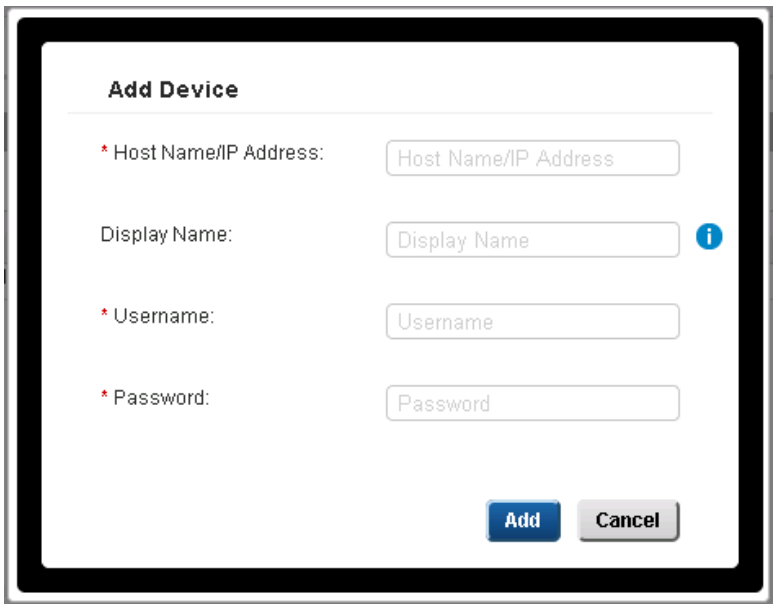

Figure 4. Add Device window

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

   NOTE: Dell recommends 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 in 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 provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist. For information on configuring the sudo user, see Configuring sudo access for SupportAssist (Linux).

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 (if applicable) and install/upgrade OMSA on the device (if applicable).

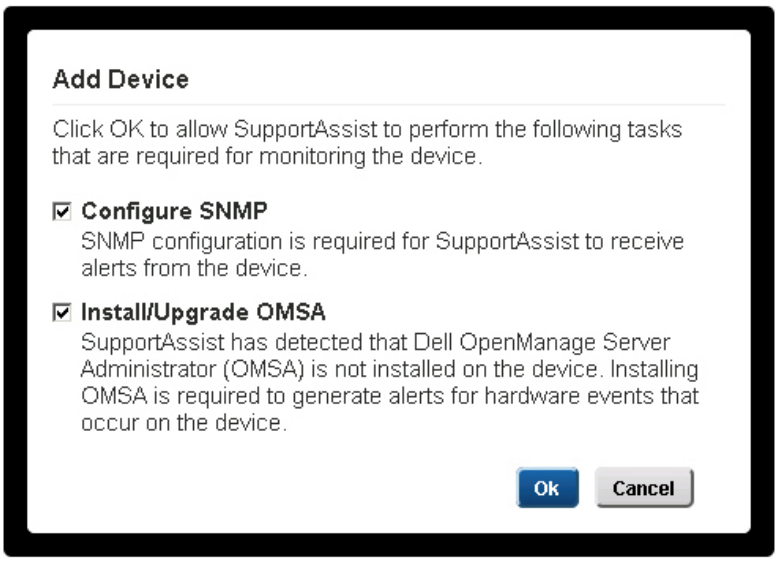

Figure 5. Add device tasks

If SupportAssist can configure the SNMP settings of the device, the **Configure SNMP** option is automatically selected in the **Add Device** window.

NOTE: The Configure SNMP option is disabled in the Add Device window if the device is running Citrix XenServer, VMware ESXi, or Oracle Virtual Machine.

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.

If SupportAssist has detected that OMSA is either not installed or requires an upgrade, the **Install/Upgrade OMSA** option is selected in the **Add Device** window.

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

- SupportAssist has detected that the recommended version of OMSA is already installed on the device.
- SupportAssist does not support the automatic installation of OMSA on the device.
- Installation of OMSA is not supported on the device.
- SupportAssist has detected that OMSA is installed on the device, but is unable to identify the version of OMSA.

NOTE: Automatic installation of OMSA through SupportAssist is not supported on devices running Citrix XenServer, VMware ESXi, or ESX. To allow SupportAssist to detect hardware issues on these devices, you must manually download and install OMSA.

NOTE: Installation of OMSA is not supported on devices running CentOS, Oracle Virtual Machine, and Oracle Enterprise Linux. SupportAssist will only collect and upload system information from these devices. SupportAssist will not detect, through agent-based monitoring, hardware issues that may occur on these devices.

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:

   - When SupportAssist is configuring the SNMP settings, the device displays a **Configuring SNMP** status.
   - When SupportAssist is installing or upgrading 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, 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 links

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 enables 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 by 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.

NOTE: You can retry the automatic configuration of the alert destination at any time using the Configure SNMP option available in SupportAssist. For information on using the Configure SNMP option, see Configuring SNMP settings using SupportAssist.

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

Related links

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 2008
- Windows Small Business Server 2011
- Windows Server 2012
- Windows Server 2012 R2
- Server Core for Windows Server 2012

Steps

1. On the server on which SupportAssist is installed, browse to the **C:\Program Files\Dell\SupportAssist\scripts** folder.
2. Copy the script file (**WindowsSNMPConfig.ps1**) located in the folder and paste the file at a desired location (for example, **C:\temp**) on the device.
3. Perform one of the following, depending on the operating system running on the device:
   - In Windows Server 2012, on the **Start** screen, right-click the **Windows PowerShell** tile, and in the app bar, click **Run as administrator**.
   - In Windows Server 2003, 2008, or Windows Small Business Server 2011, click **Start**, type `PowerShell`, right-click **Windows PowerShell**, and then click **Run as administrator**.
4. Set the PowerShell execution policy as appropriate on the device. For example, type the following command: `Set-ExecutionPolicy RemoteSigned` or `Set-ExecutionPolicy AllSigned`.
5. Run the script file on the device using the following syntax: `<script file path> -hosts <IP address of server 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 links

Configuring the alert (SNMP trap) destination

Manually configuring the alert destination (Windows)

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** window is displayed.
4. Click the **Traps** tab, and perform the following:
   a. In the **Community name** box, type the community name, and click **Add to list**.
   b. In **Trap destinations**, click **Add**.

      The **SNMP Service Configuration** window is displayed.
   c. In the **Host name, IP or IPX address** field, type the host name or IP address of the server on which SupportAssist is installed, and click **Add**.
5. Click **Apply**.
6. In the **Services** window, right-click **SNMP Service** and click **Restart**.

Related links

Configuring the alert (SNMP trap) destination

Configuring the alert destination using the script file (Linux)

Prerequisites

- Ensure that Net-SNMP is installed on the system. For information on installing Net-SNMP, see Installing Net-SNMP (Linux only)
- Ensure that you have root privileges on the device.

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

- Red Hat Enterprise Linux 5.5 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.7 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.8 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.9 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.10 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.11 (32-bit and 64-bit)
- Red Hat Enterprise Linux 6.1 (64-bit)
- Red Hat Enterprise Linux 6.2 (64-bit)
- Red Hat Enterprise Linux 6.3 (64-bit)
- Red Hat Enterprise Linux 6.4 (64-bit)
- Red Hat Enterprise Linux 6.5 (64-bit)
- Red Hat Enterprise Linux 6.7 (64-bit)
- Red Hat Enterprise Linux 6.8 (64-bit)
- Red Hat Enterprise Linux 7.0 (64-bit)
- Red Hat Enterprise Linux 7.1 (64-bit)
- Red Hat Enterprise Linux 7.2 (64-bit)
- SUSE Linux Enterprise Server 10 SP3 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 11 (64-bit)
- SUSE Linux Enterprise Server 11 SP1 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 11 SP2 (64-bit)
- SUSE Linux Enterprise Server 11 SP3 (64-bit)
- SUSE Linux Enterprise Server 11 SP4 (64-bit)
- SUSE Linux Enterprise Server 12 (64-bit)
- SUSE Linux Enterprise Server 12 SP1 (64-bit)
- CentOS 7.0
- CentOS 6.0
- Oracle Linux 7.1
- Oracle Linux 6.7
- VMware ESX 4.1

Steps

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

Related links

Configuring the alert (SNMP trap) destination

Manually configuring the alert destination (Linux)

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 links

Configuring the alert (SNMP trap) destination

Adding a device (agentless monitoring)

Prerequisites

- Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.
- Ensure that the device is a 12th or 13th generation Dell PowerEdge server (iDRAC7 or iDRAC8). For information on identifying the generation of a PowerEdge server, see Identifying the generation of a PowerEdge server.
- 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.
- If the device connects to the internet through a proxy server, ensure that the following ports are open on the proxy server firewall: 161 and 443.
- 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.

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.

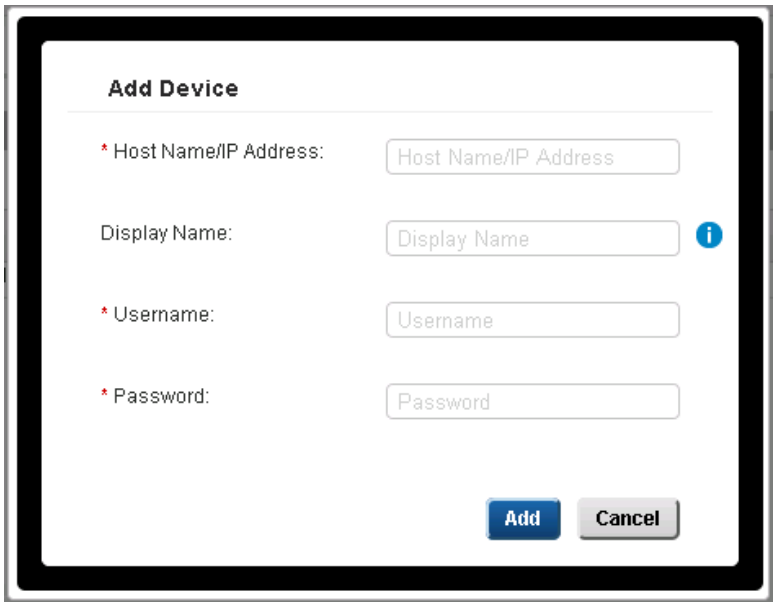

Figure 6. Add Device window

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 in 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 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.

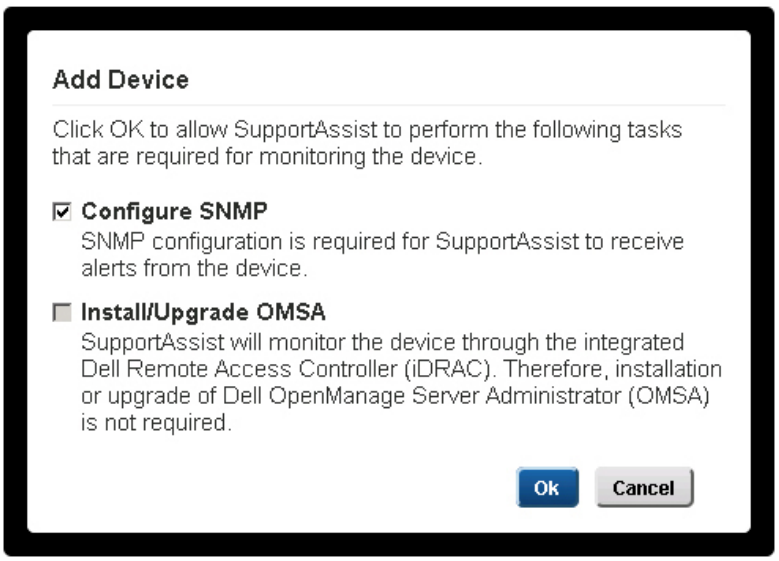

Figure 7. Add device task

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.

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 the device through the agentless method.

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, click the error link to see a description of the issue and the possible resolution steps.

Next steps

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

Related links

Add Device

Manually configuring the alert destination of iDRAC by using the web interface

Perform the following steps to manually configure the alert destination of an iDRAC:

1. Log in to the iDRAC web interface.
2. Go to **Overview** → **Server** → **Alerts**.
3. In the **Alerts** section, make sure that the **Enabled** option is selected.
4. In the **Alerts Filter** section, make sure that the following options are selected:
   - **System Health**
   - **Storage**
   - **Configuration**
   - **Audit**
   - **Updates**
   - **Warning**
   - **Critical**
5. In the **Alerts and Remote System Log Configuration** section, make sure that all fields in the **SNMP Trap** column are selected.
6. Click **SNMP and Email Settings**.
7. In the **IP Destination List** section, select the **State** option to enable the alert destination field.

   You can specify up to eight destination addresses. For more information about the options, see the *iDRAC Online Help*.
8. In the **Destination Address** field, type the IP address of the server 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 *iDRAC Online Help*.

   NOTE: The community string value indicates the community string to be used in a Simple Network Management Protocol (SNMP) alert trap sent from iDRAC. Ensure that the destination community string is the same as the iDRAC community string. The default community string is Public.
10. Click **Apply**.

    The alert destination is configured.
11. In the **SNMP Trap Format** section, make sure that either **SNMP v1** or **SNMP v2** is selected, and click **Apply**.

iDRAC is now configured to forward alerts to the server 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.

4

Viewing cases and devices

The SupportAssist user interface displays the support cases that are open and the devices that you have added for monitoring. The case management options that are available on the **Cases** page enable you to request Dell Technical Support to suspend, resume, or close activities related to a support case. From the **Device Inventory** page, you can check for the support cases that are open for a specific device. You can filter and sort the displayed cases and devices data based on your preference.

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.

Viewing all support cases

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

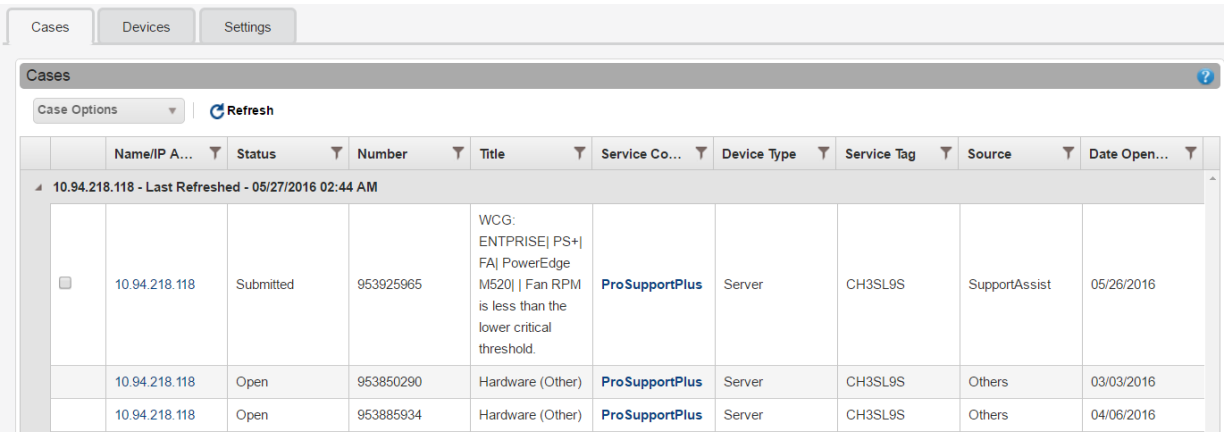

Figure 8. Cases page

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

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

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

After SupportAssist has completed its open support cases update, the **Cases** page displays the current support cases. For information on the fields and details displayed on the **Cases** page, see Case list.

Case management options

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

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

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

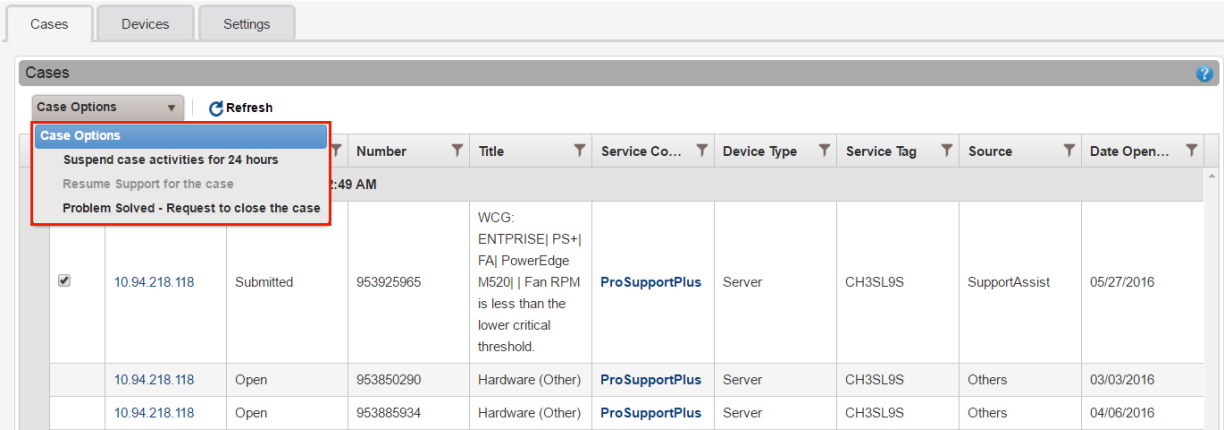

Figure 9. Case options

Requesting to suspend case activities for 24 hours

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

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

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

Steps

1. Click the **Cases** tab.
   The **Cases** page is displayed.
2. From the list of cases, select a case that was opened by SupportAssist.

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

   NOTE: The Suspend case activities for 24 hours option is disabled if you have already requested to suspend notifications for the selected support case.
3. From the **Case Options** list, select **Suspend notifications for 24 hours**.
   The **Suspend case activities for 24 hours** window is displayed.
4. (Optional) Type your reason for requesting to suspend activities for the support case.
5. Click **OK**.
   The **Updating Case** message is displayed. After the case is updated successfully, the **Case Updated** message is displayed.
6. Click **OK**.
   The support case displays a **Suspended** status.

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

Related links

Testing the case creation capability

Requesting to resume support activities

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

Steps

1. Click the **Cases** tab.

   The **Cases** page is displayed.
2. From the list of cases, select a case that you had requested for suspending case activities.

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

   NOTE: The Resume support for this case option is enabled only if you had previously requested to suspend notifications for the selected support case.
3. From the **Case Options** list, select **Resume support for the case**.

   The **Resume support for the case** window is displayed.
4. (Optional) Type your reason for requesting to resume activities for the support case.
5. Click **OK**.

   The **Updating Case** message is displayed. After the case is updated successfully, the **Case Updated** message is displayed.
6. Click **OK**.

   The support case displays the appropriate status.

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

Related links

Testing the case creation capability

Requesting to close a support case

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

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

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

Steps

1. Click the **Cases** tab.

   The **Cases** page is displayed.
2. From the list of cases, select a case that was opened by SupportAssist.

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

3. From the **Case Options** list, select **Problem solved – request to close the case**.
   The **Request to close the case** window is displayed.
4. (Optional) Type your reason for requesting to resume activities for the support case.
5. Click **OK**.
   The **Updating Case** message is displayed. After the case is updated successfully, the **Case Updated** message is displayed.
6. Click **OK**.
   The support case displays a **Closure requested** status.

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

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

Related links

Testing the case creation capability

Viewing the device inventory

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

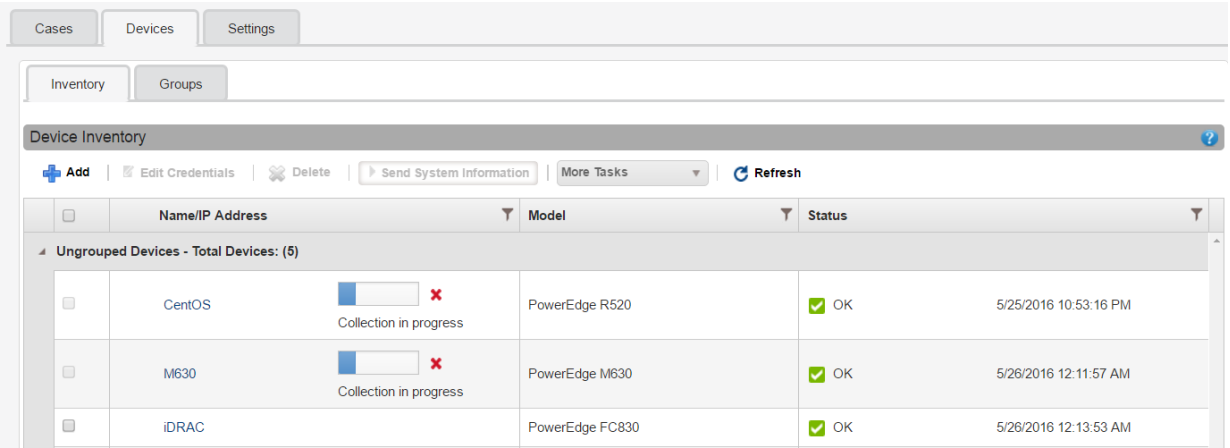

Figure 10. Device Inventory page

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 on the fields and details displayed on the **Device Inventory** page, see Device inventory.

Viewing the device overview

You can view details of a device such as the IP address, device type, model number, Service Tag, collection status, collection history, and so on in the **Device Overview** window. From the **Device Overview** window, you can also access the configuration viewer that allows you to view the data collected from a device by SupportAssist.

1. Click the **Devices** or **Cases** tab.
2. Click the name of a device.

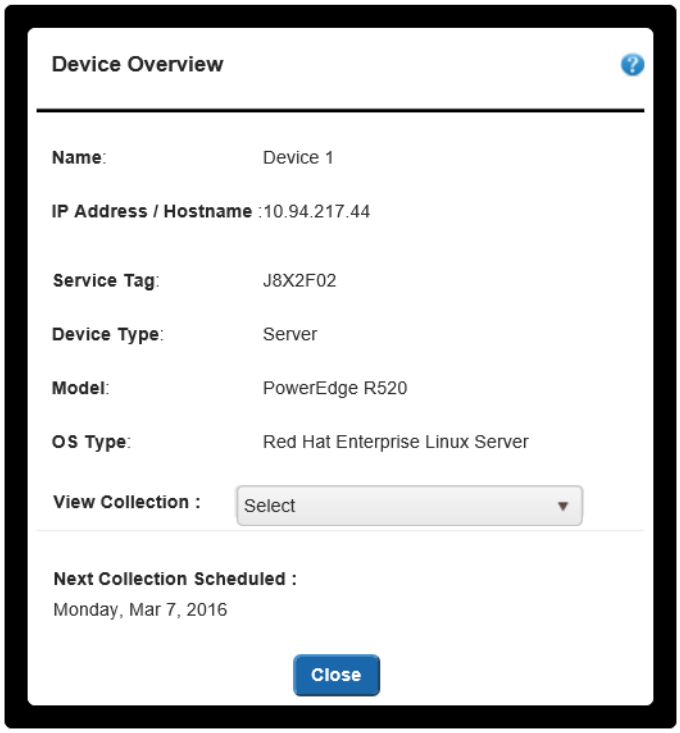

Figure 11. Device Overview

The **Device Overview** window is displayed.

Filtering the displayed data

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

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 depending on the criteria and the column header displays the filtered icon .

Clearing the data filter

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

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

Sorting the displayed data

To sort the data displayed on the **Cases** and **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.

Checking support cases for a specific device

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

Steps

1. Click the **Devices** tab.

   The **Device Inventory** page is displayed.
2. Select the device for which you want to check for support cases.
3. From the **More Tasks** list, select **Check for cases**.

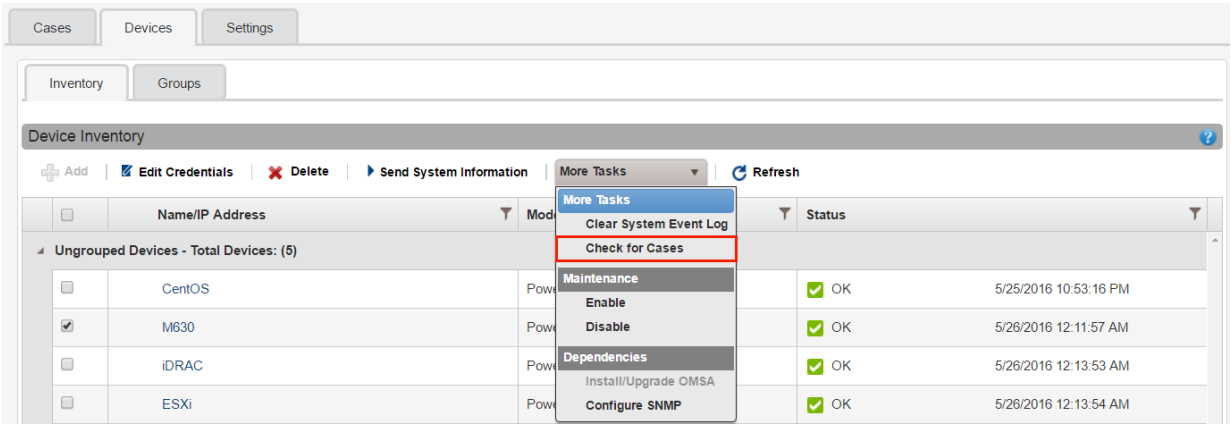

Figure 12. Check for cases

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

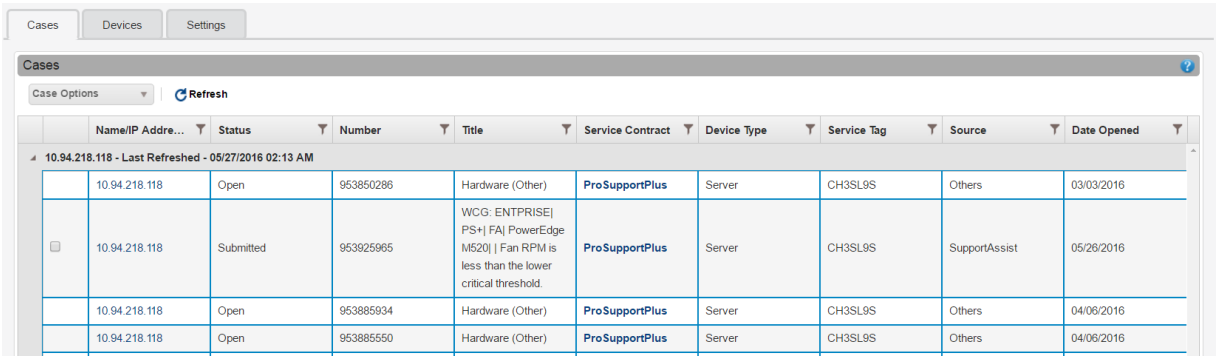

Figure 13. Cases for the device

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

5

Device grouping

The **Device Groups** page on the **Devices** tab allows you to create groups of devices based on your preference. For example, you can create device groups that may include devices based on the following:

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

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

Creating a device group allows you to manage devices as a group. After you create a device group, you can:

- **Manage Devices** — Add or remove devices from the device group.
- **Manage Credentials** — Configure credentials for each device type included in the device group.
- **Manage Contacts** — Configure the contact information and parts dispatch information for the device group.
- **Edit/Delete Group** — Edit the device group details or delete the device group.

NOTE: You can create and manage device groups only if you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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

Related links

Viewing device groups
Creating a device group
Managing devices in a device group
Managing the credentials of a device group
Viewing and updating the contact information of a device group
Editing device group details
Deleting a device group

Viewing device groups

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

1. Click **Devices**.
   The **Device Inventory** page is displayed.
2. Click **Groups**.
   The **Device Groups** page is displayed.

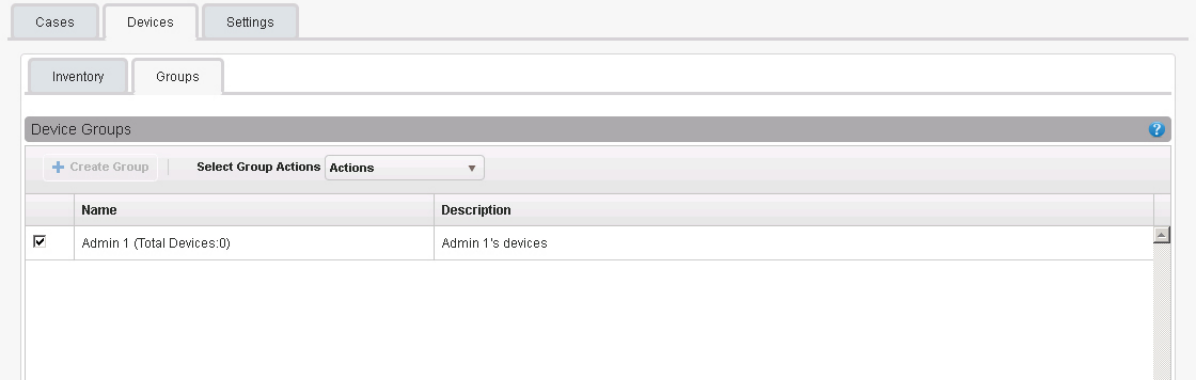

Figure 14. Device Groups page

Creating a device group

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

Steps

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

Managing devices in a device group

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

Prerequisites

- Ensure that you have already created a device group. See Creating a device group.
- Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

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

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

Steps

1. Click the **Devices** tab.
   The **Device Inventory** page is displayed.
2. Click the **Groups** tab.
   The **Device Groups** page is displayed.
3. Select a device group.

4. In the **Select group actions** list, select **Manage Devices**.
   The **Manage Devices** window is displayed.

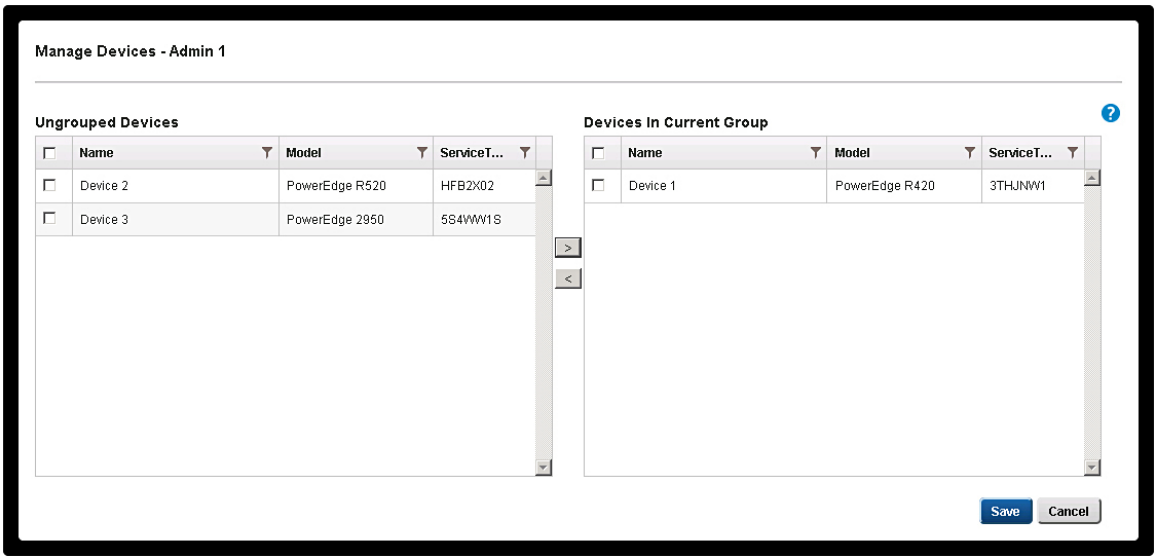

Figure 15. Manage Devices window

5. To add devices to the device group, select the devices in the **Ungrouped Devices** pane, and click > .
   The selected devices are moved to the **Devices In Current Group** pane.
6. To remove devices from the device group, select the devices in the **Devices In Current Group** pane, and click <.
   The selected devices are moved to the **Ungrouped Devices** pane.
7. Click **Save**.

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

Managing the credentials of a device group

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

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

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

Steps

1. Click the **Devices** tab.
   The **Device Inventory** page is displayed.
2. Click the **Groups** tab.
   The **Device Groups** page is displayed.

3. Select a device group.
4. In the **Select group actions** list, select **Manage Credentials**.
   The **Manage Credentials** window is displayed.

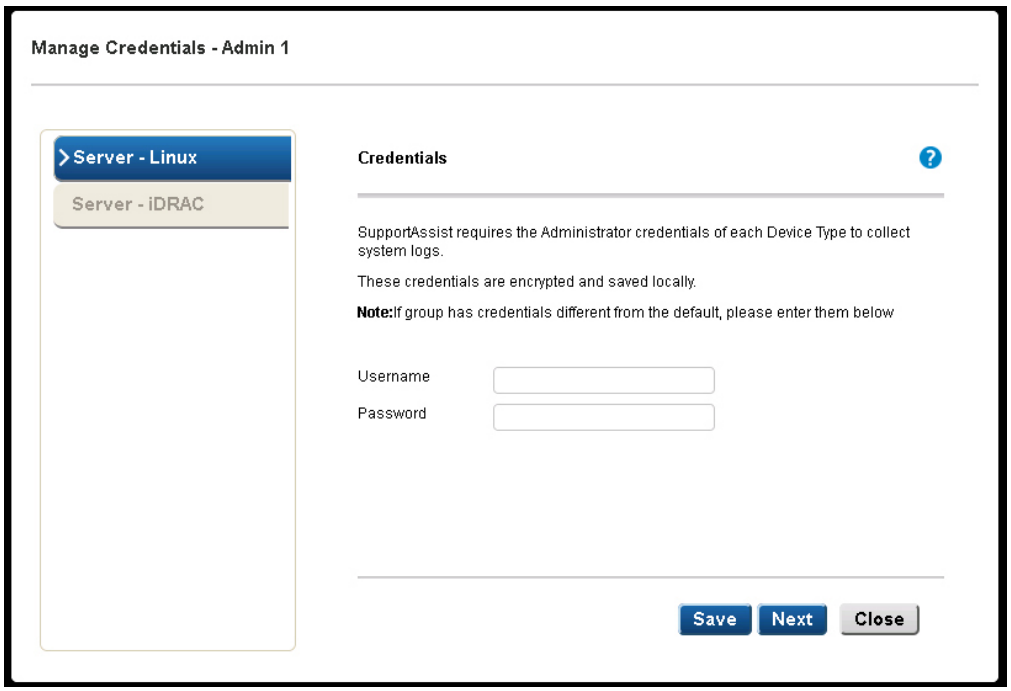

Figure 16. Manage Credentials window

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

Viewing and updating the contact information of a device group

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

NOTE: The device group contact information overrides the default contact information configured through the Settings → Contact Information page. If there is a problem with devices included in a group, SupportAssist sends notifications to the device group contact (not the default contact).

Steps

1. Click the **Devices** tab.
   The **Device Inventory** page is displayed.
2. Click the **Groups** tab.
   The **Device Groups** page is displayed.
3. Select a device group.
4. From the **Select group actions** list, select **Manage Contacts**.

The **Manage Contacts** window is displayed.

5. If you want to use the contact information provided in the **Settings** → **Contact Information** page, select **Use Default**.
6. Select the type of contact:
   - **Primary**
   - **Secondary**
7. Type the first name, last name, phone number, alternate phone number (optional), and email address in the appropriate fields.
8. Select the preferred contact method, preferred contact hours, and time zone.
9. In the **Parts Dispatch (Optional)** section:

   NOTE: The parts dispatch information is optional. If the Dell Technical Support agent determines that a part must be replaced in your system to resolve a support case, the replacement part is dispatched with your consent to the provided address.

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

   a. Type the address and city/town in the appropriate fields.
   b. Select the country.
   c. Type the state/province/region and zip/postal code in the appropriate fields.
10. Click **Save**.

Editing device group details

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

Steps

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

Deleting a device group

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

You can delete device groups based on your preference.

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

Steps

1. Click the **Devices** tab.

The **Device Inventory** page is displayed.

2. Click the **Groups** tab.
   The **Device Groups** page is displayed.
3. Select a device group.
4. From the **Select group actions** list, select **Edit/Delete Group**.
5. In the window that is displayed, click **Delete**.

6

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 more information about the maintenance mode functionality.

Global-level maintenance mode

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

Device-level maintenance mode

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

- **Automated device-level maintenance mode** — By default, if SupportAssist 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** page. 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: When a device is placed automatically in maintenance mode, an email notification is sent to your primary or secondary contact. However, you can receive the email notification for automated device-level maintenance mode only if the SMTP server (email server) settings are configured in SupportAssist. See Configuring SMTP server settings.

- **Manual device-level maintenance mode** — If you have a planned maintenance activity for a device, and do not want SupportAssist 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 functionalities work independent of each other. For example:

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

Enabling or disabling global-level maintenance mode

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

Steps

1. Click the **Settings** tab.

   The **System Logs** page is displayed.
2. Click **Preferences**.

   The **Preferences** page is displayed.
3. In **Maintenance Mode**, depending on your requirement, select or clear the **Temporarily suspend case generation activity (for example, for purposes of downtime, external troubleshooting, etc.)** option.
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 links

Preferences

Enabling or disabling device-level maintenance mode

If you have a planned maintenance activity for a specific device and do not want SupportAssist 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 in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

Steps

1. Click **Devices**.

   The **Devices Inventory** page is displayed.
2. Select a device on the **Device Inventory** page.
3. From the **More Tasks** list, select one of the following:

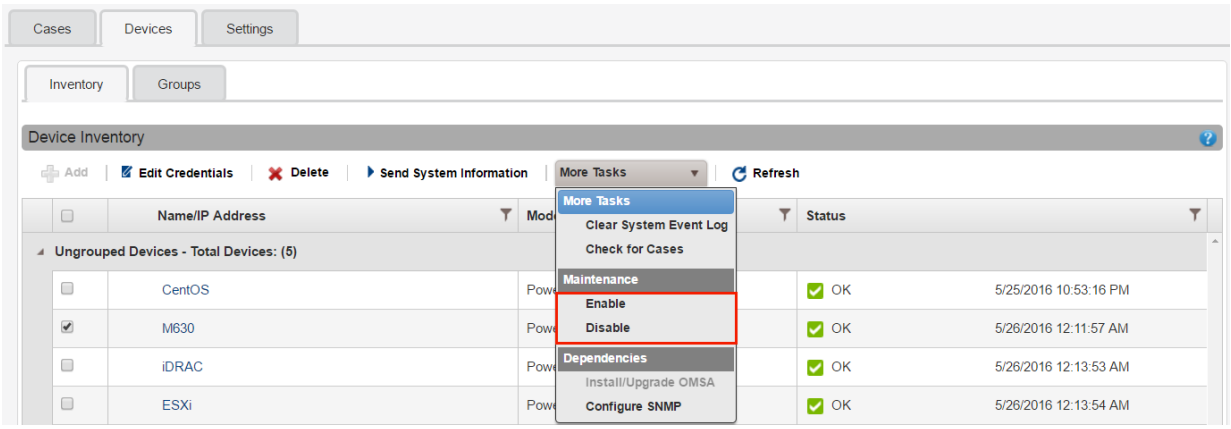

Figure 17. Maintenance mode options

- **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 against the name of the device on the **Device Inventory** page. If you disable maintenance mode for a device, the maintenance mode icon is removed from the **Device Inventory** page.

7

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.
- Perform the case creation test to verify the automatic case creation capability of SupportAssist. See Testing the case creation capability.
- Clear the System Event Log of a server. See Clearing the System Event Log (SEL).
- Upgrade or update SupportAssist. See Automatic 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 in to the device, collect system information, and send it securely to Dell. If the credentials of a device are changed because of your company's security policy or other reasons, you must ensure that the credentials of the devices are updated in SupportAssist.

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

Steps

1. Click the **Devices** tab.
   The **Device Inventory** page is displayed.
2. Select a device on the **Device Inventory** page.
   The **Edit Credentials** link is enabled.

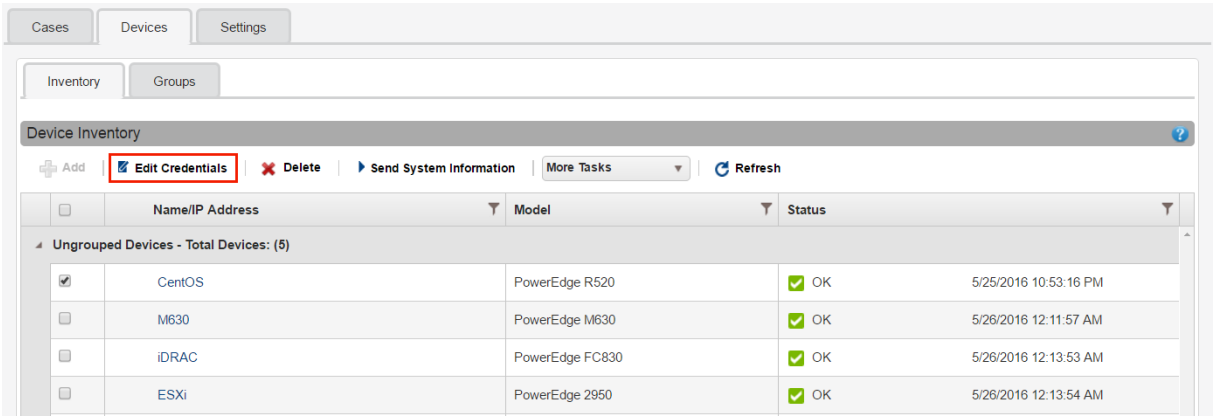

Figure 18. Edit Credentials option

3. Click **Edit Credentials**.

   The **Edit Credentials** window is displayed with the existing user name and password.

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

Related links

Add Device

Installing or upgrading OMSA by using SupportAssist

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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 OMSA** option to automatically download and install the recommended version of OMSA on a device.

NOTE: The SupportAssist recommended version of OMSA may vary depending on the generation of the PowerEdge server and the operating system running on the server. For information on the recommended versions of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.

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

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

Steps

1. Click **Devices**.

The **Devices Inventory** page is displayed.

2. Select the device on which you want to install or upgrade OMSA.

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

3. Click **More Tasks** → **Install/Upgrade OMSA**.

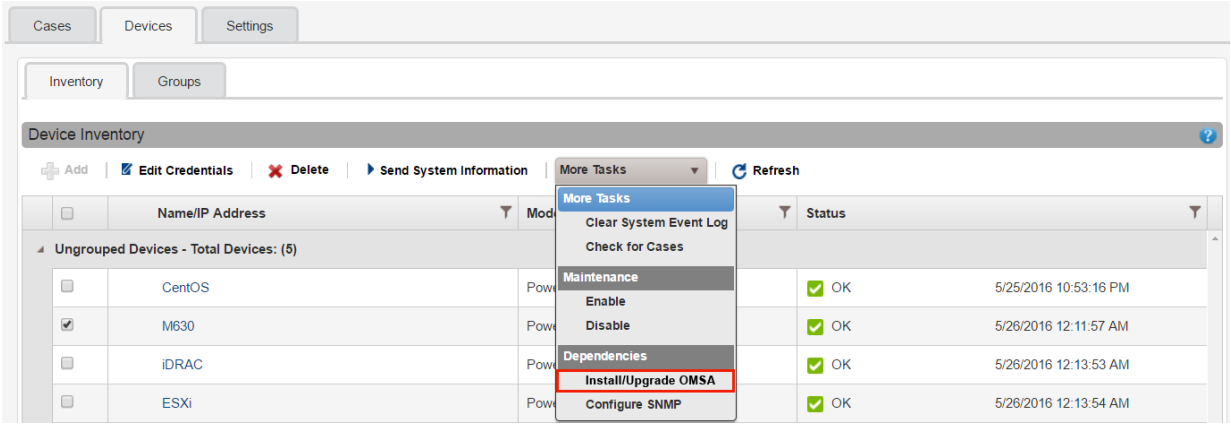

Figure 19. Install/Upgrade OMSA option

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

Related links

Support for automatically installing or upgrading OMSA

Configuring SNMP settings by using SupportAssist

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

Configuring SNMP settings sets the alert destination of a device, and ensures that alerts from the device are forwarded to the server that is running SupportAssist. If the SNMP settings of a device are 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.

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

- Oracle Enterprise Linux
- VMware ESXi
- Oracle Virtual Machine

Steps

1. Click **Devices**.

   The **Devices Inventory** page is displayed.

2. Select the device on which you want to configure the SNMP settings.

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

3. Click **More Tasks** → **Configure SNMP**.

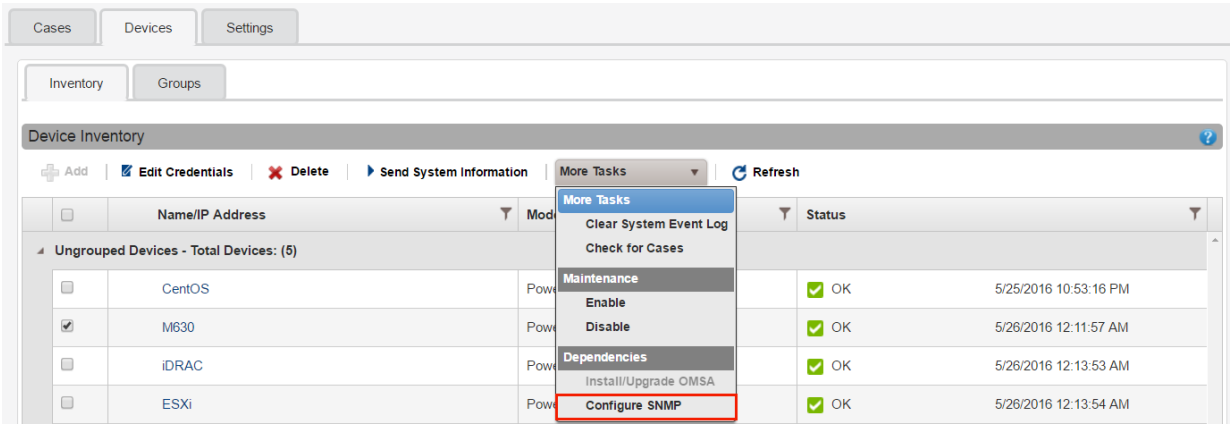

Figure 20. Configure SNMP option

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

Related links

Support for automatically configuring SNMP settings

Viewing and updating the contact information

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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. In the contact details section:
   a. Type or edit the first name, last name, phone number, alternate phone number, and email address.
   b. Select the preferred contact method.
   c. Select the preferred contact hours.
   d. Select the time zone.
5. In the **Parts Dispatch (Optional)** section:
   a. Type or edit the shipping address and city.
   b. Select the country.
   c. Type or edit the state/province/region and zip/postal code.
6. Click **Apply**.

Configuring proxy server settings

If the server on which SupportAssist is installed connects to the Internet through a proxy server, you must ensure that the proxy settings are configured in SupportAssist. 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 in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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), Kerberos, and basic proxy authentication protocols.
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 are required to connect to the proxy server, select **Proxy requires authentication** and then type the user name and password in the corresponding fields.:
   - **User Name** — The user name must contain one or more printable characters, and not exceed 104 characters.
   - **Password** — The password must contain one or more printable characters, and not exceed 127 characters.
6. Click **Apply**.

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

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

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

Related links

Proxy Settings

Connectivity test

The **Connectivity Test** page enables you to verify and test connectivity status to the resources that affect the functionality of SupportAssist. You can use the connectivity tests to verify if SupportAssist is able to connect successfully to the following 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 FTP server
- File upload server hosted by Dell
- SupportAssist server hosted by Dell

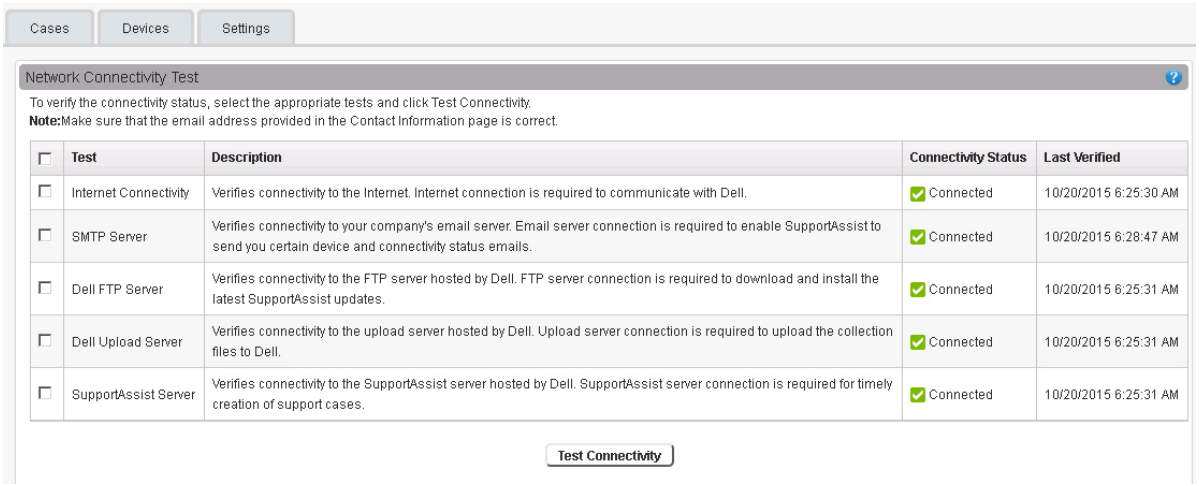

Figure 21. Connectivity Test page

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

NOTE: You can receive the connectivity status email only if you have configured the details of the SMTP server (email server) utilized by your company in SupportAssist. 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

Point to the ***user name*** link, and then click **Connectivity Test**.

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

Performing the connectivity test

1. Point to the ***user name*** 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.

Related links

Connectivity Test

Testing the case creation capability

About this task

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

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

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

Steps

1. Point to the ***user name*** link that is displayed at the top-right of the SupportAssist user interface and click **Test SupportAssist**.
   The **Test SupportAssist** page is displayed.
2. Select the check box for the **Case Creation** test.

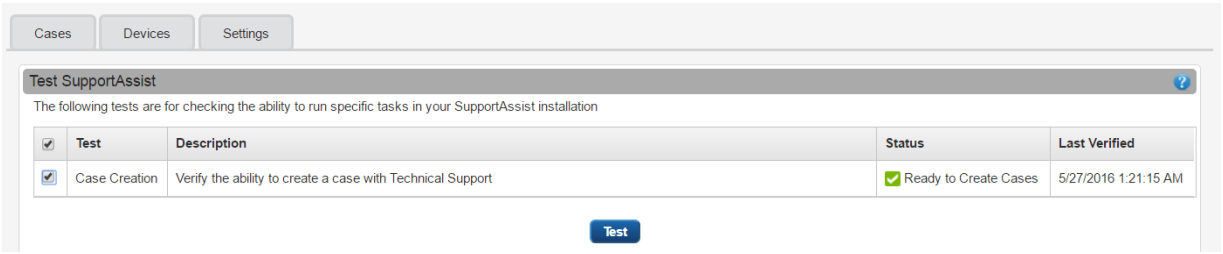

Figure 22. Testing case creation

3. Click **Test**.

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

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

Related links

Test SupportAssist

Clearing the System Event Log (SEL)

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

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

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

Steps

1. Click **Devices**.
   The **Device Inventory** page is displayed.
2. Select a device on the **Device Inventory** page.

   NOTE: If OMSA is not installed on a device that you have added in SupportAssist by using the operating system IP address or host name, the Clear System Event Log option is disabled.

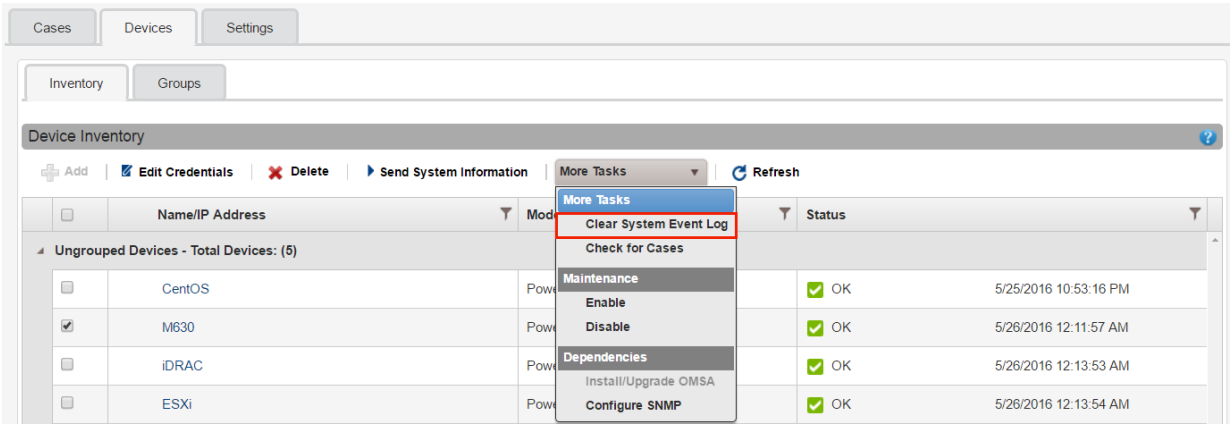

Figure 23. Clear System Event Log option

3. From the **More Tasks** list, select **Clear System Event Log**.
   A message requesting your confirmation is displayed.
4. Click **Yes**.

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

Automatic update

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

The automatic 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 a.m. (date and time as on the server on which SupportAssist is installed).

- If updates are available and automatic update is enabled, the updates are downloaded and automatically installed in the background.
- If updates are available, but automatic 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** option and click **Cancel**, SupportAssist does not display the **Update Available** notification until a newer upgrade is available.

For instructions to enable automatic update, see Enabling automatic update.

The **Update Available** notification is displayed at the top-right of the SupportAssist user interface in the following scenarios:

- If you click **Cancel** in the **An upgrade to SupportAssist is available** notification window
- If an error occurs during the update process

You can click the **Update Available** notification to download and install the updates at any point in 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 user interface.

Information related to the SupportAssist update is logged in the log file located at the following location based on the operating system on which SupportAssist is installed:

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

NOTE: By default, automatic update is enabled. If you disable automatic update, you must manually download and install the latest updates from Dell.com/SupportAssistGroup.

Enabling automatic updates

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

Steps

1. Click the **Settings** tab.
   The **System Logs** page is displayed.
2. Click **Preferences**.
   The **Preferences** page is displayed.
3. In **Automated Tasks**, select **Accept and install updates**.
4. Click **Apply**.

Related links

Preferences

Deleting a device

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

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

Steps

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

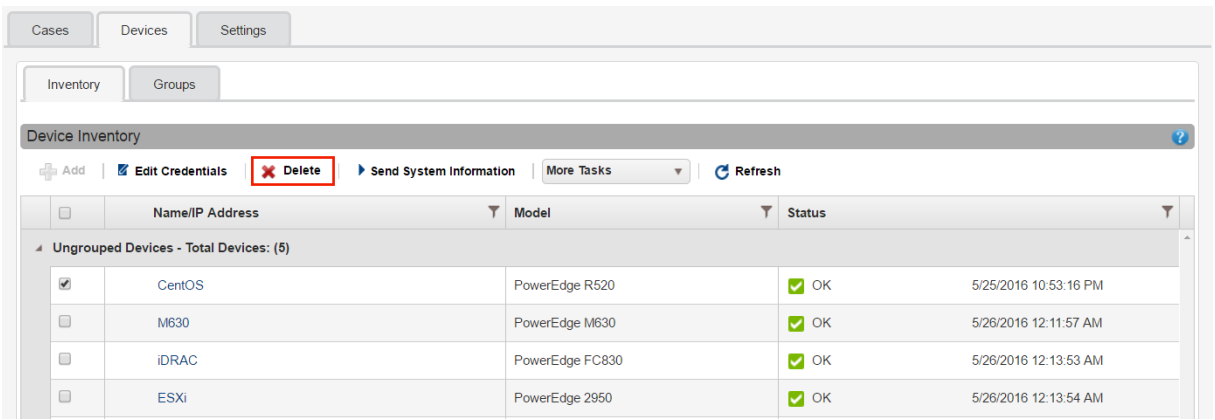

Figure 24. Delete option

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

4. Click **Yes**.

   The device is deleted from the **Device Inventory** page.

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

8

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 preference. For example, you can:

- Disable the case creation email notification and/or select the preferred language for email notifications. See Configuring email notification settings.
- Configure SupportAssist 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 in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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, in **Email Settings**, select **Receive email notification when a new support case is opened**.

   NOTE: Disabling support case email notifications also disables the automatic email notifications that are sent if an issue occurs while:
   - Creating a support case
   - Collecting the system information from a device
   - Sending the system information from a device to Dell
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 links

Preferences

Configuring SMTP server settings

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

If your company utilizes an SMTP server (email server), Dell recommends that you configure the SMTP server settings in SupportAssist. 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 has 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 host name or the IP address of the SMTP server
   - **Port**— the port number of the email server
5. If the SMTP server requires authentication for sending emails, select **Requires authentication**.
6. Type the user name and password in the corresponding fields.
7. To send email notifications securely, select **Use SSL**.
8. Click **Apply**.

Related links

SMTP Settings

9

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 when a support case is created for an issue with the device. If required, you can configure the data collection options based on your preference. For example, you can:

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

Prerequisites for collecting system information

The following are the SupportAssist prerequisites for collecting system information:

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

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

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

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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 on case creation based on your preference.

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. In **Automated Tasks**, depending on your requirement, select or clear the **Start a collection when a new support case is created** option.

   NOTE: By default, the Start a collection when a new support case is created option is selected.
4. Click **Apply**.

Related links

Preferences

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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 preference.

NOTE: Selecting the Enable scheduled system log collection 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 type through the System Logs page. 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. In **Automated Tasks**, depending on your requirement, select or clear the **Enable scheduled system log collection** option.

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

4. Click **Apply**.

Related links

Preferences

Customizing the schedule for periodic collection of system information

Prerequisites

- Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.
- Ensure that the **Enable scheduled system log collection** 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 collection of system information, see Default schedule for collection of system information. If required, you can customize the schedule for periodic collection of system information from monitored devices based on your preference.

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

Steps

1. Click the **Settings** tab.

   The **System Logs** page is displayed.
2. From the **Credential Type** list, select one of the following:
   - **Windows**
   - **Linux**
   - **iDRAC**
   - **ESX**
   - **ESXi**
3. In **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 links

System Logs

Disabling the periodic collection of system information from specific devices

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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 periodic collection of system information from devices of a specific type based on your preference. 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. From the **Credential Type** list, select the credential type for which you want to disable scheduling.
3. In the **System Log Collection Schedule** section, set **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.`

Enabling or disabling the collection of identity information

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

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

- Host name
- IP address
- Subnet mask
- Default gateway
- MAC address
- DHCP server
- DNS server
- Processes
- Environment variables
- Registry
- Logs
- iSCSI data
- Fibre Channel data — host World Wide Name (WWN) and port WWN

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

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

Steps

1. Click the **Settings** tab.
   The **System Logs** page is displayed.
2. Click **Preferences**.
   The **Preferences** page is displayed.
3. In **Identification Information Settings**, depending on your requirement, select or clear the **Include identification information in data sent to Dell** option.

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

NOTE: If you clear the Include identification information in data sent to Dell option, the Include system log in collections option is also cleared automatically. Therefore, the system log is not collected when you disable the collection of identity information.

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

4. Click **Apply**.

Related links

Preferences

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

Steps

1. Click the **Settings** tab.

   The **System Logs** page is displayed.

2. Click **Preferences**.

   The **Preferences** page is displayed.

3. In **Collection Data Settings**, perform the following steps depending on your requirement:
   - Select or clear the **Include software information in collections** option.
   - Select or clear the **Include system log in collections** option.

   NOTE: By default, the Include software information in collections and Include system log in collections options are selected.

   NOTE: For information about the logs that are collected by SupportAssist, see the *Dell SupportAssist Version 1.3 for Servers Reportable Items* documents at Dell.com/ServiceabilityTools.

4. Click **Apply**.

10

Accessing the collected data

The collected system information is saved in the SupportAssist installation folder on the server on which SupportAssist is installed. You can access and view the collected system information by using the configuration viewer that is available in the SupportAssist user interface.

Viewing the collected system information

About this task

SupportAssist collects system information from each monitored device and sends the information securely to Dell. Typically, the system information is collected as follows:

- Periodically — At regular intervals, depending on the configured collection frequency. By default, SupportAssist is configured to collect system information from Dell PowerEdge servers once a month.
- On case creation — When a support case is created for an issue that has been identified by SupportAssist.
- On demand — If requested by Dell Technical Support, you can initiate the collection of system information from a device at any time.

The collected system information is saved in a secured database on the system on which SupportAssist is installed. You can view the collected system information through the configuration viewer available in SupportAssist.

NOTE: You can only view the last 5 system information collections through the configuration viewer. System information collections that are 30 days or older and collections that are older than the last 5 collections within the last 30 days are automatically purged. The purge collections task runs automatically every day at 10 p.m. (time as on the system on which SupportAssist is installed).

Steps

1. Click the **Devices** tab.
   The **Device Inventory** page is displayed.
2. Click the name of a device.
   The **Device Overview** window is displayed.
3. From the **View Collection** list, select a collection date and time.

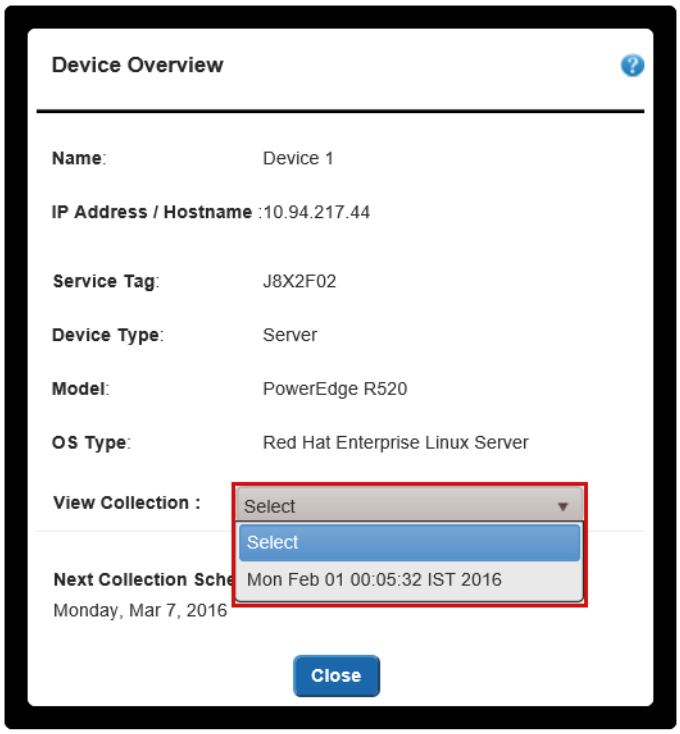

Figure 25. Selecting a collection

The configuration viewer is displayed in a new web browser window.

4. Click a main category listed in the configuration viewer. For example, click **System**.
5. Click a subcategory. For example, click **Main Chassis**.
   Data related to the **Main Chassis** subcategory is displayed.

Configuration Viewer

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

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

NOTE: From SupportAssist version 1.3 onwards, the Configuration Viewer does not support the display of data in the column view format. The Configuration Viewer displays data only in the tree view format.

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

User interface	Description
Left pane	Displays the various categories and sub categories of data in an expanded tree format. A category may display a warning or critical icon to indicate the health status roll-up of its subcategories. When you can click a category, the category is expanded, enabling you to view its sub categories. You can click **Expand All** or **Collapse All** to quickly expand or collapse all categories.
Divider	Is displayed between the left and right panes. You can click and drag the divider to the left or right to increase or decrease the viewable area of the right pane. You can also hide the left pane if necessary. To

User interface	Description
	hide the left pane, click the **<** icon that is displayed at the top of the divider. To view the left pane again, click the **>** icon that is displayed at the top of the divider.
Right pane	Displays the data available for the category or subcategory that is selected in the left pane. This pane includes a navigation trail, which you can click to navigate backward on the current trail.

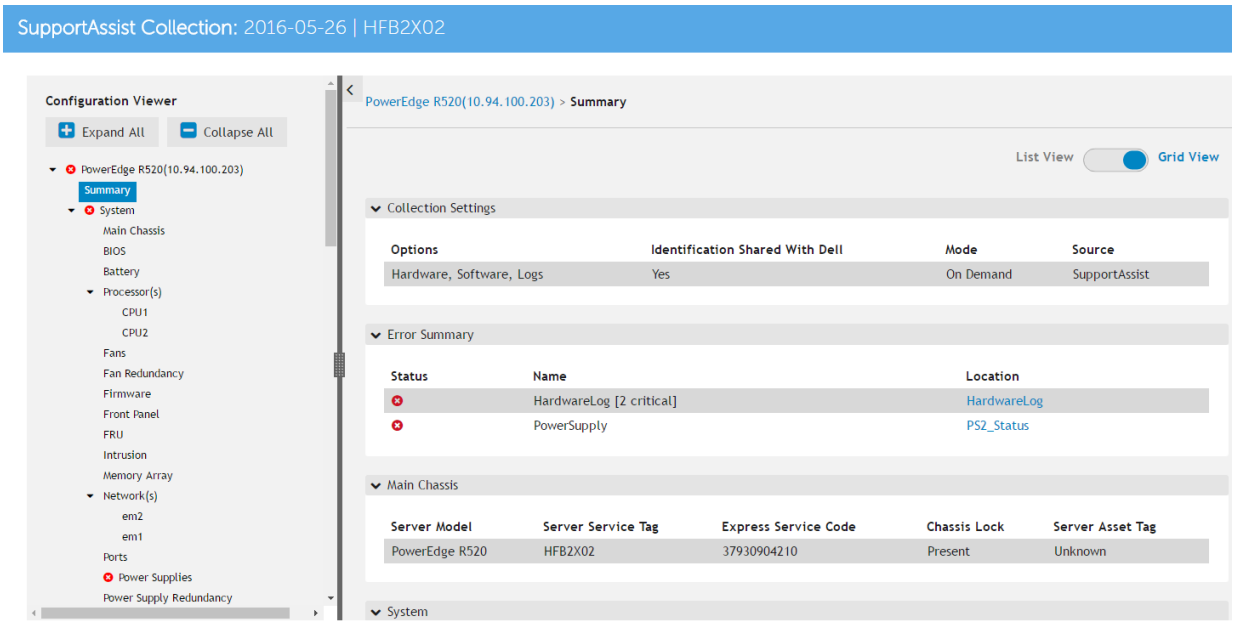

Figure 26. Configuration Viewer

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

NOTE: For a list of items that may be reported in the collected data, see Items reported in periodic collections.

Data views

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

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

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

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

Log types

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

Log types	Description
Structured logs	Contain application logs, Embedded Server Management (ESM) logs, and event logs. When you click the **Structured Logs** category, the configuration viewer displays the list of available structured logs. You can click any of the listed structured logs to view the details of the log in a new web browser window.
Unstructured logs	Contain a snapshot of the system files such as the Remote Access Controller (RAC) logs, Windows event logs, and other logs. When you click the **Unstructured Logs** category, the configuration viewer displays the list of available unstructured logs.

NOTE: Unstructured logs cannot be viewed within the configuration viewer. You can only save the unstructured logs and view the log details using an appropriate application.

Items reported in periodic collections

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

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

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

NOTE: Data in a collection that is triggered by a support case creation and a manually initiated collection is more detailed in comparison with the data collected in a periodic collection. For the complete list of items that are collected by SupportAssist, see the *Dell SupportAssist Version 1.3 for Servers Reportable Items* documents at Dell.com/ServiceabilityTools.

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

Table 5. Items reported in periodic collections

Items reported	Device added in SupportAssist with the operating system IP address (agent-based monitoring)		Device added in SupportAssist with the iDRAC IP address (agentless monitoring)
	OMSA is installed on the device	OMSA is not installed on the device	
Memory	✓	✗	✓
Memory Array	✓	✗	✓
Memory Operating Mode	✓	✗	✗
Memory Redundancy	✓	✗	✗
Slot	✓	✗	✓
Controller	✓	✗	✓
Connector	✓	✗	✗
PCIe-SSD-Extender	✓	✗	✓
Enclosure	✓	✗	✓

Items reported	Device added in SupportAssist with the operating system IP address (agent-based monitoring)		Device added in SupportAssist with the iDRAC IP address (agentless monitoring)
	OMSA is installed on the device	OMSA is not installed on the device	
Array Disk	✓	✗	✓
Intrusion Switch	✓	✗	✓
Hardware Log	✓	✗	✓
Main Chassis	✓	✗	✓
Additional Information	✓	✗	✓
Modular Enclosure Information	✓	✗	✓
Firmware	✓	✗	✓
Processor	✓	✗	✓
Fan	✓	✗	✓
Fan Redundancy	✓	✗	✓
Temperature	✓	✗	✓
Voltage	✓	✗	✓
Power Supply	✓	✗	✓
Power Supply Redundancy	✓	✗	✓
Network	✓	✗	✓
IPv4 Address	✓	✗	✗
IPv6 Address	✓	✗	✗
Network Team Interface	✓	✗	✗
Interface Member	✓	✗	✗
Remote Access Device	✓	✗	✓
DRAC Information	✓	✗	✗

Items reported	Device added in SupportAssist with the operating system IP address (agent-based monitoring)		Device added in SupportAssist with the iDRAC IP address (agentless monitoring)
	OMSA is installed on the device	OMSA is not installed on the device	
Serial Over LAN Configuration	✓	✗	✓
IPv6 Detail	✓	✗	✗
User Setting	✓	✗	✓
User Information	✓	✗	✓
iDRAC User Privilege	✓	✗	✓
DRAC User Privilege	✓	✗	✗
Serial Port Configuration	✓	✗	✓
NIC Configuration	✓	✗	✓
Component Detail	✓	✗	✓
Controller TTY Log	✓	✗	✓
Operating System	✓	✓	✗

11

Using SupportAssist to collect and send system information

SupportAssist automates the detection of hardware issues, creation of support cases, and collection of system information from supported Dell devices. You can also use SupportAssist to manually collect and send system information to Dell.

NOTE: For information on the devices from which SupportAssist can collect and send system information to Dell, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.

This chapter provides information about using SupportAssist to manually collect and send the system information to Dell.

Setting up SupportAssist for collecting and sending system information

About this task

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

NOTE: The following steps are only required if you have not installed SupportAssist. If you have already installed SupportAssist, follow the instructions in Sending the system information manually to manually collect and send the system information to Dell.

Steps

1. Install SupportAssist. See Installing SupportAssist.
2. Register SupportAssist. See Registering SupportAssist.

   SupportAssist is now ready to collect system information from the local system.
3. Add each remote device in SupportAssist. See Adding devices for monitoring.

   NOTE: While adding the device, you may be prompted to allow SupportAssist to install or upgrade OMSA and configure the SNMP settings on the device. Even though installing OMSA and configuring the SNMP settings are not required for collecting system information from the device, Dell recommends that you install OMSA and configure the SNMP settings on the device. System information collected from devices running OMSA contains additional troubleshooting information that may not be available in the data collected from devices that are not running OMSA.

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

Collecting and sending system information

You can perform the following steps to use SupportAssist to collect and send system information from the local system or a remote device to Dell.

Prerequisites

- Ensure that you have completed setting up SupportAssist. See Setting up SupportAssist for collecting and sending system information.
- Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

Steps

1. Click the **Devices** tab.

   The **Device Inventory** page is displayed.

2. Select the local system or a remote device listed in the **Device Inventory** page.

   The **Send System Information** link is enabled.

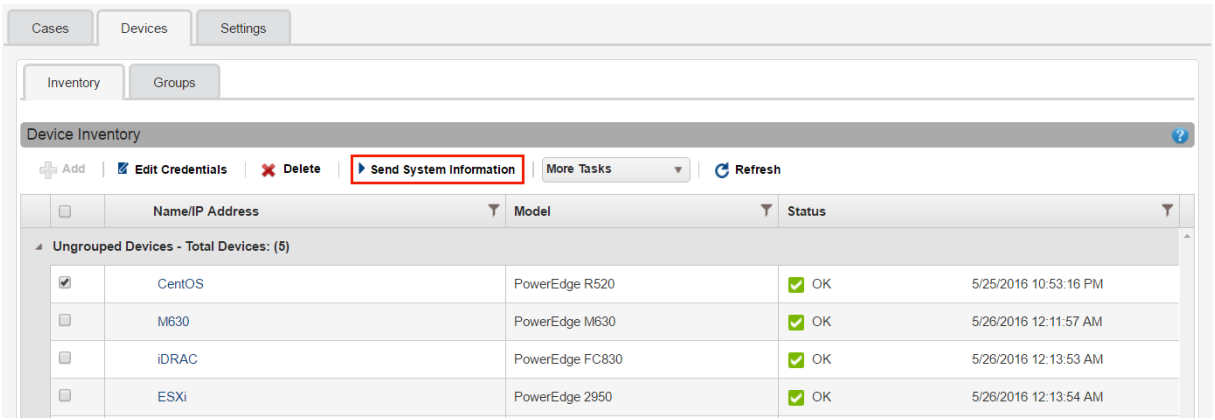

Figure 27. Send System Information option

3. Click **Send System Information**.

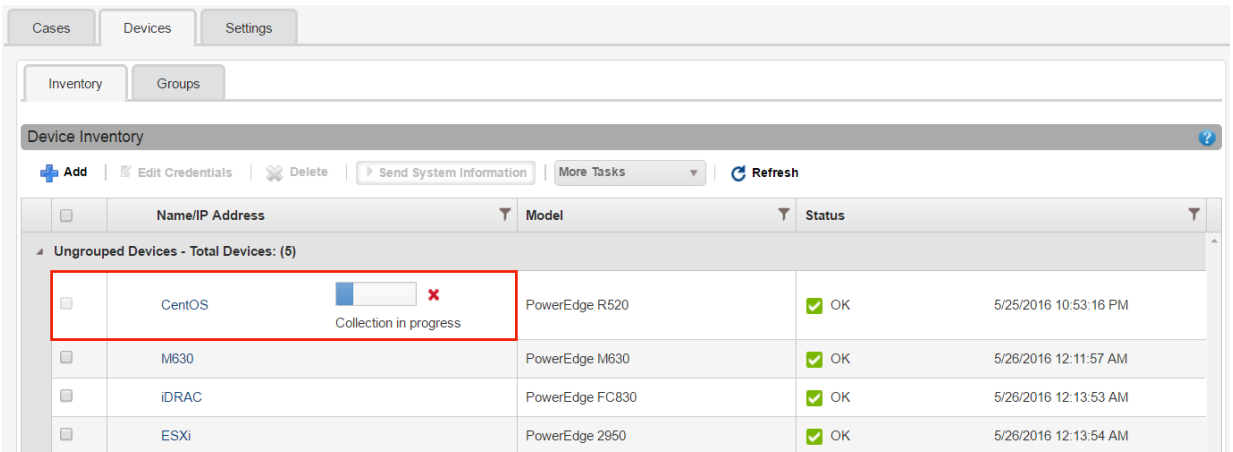

Figure 28. Manual collection in progress

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

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

12

Other useful information

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

SupportAssist user groups

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

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

After the installation of SupportAssist, by default, the operating system user groups specified in the following table are automatically added to the SupportAssist user groups.

Table 6. Operating system user groups that are added to the SupportAssist user groups

Operating system on which SupportAssist is installed	SupportAssistAdmins	SupportAssistUsers
Microsoft Windows	Local Administrators	Users
Windows domain controller	Domain Admins	Domain Users
Linux	root user	—

If you have Administrator privileges (Windows) or root privileges (Linux) on the system, you can add user accounts to the appropriate SupportAssist user groups based on your requirement. Users who are members of the operating system user groups on the system where SupportAssist is installed have the following privileges in SupportAssist:

- If SupportAssist is installed on Windows:
  - Users who are members of the **Administrators** user group have elevated or administrative privileges in SupportAssist.
  - Users who are members of the **Users** user group have normal privileges in SupportAssist.
- If SupportAssist is installed on Linux:
  - Users who are members of the **root** group have elevated or administrative privileges in SupportAssist.
  - Users who are members of the **users** group have normal privileges in SupportAssist.

The following table provides a list of functions that can be performed by the SupportAssist users depending on their privileges.

Table 7. SupportAssist functions and user privileges

SupportAssist functions	SupportAssistAdmins and users with elevated or administrative privileges	SupportAssistUsers and users with normal privileges
View cases and check for cases	✔	✔
Perform case management actions	✔	✘

SupportAssist functions	SupportAssistAdmins and users with elevated or administrative privileges	SupportAssistUsers and users with normal privileges
View the device inventory and device groups	✓	✓
View the collected system information	✓	✓
Perform connectivity tests	✓	✓
Test SupportAssist	✓	✓
Create, manage, edit, or delete device groups	✓	✗
Set up SupportAssist and complete registration through the setup wizard	✓	✗
Add devices	✓	✗
Edit device credentials	✓	✗
Delete devices	✓	✗
Install/upgrade OMSA using the **More Tasks** option	✓	✗
Configure SNMP using the **More Tasks** 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 automatic update	✓	✗
Clear System Event Log	✓	✗
Uninstall SupportAssist	✓	✗

Granting elevated or administrative privileges to users

You can grant elevated or administrative privileges to users by adding them to specific user groups on the system on which SupportAssist is installed. The user groups to which a user must be added to grant elevated or administrative privileges vary depending on the operating system on which SupportAssist is installed.

- If SupportAssist is installed on Windows, you can grant elevated or administrative privileges through one of the following methods:
  - Add the user to the **SupportAssistAdmins** user group. See Adding users to the SupportAssist user groups (Windows).

- Add the user to the Windows **Administrators** user group.

- If SupportAssist is installed on Linux, you can grant elevated or administrative privileges through one of the following methods:
  - Add the user to the **SupportAssistAdmins** user group. See Adding users to the SupportAssist user groups (Linux).
  - Add the user to the Linux **root** group.

Adding users to the SupportAssist user groups (Windows)

Prerequisites

Ensure that you are logged in to the server on which SupportAssist is installed with administrator privileges.

Steps

1. Open the command prompt window.
2. To add an existing user account to a SupportAssist user group, use the following syntax: `net localgroup SupportAssist_user_group_name user_name`.

   For example:

   - To add an existing user account (for example, User1) to the **SupportAssistAdmins** user group, type `net localgroup SupportAssistAdmins User1` and press Enter.
   - To add an existing user account (for example, User2) to the **SupportAssistUsers** user group, type `net localgroup SupportAssistUsers User2` and press Enter.

Adding users to the SupportAssist user groups (Linux)

Prerequisites

Ensure that you are logged in to the server on which SupportAssist is installed with root privileges.

Steps

1. Open the terminal window.
2. To create a new user account and add the user account to a SupportAssist user group, use the following syntax:

   `useradd -G SupportAssist_user_group_name User_name`

   For example:

   - To create a new user account (for example, User1) and add it to the **SupportAssistAdmins** user group, type `useradd -G Supportassistadmins User1` and press Enter.
   - To create a new user account (for example, User2) and add it to the **SupportAssistUsers** user group, type `useradd -G Supportassistusers User2` and press Enter.
3. To add an existing user account to a SupportAssist user group, use the following syntax:

   `usermod -G SupportAssist_user_group_name User_name`

   For example:

   - To add an existing user account (for example, User1) to the **SupportAssistAdmins** user group, type `usermod -G SupportAssistAdmins User1` and press Enter.
   - To add an existing user account (for example, User2) to the **SupportAssistUsers** user group, type `usermod -G SupportAssistUsers User2` and press Enter.

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

Prerequisites

Ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

About this task

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

NOTE: The ProSupport Plus server recommendation reports are applicable only for devices with an active ProSupport Plus entitlement.

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

Steps

1. Click the **Settings** tab.

   The **System Logs** page is displayed.
2. Click **Preferences**.

   The **Preferences** page is displayed.
3. In **Recommendation Report Settings**, select or clear the **Automatically receive recommendation reports via email** option to opt in or opt out from receiving ProSupport Plus server recommendation reports through email.
   - If you select this option, ProSupport Plus server recommendation reports will be sent to your primary contact through email.
   - If you clear this option, ProSupport Plus server recommendation reports will not be sent through email.

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

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 in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

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.

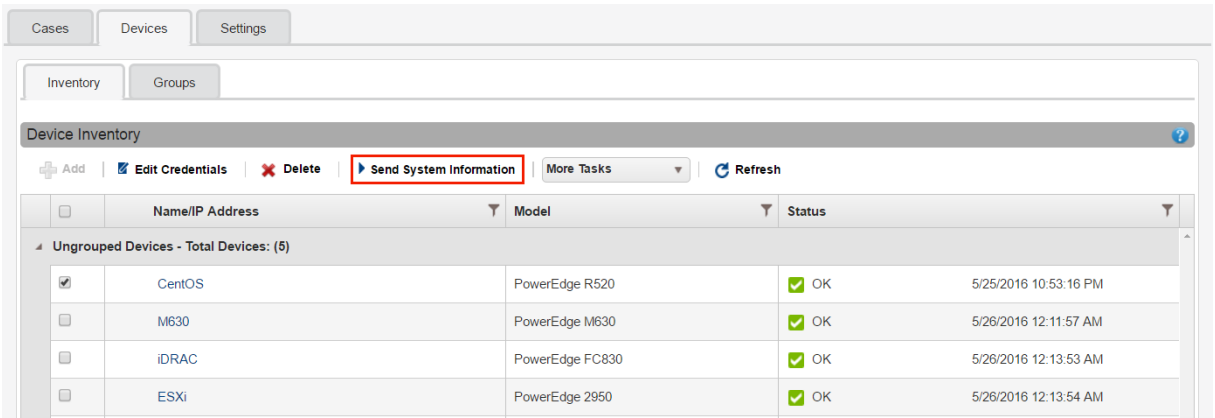

Figure 29. Send System Information option

3. Click **Send System Information**.

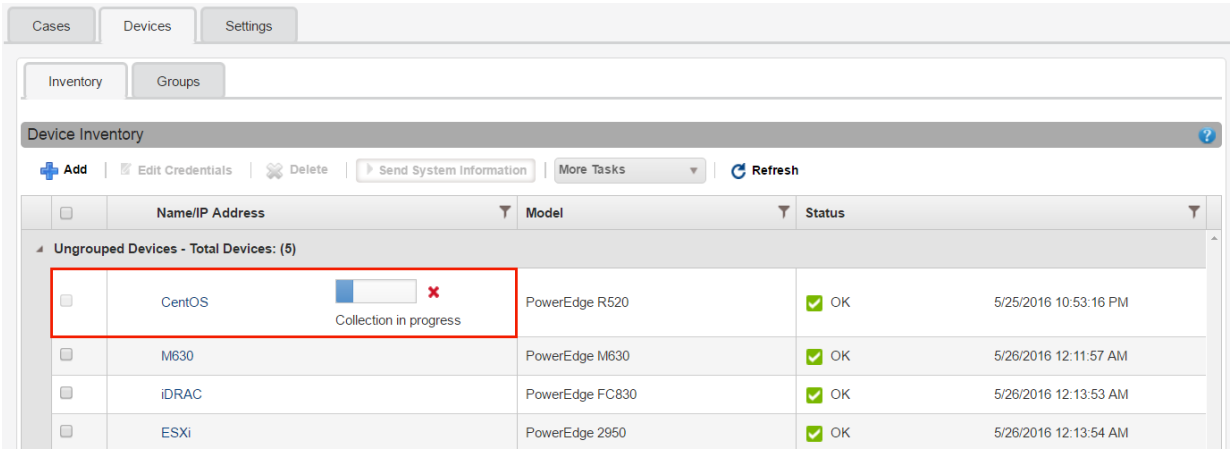

Figure 30. Manual collection in progress

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

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

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.

NOTE: The SupportAssist recommended version of OMSA may vary depending on the generation of the PowerEdge server and the operating system running on the server. For information on the recommended versions of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at 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, 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**.

NOTE: Automatic installation of OMSA through SupportAssist is not supported on devices running Citrix XenServer, VMware ESXi, or ESX. To allow SupportAssist to detect hardware issues on these devices, you must manually download and install OMSA.

Related links

Installing or upgrading OMSA by using SupportAssist

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.

Related links

Configuring SNMP settings by using SupportAssist

Device correlation

You can add (discover) a single device in SupportAssist by using both the host operating system IP address and iDRAC IP address of the device. In such a scenario, the **Device Inventory** page displays two separate listings for the same device. SupportAssist receives alerts from the device through both the operating system and the iDRAC. However, for operational purposes, SupportAssist correlates the operating system IP address and iDRAC IP address of the device and considers the device as a single device. The following are the expected behaviors when a device is correlated:

- Alerts originating from the operating system and the iDRAC are correlated and a support case is created for the Service Tag of the device.
- When system information is collected, both the **Device Inventory** listings display the same status.
- For manual collection of system information — System information is gathered through the selected device listing in the **Device Inventory** page. For example, if the operating system listing is selected, system information is gathered through the operating system. However, if SupportAssist is unable to connect to the device by using the operating system IP address, system information is gathered through the iDRAC.
- For periodic collections and on case creation — System information is typically gathered through the operating system. However, if SupportAssist is unable to connect to the device by using the operating system IP address, system information is gathered through the iDRAC.

Detection of hardware issues in attached storage devices

In addition to monitoring PowerEdge servers, SupportAssist 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. On ProSupport Plus reports, OEM-ready devices are listed with the re-branded name.

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

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

Installing Net-SNMP (Linux only)

Prerequisites
Ensure that you are logged in to the device with a user account that has root privileges.

About this task
SupportAssist receives alerts that are forwarded from remote devices through an SNMP agent. Net-SNMP consists of a suite of SNMP tools, including an SNMP agent. On devices running Linux operating systems, Net-SNMP must be installed to allow SupportAssist to receive alerts.

Steps

1. Open the terminal window on the device running the Linux operating system.
2. Type the following commands based on the operating system:
   - Red Hat Enterprise Linux, CentOS, and VMware ESX: **yum install net-snmp**
   - Oracle Linux: **rpm -ivh net-snmp-x.x-xx.x.x.xxx.x86_64.rpm**, where x.x-xx.x.x.xxx.x represents the version number included in the rpm file name.
   - SUSE Linux Enterprise Server:
     1. **zypper addrepo http://download.opensuse.org/repositories/net-snmp:factory/SLE_12/net-snmp:factory.repo**
     2. **zypper refresh**
     3. **zypper install net-snmp**

Configuring sudo access for SupportAssist (Linux)

In Linux operating systems, users with sudo access may be granted administrative privileges to run certain commands. If you have added a remote device in SupportAssist using the credentials of a sudo user, you must perform the following steps to allow SupportAssist to monitor and collect system information from the device.

Prerequisites
Ensure that you are logged in to the remote device as a user with root privileges.

Steps

1. Open the terminal window.
2. Set the home directory path for the user — Type `useradd user_name -d /home` and press Enter.
3. Open the **/etc/sudoers** file.
4. Insert an exclamation mark [`!`] on the requiretty line. For example, `!requiretty`

5. Add one of the following based on your preference:
   - `%root ALL=(ALL) NOPASSWD: ALL` — To grant permission to all users in the root group.
   - *`user_name`* `ALL=(ALL) NOPASSWD: ALL` — To grant permission to only a specific user.
6. Save the **/etc/sudoers** file.

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.

Table 8. Default collection schedule

Device type	Operating system or component	Schedule
Server	Windows	Monthly; First Monday of the month at 12:00 AM
	Linux	Monthly; First Monday of the month at 12:00 AM
	iDRAC	Monthly; First Monday of the month at 12:00 AM
	ESX	Monthly; First Monday of the month at 12:00 AM
	ESXi	Monthly; First Monday of the month 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.

Table 9. Types of email notifications

Email notification type	When the email notification is sent	Origin of the email notification
Registration confirmation and welcome email	After the **Registration** step of the **Dell SupportAssist Setup Wizard** 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 to send the collected system information from the device to Dell.	SupportAssist server hosted by Dell

Email notification type	When the email notification is sent	Origin of the email notification
Inactive notification	If SupportAssist is not monitoring any device and no device has been added in the past 30 days.	SupportAssist server hosted by Dell
Connectivity test alert	At 11 p.m. each day (date and time as on the server on which SupportAssist is installed). **NOTE: The connectivity test alert notification is sent only if an issue is detected with connectivity to dependent resources.**	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	At 5 p.m. 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. **NOTE: The device alert notification is sent only if an issue exists (warning or error status) with the setup or configuration of the monitored devices.**	SupportAssist application
Case creation connectivity alert	Between 11 p.m. and 4 a.m. each day (date and time as on the server on which SupportAssist is installed). **NOTE: The case creation connectivity alert notification is sent only if an issue is detected with connectivity to dependent resources.**	SupportAssist application

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

NOTE: Email notifications originating from the SupportAssist 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://apidp.dell.com** and **https://api.dell.com** — end point for the SupportAssist server. On the server on which SupportAssist is installed, verify if you can access the following locations using the web browser: **https://apidp.dell.com** and **https://api.dell.com** .
  - **https://is.us.dell.com/FUS/api/2.0/uploadfile** — the file upload server where the collected system information is uploaded.
  - **https://downloads.dell.com/** — for downloading Dell OpenManage Server Administrator (OMSA) and also 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://downloads.dell.com/**
  - On the server on which SupportAssist is installed, verify if port 443 is open for **is.us.dell.com**, **downloads.dell.com**, **apidp.dell.com**, and **api.dell.com**. You can use a telnet client to test the connection. For example, use the following command: `o downloads.dell.com 443`
- On the server 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.

Accessing the SupportAssist application logs

SupportAssist stores system events and log messages in the following locations:

- On Windows:
  - Windows Event Log
  - The installation logs folder (**C:\Program Files\Dell\SupportAssist\logs**).
- On Linux:
  - var logs
  - The installation logs folder (**/opt/dell/supportassist/logs**).

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

- **application.log**
- **application.log.** *20151001*
- **application.log.** *20151002* **.zip**
- **application.log.** *20151003* **.zip**

The log files are purged from storage after 30 days.

The log file contains log messages that correspond to the following values (or higher) in the **log4j.xml** file: FATAL, ERROR, WARN, INFO, and DEBUG, with special values of OFF and ALL. The **log4j.xml** file is available at **C:\Program Files\Dell\SupportAssist\config** (on Windows) and **/opt/dell/supportassist/config** (on Linux). A value of ERROR in the **log4j.xml** file results in log messages of FATAL, and ERROR, since FATAL is a higher level than ERROR.

Event storm handling

SupportAssist intelligently handles event storm conditions, allowing up to nine separate alerts from a monitored device within a 60-minute timespan. However, if 10 or more separate alerts are received from a device, SupportAssist automatically places the device in

maintenance mode. Maintenance mode prevents any further processing of alerts from the device, enabling you to make infrastructure changes without creating unnecessary support cases. After 30 minutes in maintenance mode, SupportAssist automatically removes the device from maintenance mode and resumes normal alert processing for the device. For more information about maintenance mode, see Understanding maintenance mode.

Accessing the context-sensitive help

Context-sensitive help provides information about features and tasks that are applicable to the current view on the user interface. Once you invoke the context-sensitive help, you can navigate or search through the entire SupportAssist help system.

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

Viewing SupportAssist product information

1. Point to the **Help** link that is displayed at the top-right 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

You can uninstall SupportAssist based on your preference. During the uninstallation, you can choose to provide a reason for the uninstallation and also provide feedback to Dell. Your feedback will remain confidential and will allow Dell to make product improvements. The following sections provide information about uninstalling SupportAssist on Windows and Linux operating systems.

Uninstalling SupportAssist (Windows)

Prerequisites

Ensure that you are logged in to the server on which SupportAssist is installed with administrator privileges.

Steps

1. Perform one of the following based on the operating system:
   - On Windows Server 2012, point to the bottom-left corner of the screen, and then click the **Start** icon. On the **Start** screen, click the **Control Panel** tile. On the **Control Panel**, click **Uninstall a program**.
   - On Windows Server 2008 or Windows Small Business Sever 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.

Uninstalling SupportAssist (Linux)

Prerequisites

Ensure that you are logged in to the server on which SupportAssist is installed with root privileges.

Steps

1. Open the terminal window.
2. Browse to the **/opt/dell/supportassist/bin** folder.
3. Type `./uninstall` and press Enter.
4. To continue the uninstallation, type `c`.
5. When prompted for your feedback, perform one of the following:
   - To skip the feedback and start the uninstallation, type `n`.
   - To provide feedback, type `y`.
6. If you selected to provide feedback, press a number that matches your reason for uninstalling SupportAssist.

The **Dell SupportAssist uninstallation is complete** message is displayed.

Uninstalling SupportAssist in silent mode (Linux)

Prerequisites

Ensure that you are logged in to the server on which SupportAssist is installed with root privileges.

Steps

1. Open the terminal window on the system on which SupportAssist is installed.
2. Browse to the **/opt/dell/supportassist/bin** folder.
3. Type **./uninstall silent** and press Enter.

Identifying the generation of a Dell PowerEdge server

You can quickly identify the generation of a PowerEdge server by observing the representation of the server model. The following table provides information about the various generations of PowerEdge servers and their model representation.

Table 10. PowerEdge server examples

PowerEdge server generation	Representation of the server model	Examples of server models
9th	PowerEdge *x*9*xx*	PowerEdge 2900 Power Edge 6950
10th	PowerEdge *yx*0*x*	PowerEdge M600 PowerEdge R300 Power Edge T105
11th	PowerEdge *yx*1*x*	PowerEdge M610 PowerEdge R310 PowerEdge T110
12th	PowerEdge *yx*2*x*	PowerEdge M620 PowerEdge R620 PowerEdge T620
13th	PowerEdge *yx*3*x*	PowerEdge M630 PowerEdge R630 PowerEdge R730

NOTE: In the representation of the server models, *x* denotes numbers (0 to 9) and *y* denotes alphabets such as M, R, and T. The alphabets denote the type of server as follows: M = Modular; R = Rack; T = Tower.

13

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 the system is running a 64-bit operating system.
- On Windows operating systems — Ensure that you right-click the installer package and select **Run as administrator** to start the installation.
- On Linux operating systems — Ensure that the permission of the installer file is updated.
- Ensure that you agree to allow Dell to save your Personally Identifiable Information (PII) on the **License Agreement** page of the installation wizard.
- Ensure that the server on which you are installing SupportAssist for Servers does not have any other SupportAssist application installed already.

SupportAssist registration

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 have provided are valid.
- Verify if port 443 is open on the firewall to access **https://apidp.dell.com** and **https://api.dell.com**.
- Perform **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.
- 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 service.
- Check the log file, **application.log**, available at **C:\Program Files\Dell\SupportAssist\logs** (on Windows) or **/opt/dell/supportassist/logs** (on Linux) to identify the component that failed to load.

Logging in to SupportAssist

If you experience any issues while logging in to SupportAssist:

- Verify if the user account you are using to log in is a member of the **SupportAssistAdmins** or **SupportAssistUsers** user groups:

- Open a command prompt as an administrator and type the following commands: `net localgroup SupportAssistAdmins` and `net localgroup SupportAssistUsers`. If the user account is not listed in the **SupportAssistAdmins** or **SupportAssistUsers** group, add the user account to one of the SupportAssist 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 1.3 for Servers Support Matrix* at 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 operating system details (agent-based monitoring) and the device is running a Windows operating system:
  - Verify if the credentials you provided have administrator rights on the device.
  - Verify if the Windows Management Instrumentation (WMI) service is running on the device.
  - If the issue persists, review the instructions in “Securing a Remote WMI Connection” technical documentation at msdn.microsoft.com.
- If you are adding a device by providing the operating system details (agent-based monitoring) and the device is running a Linux operating system:
  - Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist. For information on configuring the sudo user, see Configuring sudo access for SupportAssist.
  - 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.
- If the error message states that the device could not be added within the predefined time limit, retry adding the device.

- If the error message states that SupportAssist is unable to add the device because the SSL encryption level of the device is set to 256 bit or higher:
  a. Download the Zulu Cryptographic Extension Kit available at the Azul Systems website.
  b. Extract the downloaded file.
  c. Copy the **local_policy.jar** and **US_export_policy.jar** files and paste them at one of the following location on the system on which SupportAssist is installed:
     - On Windows: **C:\Program Files\Dell\SupportAssist\jre\lib\security**
     - On Linux: **/opt/dell/supportassist/jre/lib/security**
  d. Restart the SupportAssist service and retry the operation.

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 in to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.

SNMP not configured

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

- Configure the SNMP settings on the device 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 a  **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 in to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.

Unable to configure SNMP

If a device displays an  **Unable to configure SNMP** status:

- Ensure that the network settings are correct.
- Ensure that the SNMP port (162) is open.
- Ensure that the firewall settings are correct.
- Configure the SNMP settings of the device using the **Configure SNMP** option. See Configuring SNMP settings.

If the SNMP configuration is still unsuccessful, you can manually configure the SNMP. 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 a device displays an **Unable to install OMSA** status:

- 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 remote 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 provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist. For information on configuring the sudo user, see Configuring sudo access for SupportAssist.
  - Ensure that the device has all the required OMSA dependencies installed. For more information about OMSA dependencies, see the "Remote Enablement Requirements" section in the *Dell OpenManage Server Administrator Installation Guide* at DellTechCenter.com/OMSA.
- Retry the installation of OMSA. See Installing or upgrading OMSA.
- If the installation of OMSA cannot be completed successfully even after repeated attempts, log in to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.

NOTE: Upgrade from a 32-bit version of OMSA to a 64-bit version of OMSA is not supported. In this scenario, you must uninstall the existing version of OMSA, and install OMSA 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 in to the device and manually download and install the recommended version of OMSA on the device. For information on the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.

OMSA not supported

If a device may displays the **OMSA not supported** status:

- Log in to the device and uninstall the existing version of OMSA.
- Select the device in the **Devices Inventory**, and then click **Actions** → **Install/Upgrade OMSA**.

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, Dell recommends that you provide the host name of the device (instead of the IP address) while adding the device.

Unable to gather system information

If a device displays an **Unable to gather system information** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Verify if the device is reachable from the server 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 operating system details (agent-based monitoring) and the device is running a Windows operating system:
  - Verify if the credentials you provided have administrator rights on the device.
  - Verify if the WMI service is running on the device.
- If you have added the device by providing the operating system details (agent-based monitoring) and the device is running a Linux operating system:
  - Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist. For information on configuring the sudo user, see Configuring sudo access for SupportAssist.
  - Verify if the SSH service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).
  - Ensure that OpenSSL is updated. For more information, see the resolution for *OpenSSL CCS injection vulnerability (CVE-2014-0224)* available in the support website of the operating system.
- If you 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.
- If the error message states that SupportAssist is unable to gather system information from the device because the SSL encryption level of the device is set to 256 bit or higher:

a. Download the Zulu Cryptographic Extension Kit available at the Azul Systems website.
b. Extract the downloaded file.
c. Copy the **local_policy.jar** and **US_export_policy.jar** files and paste them at one of the following location on the system on which SupportAssist is installed:
   - On Windows: **C:\Program Files\Dell\SupportAssist\jre\lib\security**
   - On Linux: **/opt/dell/supportassist/jre/lib/security**
d. Restart the SupportAssist service and retry the operation.

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

Unable to export collection

If a device displays an **Unable to export collection** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Manually initiate the collection and upload of system information. See Sending the system information manually.

If the problem persists, contact Dell Technical Support for assistance.

Unable to send system information

If a device displays an **Unable to send system information** status:

- Click the error status link in the **Status** column to view the possible resolution steps.
- Verify if the server 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.

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 operating system details (agent-based monitoring) and the device is running a Windows operating system:
  - Verify if the credentials you provided have administrator rights on the device.
  - Verify if the WMI service is running on the device.
  - If the issue persists, review the instructions in “Securing a Remote WMI Connection” technical documentation at msdn.microsoft.com.

- If you added the device by providing the operating system details (agent-based monitoring) and the device is running a Linux operating system:
  - Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist. For information on configuring the sudo user, see Configuring sudo access for SupportAssist.
  - Verify if the SSH service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).

Clearing System Event Log failed

If the device displays a **Clearing System Event Log failed** status, ensure that the following requirements are met and then retry clearing the System Event Log:

- The device is reachable from the server on which SupportAssist is installed.
- If the device is a member of a domain, the host name of the device is added in the DNS server.
- The credentials you have provided for the device in SupportAssist are correct.
- The credentials you have provided for the device in SupportAssist have administrative privileges.
- If you have added the device in SupportAssist with the operating system IP address, ensure that the following requirements are met depending on the operating system running on the device:
  - For Windows, the WMI service is running on the device and the firewall allows WMI communication.
  - For Linux, the SSH service is running on the device and the firewall allows SSH communication.
- If you have added the device in SupportAssist with the iDRAC IP address, the WS-MAN service is running on the device.

If the problem persists, try clearing the System Event Log by using one of the following methods:

- Clearing the System Event Log by using iDRAC
- Clearing the System Event Log by using OMSA

Clearing the System Event Log by using iDRAC

Prerequisites

Ensure that you are logged in to the iDRAC web console with administrative privileges.

About this task

You can perform the following steps to clear the System Event Log by using the iDRAC web console.

NOTE: If you want to clear the System Event Log using the command line interface (CLI), connect to the iDRAC over SSH protocol using any telnet client and run the following command: racadm clrsel

Steps

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

Clearing the System Event Log by using OMSA

Prerequisites

Ensure that you are logged in to OMSA with administrative privileges.

About this task

If OMSA is installed on the device, you can perform the following steps to clear the System Event Log.

NOTE: If you want to clear the System Event Log using the CLI, log in to the device and run the following command from a command prompt (Windows) or terminal (Linux): omconfig system esmlog action=clear

NOTE: If the device is running VMware ESX, log in to OMSA from another remote device using the Server Administrator Managed System Login option, and then perform the following steps.

Steps

1. In OMSA, perform one of the following, depending on the type of server:
   - If the device is a modular server, click **Modular Enclosure** → **Server Module**.
   - If the device is not a modular server, click **System** → **Main System Chassis**.
2. Click the **Logs** tab.
3. Click **Clear Log**.

Maintenance mode

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

- Ensure that the issue with the device is resolved.
- If more time is required to resolve the issue, you may place the device in manual maintenance mode. See Enabling or disabling device-level maintenance mode.
- If required, you may place SupportAssist 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 and 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 "Securing a Remote WMI Connection" technical documentation at msdn.microsoft.com.
- If you are editing the credentials of a device running a Linux operating system:
  - Verify if the credentials you provided have root, super user, or sudo user rights on the device. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist. For information on configuring the sudo user, see Configuring sudo access for SupportAssist.
  - Verify if the Secure Shell (SSH) service is running on the device.
  - Verify if SSH password authentication is enabled (enabled by default).
- If the error message states that SupportAssist is unable to edit the credentials of the device because the SSL encryption level of the device is set to 256 bit or higher:
  a. Download the Zulu Cryptographic Extension Kit available at the Azul Systems website.
  b. Extract the downloaded file.
  c. Copy the **local_policy.jar** and **US_export_policy.jar** files and paste them at one of the following location on the system on which SupportAssist is installed:
     - On Windows: **C:\Program Files\Dell\SupportAssist\jre\lib\security**
     - On Linux: **/opt/dell/supportassist/jre/lib/security**

d. Restart the SupportAssist service and retry the operation.

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.
- Perform the connectivity test and ensure that the connectivity to the SupportAssist server is successful. See Performing the connectivity test.
- Perform the case creation test and ensure that the **Ready to Create Cases** status is displayed. See Testing the case creation capability.
- Check the **application.log** file available at **C:\Program Files\Dell\SupportAssist\logs** (on Windows) or **/opt/dell/supportassist/logs** (on Linux) to identify if the alert was received successfully by SupportAssist.

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 service

If the SupportAssist application does not respond appropriately, ensure that the SupportAssist service is running:

1. On the server on which SupportAssist is installed, verify if the SupportAssist service is running. For information on verifying the status of the SupportAssist service, see Verifying the SupportAssist service status (Windows) or Verifying the SupportAssist service status (Linux).
2. If the service cannot or does not start, open the most recent SupportAssist application log file (**application.log**), and then search for text with a timestamp of when you tried to start the service. The log file may contain a message indicating any user interface startup errors and a possible problem diagnosis.

   NOTE: You can access the SupportAssist application log file (application.log) at the following location depending on the operating system:

   - On Windows — **C:\Program Files\Dell\SupportAssist\logs**
   - On Linux — **/opt/dell/supportassist/logs**
3. To verify 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 is the scenario, check the **application.log** file to find details. If there are no discernible details in the log file, and the server is not reachable, contact Dell Technical Support for assistance.
   - If communication is successful, but no data updates occur, the SupportAssist application may be identifying itself with an ID that is unknown to the server. If this is the scenario, check the **application.log** file to find details. The log file may contain a message stating that the SupportAssist application was not recognized. If the SupportAssist application is not recognized by the SupportAssist server, uninstall and reinstall the SupportAssist application.

Verifying the SupportAssist service status (Windows)

To verify the status of the SupportAssist service on Windows operating systems:

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** displays the status as **Running**.
4. If the service is not running, right-click the service and select **Start**.

Verifying the SupportAssist service status (Linux)

To verify the status of the SupportAssist service on Linux operating system:

1. Open the terminal window on the system on which SupportAssist is installed.
2. Type `service supportassist status` and press Enter.
   The status of the SupportAssist service is displayed.
3. If the service is not running, type `service supportassist start` and press Enter.
   The SupportAssist service is restarted.

Other services

To add a device for agent-based monitoring 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** and click **Start**.

SSH service

You can use the following commands to verify the status of the SSH service and to start the service (if required):

- `service sshd status` — Displays the status of the SSH service.
- `service sshd start` — Starts the SSH service.

Security

If the **Edit Credentials** or **Send System Information** links remain disabled even after selecting a device in the **Device Inventory**, ensure that you are logged in to SupportAssist with elevated or administrative privileges. See SupportAssist user groups and Granting elevated or administrative privileges to users.

14

Error code appendix

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

Table 11. Error code appendix

Error code	Error message	Possible resolution
3000_1 3000_2 3000_3 3000_4 3000_5	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on *device name*.	Do one of the following: • Select the device in the **Devices Inventory**, and then click **Actions** → **Install/Upgrade OMSA**. • Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools. 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.	1. Make sure that the system has internet connectivity. 2. Perform the Connectivity Test and ensure that the system has connectivity to the dependent resources. 3. Select the device in the **Devices Inventory**, and then click **Actions** → **Install OMSA** If the problem persists, contact Dell Technical Support for assistance.
3000_7	Installation of Dell OpenManage Server Administrator (OMSA) is not supported on the operating system running on *device name*.	Do one of the following: • Select the device in the **Devices Inventory**, and then click **Actions** → **Install OMSA**. • Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools. If the problem persists, contact Dell Technical Support for assistance.
3000_8	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on *device name*.	Try to repair the SupportAssist installation: 1. Open **Control Panel**. 2. In **Programs**, click **Uninstall a Program**. 3. In the **Programs and Features** window, select **Dell SupportAssist** and click **Change**. 4. In the **Welcome to Dell SupportAssist Installer** window, click **Next**. 5. Click **Repair** and then click **Install**. If the problem persists, contact Dell Technical Support for further assistance.

Error code	Error message	Possible resolution
3000_10 3000_12 3000_13 3000_14	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on *device name*.	Do one of the following: • Select the device in the **Devices Inventory**, and then click **Actions** → **Install OMSA**. • Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools. If the problem persists, contact Dell Technical Support for assistance.
3000_15 3000_16 3000_17 3000_22 3000_23 3000_29 3000_47 3000_48 3000_50 3000_56 3000_61	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on *device name*.	Make sure that the device is reachable and the configured device credentials have Administrator rights, and then do one of the following: • Select the device in the **Devices Inventory**, and then click **Actions** → **Install OMSA** • Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools If the problem persists, contact Dell Technical Support for assistance.
3000_18	A service required for the installation of Dell OpenManage Server Administrator (OMSA) is either not running or not enabled on *device name*.	• If the device is running Microsoft Windows, make sure that the WMI service is running. • If the device is running Linux, make sure that SSH is enabled. For more information, see Other services.
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 Other services.
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	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on *device name*.	Do one of the following: • Select the device in the **Devices Inventory**, and then click **Actions** → **Install OMSA**. • Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools. If the problem persists, contact Dell Technical Support for assistance.

Error code	Error message	Possible resolution
3000_42 3000_43 3000_44 3000_45 3000_46 3000_49 3000_51 3000_54 3000_55 3000_57 3000_58 3000_59		
3000_52 3000_53	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on *device name*.	Make sure that port 22 is open and SSH is enabled on the system, and then do one of the following: · Select the device in the **Devices Inventory**, and then click **Actions** → **Install OMSA**. · Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools. If the problem persists, contact Dell Technical Support for assistance.
3000_60	An unexpected error occurred during the installation of Dell OpenManage Server Administrator (OMSA) on *device name*.	· Verify if the device is reachable. · Verify if the configured device credentials have Administrator rights. · Select the device in the **Devices Inventory**, and then click **Actions** → **Install OMSA**. · Manually install the recommended version of OMSA. To identify the recommended version of OMSA, see the *Dell SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools. If the problem persists, contact Dell Technical Support for assistance.
3000_62	The time allowed for OMSA installation has expired.	Log on to the device and verify if OMSA is installed. If OMSA is not installed, select the device and click **More Tasks** → **Install/Upgrade OMSA**. 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 that the health of this device is restored for optimal SupportAssist operations.
5000_1	SNMP settings of the device could not be configured because of an unexpected error.	You must either try to configure the SNMP settings through the **More TasksConfigure SNMP** option or manually configure the SNMP settings. For instructions to manually configure the SNMP settings, Configuring the alert destination of an iDRAC using the web interface.

Error code	Error message	Possible resolution
5000_2	SNMP settings of the device could not be configured because the integrated Dell Remote Access Controller (iDRAC) does not have the required license installed.	Make sure that iDRAC has an Enterprise or Express license installed, and then try to configure the SNMP settings through the **More Tasks** → **Configure SNMP** 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 Configuring the alert destination of an iDRAC using the web interface.
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 **More Tasks** → **Configure SNMP** 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 iDRAC is reachable from the system on which SupportAssist is installed, and then try to configure the SNMP settings through the **More Tasks** → **Configure SNMP** 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 **More Tasks** → **Configure SNMP** option. If the problem persists, contact your system administrator for assistance.
5000_7 5000_8	SNMP settings of the device could not be configured because of an unexpected error.	You must manually configure the SNMP settings of the device. For instructions to manually configure the SNMP settings, see Configuring the alert destination of an iDRAC using the web interface.
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 Manually configuring the alert destination (Windows) or Manually configuring the alert destination (Linux).
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 **More Tasks** → **Configure SNMP** 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 *SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.
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 **More Tasks** → **Configure SNMP** 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 **More Tasks** → **Configure SNMP** option.

Error code	Error message	Possible resolution
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.
SA-0005	SupportAssist is unable to add the *device name* because an attempt to connect to the device is unsuccessful.	Make sure that both the system running SupportAssist and the device you are trying to add are connected to the network, and then retry adding the device.
SA-0010	SupportAssist is unable to add the *device name* because the entered host name or IP address is incorrect.	Retry adding the device with the correct host name or IP address.
SA-0015	SupportAssist is unable to add the *device name* because an unknown error occurred while discovering the device.	Verify the following and then retry adding the device: • Make sure that the device is supported by SupportAssist. For the list of supported device models, see the *SupportAssist Version 1.3 for Servers Support Matrix* atDell.com/ServiceabilityTools. • Make sure that the user account has administrator/root privileges.
SA-0020	SupportAssist is unable to add the *device name* because the device is already added.	Not applicable.
SA-0025	SupportAssist is unable to add the *device name* because of an unknown error.	Verify if the device is supported by SupportAssist. For the list of supported device models, see the *SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools. If the problem persists, contact Dell Technical Support for assistance.
SA-0030	SupportAssist is unable to add the *device name* because the User Name or Password is incorrect.	Verify the device information, ensure that the user account has administrator/root privileges, and then retry adding the device. If the problem persists, contact your network administrator for assistance.
SA-0040	SupportAssist is unable to add the *device name* because the Display Name is already in use by another device.	Retry adding the device with any other Display Name.
SA-0045	Identification or cancellation for this device is already in progress.	N/A
SA-0050	SupportAssist is unable to add the *device name* because of an unknown error.	Verify if the device is supported by SupportAssist. For the list of supported device models, see the *SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.
SA-0055	SupportAssist is unable to add the *device name* because the device is not supported.	For the list of supported device models, see the *SupportAssist Version 1.3 for Servers Support Matrix* at Dell.com/ServiceabilityTools.
SA-0060	SupportAssist is unable to add the *device name* because a required file has either been deleted or moved.	Restart the Dell SupportAssist service on the system running SupportAssist, and then retry adding the device.
SA-0065	SupportAssist is unable to add the *device name* because the entered credentials do not have superuser privileges.	Enter the credentials that have superuser privileges, and then retry adding the device.

Error code	Error message	Possible resolution
SA-0070	Installation of Dell OpenManage Server Administrator (OMSA) is not supported on this device	Not applicable.
SA-0075	SupportAssist has detected that Dell OpenManage Server Administrator (OMSA) is not installed on the device. Installing OMSA is required to generate alerts for hardware events that occur on the device.	Not applicable.
SA-0080	SupportAssist has detected that the Dell OpenManage Server Administrator (OMSA) services are not running on the device.	For optimal SupportAssist capability, you must restart the OMSA services.
SA-0085	SupportAssist has detected that Dell OpenManage Server Administrator (OMSA) version *x.x* is installed on the device.	For optimal SupportAssist capability, Dell recommends that you upgrade OMSA to version *x.x*.
SA-0090	SupportAssist has detected that Dell OpenManage Server Administrator (OMSA) version *x.x* is installed on the device.	It is recommended that you download and install OMSA version *x.x* on the device.
SA-0095	SupportAssist is unable to verify the OMSA version installed on the device.	To resolve the issue, see Unable to verify OMSA version
SA-0100	The recommended version of Dell OpenManage Server Administrator (OMSA) is already installed on the device.	Not applicable.
SA-0105	SupportAssist will monitor the device through the integrated Dell Remote Access Controller (iDRAC). Therefore, installation or upgrade of Dell OpenManage Server Administrator (OMSA) is not required.	Not applicable.
SA-0110	SupportAssist is unable to add the *device name* because it does not have a valid license.	Make sure that the iDRAC has a valid Enterprise or Express license, and then retry the operation.
SA-0115	SupportAssist is unable to add the *device name* because the operating system is not supported.	Not applicable.
SA-0120	SupportAssist is unable to add the device because a required service is disabled on the *device name*.	Make sure that the required service is running on the device, and then retry adding the device. For information on the required service, see Other services.
SA-0125	SupportAssist is unable to add the *device name* because a response was not received within the predefined time limit.	Try adding the device again. For additional troubleshooting information, see Unable to add the device.
SA-0130	SupportAssist is unable to add the *device name* because the SSL encryption level of the device is set to 256 bit or higher.	For troubleshooting steps, see Unable to add the device.
SA-1005	SupportAssist is unable to edit the credentials of the device because an attempt to connect to the device is unsuccessful.	Make sure that both the system running SupportAssist and the device are connected to the network, and then retry the operation.
SA-1010	SupportAssist is unable to edit the credentials of the device name because of an unexpected error.	Verify the following and then retry editing the device credentials: • Make sure that the required services are running on the device. For information on the required services, see the Online Help.

Error code	Error message	Possible resolution
		• Make sure that the entered credentials have administrator or root privileges.
SA-1015	SupportAssist is unable to edit the credentials of the device name because the user name or password is incorrect.	Verify the user name and password, ensure that the user account has administrator/root privileges, and try again. If the problem persists, contact your network administrator for assistance.
SA-1025	SupportAssist is unable to edit the credentials of the device name because the entered Display Name it is already in use by another device.	Enter any other Display Name, and then retry editing the device credentials.
SA-1030	SupportAssist is unable to edit the device credentials because the entered credentials do not have superuser rights.	Enter the credentials that have superuser rights, and then retry editing the device credentials.
SA-1035	SupportAssist is unable to update the device credentials because a required service is disabled on the device.	Make sure that the required services are running on the device, and then retry editing the device credentials. For information on the required services, see Other services.
SA-1040	SupportAssist is unable to edit the credentials of the *device name* because the SSL encryption level of the device is set to 256 bit or higher.	For troubleshooting steps, see Unable to edit device credentials.
SA-2000	SupportAssist is unable to establish connections required to auto create cases with Dell Technical Support.	Perform the connectivity test and ensure that the internet connectivity is successful.
SA-2001 SA-2002 SA-2003 SA-2004	SupportAssist is unable to establish connections required to auto create cases with Dell Technical Support.	Not applicable.
SA-4015 SA-4020 SA-4025 SA-4030 SA-4035 SA-4045 SA-4050 SA-4055 SA-4065 SA-4070 SA-4071 SA-4072	SupportAssist is unable to collect system information from the *device name* because of an unknown error.	To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact Dell Technical Support for assistance.
SA-4040 SA-4073 SA-4074	SupportAssist is unable to package the system information collected from the *device name* because of an unknown error.	To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact Dell Technical Support for assistance.
SA-4075 SA-4080	SupportAssist is unable to collect system information from the *device name* because an attempt to connect to the device is unsuccessful.	• Make sure that WMI service is running on the device. • To retry collecting the system information, select the device and click **Send System Information**.

Error code	Error message	Possible resolution
SA-4085 SA-4090 SA-4110 SA-4115 SA-4120 SA-4125 SA-4130 SA-4135 SA-4140 SA-4145 SA-4150 SA-4175	SupportAssist is unable to collect system information from the *device name* because an attempt to connect to the device is unsuccessful.	To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact Dell Technical Support for assistance.
SA-4095 SA-4100 SA-4105		• Make sure that the SSH service is running on the device. • To retry collecting the system information, select the device and click **Send System Information**.
SA-4155	SupportAssist is unable to collect system information from the *device name* because the device is not reachable.	• Make sure that the device is reachable from the server running SupportAssist. • To retry collecting the system information, select the device and click **Send System Information**.
SA-4160	SupportAssist is unable to collect system information from the *device name* because the IP address of the device is invalid.	• Make sure that SupportAssist is updated with the correct IP address of the device. • To retry collecting the system information, select the device and click **Send System Information**.
SA-4165	SupportAssist is unable to collect system information from the *device name* because the download of a certificate file could not be completed successfully.	• Verify the firewall and network settings to make sure that download of the certificate file is not blocked. • To retry collecting the system information, select the device and click **Send System Information**.
SA-4170	SupportAssist is unable to collect system information from the *device name* because the credentials of the device are either incorrect or do not have the required privileges.	• Make sure that SupportAssist is updated with the correct user name and password of the device. • Make sure that the user account has administrator or root privileges on the device. • To retry collecting the system information, select the device and click **Send System Information**.
SA-4180	SupportAssist is unable to collect system information from the *device name* because the device is not supported.	For the list of supported device models, see the *SupportAssist Version 1.3 for Servers Support Matrix* atDell.com/ServiceabilityTools.
SA-4185	SupportAssist is unable to collect system information from the *device name* because of an attempt to connect to the device is unsuccessful.	• Make sure SupportAssist is updated with the credentials of a user account that has root privileges. See Configuring sudo access for SupportAssist (Linux) • To retry collecting the system information, select the device and click **Send System Information**.
SA-4190	SupportAssist is unable to gather system information from the *device name* because the SSL encryption level of the device is set to 256 bit or higher.	For troubleshooting steps, see Unable to gather system information.

Error code	Error message	Possible resolution
SA-4500	SupportAssist is unable to send the collected system information from the *device name* because the receiving server hosted by Dell is unreachable.	To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact Dell Technical Support for assistance.
SA-4501 SA-4502	SupportAssist is unable to collect system information from the *device name* because of an unknown error.	To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact Dell Technical Support for assistance.
SA-4511 SA-4512	SupportAssist is unable to send the collected system information from the *device name* because of an unknown error.	• Perform **Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful. • To retry collecting the system information, select the device and click **Send System Information**.
SA-4513	SupportAssist is unable to send the collected system information from the *device name* because of an invalid file token.	• Perform **Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful. • To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact Dell Technical Support for assistance.
SA-4514	SupportAssist is unable to send the collected system information from the *device name* because the collection file is corrupted.	• Perform **Connectivity Test** and make sure that connectivity to the **Dell Upload Server** is successful. • To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact Dell Technical Support for assistance.
SA-4521	SupportAssist is unable to send the collected system information from the *device name* because the proxy server is not reachable.	• Verify the proxy server settings in SupportAssist. • Make sure that the proxy server is reachable. • To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact your network administrator for assistance.
SA-4522	SupportAssist is unable to send the collected system information from the *device name* because an attempt to connect to proxy server is unsuccessful.	• Verify the proxy server settings in SupportAssist. • Make sure that the proxy server is reachable. • To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact your network administrator for assistance.
SA-4523	SupportAssist is unable to send the collected system information from the *device name* because the proxy server user name or password is incorrect.	• Make sure that the proxy server user name and password you have entered in SupportAssist are correct. • To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact your network administrator for assistance.

Error code	Error message	Possible resolution
SA-4524	SupportAssist is unable to send the collected system information from the *device name* because of an unknown error with reaching the proxy server.	• Verify the proxy server settings in SupportAssist. • Make sure that the proxy server is reachable. • To retry collecting the system information, select the device and click **Send System Information**. If the problem persists, contact your network administrator for assistance.
SA-4550	SupportAssist is unable to collect system information from the *device name* because the hard-drive space available on the server on which SupportAssist is installed has become critically low.	For information about the hard-drive space requirements for a SupportAssist environment, see Hardware requirements.

15

Dell SupportAssist user interface

The SupportAssist user interface displays the following tabs:

- **Cases** — Displays the support cases that are present for the devices that are monitored by SupportAssist
- **Devices** — Displays the devices that you have added in SupportAssist
- **Settings** — Allows you to configure SupportAssist

At the top-right of the SupportAssist header area, you can access links that allow you to perform certain tasks. The following table describes the links that you can access.

Table 12. Links in the SupportAssist header area

Link	Description
SupportAssist Community	Opens the SupportAssist community website in a new browser window.
Help	Point to the **Help** link to view a drop-down list that contains the following options: · **Help** — Opens the **Help** window that provides links to Dell technical support and product manuals. · **About** — Opens the **About** window that provides information about the SupportAssist version, copyright information, and also notifies if a newer version of SupportAssist is available.
User name	Displays the user name of the currently logged in user. Point to the ***user name*** link to view a drop-down list that contains the following links: · **Connectivity Test** — Opens the **Connectivity Test** page. · **Test SupportAssist** — Opens the **Test SupportAssist** page. · **Logout** — Allows you to log out of SupportAssist. **NOTE: The Connectivity Test and Test SupportAssist links are enabled only if you are logged in to SupportAssist with administrative or elevated privileges.**
Update Available	Displays, in the SupportAssist header area, in the following situations: · If an error occurred during the update of SupportAssist. · If the **Settings** → **Preferences** → **Accept and install updates** is not selected, and you cancel the **SupportAssist Update** notification that is displayed. You can click the link to download and install the SupportAssist update. **NOTE: The Update Available link is displayed only if you are logged in to SupportAssist with administrative or elevated privileges.**

Related links

Setup Wizard
Login
Cases
Device Inventory
Settings
Connectivity Test
Test SupportAssist

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 links

Welcome
Proxy Settings
Registration
Summary
Registering SupportAssist

Welcome

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

Proxy Settings

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

NOTE: The Proxy Settings page is displayed only if you confirm that the system connects to the Internet through a proxy server.

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

Table 13. Proxy Settings

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

Registration

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

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

Table 14. Registration

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

Summary

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

Login

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

Table 15. Login

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

Related links

Logging in to SupportAssist

Cases

The **Cases** page displays the support cases that are present for the devices that are monitored by SupportAssist. For Service Tags with a ProSupport or ProSupport Plus entitlement that are monitored by SupportAssist, the **Cases** page displays the case status irrespective of the case creation method. By default, the displayed support cases are grouped under the respective device name or device IP address. The last refreshed date and time that is displayed in the group header indicates when the case information was last retrieved from Dell.

The **Case Options** list enables you to manage support cases that are opened by SupportAssist based on your requirement. The following are the available options:

NOTE: Only support cases that were opened by SupportAssist can be managed by using the Case Options list.

- **Suspend notifications for 24 hours** — To request Dell Technical Support to suspend activities related to a support case for 24 hours. After 24 hours, Dell Technical Support automatically resumes activities related to the support case.
- **Resume support for this case** — To request Dell Technical Support to resume activities related to a support case.

  NOTE: The Resume support for this case option is enabled only if you had previously requested to suspend activities related to a support case.

- **Problem solved — request to close this case** — To request Dell Technical Support to close a support case.

The **Refresh** link enables you to refresh the case list.

The following table describes the support case information for your Dell devices that are monitored by SupportAssist, as displayed in the **Cases** page.

Table 16. Cases

Column	Description
Check box	Use to select a support case for performing case management actions. **NOTE: The check box is displayed only for cases that are automatically created by SupportAssist.**
Name/IP Address	Displays the display name, host name, or IP address depending on the information that was provided while adding the device. The device name is displayed as a link that you can click to open the **Device Overview** page.
Status	The current state of the support case. The status of a support case may be: · **Submitted** — SupportAssist has submitted the support case. · **Open** — Dell Technical Support has opened the submitted support case. · **In Progress** — Dell Technical Support is working on the support case. · **Customer Deferred** — Dell Technical Support has deferred the support case at the customer's request. · **Reopened** — The support case was previously closed, and has been reopened. · **Suspended** — Dell Technical Support has suspended activities related to the support case for 24 hours based on your request. · **Closure Requested** — You have requested Dell Technical Support to close the support case. · **Closed** — The support case is closed. · **Case Not Created** — An issue was detected by SupportAssist, but a support case was not created because the device has either an expired warranty or Basic Hardware warranty. · **Unavailable** — The support case status could not be retrieved from Dell. · **Unknown** — SupportAssist is unable to determine the status of the support case.
Number	The numeric identifier assigned to the support case.
Title	The support case name, which identifies: · Support case generation method · Device model · Device operating system · Alert ID, if available · Alert description, if available · Warranty status · Resolution description
Service Contract	The Dell service contract level under which the device is covered. The **Service Contract** column may display: · **Unknown** — SupportAssist cannot determine the service contract. · **Invalid Service Tag** — The Service Tag of the device is invalid. · **No Service Contract** — This device is not covered under a Dell service contract. · **Expired Service Contract** — The service contract of the device has expired. · **Basic Support** — The device is covered under a Dell Basic Hardware service contract. · **ProSupport** — The device is covered under a Dell ProSupport service contract.

Column	Description
	• **ProSupport Plus** — The device is covered under a Dell ProSupport Plus service contract.
Device Type	Indicates the type of device.
Service Tag	A unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.
Source	The method by which the support case was created. The **Source** column may display: • **SupportAssist** — The support case was created automatically by SupportAssist. • **Phone** — The support case was created by contacting Dell Technical Support over phone. • **Email** — The support case was created by contacting Dell Technical Support through email. • **Chat** — The support case was created by contacting Dell Technical Support over chat. • **Others** — The support case was created by contacting Dell Technical Support through any other method.
Date Opened	The date and time when the support case was opened.

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

Related links

Case management options
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:
  - **Clear System Event Log** — To clear the System Event Log (SEL) or Embedded System Management (ESM) log.
  - **Check for cases** — To check for support cases that are present for a device.
  - **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 **Device Inventory** page displays the device list as a group:

- If no device group is created, below the column headers, the device inventory displays **Ungrouped devices (Total devices: n)** and the list of devices.
- If device groups are created, for each device group, the device inventory displays ***Device_Group_Name*** **(Total devices: n)** and the list of devices in the group. Devices that are not grouped are displayed below the existing device groups.

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

Table 17. Device Inventory

Column	Description
Check box	Use to select a device for performing tasks on the device. **NOTE: The check box is disabled while the following SupportAssist initiated tasks are in progress:** • SNMP configuration • Installation or upgrade of OMSA • Clear System Event Log • Collection of system information immediately after an automatic support case creation and also during a manually initiated collection
Name/IP Address	Displays the following information: • Device name — Displays the display name, host name, or IP address depending on the information that was provided while adding the device. The device name is displayed as a link that you can click to open the **Device Overview** page. • Collection status — When a collection occurs, a progress bar and a corresponding message are displayed to indicate the status of the collection. The possible collection status messages are as follows: – For a collection that you manually initiate: **NOTE: When a manually initiated collection is in progress, a icon is displayed next to the progress bar. Click the icon to cancel the collection, if necessary. After your confirmation, the collection is canceled.** **NOTE: You can cancel a collection only when SupportAssist is collecting data from the device. You cannot cancel a collection while the collection data is being sent to Dell.** * **Starting collection** * **Collection in progress** * **Sending collection** * **Canceling collection** – For an automated collection that is initiated because a support case was created for a detected hardware issue: * **Starting collection for support case** * **Collection for support case in progress** * **Sending collection for support case** **NOTE: If a critical hardware issue is detected on a device with a Dell Basic Service entitlement, the automated collection is initiated. However, a support case is not created for that device.** – For an automated collection based on the default or configured collection schedule: * **Starting periodic collection** * **Periodic collection in progress** * **Sending periodic collection** **NOTE: When a collection that is initiated either manually or because of a support case is in progress on a device, by default, the check box that is used to select the device is disabled. Therefore, you cannot perform other SupportAssist enabled operations (for example, install OMSA) on the device until the collection is completed.** **NOTE: In some instances, when a collection is in progress (manual) on a device another collection (periodic) may be initiated. In such scenarios, the collection status is displayed in the following order of priority:** – Manual collection – Support case collection – Periodic collection

Column	Description
	• Maintenance mode — If the device is placed in maintenance mode, the maintenance mode icon  is displayed.
Model	Model of the device. For example, PowerEdge M820.
Status	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: **Informational status** • **OK** — The device is configured correctly for SupportAssist functionality. If the device was added for monitoring through agent-based method (OMSA), ensure that the device is configured to forward alerts to the local system. • **Installing OMSA** — Installation or upgrade of Dell OpenManage Server Administrator (OMSA) is in progress. • **Configuring SNMP** — Configuring the SNMP settings of the device is in progress. • **Clearing System Event Log** — Clearing of the System Event Log is in progress. • **System Event Log cleared** — System Event Log has been cleared successfully. **Warning status** • **OMSA not installed** — OMSA is not installed on the device. • **SNMP not configured; OMSA not latest** — SNMP settings of the device is not configured and the OMSA version installed on the device is prior to the recommended version of OMSA for SupportAssist. • **SNMP not configured** — SNMP settings of the device is not configured. • **New version of OMSA available** — A newer version of OMSA is available for installation on the device. **Error status** • **Unable to configure SNMP** — SupportAssist is unable to configure the SNMP trap destination of the device. • **Unable to verify SNMP configuration** — SupportAssist is unable to verify the SNMP configuration of the iDRAC. • **Unable to install OMSA** — Installation of OMSA could not be completed. • **OMSA not supported** — Installation of OMSA is not supported. • **Unable to reach device** — SupportAssist is unable to communicate with the device. • **Authentication failed** — SupportAssist cannot log in to the device. • **Unable to gather system information** — SupportAssist is unable to gather system information from the device. • **Insufficient storage space to gather system information** — The system on which SupportAssist is installed does not have sufficient space to gather system information from the device. • **Unable to export collection** — SupportAssist is unable to process the collected system information.

Column	Description
	• **Unable to send system information** — SupportAssist is unable to send the collected system information to Dell. • **Clearing System Event Log failed** — SupportAssist is unable to clear the System Event Log or Embedded System Management logs on the device. • **Maintenance Mode** — SupportAssist has placed the device in automatic maintenance mode because of an alert storm. No new support cases are created while the device is in maintenance. For more information, see Understanding maintenance mode. **NOTE: The error status may be displayed as a link that you can click to view a description of the issue and the possible resolution steps.**

Related links

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 by using SupportAssist
Checking support cases for a specific device
Filtering the displayed data
Clearing the data filter
Sorting the displayed data

Add Device

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

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

Table 18. Add Device

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

Related links

Adding a device (agent-based monitoring)
Adding a device (agentless monitoring)
Editing device credentials

Device Overview

The **Device Overview** window displays details of a device such as the IP address, device type, model number, Service Tag, and so on. From the **Device Overview** window, you can access the configuration viewer that allows you to view the data collected from the device by SupportAssist.

Table 19. Device Overview

Field	Description
Name	Displays the display name that you have provided for the device.
IP Address / Hostname	Displays the IP address or host name of the device.
Service Tag	Displays a unique, alphanumeric identifier that allows Dell to individually recognize the device.
Device Type	Displays the type of the device. For example, Server.
Model	Displays the model information of the device. For example, PowerEdge M820.
OS Type	Displays the operating system installed on the device.
View Collection	Displays a drop-down list that contains the data collection history. You can select a date and time from the list to view the data that was collected. **NOTE: The drop-down list is only displayed if data has been collected from the device.**
Next Collection Scheduled	Displays the date and time of the next scheduled data collection.

Device Groups

The **Device Groups** page allows you to create and manage devices groups.

The following table provides information about the fields displayed in the **Device Groups** page.

Table 20. Device Groups

Field	Description
Create Group	Click to create a device group.
Select group actions	Displays the actions that you can perform on the devices groups. The following are the actions you can select: · **Manage Devices** — Displays the **Manage Devices** window that allows you to add or remove devices from a device group. · **Manage Credentials** — Displays the **Manage Credentials** window that allows you to provide the credentials for the devices types included in a device group. · **Manage Contacts** — Displays the **Manage Contacts** window that allows you to provide the contact information and parts dispatch information for each device type included in a device group. · **Edit/Delete Group** — Displays a window that allows you to edit the group details or delete a device group.
Name	Displays the name of the device group and the total number of devices in the device group.
Description	Displays the description provided for the device group.

Related links

Manage Devices
Manage Credentials
Manage Contacts
Edit/Delete Group

Manage Devices

The **Manage Devices** window allows you to add or remove devices from a device group.

On the **Manage Devices** window:

- The **Ungrouped Devices** pane displays all devices that are not included in any device group.
- The **Devices in Current Group** pane displays devices that are included in the current device group.

The following table provides information about the fields displayed in the **Manage Devices** window.

Table 21. Manage Devices

Field	Description
Name	Displays the display name, host name, or IP address provided when adding the device.
Model	Model of the device. For example, PowerEdge M820.
Service Tag	Displays a unique, alphanumeric identifier that allows Dell to individually recognize each Dell device.
Save	Click to save the changes you have made.
Cancel	Click to discard the changes you have made.

NOTE: You can use the filter icon displayed in the column titles to filter the displayed data.

Related links

Device Groups
Managing devices in a device group

Manage Credentials

The **Manage Credentials** window allows you to provide the credentials for the device types included in a device group.

The left pane on the **Manage Credentials** window displays the device types, and the right pane allows you to provide the credentials. The following table provides information about the fields displayed in the **Credentials** section.

Table 22. Manage Credentials

Field	Description
Username	Allows you to view or edit the user name of a device type.
Password	Allows you to edit the password of a device type in a masked format.
Save	Click to save the credentials.
Next	Click to navigate to the next device type displayed in the left pane.
Close	Click to close the **Manage Credentials** window.

Related links

Device Groups
Managing the credentials of a device group

Manage Contacts

The **Manage Contacts** window allows you to provide the contact information and parts dispatch information for a device group.

The following table provides information about the fields displayed in the **Manage Contacts** window.

Table 23. Manage Contacts

Field	Description
Use default	Select to use the contact information already available in the **Settings** → **Contact Information** page.
Primary	Select to provide the primary contact details.
Secondary	Select to provide the secondary contact details.
First Name	Allows you to view or edit the first name of the primary or secondary contact.
Last Name	Allows you to view or edit the last name of the primary or secondary contact.
Phone	Allows you to view or edit the phone number of the primary or secondary contact.
Alternate Phone	Allows you to view or edit the alternate phone number of the primary or secondary contact.
Email Address	Allows you to view or edit the email address of the primary or secondary contact.
Preferred Contact Method	Allows you to select the preferred contact method. The available options are: · **Phone** · **Email**
Preferred Contact Hours	Allows you to view or edit the preferred hours at which Dell Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.
Time Zone	Allows you to select the time zone of the primary or secondary contact.
Parts Dispatch (Optional)	
Address **City/Town** **Country** **State/Province/Region** **Postal Code**	Allows you to view or edit the address to which a replacement part must be dispatched.

Related links

Device Groups

Viewing and updating the contact information of a device group

Edit/Delete Group

The **Edit/Delete Group** window allows you to edit the device group details or delete a device group.

The following table provides information about the fields displayed on the **Edit/Delete Group** window.

Table 24. Edit/Delete Group

Field	Description
Name	Allows you to view or edit the name of the device group.
Description	Allows you to view or edit the description of the device group.

Field	Description
Update	Click to save the edited device group information.
Delete	Click to delete the device group.
Cancel	Click to discard the changes you have made.

Related links

Device Groups
Editing device group details
Deleting a device group

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**
- **SMTP Settings**

Related links

System Logs
Proxy Settings
Preferences
Contact Information
SMTP Settings

System Logs

The **System Logs** page allows 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.

Table 25. System Logs

Field	Description
Device Type	The available device type is **Server**.
Credential Type	Select the specific device for which you want to schedule the collection of system information. The available options are: - **Windows** - **Linux** - **iDRAC** - **ESX** - **ESXi**

Field	Description
Frequency	Allows you to select the frequency of at which system information will be collected. The available options are: · **None** · **Weekly** · **Monthly**
Specify day and time	Allows you to select the day and time when the system information will be collected. · If the **Frequency** is set to **None**, the periodic collection of system logs is disabled for the selected **Device Type** and **Credential Type**. · If the **Frequency** is set to **Weekly**, the available options are: weeks (**1** or **2**), day of the week (**sunday**, **monday**, **tuesday**, **wednesday**, **thursday**, **friday**, and **saturday**), hour (in hh:mm format), and **AM**/**PM**. · If the **Frequency** is set to **Monthly**, the available options are: week of the month (**first**, **second**, **third**, **fourth**, and **last**), day of the week (**sunday**, **monday**, **tuesday**, **wednesday**, **thursday**, **friday**, and **saturday**), hour (in hh:mm format), **AM**/**PM**, and months (**1** or **3**).
Start Date	Displays the date and time at which the system information will be collected next.
Apply	Click to save the settings.
Cancel	Click to cancel the changes.

Related links

Customizing the schedule for periodic collection of system information

Proxy Settings

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

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

Table 26. Proxy Settings

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

Related links

Configuring proxy server settings

Preferences

The **Preferences** page allows you to configure data collection settings, automatic updates, recommendation report settings, and maintenance mode. The following table provides information about the options displayed in the **Preferences** page.

Table 27. Preferences

Field	Description
Automated Tasks	
Accept and install updates	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. **NOTE: Dell recommends that you select the Accept and install updates option to ensure that SupportAssist is up-to-date with the latest features and enhancements.**
Enable scheduled system log collection	Select this option to enable scheduling of the system log collection. To schedule the system log collection, configure the **System Log Collection Schedule** in the **System Logs** tab.
Start a collection when a new support case is created	Select this option to automatically start a system log collection when a new support case is generated.
Email Settings	
Receive email notification when a new support case is opened	Select this option to receive an email notification when a new support case is opened.
Preferred email Language	Select the preferred language for email notifications.
Recommendation Report Settings	
Automatically receive recommendation reports via email	Select this option to automatically receive ProSupport Plus server recommendation reports through email.
Collection Data Settings	
Include software information in collections	Select this option to allow SupportAssist to collect software-related information from the device.
Include system log in collections	Select this option to allow SupportAssist to collect logs from the device. **NOTE: For information about the logs that are collected by SupportAssist, see the *Dell SupportAssist Version 1.3 for Servers Reportable Items* documents at Dell.com/ServiceabilityTools.**
Identification Information Settings	
Include identification information in data sent to Dell	Select this option to allow sending identity information to Dell.
Maintenance Mode	
Temporarily suspend case generation activity (e.g., for purposes of downtime, external troubleshooting, etc.)	Select this option to set all devices to maintenance mode. While in maintenance mode, no new support cases are opened.
Apply	Click to save the settings.

Field	Description
Cancel	Click to cancel the changes.

Related links

- Enabling automatic updates
- Configuring email notification settings
- Enabling or disabling the automatic collection of system information on case creation
- Enabling or disabling the periodic collection of system information from all devices
- Enabling or disabling the collection of identity information
- Enabling or disabling global-level maintenance mode

Contact Information

The **Contact Information** page allows 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.

Table 28. Contact Information

Field	Description
Company	View or edit the company name.
Primary	Select this option to view the primary contact information.
Secondary	Select this option to view the secondary contact information.
First Name	View or edit the first name of the primary or secondary contact.
Last Name	View or edit the last name of the primary or secondary contact.
Phone	View or edit the phone number of the primary or secondary contact.
Alternate Phone	View or edit the alternate phone number of the primary or secondary contact.
Email	View or edit the email address of the primary or secondary contact.
Country	View or select the country.
Preferred Contact Method	Select the preferred contact method. The available options are: · **Phone** · **Email**
Preferred Contact Hours	View or edit the preferred hours at which Dell Technical Support can contact your primary or secondary contact in case of any issues with the monitored devices.
Time Zone	Select the time zone of the primary or secondary contact.
Parts Dispatch (Optional)	
Address	View or edit the address to which a replacement part must be dispatched.

Field	Description
City/Town **Country** **State/Province/Region** **Postal Code**	
Apply	Click to save the updated information.
Cancel	Click to cancel the changes.

Related links

Viewing and updating the contact information

SMTP Settings

The **SMTP Settings** page allows you to configure the SMTP server (email server) settings. If your company utilizes an SMTP server, Dell recommends that you configure the SMTP server settings.

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.

Table 29. SMTP Settings

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

Related links

Configuring SMTP server settings

Connectivity Test

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

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

Table 30. Connectivity Test

Field	Description
Check box	Select the appropriate check boxes to test the connectivity status you want to verify.
Test	Displays the dependent network resources that you can test. The available options are: · **Internet Connectivity** · **SMTP Server** · **Dell FTP Server** · **Dell Upload Server** · **SupportAssist Server**
Description	Describes the purpose of each test.
Connectivity Status	Displays an icon and a message that indicates the connectivity status. The possible statuses are: · **Not Configured** (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), Dell recommends that you configure **SMTP Settings** in SupportAssist. · **In Progress** — The connectivity test is in progress. · **Connected** — The connectivity test is successful. · **Error** — The connectivity test is unsuccessful. **NOTE: The Error status is displayed as a link that you can click to view a description of the issue and the possible resolution steps.**
Last Verified	Displays the date and time the connectivity status was last verified.
Test Connectivity	Click to perform the selected connectivity tests.

Related links

Performing the connectivity test

Test SupportAssist

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

The following table describes the fields that are displayed in the **Test SupportAssist** page.

Table 31. Test SupportAssist

Field	Description
Check box	Select the appropriate check box to test the task that you want to verify.
Test	Displays the task that you can test. The available option is **Case Creation**, which enables you to verify the ability of SupportAssist to create a support case with Dell Technical Support.
Description	Describes the purpose of the test.
Status	Displays an icon and a message that indicates the test status. The possible statuses are: · **Not validated** — The support case creation task has not been tested. · **In Progress** — The support case creation test is in progress. · **Ready to Create Cases** — SupportAssist can create cases successfully.

Field	Description
	• **Unable to Create Case** — SupportAssist cannot create support cases because of a possible issue with the support case creation workflow.
Last Verified	Displays the date and time the status was last verified.
Test	Click to perform the selected test.

Related links

Testing the case creation capability

16

Related documents and resources

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

Table 32. Related documents

Document title	How to access the document
Dell SupportAssist Version 1.3 for Servers Online Help	Click the  icon in the SupportAssist user interface.
Dell SupportAssist Version 1.3 for Servers Quick Setup Guide	1. Visit Dell.com/ServiceabilityTools. 2. Click **SupportAssist Version 1.3 for Servers**. 3. Click **Manuals**.
Dell SupportAssist Version 1.3 for Servers Support Matrix	
Dell SupportAssist Version 1.3 for Servers Release Notes	
Dell SupportAssist Version 1.3 for Servers Reportable Items for Windows	
Dell SupportAssist Version 1.3 for Servers Reportable Items for Linux	
Dell OpenManage Server Administrator Installation Guide	Visit Dell.com/OpenManageManuals and click **OpenManage Server Administrator**.
Dell OpenManage Server Administrator User's Guide	
iDRAC User's Guide	Visit Dell.com/ESMmanuals and click **Remote Access Controller**.
Dell SupportAssist: Alert Policy	Visit Dell.com/SupportAssistGroup.
Managing Windows Device Credentials in SupportAssist Using Service Account	

Video tutorials

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

Table 33. Video tutorials

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

Video title	How to access the videos
Clearing System Event Log	
Check for Cases	
Case Management	
Case Creation Test	

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.

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**
  - For OpenManage documents — **Dell.com/OpenManageManuals**
  - For Remote Enterprise Systems Management documents — **Dell.com/esmmanuals**
  - For OpenManage Connections Enterprise Systems Management documents — **Dell.com/OMConnectionsEnterpriseSystemsManagement**
  - For Serviceability Tools documents — **Dell.com/ServiceabilityTools**
  - For OpenManage Connections Client Systems Management documents — **Dell.com/DellClientCommandSuiteManuals**
- From the Dell Support site:
  a. Go to **Dell.com/Support/Home**.
  b. Under **Select a product** section, click **Software & Security**.
  c. In the **Software & Security** group box, click the required link from the following:
     - **Enterprise Systems Management**
     - **Remote Enterprise Systems Management**
     - **Serviceability Tools**
     - **Dell Client Command Suite**
     - **Connections Client Systems Management**
  d. To view a document, click the required product version.
- Using search engines:
  - Type the name and version of the document in the search box.

Contacting Dell

Prerequisites

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

About this task

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

Steps

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