Dell SupportAssist Version 2.0 for Dell OpenManage Essentials
Quick Start 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.

2014 - 09

Rev. A00

Contents

1 Getting started with SupportAssist....4

Setting up OpenManage Essentials for SupportAssist....4

Configuring SNMP service on Windows....5

Configuring SNMP service on Linux....6

Installing SNMP tools (Windows Server 2012 or later)....6

Enabling network discovery (Windows Server 2008 only)....7

Setting up SupportAssist....7

Configuring the system credentials....8

Configuring the default device type credentials....8

Configuring the local SMTP e-mail server settings....9

Configuring periodic collection of system logs....9

Performing the connectivity test....10

Verifying the system log collection or upload configuration....11

Enabling auto update....11

Troubleshooting registration problem....11

Troubleshooting collection error....12

Troubleshooting collection upload error....12

Ensuring successful communication between the SupportAssist application and the SupportAssist server....12

Sending the system logs manually....13

Troubleshooting SSL connection failure....13

Exporting the root certificate....14

Installing the root certificate....14

Getting started with SupportAssist

Dell SupportAssist for Dell OpenManage Essentials is a service capability that enables automated support for Dell server, storage, and networking solutions. OpenManage Essentials interacts with supported devices that are to be monitored and receives SNMP traps. The SNMP traps are periodically retrieved as alerts by SupportAssist. The alerts are filtered using various policies to decide if the alerts qualify for creating a new support case or updating an existing support case.

All qualifying alerts are securely sent to the SupportAssist server hosted by Dell, for creating a new support case or updating an existing support case. After the support case is created or updated, SupportAssist runs the appropriate collection component on the device that generated the alert, and uploads the log collection to Dell. The information in the log collection is used by Dell technical support to troubleshoot the issue and provide an appropriate solution.

This document provides information required to make sure that SupportAssist works as expected in your environment. To quickly get started with SupportAssist, follow the instructions in Setting up OpenManage Essentials for SupportAssist and Setting up SupportAssist.

NOTE: If you need assistance with deploying OpenManage Essentials and SupportAssist, you can order and utilize Dell Remote Consulting Services (RCS). After you order for RCS, you can schedule time with a systems management deployment expert for OpenManage Essentials and SupportAssist installation, set up, and configuration from start to finish. For more information about RCS, click the **Dell Remote Consulting Services** link at **Dell.com/learn/enterprise-deployment-and-configuration**.

Setting up OpenManage Essentials for SupportAssist

To enable SupportAssist to retrieve alerts from supported devices and automatically generate support cases if there is a hardware issue, you must set up OpenManage Essentials as follows:

1. Make sure that OpenManage Essentials version 2.0 is installed on the management server. For information on installing OpenManage Essentials version 2.0, see the *Dell OpenManage Essentials Version 2.0 User's Guide* at **Dell.com/OpenManageManuals**.
2. Configure all managed nodes to send SNMP traps to the management server running OpenManage Essentials. See Configuring SNMP service on Windows and Configuring SNMP service On Linux.

   NOTE: On managed nodes running Microsoft Windows Server 2012 or later, before configuring the SNMP service, you must install SNMP tools. See Installing SNMP tools.
3. On all managed nodes, make sure that Dell OpenManage Server Administrator (OMSA) is installed and operational. For information on installing OMSA, see the *Dell OpenManage Server Administrator User's Guide* at **Dell.com/OpenManageManuals**.

   NOTE: Dell's 12th generation or later PowerEdge servers can provide status, alerts, and limited inventory through Integrated Dell Remote Access Controller (iDRAC), even if OMSA is not installed.
4. On all managed nodes running Windows Server 2008, make sure that network discovery is enabled. See Enabling network discovery (Windows Server 2008 only).
5. Configure the supported Dell devices in your environment so that they can be discovered and managed by OpenManage Essentials. For instructions to configure the supported Dell devices, see the *Making My Environment Manageable for Dell OpenManage Essentials* technical white paper at **DellTechCenter.com/OME**.

6. Verify the firewall configuration and make sure that the following ports are open:

System	Port	Usage
Management server	2607	Console launch NOTE: The default port for console launch is 2607. If you selected a custom port for console launch, make sure that the port you selected is open.
	162	Event reception through SNMP
	443	Secure Socket Layer (SSL) communication and SupportAssist update information
	9399	Hosting the Windows Communication Foundation (WCF) service
	25	SMTP communication
Managed nodes	161	Sending and receiving SNMP requests
	1311	OMSA communication

7. Discover and inventory the supported devices in OpenManage Essentials using the recommended protocols. For information on discovery and inventory of devices, see the *Dell OpenManage Essentials Version 2.0 User's Guide* at **Dell.com/OpenManageManuals**.

Configuring SNMP service on Windows

Configuring the SNMP service enables the managed nodes to send SNMP traps to the management server running OpenManage Essentials.
To configure the SNMP service on managed nodes running Windows operating system:

1. Open a Command Prompt, type `services.msc`, and press Enter.
   The **Services** window is displayed.
2. Browse the list of services, and make sure that the status of the **SNMP Service** is displayed as **Started**.
3. Right-click **SNMP Service** and select **Properties**.
   The **SNMP Service Properties** dialog box is displayed.
4. Click the **Security** tab and perform the following:

   NOTE: If the **Security** tab is not displayed, reopen the **Services** window and try again.

   a. Clear **Send authentication trap**.
   b. Under **Accepted community** names, click **Add**.
      The **SNMP Service Configuration** dialog box is displayed.
   c. From the **Community rights** list, select **READ ONLY**.
   d. In the **Community Name** box, type the community name and click **Add**.
   e. Select either **Accept SNMP packets from any hosts** or **Accept SNMP packets from these hosts**, and click **Add**.
      The **SNMP Service Configuration** dialog box is displayed.
   f. In the **Host name, IP or IPX address** box, type the OpenManage Essentials server name or IP address, and click **Add**.
5. Click the **Traps** tab and perform the following:
   a. In the **Community name** box, type the community name, and click **Add to list**.
   b. Under **Trap destinations**, click **Add**.

The **SNMP Service Configuration** dialog box is displayed.

c. In the **Host name, IP or IPX address** box, type the OpenManage Essentials server name or IP address, and click **Add**.

6. Click **Apply**.
7. In the **Services** window, right-click **SNMP Service** and click **Restart**.

NOTE: The default port for sending SNMP traps is 162. To configure the managed node to use a non-default port, see the "Changing the Default SNMP Port" section in the *Dell OpenManage Essentials User's Guide* at **Dell.com/OpenManageManuals**.

Configuring SNMP service on Linux

Configuring the SNMP service enables the managed nodes to send SNMP traps to the management server running OpenManage Essentials.
To configure the SNMP service on managed nodes running Linux operating system:

1. Run the command `rpm -qa | grep snmp`, and make sure 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 make sure 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**, type the OpenManage Essentials console IP address in the following format: `trapsink <OpenManage Essentials Console IP> <community string>`. For example, `trapsink 10.94.174.190 public`.
6. Start the SNMP service (`service snmpd restart`).

Installing SNMP tools (Windows Server 2012 or later)

The SNMP configuration options are disabled by default in Windows Server 2012 or later. You must install SNMP tools to view the **Security** and **Traps** tabs in the **SNMP Service Properties** window.
To install SNMP tools:

1. Open **Server Manager**.
2. Click **Manage** → **Add Roles and Features**.

   The **Add Roles and Features Wizard** is displayed.
3. Click **Next** until you navigate to **Server Selection**.
4. Under **Server Pool**, select the local server as the destination server and click **Next**.
5. In **Features**, select **Remote Server Administrator Tools** → **Feature Administration Tools** → **SNMP Tools** and click **Next**.
6. Click **Install**.
7. In a Command Prompt, type `services.msc` and press Enter to open the **Services** window.
8. Right-click **SNMP Service** and click **Restart**.
9. Close the **Services** window.
10. Open the **Services** window again, right-click **SNMP Service** and click **Properties**.
11. Make sure that the **Security** and **Traps** tab are displayed in the **SNMP Service Properties** window.

Enabling network discovery (Windows Server 2008 only)

Enabling network discovery is a prerequisite for discovering managed nodes running on managed nodes running Windows Server 2008 in OpenManage Essentials.
To enable network discovery:

1. Click **Start** → **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Change advanced sharing settings**.
2. Choose the drop-down arrow for the applicable network profile (**Home or Work**, or **Public**).
3. Under **Network discovery**, select **Turn on network discovery**.
4. Click **Save changes**.

Setting up SupportAssist

To set up SupportAssist in your environment:

NOTE: For information on the prerequisites and minimum requirements for installing and using SupportAssist, see the *Dell SupportAssist Version 2.0 for Dell OpenManage Essentials User's Guide* at **Dell.com/ServiceabilityTools**.

1. Make sure that SupportAssist version 2.0 is installed on the management server running OpenManage Essentials version 2.0.
2. Make sure that you have completed all applicable steps in the **SupportAssist Setup Wizard**. For more information, see the "Setting up SupportAssist" section in the *Dell SupportAssist Version 2.0 for Dell OpenManage Essentials User's Guide* at **Dell.com/ServiceabilityTools**.
3. Make sure that you have configured the system credentials correctly in SupportAssist. See Configuring the System Credentials.
4. Configure the Administrator credentials of each supported device type in your environment in SupportAssist. See Configuring the default device type credentials.
5. If a local SMTP e-mail server is available in your environment, it is recommended that you configure the local SMTP server settings in SupportAssist. See Configuring the local SMTP e-mail server settings.

   NOTE: SupportAssist utilizes the local SMTP server to send you e-mail notifications on the device status and connectivity status. You may not receive certain device status and connectivity status e-mails in the following scenarios:

   - An SMTP server is available in your environment, but:
     - The SMTP server settings are not configured in SupportAssist.
     - The SMTP server credentials you have provided in SupportAssist are incorrect.
     - The Secure Socket Layer (SSL) certificate of the SMTP server is expired.
     - An anti-virus software is blocking the SMTP server port configured in SupportAssist.
   - An SMTP server is not available in your environment.
6. If the devices in your environment are covered under the Dell ProSupport Plus service contract, configure SupportAssist to collect the system logs periodically. See Configuring periodic collection of system logs.
7. Verify SupportAssist connectivity status to ensure that SupportAssist is able to connect to all dependent network resources successfully. See Performing the connectivity test.
8. Verify the status of devices and make sure that the **Device Inventory** page does not display an **Error** status for any of the devices. If the **Error** status is displayed, click the **Error** link to view the description of the issue and the possible resolution steps.

9. Verify if SupportAssist is able to generate the system log collection and upload it to Dell successfully. See Verifying the system log collection or upload configuration.
10. If you want to automatically download and install the latest SupportAssist and collection component updates when they are available, enable auto update. See Enabling auto update.

Configuring the system credentials

System credentials refers to the credentials of a user account that is a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group. SupportAssist requires the system credentials to connect to OpenManage Essentials for retrieving device and alert information.

To configure the system credentials:

NOTE: If you change the system credentials because of the security policy requirements of your company or for other reasons, you must ensure that the system credentials are also updated in SupportAssist. Alternatively, you can create a service account that never expires, and provide the service account credentials in SupportAssist.

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

1. Click the **Settings** tab.

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

   The **System Credentials** page is displayed.
3. Type the user name, password, and confirm the password in the appropriate fields.

   NOTE: The user account must be a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.
4. Click **Save Changes**.

Configuring the default device type credentials

SupportAssist runs the appropriate collection component and gathers the system log collection from supported devices in your environment. To enable SupportAssist to run the collection component on the devices, you must configure the Administrator credentials for each managed device type.

To configure the default device type credentials:

NOTE: If the Administrator credentials of supported devices are changed, you must ensure that the **Default Device Type Credentials** are also updated in SupportAssist. Alternatively, you can create a service account that never expires, and provide the service account credentials in SupportAssist. For more information, see the *Managing Device Credentials in SupportAssist Using Service Account* technical white paper at **Dell.com/SupportAssistGroup**.

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

1. Click the **Settings** tab.

   The **System Logs** page is displayed.
2. Under **Edit Device Type Credentials**, select **Device Type** and **Credential Type**.
3. Type the Administrator credentials [**Username**, **Password**, **Enable Password** (for Ethernet switches only), and **Community String** (for Dell EqualLogic storage arrays only)] of the selected **Device Type** and **Credential Type** in the corresponding fields.

NOTE: Windows user names must be of the form [Domain\Username]. You can also use a period [.] to indicate the local domain. This rule does not apply to Linux or ESX/ESXi credentials.

NOTE: For Dell Networking switches the domain name need not be specified.

Examples of Windows user names: `.\Administrator; MyDomain\MyUsername`.

Example of Linux or ESX/ESXi user name: `Username`.

4. Repeat step 2 and step 3 until you have configured the **Default Device Type Credentials** for each managed device type.
5. Click **Save Changes**.

NOTE: If the credentials for a device differs from the **Default Device Type Credentials** you provided, you can edit the credentials for that particular device. To edit the credentials for a device, select the device in the **Device Inventory** page, click **Edit Device Credentials**, and provide the details.

Configuring the local SMTP e-mail server settings

If a Simple Mail Transfer Protocol (SMTP) server is available in your environment, you can configure SupportAssist to send you device status and connectivity status e-mail notifications through the local SMTP server.

To configure the SMTP server settings:

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

1. Click the **Settings** tab.

   The **System Logs** page is displayed.
2. Click **SMTP Settings**.

   The **SMTP Settings** page is displayed.
3. Provide the SMTP server name/IP address and port number in the appropriate fields.
4. If the SMTP server requires authentication for sending e-mails, select **SMTP server requires authentication**.
5. Provide the user name, password, and confirm the password in the appropriate fields.
6. If your environment supports SSL communication, select **Enable SSL**.
7. Click **Save Changes**.

Configuring periodic collection of system logs

To receive the full benefits of the support, reporting, and maintenance offering of your ProSupport Plus service contract, you must configure SupportAssist to collect the system logs at periodic intervals for each supported device type.

To configure the periodic collection of system logs:

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

1. Click the **Settings** tab.

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

The **Email Settings**, **Support Collection**, and **Maintenance Mode** page is displayed.

3. Under **Support Collection**, ensure that **Enable scheduling** is selected.
4. Click **System Logs**.

   The **System Logs** page is displayed.
5. Under **Edit Device Credentials**, select the **Device Type** and **Credential Type**.
6. Verify or provide the credentials (**Username**, **Password**, **Confirm Password**, and **Community String**) for the selected credential type. For more information, see Configuring the default device type credentials.
7. Under **System Log Collection Schedule**, set the **Frequency**, and select the appropriate fields in **Specify day and time**.

   NOTE: For recommendations on setting the frequency of periodic collection, see Network bandwidth consumption and recommendations for scheduling periodic collection.
8. Repeat step 5 to step 7 until you have scheduled the collection of system logs for all supported device types in your environment.
9. Click **Save Changes**.

Network bandwidth consumption and recommendations for scheduling periodic collection

NOTE: In an environment that consists of less than 300 devices, the network bandwidth consumed for uploading the system log collection is about 4 MB/second.

The following table provides information about network bandwidth consumption and recommendations for scheduling periodic collections in an environment that consists of 75 percent servers and 25 percent switch and storage devices. The recommendations also assume compliance with the hardware, software, and networking requirements for SupportAssist.

Total number of devices	Network bandwidth consumed for uploading the collection (GB/month)	Time taken for generating the collection (hours)	Recommendations for scheduling periodic collection
Less than 300	16	20	Weekly (overnight)
300 or more	7.2 to 47	22.5	For EqualLogic and Dell Networking devices — Weekly (overnight) For Dell PowerEdge — Monthly (at different times during the week for each device type)

Performing the connectivity test

The connectivity test enables you to verify and test SupportAssist connectivity status to the dependent resources.

To perform the connectivity test:

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

   The **Connectivity Test** page is displayed.
2. Select the tests that you want to perform.

NOTE: The **Test Connectivity** button is enabled only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

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 the description of the problem and the possible resolution steps.

Verifying the system log collection or upload configuration

To verify if SupportAssist is configured correctly to generate and upload the system logs to Dell:

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

   NOTE: The **Send System Logs** link is enabled only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

   The **Send System Logs** link is enabled.
3. Click **Send System Logs**.
   The status of the system log collection is displayed in the **Status** column.
4. To add other devices to the system log collection queue, select each device in the **Device Inventory**, and then click **Send System Logs**.

If SupportAssist is able to successfully generate the system log collection and upload it to Dell, the **Status** column displays **Collection Uploaded**. For information on troubleshooting problems with the generation and upload of the system log collection, see Collection error and Collection upload error.

Enabling auto update

Enabling auto update ensures that SupportAssist and the associated collection components are automatically updated, when an update is available.
To enable auto update:

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

1. Click the **Settings** tab.
   The **System Logs** page is displayed.
2. Click **Preferences**.
   The **Auto Update**, **Email Settings**, **Support Collection**, and **Maintenance Mode** page is displayed.
3. Under **Auto Update**, select **Enable auto update**.
4. Click **Save Changes**.

Troubleshooting registration problem

The **SupportAssist Setup Wizard** guides you through the registration of SupportAssist. If the registration is successful:

- A registration confirmation e-mail is sent to your primary contact.

- The **Help** → **About** window in SupportAssist displays a **Registration ID** value.

Registration problem occurs if the SupportAssist application has problems communicating with the SupportAssist server hosted by Dell. To resolve the communication problems, see see Ensuring successful communication between the SupportAssist application and the SupportAssist server.

Troubleshooting collection error

If you receive a SupportAssist e-mail notification indicating a collection issue with a specific device and the **Status** of the device displays **Error**:

1. Click the **Error** link in the **Status** column to view the possible resolution steps.
2. Verify if the device is connected to the network.
3. Verify the credentials you have provided for the device. You must provide the Administrator credentials in the **Settings** → **System Logs** page. For more information, see Configuring the default device type credentials. If you want to edit the credentials for a particular device, select the device in the **Devices** tab, click **Edit Device Credentials**, and provide the details.

Troubleshooting collection upload error

If you receive a SupportAssist e-mail notification indicating an issue uploading the collection for a specific device and the **Status** of the device displays **Error**:

1. Click the **Error** link in the **Status** column to view the possible resolution steps.
2. Verify if the management server on which SupportAssist is installed is able to connect to the internet.
3. If the management server on which SupportAssist is installed connects to the internet through a proxy server, ensure that you configure the proxy settings in SupportAssist. To configure the proxy settings, click **Settings** → **Proxy Settings** and provide the proxy details.
4. Verify SupportAssist connectivity status to make sure that SupportAssist is able to connect to all dependent network resources successfully. See Performing the connectivity test.
5. Verify if SupportAssist is able to successfully communicate with the SupportAssist server hosted by Dell. See Ensuring successful communication between the SupportAssist application and the SupportAssist server.

After resolving the issue, initiate the collection and upload of system logs from the device to Dell. See Sending the system logs manually.

Ensuring successful communication between the SupportAssist application and the SupportAssist server

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

- The management server on which the SupportAssist application is installed must be able to connect to the following destinations:
  - **https://api.dell.com/support/case/v2/WebCase** — end point for the SupportAssist server. On the management server, verify if you can access the following location using the web browser: **https://api.dell.com/support/case/v2/WebCase?wsdl**.
  - **https://ddldropbox.us.dell.com/upload.ashx/** — the file upload server where the diagnostic test results are uploaded. Verify if the server certificate on **ddldropbox.us.dell.com** is valid. See Verifying the server certificate.

  - **https://ftp.dell.com/** — for getting SupportAssist update information. On the management server, verify if you can access the following location using the web browser: **https://ftp.dell.com/**.
- Verify if port 443 is open on the management server for **ddldropbox.us.dell.com** and **ftp.dell.com**. You can use a telnet client to test the connection. For example, you can use the following command: `o ddldropbox.us.dell.com 443`.
- Verify if the network settings on the management server are correct.
- If the management server on which SupportAssist is installed connects to the internet through a proxy server, configure the proxy settings in SupportAssist. To configure the proxy settings, click **Settings** → **Proxy Settings** and provide the proxy details.

  NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

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

Verifying the server certificate

To verify the server certificate on **ddldropbox.us.dell.com** using Internet Explorer:

1. Open **https://ddldropbox.us.dell.com** .
   A **404 — File or directory not found** error may be displayed.
2. On the address bar, click the **Security Report** icon , and then click **View Certificates**.
   The **Certificate** is displayed.
3. In the **General** tab, verify if the certificate displays a valid date.
4. Click the **Certification Path** tab, and verify if the **GTE CyberTrust Global Root** certificate is listed.

Sending the system logs manually

To send the system logs manually:

NOTE: The **Send System Logs** option is enabled only if you are logged on as a member of the OpenManage Essentials Administrators, Power Users, or Site Administrators group.

1. Click the **Devices** tab.
   The **Device Inventory** is displayed.
2. Select the device in the **Device Inventory**.
   The **Send System Logs** button is enabled.
3. Click **Send System Logs**.
   The **Status** column in the **Device Inventory** page displays the status of the collection and upload of the system logs.

Troubleshooting SSL connection failure

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

To verify if the certificate is installed in Internet Explorer:

1. Click **Tools** → **Internet Options**.

The **Internet Options** dialog box is displayed.

2. Click the **Content** tab, and then click **Certificates**.

   The **Certificates** dialog box is displayed.
3. Click the **Trusted Root Certification Authorities** tab.
4. Scroll to verify if **GTE CyberTrust Global Root** is listed in the **Issued To** and **Issued By** columns.

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

Exporting the root certificate

To export the root certificate:

1. In Internet Explorer, go to **https://dell.com**.
2. If the **Certificate Error: Navigation Blocked** page is displayed, click **Continue to this website (not recommended)**.
3. At the **Do you want to view only the webpage content that was delivered securely?** prompt, click **Yes**.
4. On the address bar, click the **Security Report** icon  .
5. Click **View certificates**.

   The **Certificate** window is displayed.
6. Click **Details**.
7. Click **Copy to File**.

   The **Certificate Export Wizard** is displayed.
8. Click **Next**.
9. In the **Export File Format** page, click **Next**.
10. In the **File to Export** page, click **Browse**.

    The **Save As** window is displayed.
11. Navigate to the location you want to save the certificate file.
12. Type a file name and click **Save**.
13. In the **Export File Format** page, click **Next**.
14. Click **Finish**.

    The status of the export is displayed.
15. Click **OK**.

Installing the root certificate

Before you begin, ensure that:

- You are logged on using the user account with which SupportAssist was installed.
- You have administrator privileges.
- The SupportAssist service is running.
- You have exported the certificate file. See Exporting the root certificate.

To install the root certificate:

1. Click **Start** → **Run**.

The **Run** dialog box is displayed.

2. In the **Open** box, type `mmc` and click **OK**.
   The **Console1 – [Console Root]** window is displayed.
3. Click **File** → **Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box is displayed.
4. Under **Available snap-ins**, select **Certificates**, and click **Add >**.
   The **Certificates snap-in** dialog box is displayed.
5. Ensure that **My user account** is selected, and then click **Finish**.
6. In the **Add or Remove snap-ins** dialog box, click **Add >**.
   The **Certificates snap-in** dialog box is displayed.
7. Select **Computer account** and click **Next**.
   The **Select Computer** dialog box is displayed.
8. Ensure that **Local computer: (the computer this console is running on)** is selected and click **Finish**.
9. In the **Add or Remove snap-ins** dialog box, click **OK**.
10. Under the **Console Root**, click **Certificates – Current User**.
11. Right-click **Trusted Root Certification Authorities** → **All Tasks** → **Import**.
    The **Certificate Import Wizard** is displayed.
12. Click **Next**.
    The **File to Import** dialog box is displayed.
13. Browse to select the exported certificate file and click **Next**.
    The **Certificate Store** information is displayed.
14. Click **Next**.
15. Click **Finish**.
16. Right-click **Intermediate Certification Authorities** → **All Tasks** → **Import**.
    The **Certificate Import Wizard** is displayed.
17. Browse to select the exported certificate file and click **Next**.
    The **Certificate Store** information is displayed.
18. Click **Next**.
19. Click **Finish**.
20. Under the **Console Root**, click **Certificates (Local Computer)**.
21. Perform step 11 to step 19 to install the root certificate.