

Dell SupportAssist Version 1.1 For Microsoft System Center Operations Manager 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.


Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 12

Rev. A00

Introduction

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

 **NOTE:** SupportAssist capabilities supported on a Dell server may vary based on the Dell service contract. For more information, see the "Features supported with Dell Service Contracts" section in the *Dell SupportAssist Version 1.1 For Microsoft System Center Operations Manager User's Guide* at Dell.com/ServiceabilityTools.

This document provides the information required to get started with SupportAssist in your IT environment.

Getting started with SupportAssist


To quickly get started with SupportAssist:

1. Ensure that Microsoft System Center Operations Manager 2012 R2, 2012 SP1, or 2007 R2 is installed on the management server.
2. Ensure that Dell Server Management Pack Suite Version 5.0.1, 5.1, or 6.0 For Microsoft System Center Operations Manager And System Center Essentials is installed on the management server.
For information on installing the management pack suite, discovering and monitoring of supported Dell devices using Operations Manager, see the following documents at dell.com/OpenManageManuals (under **Server Management Pack Versions for Microsoft System Center Operations Manager**):
 - *Dell Server Management Pack Suite For Microsoft System Center Operations Manager And System Center Essentials Installation Guide*
 - *Dell Server Management Pack Suite For Microsoft System Center Operations Manager And System Center Essentials User's Guide*
3. Ensure that Operations Manager is setup for discovery and monitoring of supported Dell devices.
4. Install SupportAssist on the management server running Operations Manager.
For information on installing SupportAssist, including the prerequisites, see the *Dell SupportAssist Version 1.1 For Microsoft System Center Operations Manager User's Guide* at Dell.com/ServiceabilityTools.
5. If the management server connects to the Internet through a proxy server, you must configure the proxy server settings in SupportAssist. To configure the proxy server settings, click **Settings** → **Proxy Settings**, and follow the instructions on the screen.
6. Configure the administrator credentials of each supported device type in SupportAssist.
For more information, see [Configuring the default credentials](#).
7. If SupportAssist is installed on either a non-host system (Operations Manager 2012 R2 or 2012 SP1) or non-RMS system (Operations Manager 2007 R2), configure SupportAssist to establish a remote connection with the management groups.
For more information, see [Configuring a remote connection](#).


8. Verify if the SupportAssist application is able to communicate with the SupportAssist server hosted by Dell by performing the connectivity test.
For more information, see [Connectivity test](#).
9. If the monitored devices are covered under the Dell ProSupport Plus service contract, you must configure SupportAssist to collect the system information from the devices periodically.
For more information, see [Configuring the periodic collection of system information](#).
10. Verify if SupportAssist is able to collect the system information and send it to Dell successfully. See [Verifying the system information collection or upload settings](#).
11. Verify if the management server is able to connect to the following destinations:
 - <https://api.dell.com/support/case/v2/WebCase> — end point for the SupportAssist server.
 - <https://ddldropbox.us.dell.com/upload.ashx/> — the file upload server where the collected system information is uploaded.
 - <http://ftp.dell.com/> — for getting new SupportAssist release information.

Configuring the default credentials


Configuring the default credentials of the devices enables SupportAssist to collect system information from the devices.

 **NOTE:** The **Settings** tab is accessible only if you are logged on as a member of either the **Administrators** or **Domain Admins** group.

1. Click the **Settings** tab.
The **System Logs** page is displayed.
2. Under **Edit Device Type Credentials**, select the device type and credential type.
3. Type the administrator credentials (user name and password) of the selected **Device Type** and **Credential Type** in the corresponding fields.


 **NOTE:** Windows user names must be in the [Domain\Username] format. You can also use a period [.] to indicate the local domain. Examples of Windows user names: .
`\Administrator; MyDomain\MyUsername.`

4. Click **Save Changes**.


 **NOTE:** If the credentials of a device is not the same as the default credentials you have provided, you must provide the credentials of that device using the **Edit Device Credentials** option in the **Devices** tab.

Configuring a remote connection


Establishing a remote connection to the management groups enables SupportAssist to retrieve monitoring data such as alerts and discovery information from Operations Manager.

 **NOTE:** Whenever Operations Manager is configured to connect to either a new host (Operations Manager 2012 R2 or 2012 SP1) or RMS (Operations Manager 2007 R2), SupportAssist must also be configured with the new management group credentials.

To configure a remote connection:

 **NOTE:** The **Settings** tab is accessible only if you are logged on as a member of either the **Administrators** or **Domain Admins** group.


1. Click the **Settings** tab.
The **System Logs** page is displayed.
2. Click **Remote Connection**.
The **Management Groups Connection** page is displayed.
3. Select **Establish a remote connection with the management group**.
4. Provide the IP address or name, domain\username, password, and confirm the password of the host (Operations Manager 2012 R2 or 2012 SP1) or RMS (Operations Manager 2007 R2) in the appropriate fields.

 **NOTE:** The username must be provided in the domain\username format. You can use a period [.] to indicate the local domain.

5. Click **Apply**.
SupportAssist verifies the management group credentials by attempting to establish a remote connection. If the remote connection is successful, the management group credentials are saved.

Connectivity test


The connectivity test enables you to verify if the SupportAssist application can communicate successfully with the SupportAssist server hosted by Dell.

 **NOTE:** The **Connectivity Test** link is enabled only if you are logged on as a member of either the **Administrators** or **Domain Admins** group.

1. Move the mouse pointer over the **<user name>** link displayed beside the **Help** link in the SupportAssist header area, and then click **Connectivity Test**.
2. On the **Connectivity Test** page, click **Send**.
The SupportAssist server receives the connectivity test, and sends a sample email with the connectivity status to the primary and secondary (optional) contact. If the connectivity status email is not received, follow the instructions in [Troubleshooting connectivity test issues](#).

Configuring the periodic collection of system information (ProSupport Plus only)

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

 **NOTE:** The **Settings** tab is accessible only if you are logged on as a member of either the **Administrators** or **Domain Admins** group.

1. Click the **Settings** tab.
The **System Logs** page is displayed.
2. Click **Preferences**.
The **Preferences** page is displayed.
3. Under **Support Collection**, select **Enable system log collection scheduling**.
4. Click **System Logs**.

The **System Logs** page is displayed.

5. Under **Edit Device Credentials**, select the device type and credential type.
6. Under **System Log Collection Schedule**, set the **Frequency**, and select the appropriate fields in **Specify day and time**.
7. Repeat step 5 and step 6 until you have scheduled the collection of system information from all supported device types in your IT environment.
8. Click **Save Changes**.

Verifying the system information collection or upload settings

To verify if SupportAssist is configured correctly to collect the system information and upload it 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 either the **Administrators** or **Domain Admins** group.

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

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

If SupportAssist is able to successfully generate the system information and upload it to Dell, the **Status** column displays **Collection Uploaded**. For information on troubleshooting issues with the collection and upload of system information, see [Troubleshooting system information collection or upload issues](#).

Troubleshooting connectivity test issues

The connectivity test may fail due to:

- Proxy settings — If your network requires passing the web browser traffic through a proxy server, ensure that the proxy is enabled and configured in SupportAssist.
- SSL connection failure — If the proxy settings are configured properly, but the connectivity test fails, there may be a SSL connection failure.

If there is an SSL connection failure, you must install the required root certificates. The following sections provide information required to verify and install the root certificates.

Verifying the installation of the root certificate

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 root certificate is installed in Internet Explorer:

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

- The **Internet Options** dialog box is displayed.
- Click the **Content** tab, and then click **Certificates**.
The **Certificates** dialog box is displayed.
 - Click the **Trusted Root Certification Authorities** tab.
 - 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. To install the certificates, see [Installing root certificates](#).

Installing Root Certificates

Before you begin, ensure that:

- You are logged in to the user account with which SupportAssist was installed.
- You have administrator privileges.
- The SupportAssist service is running.

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

Table 1. Certificate Files And Installation Folder

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

To install root certificates:

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

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

Troubleshooting system information collection or upload issues

- If an issue occurs with the collection of system information (**Collection Status** displays **Failed to Run**):
 - Ensure that the default credentials for the device are configured correctly in the **Settings** → **System Logs** tab. To edit the credentials of the device, select the device in the **Device Inventory** page, and click **Edit Device Credentials**.
- If an issue occurs with the upload of system information (**Collection Status** displays **Collection Failed to Upload**):
 - Ensure that the proxy server credentials are configured correctly in the **Settings** → **Proxy Settings** page in SupportAssist.
 - Confirm if you can access the Internet using the web browser.
 - Perform the connectivity test and ensure that the test is successful. See [Connectivity test](#).

To verify if the issue is resolved, select a device in the **Device Inventory** page, and click **Send System Logs**. If the collection and upload of system information is successful, the **Collection Status** is displayed as **Collection Uploaded**.