

**Dell SupportAssist Version 1.2 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.

© 2013 Dell Inc. All Rights Reserved.

Trademarks used in this text: Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™, Venue™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, vMotion®, vCenter®, vCenter SRM™ and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

2013 - 09

Rev. A01

Introduction

Dell SupportAssist plugin for Dell OpenManage Essentials provides proactive support capabilities for supported 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 the SupportAssist client. 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 a creating a new support case or updating an existing support case. After the support case is created or updated, the SupportAssist client, runs the appropriate collection tools on the devices that generated the alerts, and uploads the log collection to Dell. This information in the log collection is used by Dell technical support to troubleshoot the issue and provide an appropriate solution.


This document provides information you require to set up OpenManage Essentials and SupportAssist, and thereby ensure that SupportAssist works as expected in your environment.

Getting Started With Dell SupportAssist

To quickly get started with SupportAssist:

1. Ensure that OpenManage Essentials is installed on the management server and is configured to discover the supported devices in your environment. For information on installing, configuring, and setting up your environment for OpenManage Essentials, see the *Dell OpenManage Essentials User's Guide* at dell.com/OpenManageManuals.
2. Install SupportAssist on the management server running OpenManage Essentials. For information on installing SupportAssist, see the *Dell SupportAssist Plugin For Dell OpenManage Essentials User's Guide* at dell.com/ServiceabilityTools.
3. If the management server connects to the Internet through a proxy server, you must configure **Proxy Settings** in SupportAssist. To configure the proxy server settings, click **Settings** → **Proxy Settings**, and follow the instructions on the screen.
4. Configure the Administrator credentials of each supported device type in your environment in SupportAssist. See [Configuring The Default Device Type Credentials](#).
5. Verify if the SupportAssist client is able to communicate with the SupportAssist server hosted by Dell by performing the email connectivity test. See [Email Connectivity Test](#).
6. If there is a SSL connection failure, you must install the required root certificates. To identify and resolve a SSL connection failure, see [Identifying SSL Connection Failure](#) and [Installing Root Certificates](#).
7. If your devices are covered under the Dell ProSupport Plus service contract, you must:
 - Upgrade to SupportAssist version 1.2 or later.
 - * To identify the version of SupportAssist installed on the system, click **About** in the SupportAssist dashboard.
 - * To download the latest version of SupportAssist, go to dell.com/SupportAssistGroup.
 - Configure SupportAssist to collect the system logs periodically. See [Configuring Periodic Collection Of System Logs \(ProSupport Plus Only\)](#).

 **NOTE:** If you want SupportAssist to monitor Dell Force10 S4810 Ethernet switches, you must rediscover Force10 S4810 Ethernet switches in OpenManage Essentials. For information about discovering devices in OpenManage Essentials, see the *Dell OpenManage Essentials User's Guide* at dell.com/OpenManageManuals.

 **NOTE:** SupportAssist version 1.2 provides limited support for Dell PowerEdge VRTX. In SupportAssist version 1.1.1, the PowerEdge VRTX device is displayed as an iDRAC7 device. After upgrading SupportAssist from version 1.1.1 to 1.2, the PowerEdge VRTX device continues to display as an iDRAC7 device. To ensure that the PowerEdge VRTX device is displayed as expected after the upgrade, in OpenManage Essentials, remove the PowerEdge VRTX device and discover it again.

8. Verify that SupportAssist is able to generate the system log collection and upload it to Dell successfully. See [Verifying the System Log Collection/Upload Configuration](#).

Setting Up OpenManage Essentials For SupportAssist


For SupportAssist to automatically generate support cases if there is a hardware issue in your environment, you must set up OpenManage Essentials as follows:

1. Configure SNMP services on all managed nodes. See [Configuring SNMP Services On Systems Running Windows](#).
2. On all managed nodes that are not Dell 12G servers, ensure that Dell OpenManage Server Administrator (OMSA) is installed. For information on installing OMSA, see the *Dell OpenManage Server Administrator User's Guide* at [dell.com/OpenManageManuals](#).
3. On all managed nodes running Microsoft Windows Server 2008, ensure that network discovery is enabled. See [Enabling Network Discovery \(Windows Server 2008 Only\)](#).
4. 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* white paper at [DellTechcenter.com/OME](#).
5. Verify the firewall and ensure that the following ports are open:
 - On the management server, port 162 for SNMP, port 443 for SSL communication, and port 80 for getting new SupportAssist release information.
 - On the managed node, port 161 for SNMP and port 1311 for OMSA.

Configuring SNMP Services On Systems Running Windows

To allow OpenManage Essentials to receive SNMP alerts from supported devices, you must configure SNMP services on all managed nodes.

1. Click **Start** → **Run**.
The **Run** dialog box is displayed
2. In the **Open** box, type `services.msc`, and click **OK**.
The **Services** window is displayed
3. Browse the list of services, and ensure that the status of the **SNMP Service** is displayed as **Started**.
4. Right-click **SNMP Service** and select **Properties**.
The **SNMP Service Properties** dialog box is displayed.
5. Click the **Security** tab, and perform the following:
 - 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** field, 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** field, type the OpenManage Essentials server name or address, and click **Add**.

6. Click the **Traps** tab, and perform the following:
 - a) In the **Community name** box, type the community name, and click **Add to list**.
 - b) Under **Trap destinations**, click **Add**.
The **SNMP Service Configuration** dialog box is displayed.
 - c) In the **Host name, IP or IPX address** field, type the OpenManage Essentials server name or address, and click **Add**.
7. Click **Apply**.
8. In the **Service** 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.

Enabling Network Discovery (Windows Server 2008 Only)

On all managed nodes running Microsoft Windows Server 2008, you must enable network discovery, to allow the nodes to be discovered by the management server.

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:


1. If the management server connects to the Internet through a proxy server, you must configure **Proxy Settings** in SupportAssist. To configure the proxy server settings, click **Settings** → **Proxy Settings**, and follow the instructions on the screen.
2. Configure the Administrator credentials of each supported device type in your environment in SupportAssist. See [Configuring The Default Device Type Credentials](#).
3. Verify that the SupportAssist client is able to communicate with the SupportAssist server hosted by Dell by performing the email connectivity test. See [Email Connectivity Test](#).
4. If there is a SSL connection failure, you must install the required root certificates. To identify and resolve a SSL connection failure, see [Identifying SSL Connection Failure](#) and [Installing Root Certificates](#).
5. 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 diagnostic test results are uploaded.
 - <http://ftp.dell.com/> — for getting new SupportAssist release information.

Configuring The Default Device Type Credentials

SupportAssist runs the appropriate collection tools and gathers the system logs when a hardware issue is detected in your environment. To run the collection tools on your supported devices, you must configure SupportAssist with the Administrator credentials for each managed device type.

 **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.
2. Under **Edit Device Type Credentials**, select the **Device Type** and **Credential Type**.
3. Type the Administrator credentials [**Username**, **Password**, **Enable Password** (for Ethernet switches only), and **Community String** (for Dell EqualLogic devices 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 Force10 and PowerConnect Ethernet switches the domain name need not be specified.

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


Example of Linux, 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 using the **Edit Device Credentials** link in the **Devices** tab.


Configuring Periodic Collection Of System Logs (ProSupport Plus Only)

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.

 **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.
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. 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 [Recommendations For Scheduling Periodic Collection](#).

 **NOTE:** When the **Frequency** is set to **None**, restart of the SupportAssist service is known to fail. To avoid this issue, before you attempt to either restart the SupportAssist service manually or restart the server running SupportAssist, it is recommended that the **Frequency** is set to either **Weekly** or **Monthly**. After the SupportAssist service is restarted, you can set the **Frequency** to **None**.

7. Repeat step 5 and step 6 until you have scheduled the collection of system logs for all supported device types in your environment.
8. Click **Save Changes**.


Recommendations For Scheduling Periodic Collection

The following table provides recommendations for scheduling periodic collections in an environment that consists of a device mix 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.

Table 1. Recommendations For Scheduling Periodic Collection

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	0.1 to 7.2	0.1 to 9	Weekly (overnight)
300 or more	7.2 to 47	9 to 60	For EqualLogic and Force10 devices — Weekly (overnight) For Dell PowerEdge and Dell PowerConnect devices — Monthly (at different times during the week for each device type)


Email Connectivity Test

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

1. In SupportAssist, move the mouse pointer over the <user name> link that is displayed beside the **Help** link, and then click **Connectivity Test**.
2. In the **Connectivity Test** page, click **Send**.
The SupportAssist server receives the connectivity test, and sends a sample email with connectivity status to the primary and secondary (optional) contact. If the connectivity status email is not received, see the [Troubleshooting](#) section.

Verifying The System Log Collection/Upload Configuration

To verify that SupportAssist is configured correctly to upload system logs to Dell:

1. Click the **Devices** tab.
The **Device Inventory** page is displayed.
2. Select the first device in the **Device Inventory**.
 **NOTE:** You can only select a device that has a valid Service Tag. If a device does not have a valid Service Tag, the check box for that device is disabled.
The **Send System Logs** link is enabled.
3. Click **Send System Logs**.
The status of the system log collection is displayed in the **Collection 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**.

When SupportAssist is able to successfully generate the system log collection and upload it to Dell, the **Collection Status** column displays **Collection Uploaded**. For information on troubleshooting problems with the generation and upload of the system log collection, see [Troubleshooting System Log Collection/Upload Failure](#).

Troubleshooting

This section provides information about the following:

- [Troubleshooting Email Connectivity Test Failure](#)
- [Troubleshooting System Log Collection/Upload Failure](#)

Troubleshooting System Log Collection/Upload Failure

- If the generation of the system log collection fails for a device (**Collection Status** displays **Failed to Run**):
 - Make sure that the default credentials for the device are configured correctly in the **Settings** → **System Logs** tab. To edit the credentials for the device, select the device in the **Device Inventory**, and click **Edit Device Credentials**
- If the upload of the system log collection fails for a device (**Collection Status** displays **Collection Failed to Upload**):
 - Make sure that the proxy server credentials are configured correctly in the web browser, and confirm if you can access the internet using the browser.

To verify if the issue is resolved, select the device in the **Device Inventory** and click **Send System Logs**. The status of the system log collection is displayed in the **Collection Status** column.

Troubleshooting Email Connectivity Test Failure

The email 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 email connectivity test fails, there may be a SSL connection failure.

If there is a SSL connection failure, you must install the required root certificates. To identify and resolve SSL connection failure, see [Identifying SSL Connection Failure](#) and [Installing Root Certificates](#).

Identifying SSL Connection Failure

SSL connection failure may occur if your 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. To install the certificates, see [Installing Root Certificates](#).

Installing Root Certificates

Before you begin, ensure the following:

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

To resolve SSL connection issues, you must install the following root certificates in the **Trusted Root Certification Authorities** and **Intermediate Certification Authorities** folders of the current user and local computer:

- **Dell_Inc_Enterprise_Issuing_CA1.cer**
- **Dell_Inc_Enterprise_CA.cer**
- **GTE_CyberTrust Global Root.cer**

To install root certificates:

1. Click **Start** → **Run**.
The **Run** dialog box is displayed.
2. In the **Open** box, type `mmc`, and click **OK**.
The **Console 1 – [Console Root]** window is displayed.
3. Click **File** → **Add/Remove Snap-in**.
The **Add or Remove Snap-ins** dialog box is displayed.
4. Under **Available snap-ins**, select **Certificates**, and click **Add >**.
The **Certificates snap-in** dialog box is displayed.
5. Ensure that **My user account** is selected, and then click **Finish**.
6. In the **Add or Remove snap-ins** dialog box, click **Add >**.
The **Certificates snap-in** dialog box is displayed.
7. Select **Computer account** and click **Next**.
The **Select Computer** dialog box is displayed.
8. Ensure that **Local computer (the computer this console is running on)** is selected, and click **Finish**.
9. In the **Add or Remove snap-ins** dialog box, click **OK**.
10. Under the **Console Root**, click **Certificates – Current User**.
11. Right-click **Trusted Root Certification Authority** → **All Tasks** → **Import**.
The **Certificate Import Wizard** is displayed.
12. Click **Next**.
The **File to Import** dialog box is displayed.
13. Browse to select the location of the certificate files, select a certificate file and click **Next**.
The **Certificate Store** information is displayed.
14. Click **Next**.
15. Click **Finish**.
16. Perform step 11 to step 15 until all three certificate files are imported.
17. Right-click **Intermediate Certification Authorities** → **All Tasks** → **Import**.
The **Certificate Import Wizard** is displayed.
18. Perform step 12 to step 15 until all three certificate files are imported.
19. Under the **Console Root**, click **Certificates – Local Computer**.
20. Right-click **Trusted Root Certification Authority** → **All Tasks** → **Import**.
The **Certificate Import Wizard** is displayed.
21. Perform step 12 to step 15 until all three certificate files are imported.
22. Right-click **Intermediate Certification Authorities** → **All Tasks** → **Import**.

The **Certificate Import Wizard** is displayed.

23. Perform step 12 to step 15 until all three certificate files are imported.