Dell OpenManage Essentials

Version 1.0

User’s Guide

Notes and Cautions

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

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

2012 - 1

Contents

1

About OpenManage Essentials

OpenManage Essentials is a hardware management application that provides a comprehensive view of Dell systems, devices, and components in the enterprise's network. With OpenManage Essentials, a web-based and one-to-many systems management application for Dell systems and other devices, you can:

- Discover and inventory the systems.
- Monitor systems' health.
- View and manage system alerts.
- Perform system updates.
- View hardware inventory and compliance reports.

2

Installing OpenManage Essentials

Installation Prerequisites and Minimum Requirements

For a list of supported platforms, operating systems, and browsers, see the *Dell OpenManage Essentials Support Matrix* at **support.dell.com/manuals**.

To install OpenManage Essentials, you require local system administrator privileges and the system you are using must meet the criteria mentioned in Table 1 and Table 2.

NOTE: It is recommended that you do not install OpenManage Essentials on a domain controller system. The installer does not allow you to proceed with the installation and displays an operating system not supported error message.

Table 1. Minimum Recommended Hardware

Minimum Recommended Hardware	Large Deployments	Medium Deployments		Small Deployments	
Number of Devices	2000	500	300	100	100
Type of System	Physical Machines / Virtual Machines	Physical Machines / Virtual Machines	Physical Machines / Virtual Machines	Physical Machines / Virtual Machines	Physical Machines / Virtual Machines
RAM	8 GB	6 GB	6 GB	6 GB	4 GB
Processors	8 cores total	4 cores total	4 cores total	2 cores total	2 cores total
Database	SQL Standard	SQL Express	SQL Express	SQL Express	SQL Express
Database Location	Remote	Local	Local	Local	Local
Hard Drive	10 GB	6 GB	6 GB	6 GB	6 GB

Table 2. Minimum Requirements

Particulars	Minimum Requirement
Operating Systems	• Microsoft Windows Server 2008 Standard Edition (x86 and x64) • Windows Server 2008 Enterprise Edition (x86 and x64) • Windows Server 2008 R2 Standard Edition • Windows Server 2008 R2 Enterprise Edition
Network	100 Mbps or higher
Web Browser	• Microsoft Internet Explorer 8 or later • Mozilla Firefox
User Interface	Microsoft Silverlight version 4.0 or version 5.0
.NET	4.0

Downloading OpenManage Essentials

You can download OpenManage Essentials from **support.dell.com** or the Dell TechCenter website.

Terms and Conditions for Using Relational Database Management Systems

The relational database management system (RDBMS) used for installing OpenManage Essentials is an SQL server. The SQL server has configuration settings separate from the OpenManage Essentials database. The server has logins (SQL or Windows) that may or may not have access to the OpenManage Essentials database.

NOTE: You require a sysadmin role to perform the SQL server tasks.

When OpenManage Essentials is installed, Internet security is modified by adding registry entries to the ZoneMaps for HKLM and HKCU. This ensures that Internet Explorer identifies the fully qualified domain name as an intranet site.

A self-signed certificate is created and this certificate is installed in the root Certificate Authorities (CA) and My certificates. However, it is recommended to use a custom certificate.

To prevent certificate errors, remote clients must install OpenManage Essentials certificate in both CA and Root Certificate Stores to remove the certificate errors.

For a Typical install of OpenManage Essentials:

- Use the local version of SQL Server that has all supported components.
- The RDBMS is altered to support both SQL and Windows authentication.
- An SQL login is generated for OpenManage Essentials' services and this login is added as a RDBMS SQL login with sysadmin privileges.

  NOTE: The password for the SQL login is controlled by the application and is different on every system.

It is recommended that a custom install is selected when you want to use a domain service account for added security and SQL Server Management Studio (SSMS) selection.

For a Custom install of OpenManage Essentials, provide the Windows or SQL login.

At runtime, when the OpenManage Essentials website determines that it has an invalid certificate or certificate binding; the self-signed certificate is regenerated.

Installing OpenManage Essentials

1 Double-click the OpenManage Essentials executable file.

  The **Dell OpenManage Install** screen is displayed. The following options are available:

  - **Dell OpenManage Essentials**—Select this option to install **Dell OpenManage Essentials** and the **Troubleshooting Tool**.
  - **Dell Repository Manager**—Select this option to install Dell Repository Manager. Using Repository Manager, you can create customized bundles and repositories of Dell Update Packages, software utilities such as update drivers, firmware, BIOS, and other applications.
  - **Dell License Manager**—Select this option to install the Dell license manager. Dell License Manager is a one-to-many license deployment and reporting tool for managing the Dell iDRAC 7 licenses.

- **Documentation**—Click this link to view the online help.
- **View Readme**—Click this link to view the readme file. To view the latest readme, go to **support.dell.com/manuals**.

2 In **Dell OpenManage Install**, select **Dell OpenManage Essentials** and click **Install**.

The Dell OpenManage Essentials Prerequisites window, displays the following requirement types:

- **Critical**—This error condition prevents the installation of a feature.
- **Warning** —This warning condition may disable the **Typical** installation but not an **Upgrade** of the feature later during installation. Also, later during installation, use the **Custom** installation setup type to select the feature.
- **Information**—This informational condition does not affect the **Typical** selection of a feature.

There are two options for resolving critical dependencies:

- Click **Install All Critical Prerequisites** to immediately begin installing all critical prerequisites without further interaction. **Install All Critical Prerequisites** may require a reboot depending on the configuration and the Prerequisites installation will resume automatically after restart.
- Install each prerequisite individually by clicking the associated link with the required software.

NOTE: To configure remote database, you do not require an SQL Express installation on the local system. See Setting Up OpenManage Essentials Database on a Remote SQL Server. If you are not configuring remote database, you can install SQL Express by clicking the warning prerequisite link. Selecting **Install All Critical Prerequisites** does not install SQL Express.

3 Click **Install Essentials**.

4 In the install wizard for OpenManage Essentials, click **Next**.

5 In the **License Agreement** page, read the license agreement, select **I accept the terms in the license agreement**, and then click **Next**.

6 In **Setup type** select either **Typical** or **Custom** installation.

If you selected **Typical**, click **Next.** Verify the installation settings in the **Ready to Install the Program** page and the click **Install**.

If you selected **Custom**, in **Custom Setup**, click **Next** and do the following:

- **a** In **Custom Setup**, click **Change** to change the installation location, and then click **Next**.
- **b** In custom settings for port numbers, if required, change default values for **Network Monitoring Service port number**, **Task Manager Service port number**, and **Console Launch port** and then click **Next**.
- **c** In **Database Server**, do any of the following and then click **Next**:
  - Local database—If you have many SQL server versions available on the management system and you want to select an SQL server on which you want to set up the OpenManage Essentials database, then select the SQL server from the **Database Server** list, the type of authentication, and provide the authentication details.
  - Remote database— Complete the prerequisites. For more information, see Setting Up OpenManage Essentials Database on a Remote SQL Server. After the prerequisites are complete, click **Browse** and select the remote system and then provide the authentication details. You can also set up the OpenManage Essentials database on a remote system by providing the IP address or host name and the database instance name of the remote system in **Database Server.**

NOTE: If you have multiple database instances running on a selected database server, you can specify the required database instance name to configure the Essentials database with it. For example, using (local)\MyInstance, you are configuring Essentials database on a local server and MyInstance named database instance.

- **d** Verify the installation settings in the **Ready to Install the Program** page and the click **Install**.

7 After the installation is complete, click **Finish**.

Setting Up OpenManage Essentials Database on a Remote SQL Server

You can configure OpenManage Essentials to use an SQL server present on a remote system. Before setting up the OpenManage Essentials database on the remote system, check for the following prerequisites:

- Network communication between the OpenManage Essentials system and the remote system is functioning.
- SQL connection works between the OpenManage Essentials system and the remote system for the specific database instance. You can use the **Windows ODBC Data Source Administrator** tool to verify the connection. On the remote database server, enable TCP/IP protocol and if you are using SQL Authentication, enable mixed mode on the remote SQL server.

You can retarget your database if:

- Your SQL credentials to the SQL server fails.
- Your Windows credentials to the SQL server fails
- Database is moved.

Installing Repository Manager

1. In **Dell OpenManageInstall**, select **Dell Repository Manager**, and then click **Install**.
2. In **Dell Repository Manager - InstallShield Wizard**, click **Next**.
3. In **License Agreement**, select **I accept the terms in the license agreement**, and click **Next**.
4. In **Customer Information**, do the following and then click **Next**.
   a. Provide user name and organization information.
   b. Select either **Anyone who uses this computer (all users)** to make this application available to everyone or **Only for me (Windows User)** to retain access.
5. In **Destination Folder**, use the default location or click **Change** to specify another location, and then click **Next**.
6. In **Setup Type**, do any of the following and then click **Next**.

- Select **Complete** to install all the Repository Manager features.
- Select **Custom** to choose program features you want to install.

7 In **Ready to Install the Program**, click **Install**.

8 After the installation is complete, click **Finish**.

Uninstalling OpenManage Essentials

△ **CAUTION: Uninstalling OpenManage Essentials deletes your database. While installing upgrades, it is recommended to install the upgrades on top of the existing version of OpenManage Essentials to preserve the database.**

1 Click **Start→ Control Panel→ Programs and Features**.

2 In **Uninstall or change a program**, select **Dell OpenManage Essentials** and click **Uninstall**.

3 In the message **Are you sure you want to uninstall OpenManage Essentials?**, click **Yes**.

Migrating IT Assistant to OpenManage Essentials

To replace IT Assistant with OpenManage Essentials while preserving the existing IT Assistant database:

1 Double-click the OpenManage Essentials executable file.

2 In **Dell OpenManage Install**, select **Dell OpenManage Essentials** and click **Install**.

The check dependencies page is displayed. This page lists the following requirement types:

- **Critical**—This error condition will prevent the installation of a feature.
- **Warning**—This warning condition disables the **Typical** installation but not an **Upgrade** of the feature later during installation. Also, later during installation, use the **Custom** installation setup type to select the feature
- **Information**—This informational condition will not affect the **Typical** selection of a feature.

There are two options for resolving critical dependencies:

- Click **Install All Critical Prerequisites** at the bottom of the page to immediately begin installing all necessary prerequisites without further interaction.
- Install each prerequisite individually by clicking the associated link with the required software.

3 Click **Install Essentials**.

4 In the install wizard for OpenManage Essentials, click **Next**.

5 In the License Agreement page, read the license agreement, select **I accept the terms in the license agreement** and then click **Next**.

6 In **Setup type**, select **Custom**.

7 In **Custom Setup**, click **Next**.

8 In **Custom Settings**, verify or change the default port numbers and click **Next**.

9 In **Database Server**, enter the required parameters to connect to the IT Assistant database and click **Next**.

NOTE: During the replacement process, a copy of the IT Assistant database is created and utilized by OpenManage Essentials.

10 In **Ready to Install the Program**, review your settings and click **Install**.

11 After the installation is complete, click **Finish**.

Migration Use Cases

If you migrate from IT Assistant to OpenManage Essentials, IT Assistant is uninstalled and replaced by OpenManage Essentials. However, the IT Assistant database (ITAssist) remains and you can retrieve it from the SQL server. Table 3 provides information about different migration use cases.

Table 3. Migration Use Cases

Number	Use Case Conditions	Outcome
1	• IT Assistant is installed on the local system. • The IT Assistant database is located on the local system. • OpenManage Essentials is installed on the local system. • The OpenManage Essentials database is installed on the local system.	Data from the IT Assistant database is copied to the OpenManage Essentials database.
2	• IT Assistant is installed on the local system. • The IT Assistant database is located on the local system. • OpenManage Essentials is installed on the local system. • The OpenManage Essentials database is installed on a remote system.	Data from the IT Assistant database is not copied to the OpenManage Essentials database.
3	• IT Assistant is installed on the local system. • The IT Assistant database is located on a remote system. • OpenManage Essentials is installed on the local system. • The OpenManage Essentials database is installed on the local system.	Data from the IT Assistant database is not copied to the OpenManage Essentials database.
4	• IT Assistant is installed on the local system. • The IT Assistant database is located on a remote system. • OpenManage Essentials is installed on the local system. • The OpenManage Essentials database is installed on a different remote system.	Data from the IT Assistant database is not copied to the OpenManage Essentials database.

Table 3. Migration Use Cases

Number	Use Case Conditions	Outcome
5	• IT Assistant is installed on the local system. • The IT Assistant database is located on a remote system. • OpenManage Essentials is installed on the local system. • The OpenManage Essentials database is installed on a the same remote system as the IT Assistant database.	Data from the IT Assistant database is copied to the OpenManage Essentials database.

List of Migrated and Non-Migrated Components

Table 4. List of Components

Components That are Migrated	Components That are not Migrated
Discovered and inventoried devices	OpenManage Server Administrator push packages
Discovery/inventory include and exclude ranges	Server Administrator push tasks
Health status of the devices	Software update tasks
Discovery, inventory, and statusing schedule/settings	Software updates (imported Dell update packages)
Alerts received in IT Assistant	Application launch, e-mail, and trap forward alert actions
Custom alert view filters	IT Assistant reports
Ignore alert actions	Device health search query data
Alert log settings and application logs	Server and client software updates
Received alerts	IPMI command line tasks
All remote tasks except IPMI and OMSA deploy tasks.	Power control device tasks

Table 4. List of Components

Components That are Migrated	Components That are not Migrated
Polling schedule configuration	Import Dell catalog task and data
On-demand statusing	Server Administrator deployment for Windows and Linux

3

Getting Started With OpenManage Essentials

Logging On to OpenManage Essentials

To log on to OpenManage Essentials:

- From the management station desktop, click the **Essentials** icon.
- From the management station desktop, click **Start→ All Programs→ Dell OpenManage Applications→ Essentials→ Essentials.**
- From a remote system, launch a supported browser. In the address field, type **https://<IP address, host name, or Fully Qualified Domain Name (FQDN) >:<Port Number>/web/default.aspx**.

  NOTE: FQDN is required to show a valid certificate. The certificate shows an error if an IP address or local host is used.

  The console launch port number (default port number 2607) is required to launch OpenManage Essentials from a browser on a remote system. While installing OpenManage Essentials, if you changed the port using the **Custom Install** option, use the selected console launch port in the preceding URL.

The **First Time Setup** page is displayed.

Configuring OpenManage Essentials

If you are logging on to OpenManage Essentials for the first time, the **First Time Setup** tutorial is displayed. The tutorial provides step-by-step instructions for setting up an environment of servers and devices to communicate with OpenManage Essentials. The steps include:

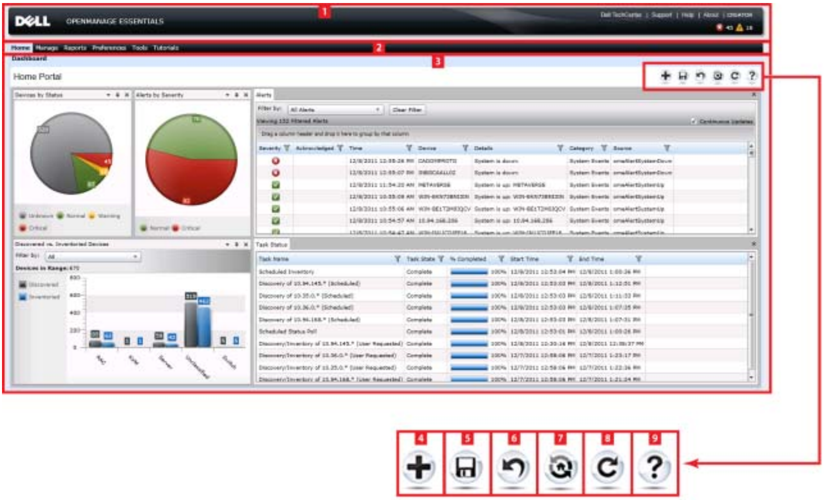
- Configuring the SNMP protocol on each target server.
- Installing Dell OpenManage Server Administrator on each target server.

- Enabling network discovery (For Windows Server 2008-based servers) on each target server.
- Discovering devices on your network.

After you have completed the **First Time Setup** wizard, the Discovery Range Configuration is displayed, for more information, see Configuring a Discovery and Inventory Task.

Using the OpenManage Essentials Home Portal

OpenManage Essentials user interface contains these components:


1
DELL
OPENMANAGE ESSENTIALS
Dell TechCenter | Support | Help | About
2
Home Manage Reports Preferences Tools Tutorials
3
Dashboard
Home Portal
Devices by Status
Alerts by Severity
Alerts
Discovered vs. Inventoried Devices
Task Status
4
5
6
7
8
9

1	Logo and banner	2	Menu items
3	Console area	4	Add a report to the home portal
5	Save the current home portal layout	6	Load the last saved home portal layout
7	Load the default home portal layout	8	Refresh the home portal page
9	Launch the online help		

Customizing the Home Portal

You can change the layout of the portal page to accomplish the following:

- Display additional available reports.
- Hide graphs and reports.
- Rearrange or resize graphs and reports by dragging and dropping.

If a pop up window on any screen is bigger than the screen and if scrolling is not possible, set the browser's zoom value to 75% or less to make it visible.

From the various reports that are available, you can select specific reports and set them to display on the Dashboard. You can click on these reports to further drill-down and get more details; for the list of available reports see Home Portal Reports.

For more information on Home portal, see OpenManage Essentials Home Portal - Reference.

Displaying Additional Available Reports and Graphs

Charts have drill-down feature.

To view additional reports and graphs, click the + icon on the top right corner to see and display the list of available reports and graphs.

- Alerts by Severity
- Devices by Status
- Discovered versus Inventoried Devices
- Alerts
- Field Replaceable Unit (FRU) Information
- Hard Drives Inventory
- HyperV Information
- Memory
- Modular Enclosures
- NIC Information
- PCI Device Information

- Server Components and Versions
- Server Overview
- Storage Controllers
- Task Status
- ESX Information

After selecting the desired report, dock the control using the ✥ control to the desired location.

Drilling-Down Charts and Reports for More Information

To drill-down for further details, do the following:

- In report charts, click the charts and further details are displayed.
- In report tables, use the drag and drop option or funnel options to filter for the required data and use right-click options to perform various tasks.

Saving and Loading the Home Portal Layout

To save and load the Home portal layout, click the 💾 icon to save changes to the portal page layout.

All the current layout settings and visible reports on the portal are saved on the portal page.

To load the previous portal layout, click the ↶ icon.

Updating the Portal Data

To refresh the portal page manually, click the ⟳ icon.

To load the default portal layout, click the ⟲ icon.

Hiding Graphs and Reports (Components)

To hide graphs and reports (components): Click the ▼ icon on the report or graph and select the **Hide** option to remove the component from the portal page or select the **Auto Hide** option to move the component to the side bar.

To remove a component from the portal page, click the **X** icon in the report or graph.

To move the report to the side bar, click the 📌 icon.

Re-arranging or Re-sizing Graphs and Reports (Components)

Click the ▾ icon and select from the following options:

- **Floating**—To move the component freely in the portal page.
- **Dockable**—To dock the component in the portal page. If the component is floating, right-click the title to dock or tab the component.
- **Tabbed Document**—To move the component into a tab in the portal page.

Select the ✥ control to dock a floating component. You can create a tabbed view by docking a pane within other panes or dock a pane at the top, bottom, left, or right side of the main window.

You can resize panes and all panes will fill the selected area when docked.

To move the component to the side bar, click the 📌 icon and to restore it, select the component and click the ⊣ icon.

To create filters in a report grid, click the ▽ icon. This is not specific to the portal page layout and the settings related to these associations are not saved.

Filtering Data

You can filter the results by dragging and dropping column headers to the top of reports. You can choose one or more attributes when revising the view to meet your specific needs.

For example, in **Devices by Status** pie chart, click a status such as **Critical**. In the **Device Summary** page, drag the **Device Type** and **Service Tag** to the top of the report. The view immediately changes to a nested information based on your preference. In this example, the information is grouped first by **Device Type**, and second by **Service Tag**. Drill-down through these filtered groups to see the remaining information for the devices.

For more information, see Viewing Device Summary.

OpenManage Essentials Home Portal - Reference

This dashboard page provides a snapshot of the managed devices that include servers, storage, switches, and so on.

OpenManage Essentials Heading Banner

The banner displays the Critical and Warning icons including the number of devices. You can view the devices in either state by clicking the icon or the number. The banner also contains links to the following:

- **Dell TechCenter—**Click to open Dell's web page that contains information on various technologies and a web page where there is sharing of knowledge, best practices, and information about Dell products and your installations.
- **Support —**Click to open **support.dell.com**.
- **Help—**Click to open the online help.
- **About—**Click to view general OpenManage Essentials product information.
- Current User (For example, Administrator)—Specifies the current user. The tool tip displays the user's OpenManage Essentials roles.

NOTE: The banner is available in all the pages.

Home Portal Reports

From the Home Portal Dashboard page, you can monitor the following:

- Alerts by Severity
- Devices by Status
- Discovered versus Inventoried Devices
- Alerts
- Field Replaceable Unit (FRU) Information

- Hard Drives Inventory
- HyperV Information
- Memory
- Modular Enclosures
- NIC Information
- PCI Device Information
- Server Components and Versions
- Server Overview
- Storage Controllers
- Task Status
- ESX Information

Device by Status

Device by status provides device status information in a pie chart format. Click a segment of the pie chart to view the device summary.

Unknown	Health status of these devices are not known.
Normal	These devices are working as expected.
Warning	These devices display behaviors that are not normal and further investigation is required.
Critical	These devices display behaviors that suggest an occurrence of a failure of a very important aspect.

Alerts by Severity

Alerts by severity provides alert information of devices in a pie chart format. Click a segment of the pie chart to view the devices.

Normal	Alert from these devices confirm to the expected behavior for the devices.
Critical	Alerts from these devices suggest that a failure of a very important aspect has occurred.

Unknown	Health status of these devices are not known.
Warning	These devices display behaviors that are not normal and further investigation is required.

Discovered Versus Inventoried Devices

See Discovered Versus Inventoried Devices.

Task Status

See Task Status.

5

Discovering and Inventorying Devices

Perform Discovery and Inventory in order to manage your network devices.

Supported Devices and Protocols

Following are the supported devices and associated protocols.

Protocol / Mechanism		**Simple Network Management Protocol (SNMP)**	**Windows Management Instrumentation (WMI)**	**Web Services-Management (WSMAN)**
Dell servers with OpenManage Server Administrator installed	Windows / Hyper-V	• Discovery • Correlation • Classification • Hardware inventory • Software inventory monitoring • Traps/alerts application launch: • OpenManage Server Administrator console • Remote desktop • Warranty	• Discovery • Correlation • Classification • Hardware inventory • Software inventory monitoring • Application launch • OpenManage Server Administrator console • Remote desktop • Warranty	NS

Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WSMAN)
	Linux/ VMware ESX	• Discovery • Correlation • Classification • Hardware inventory • Software inventory • Monitoring • Traps/alerts • Application launch: • OpenManage Server Administrator console • Warranty	NS	NS

Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WSMAN)
	VMware ESXi	Traps/Alerts	NS	• Discovery • Correlation • Classification • Hardware inventory • Software inventory • Virtual machine information • Virtual host product information • Monitoring (OpenManage Server Administrator health only) • Application launch: warranty
Dell servers without OpenManage Server Administrator installed	Windows/Hyper-V	Discovery (Unknown)	• Discovery • Correlation • Classification • Hardware inventory • Application launch • Remote desktop • Warranty	NS
	Linux/VMware ESX	Discovery (Unknown)	NS	NS

Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WSMAN)
	VMware ESXi	NS	NS	• Discovery • Correlation • Classification • Hardware inventory (no storage inventory)
iDRAC / DRAC / BMC		• Discovery • Correlation • Classification • Monitoring • Traps/Platform Event Traps (PET) • Application launch • RAC • Console • Warranty	NS	NS
Modular enclosure (M1000e)		• Discovery • Correlation • Classification • Enclosure health • Traps • Application launch • CMC • Console • Warranty	NS	NS

Supported Operating Systems (Servers), Protocols, and Features Matrix

Protocol / Mechanism		**Intelligent Platform Management Interface (IPMI)**	**Command Line Interface (CLI)**[a]
Dell servers with OpenManage Server Administrator installed	Windows /Hyper-V	NS	• OpenManage Server Administrator CLI • Deploy OpenManage Server Administrator • Server Updates • BIOS • Firmware • Driver
	Linux/ VMware ESX	NS	• OpenManage Server Administrator CLI • Deploy OpenManage Server Administrator • Server updates: • BIOS • Firmware • Driver
	VMware ESXi	NS	NS
Dell servers without OpenManage Server Administrator installed	Windows/Hyper-V	NS	Deploy OpenManage Server Administrator
	Linux/VMware ESX	NS	Deploy OpenManage Server Administrator
	VMware ESXi	NS	NS

Protocol / Mechanism	Intelligent Platform Management Interface (IPMI)	Command Line Interface (CLI)[a]
iDRAC / DRAC / BMC	• Discovery • Classification • Correlation • iDRAC health • Application launch • RAC console • Warranty[b]	• RACADM CLI • IPMI CLI
Modular Enclosure (M1000e)	NS	• RACADM CLI • IPMI CLI

a. You cannot perform this task if the device is not discovered, inventoried, or both.

b. Requires internet connection (**support.dell.com**) to view warranty information.

Supported Operating Systems (Storage), Protocols, and Features Matrix

Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Symbol	EMC NaviSphere CLI
Storage Devices	EqualLogic	• Discovery • Correlation • Classification • Hardware inventory • Monitoring • Traps/alerts • Application launch • EqualLogic console	NS	NS

Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Symbol	EMC NaviSphere CLI
	Dell|EMC **NOTE:** Both SNMP and Navisphere are required for complete management of Dell|EMC devices.	• Discovery • Correlation • Classification • Traps/Alerts	NS	• Hardware inventory • Monitoring • Application launch • EMC Navisphere Manager
	PowerVault	Traps/Alerts	• Discovery • Correlation • Classification • Hardware inventory • Monitoring • Application launch – Modular Disk Storage Manager[a]	NS
	Tape	• Discovery • Correlation • Classification • Hardware inventory • Monitoring • Traps/alerts • Application launch • Tape console • Warranty[b]	NS	NS

[a] Requires Modular Disk Storage Manager Controller software installed on the OpenManage Essentials system.

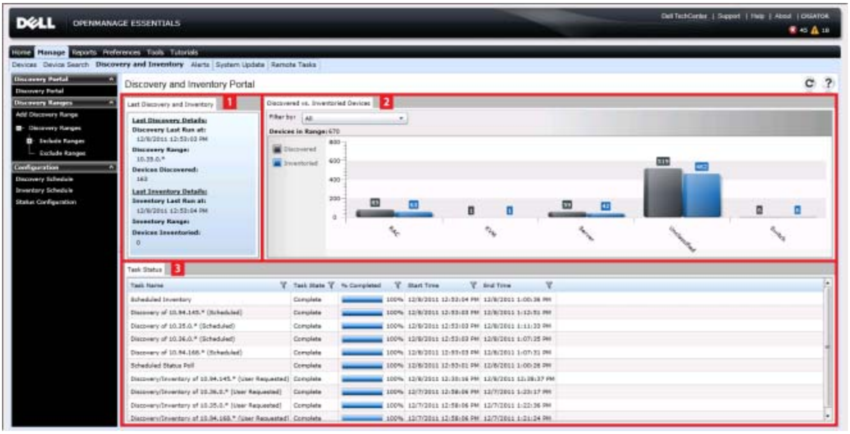
[b] Requires internet connection (**support.dell.com**) to view warranty information.

Legend and Definitions

- **NS:** Not Supported
- **Discovery:** Capability to discover the device on the network.
- **Correlation:** Capability to correlate:
  - Discovered server and DRAC, iDRAC, or BMC devices.
  - Discovered modular systems or switches.
  - ESX, ESXi, or Hyper-V host and guest virtual machines.
- **Classification:** Capability to classify the devices by type. For example, servers, network switches, storage, and so on.
- **Hardware Inventory:** Capability to obtain detailed hardware inventory of the device.
- **Monitoring or Health:** Capability to obtain health status and connection status of the device.
- **Traps, alerts, or PETs:** Capability to receive SNMP traps from the device.
- **Application Launch:** Provides a right-click action menu item on the discovered device to launch 1x1 console or application.
- **OpenManage Server Administrator CLI:** Capability to run OpenManage Server Administrator supported commands on the remote (discovered) servers.
- **Deploy OpenManage Server Administrator:** Capability to deploy OpenManage Server Administrator to the remote (discovered) servers.
- **Server Updates:** Capability to deploy BIOS, firmware, and driver updates to the remote (discovered) servers.
- **RACADM CLI:** Capability to run RACADM tool supported commands on the remote (discovered) devices.
- **IPMI CLI:** Capability to run IPMITool supported commands on the remote (discovered) devices.
- **Warranty:** Requires internet connection (**support.dell.com**) to view warranty information.

Using the Discovery and Inventory Portal

To access the discovery and inventory portal, click **Manage**→ **Discovery and Inventory**.



Last Discovery Details:
Discovery Last Run at: 12/8/2011 12:53:03 PM
Discovery Range: 10.35.0.*
Devices Discovered: 163

Last Inventory Details:
Inventory Last Run at: 12/8/2011 12:53:04 PM
Inventory Range:
Devices Inventoried: 0

Task Name	Task State	% Completed	Start Time	End Time
Scheduled Inventory	Complete	100%	12/8/2011 12:53:04 PM	12/8/2011 1:00:38 PM
Discovery of 10.94.145.* (Scheduled)	Complete	100%	12/8/2011 12:53:03 PM	12/8/2011 1:12:51 PM
Discovery of 10.35.0.* (Scheduled)	Complete	100%	12/8/2011 12:53:03 PM	12/8/2011 1:11:33 PM
Discovery of 10.36.0.* (Scheduled)	Complete	100%	12/8/2011 12:53:03 PM	12/8/2011 1:07:35 PM
Discovery of 10.94.168.* (Scheduled)	Complete	100%	12/8/2011 12:53:03 PM	12/8/2011 1:07:31 PM
Scheduled Status Poll	Complete	100%	12/8/2011 12:53:01 PM	12/8/2011 1:00:28 PM
Discovery/Inventory of 10.94.145.* (User Requested)	Complete	100%	12/8/2011 12:38:16 PM	12/8/2011 12:28:37 PM
Discovery/Inventory of 10.36.0.* (User Requested)	Complete	100%	12/7/2011 12:58:06 PM	12/7/2011 1:23:17 PM
Discovery/Inventory of 10.35.0.* (User Requested)	Complete	100%	12/7/2011 12:58:06 PM	12/7/2011 1:22:36 PM
Discovery/Inventory of 10.94.168.* (User Requested)	Complete	100%	12/7/2011 12:58:06 PM	12/7/2011 1:21:24 PM

1 Details from the last discovery and inventory task run.

2 Details of previously discovered and inventoried devices.

3 Details of tasks and their status.

Configuring a Discovery and Inventory Task

1 From OpenManage Essentials, click **Manage**→ **Discovery and Inventory**→ **Discovery Ranges**→ **Add Discovery Range**.

2 In **Discovery Range Configuration**:

   a Provide the IP address/range or host name and subnet mask. Click **Add**.

   NOTE: You can add multiple IP addresses, ranges, or host names. You can add multiple host names separated by a comma delimiter. For example, hostname1, hostname2, hostname3, and so on.

   b To import host names and IP addresses, click **Import**. You can import host names and IP addresses included as line items in a file that is in

CSV format. Using Microsoft Excel, you can create a .CSV file containing host names or IP addresses.

c Click **Next**.

3 After you have provided at least one IP address, IP range, host name, or a combination thereof, continue to customize the discovery and inventory options or complete the configuration using the default options.

Clicking **Finish** without setting any further configurations immediately runs the discovery and inventory tasks using the default SNMP and ICMP protocols. It is recommended that you review and revise your protocol configurations prior to clicking Finish.

For more information about each protocol listed below, click ? - (Why do I need this?) help.

NOTE: When discovering ESXi-based servers, to see the guest virtual machines grouped with the host, enable and configure the WS-Man protocol.

NOTE: By default, SNMP is enabled and values are assigned ICMP parameters.

NOTE: After completing any of the following steps, click either **Next** to continue or click **Finish** to complete the **Discovery Range Configuration**.

- In **ICMP Configuration**, to detect devices on the network, edit the ICMP parameters.
- In **SNMP Configuration**, to discover servers, provide the SNMP parameters. Ensure that the SNMP community string specified in **Get Community** matches the SNMP community string of the device or devices you wish to discover.
- In **WMI Configuration**, to authenticate and connect to remote devices, provide the WMI parameters. The format for entering credentials for WMI must be *domain\user name* for domain-based networks or *localhost\user name* for non-domain based networks.
- In **Storage Configuration**, to discover PowerVault modular disk array or EMC devices, edit parameters.
- In **WS-Man Credentials** configuration, to enable discovery of ESXi installed servers, provide WS-Man parameters.

- In **IPMI Configuration**, to enable server discovery, provide the IPMI parameters. IPMI is typically used to discover BMC or iDRACs on Dell servers. You can include the optional KG key when discovering RAC devices.
- In **Discovery Range Action**, choose to discover, inventory, or perform both tasks. The default option is to perform both discovery and inventory.

  Select **Perform only discovery** or **Perform both discovery and inventory** to run the task immediately.

  To schedule the task to run at a later time, select **Do not perform discovery or inventory**, and refer to the Scheduling a New Discovery Task or Scheduling a New Inventory Task sections.
- Review your selections in the Summary screen and click **Finish**. To change any of the parameters in previous configuration screens, click **Back**. When complete, click **Finish**.

Excluding Ranges

Configure exclude ranges to prevent servers from being discovered/rediscovered or limit the number of devices displayed in the device tree. To exclude a range from discovery task:

1. From OpenManage Essentials, select **Manage→ Discovery and Inventory→ Discovery Ranges**.
2. Right-click **Exclude Ranges** and then select **Add Exclude Range**.
3. In the **Create** screen, click **Ok**.
4. In **Exclude Range Configuration**, provide IP address/range or host name and click **Add**.
5. After the IP address or host name is listed, click **Finish**.

Viewing Configured Discovery and Inventory Ranges

From OpenManage Essentials, click **Manage→ Discovery and Inventory→ Discovery Ranges→ Discovery Ranges→ Include Ranges**.

Scheduling Discovery

1. Click **Manage→ Discovery and Inventory→ Configuration→ Discovery Schedule**.
2. In **Discovery Schedule Settings**:
    a. Select desired schedule parameters.
    b. **(Optional)** You may adjust the task speed slider for faster task execution; however, more system resources are consumed.
    c. Discover all instrumented devices.

Discovery Speed slider bar - This control, also known as the discovery throttle, controls how fast discovery occurs and how much network and system resources are consumed for discovery by controlling the:

- Number of discovery threads that are allowed to run at any one time.
- Delay in between the communicating devices during a network ping sweep, in milliseconds.

NOTE: Each tick on the throttle control equals 10% and the range is from 10% to 100%. By default, in OpenManage Essentials, the discovery throttle is set at 60%; Upon an upgrade from IT Assistant, the throttle control remains at its previously set value.

Multithreading

Dell OpenManage Essentials improves upon the optimized parallel threading implementation in the Network Monitoring Service introduced in IT Assistant.

As the discovery process is very I/O intensive, you can optimize the process by making it a parallel operation, where threads running in parallel (known as multi-threading) are sending requests and handling responses to several devices at once.

To an extent, the more threads that run in parallel, each communicating to a different device, the faster is the discovery; barring overall high network congestion or latency. The discovery process, by default, allows a maximum of 32 threads to run in parallel (or concurrently) at any one time for discovery.

To control the number of parallel threads executing, move the discovery throttle control either left or right. When set at the maximum, 32 parallel threads are actually allowed to run. If the throttle is at 50%, only 16 threads are allowed to run at any one time.

As the discovery service is optimized for parallel threading operations, the system can utilize more system resources even at the same throttle setting. It is recommended that you monitor the system resources so that a satisfactory trade-off is made between discovery speed versus system resources available for OpenManage Essentials. Lowering or increasing the throttle depends on the system it is running on and the available resources. Note that the discovery service may take up to several minutes to adjust to a new throttle setting.

NOTE: For minimal discovery times on medium to large size networks (several hundred to several thousand devices), it is recommended that you install OpenManage Essentials services on a multi-processor system.

Scheduling Inventory

1 Click **Manage→ Discovery and Inventory→ Configuration→ Inventory Schedule**.

2 In **Inventory Schedule Settings**, do the following:

   a Select desired schedule parameters.

   b **(Optional)** You may adjust the task speed slider for faster task execution; however, more system resources are consumed.

   Inventory Speed slider control—This control acts much like the discovery throttle, controlling the number of threads that are used during an inventory cycle. By default, there are a maximum number of 32 threads dedicated to performing the inventory process - the throttle controls the number of threads are actually used.

   NOTE: Each tick on the throttle control equals 10% and the range is from 10% to 100%. The inventory throttle is set at 60% by default.

Configuring Status Polling Frequency

You can configure OpenManage Essentials to check the health status of all discovered devices that have a means of health instrumentation such as OpenManage Server Administrator. The status can be scheduled at a given interval using Status Polling so that health status is always current. To configure status polling:

1. Click **Manage→ Discovery and Inventory→ Configuration→ Status Configuration**.
2. In **Status Polling**, select **Enable Status Polling** and provide the polling parameters including time and performance and then click **Finish**.

   By default, the status polling frequency is enabled and set to one hour.

   Polling Speed slider control - This control acts much like the discovery throttle, controlling the number of threads that are used during a status cycle. By default, there are a maximum number of 32 threads dedicated to performing the status process - the throttle controls the number of threads that are actually used.

6

Discovery And Inventory - Reference

From the Discovery and Inventory Portal page, you can:

- View graphical reports on devices and Dell servers discovered and inventoried.
- Manage discovery ranges for devices and Dell servers.
- Configure discovery, inventory, and status polling for devices and Dell servers.

Discovery and Inventory Portal Page Options

- Discovery Portal
- Discovery Ranges
    - Add Discovery Range
        - Discovery Ranges
        - Include Ranges
        - Exclude Ranges
- Configuration
    - Discovery Schedule
    - Inventory Schedule
    - Status Configuration

Discovery and Inventory Portal

The Discovery and Inventory Portal provides information about the:

- Last discovery and inventory details
- Discovered versus inventoried devices
- Task status

Last Discovery and Inventory

Last Discovery Details	
Discovery Last Run at	Displays the time and date information for the last run discovery.
Discovery Range	Displays the IP Address range or host name.
Devices Discovered	Displays information on number of devices discovered.
Last Inventory Details	
Inventory Last Run at	Displays the time and date information for the last run inventory.
Inventory Range	Displays the IP Address range or host name.
Devices Inventoried	Displays information on number of devices inventoried.

Discovered Versus Inventoried Devices

Provides a graphical report of number of devices and Dell servers discovered or inventoried. You can use this report to ascertain the discovered devices and Dell servers that are unclassified. See Viewing Device Summary for more on summary information and filter options for the summary information.

Click any section of the graph to see the device summary for the selected region. In the device summary, double-click a row to view the details (inventory view for that device). Alternatively, right-click and select details for the inventory view or right-click and select alerts for the alerts specific to that device.

Filter by	Select to refine the search results. • All • Ranges-Select to filter based on the selected range.

Task Status

Provides a list of currently executing and previously run tasks and their status. The task status grid on this page shows the status of just discovery, inventory, and tasks. However, the main portal shows all types of task statuses.

Task Name	Name of the task.
Task State	Status information: Completed Running Stopped Not Started
%Completed	Task completion status in percentage.
Start Time	Time and date information at start.
End Time	Time and date information at end.

Viewing Device Summary

1 In **OpenManage Essentials**, click **Manage**→ **Discovery and Inventory**→ **Discovery Portal**→ **Discovery Portal**.

The **Discovery and Inventory Portal** page is displayed.

2 In **Discovered vs Inventoried Devices**, in the graphical report, click the discovered or inventoried device band to open the **Device Summary** page showing the selected graph details.

The **Device Summary** page, status on health and power, and information on device name, Service Tag, device type, and model are displayed.

3 (**Optional**) Click the funnel icon to filter the summary information.

The filter options are displayed.

Select All	Select to filter per line item.
Select options, devices, or Dell servers.	Select to filter based on options, devices, or Dell servers.
Filter options	Create filter with these options: • **Is equal to**—Select to create the *same as* logic. • **Is not equal to** —Select to create the *different from* logic. • **Is Less than**—Select to find a value that is less than the value you provide. • **Is less than or equal to**—Select to find a value that is less than or equal the value you provide. • **Is greater than or equal to**—Select to find a value that is greater than or equal to the value you provide. • **Is greater than**—Select to find a value that is greater than the value you provide. **Health Status** options: • **Unknown** • **Normal** • **Warning** • **Critical** **Connection Status** options: • **On** • **Off**

4 Click **Filter** to view the filtered summary information.

5 Click **Clear Filter** to remove the filtered summary information.

6 Right-click device status and select from these options:

IP Address or iDRAC name	Displays the IP address or the iDRAC name.
Details	Select to view device details.
Alerts	Select to view the alerts generated for this device.
Application Launch	Select to launch an application.
Troubleshoot	If the Troubleshooting Tool is installed, then select this option to launch the Troubleshooting Tool. The Troubleshooting Tool is disabled by default. To enable the Troubleshooting Tool, see Preferences - Reference.
Refresh Inventory	Select to run inventory on the device.
Refresh Status	Select to run a status check on the device.
Add to New Group	Select to add the device to a group.
Exclude Range	Select to remove the device from the discovery and inventory range.
Remove	Select to remove the device information.
Export	Select to export the device information.

Discovery Ranges

From Discovery Range page, you can:

- View Discovery Range Summary
- Add Discovery Range

Discovery Range Summary

This page provides the following information:

- Discovery Ranges
  - Include Ranges
  - Exclude Ranges
- Discovery Range Summary

For list of right-click actions in this page, see Appendix—Right-Click Actions.

Add Discovery Range

1. Click **Manage**→ **Discovery and Inventory**→ **Discovery Ranges**→ **Discovery Range Summary**. Then right-click **Include Ranges** and select **Add Discovery Range**. For more information, see Configuring a Discovery and Inventory Task.

2. Provide information for protocols for discovery, inventory, or both:
   - IP Address, Range, or Host name Configuration
   - ICMP Configuration
   - SNMP Configuration
   - WMI Configuration
   - Storage Configuration
   - WS-Man Configuration
   - IPMI Configuration
   - Discovery Range Action
   - Summary

IP Address, Range, or Host Name Configuration

A discovery range is a network segment registered in OpenManage Essentials for the purpose of discovering devices. OpenManage Essentials attempts to discover devices on all registered discovery ranges that are enabled. A discovery range includes subnet, a range of IP addresses on a subnet, an individual IP address, or an individual host name.

Specify the IP address, IP address range, or host name for the discovery process.

IP address / range	Specifies the IP address or IP address range. The following are examples of valid discovery range type address specifications (* is the wildcard character, meaning all possible addresses in the specified range): 193.109.112.* 193.104.20-40.* 192.168.*.* 192.168.2-51.3-91 193.109.112.45-99 System IP address—193.109.112.99 **NOTE:** Click **Add** to add multiple ranges of IP addresses. IPV6 addresses are not supported.
Host name	Specifies the host name, for example: **mynode.mycompany.com**. Click **Add** to add multiple host names. **NOTE:** You can add multiple host names by separating them using commas. **NOTE:** Invalid characters in the host name are not checked. If the host name you provide contains invalid characters, the name is accepted. However, the device is not found during the discovery cycle.
Subnet mask	Specifies the subnet mask for the IP address range. The subnet mask is used to determine the broadcast addresses for the subnet(s) part of the range. The OpenManage Essentials Network Monitoring Service does not use the broadcast address when discovering devices in an IP address range. The following are examples of valid subnet mask specifications: • 255.255.255.0 (The default subnet mask for a Class C network.) • 255.255.0.0 (The default subnet mask for a Class B network.) • 255.255.242.0 (A custom subnet mask specification.) By default, the subnet mask is set to 255.255.255.0.

Import	Select this option to import host names and IP addresses from a file that is in CSV format. However, you can import only 500 line items per task. You can use an Active Directory export file in a.CSV format as input. You can also create a .CSV file in a spreadsheet editor using the header *Name* and filling in system IP addresses or host names in the rows below the header (one per cell). Save the file in a .CSV format and use it as the input with the import feature. If there are any invalid entries in the file, a message is displayed when the data is imported by OpenManage Essentials.

ICMP Configuration

Use ICMP during discovery to ping devices on the network. Select these options to configure the ICMP parameters.

For more information, click ? - (Why do I need this?) help.

Timeout	Set time in milliseconds.
Retries	Set number of attempts.

SNMP Configuration

SNMP provides an interface to manage devices on the network such as servers, storage, switches, and so on. The SNMP agent on the device allows OpenManage Essentials to query the health and inventory data of the device. Select these options to discover and inventory servers, storage devices, and other network devices.

For more information, click ? - (Why do I need this?) help.

Enable SNMP discovery	Enables or disables the SNMP protocol for discovery range (subnet.)

Get community	Specifies or edits the community name for SNMP **get** calls from the OpenManage Essentials user interface. The **Get Community** is a read-only password that SNMP agents installed on managed devices use for authentication. The **Get Community** allows OpenManage Essentials to browse and retrieve SNMP data. This field is case-sensitive. OpenManage Essentials uses the first successful community name to communicate with the device. You can enter multiple SNMP community strings separated with commas.
Set community	Specifies or edits the community name for SNMP **set** calls from the OpenManage Essentials UI. The **Set Community** is a read-write password that SNMP agents installed on managed devices use for authentication. The **Set Community** allows OpenManage Essentials to perform tasks that require the SNMP protocol, such as shutting down a system. This field is case-sensitive. OpenManage Essentials uses the first successful community name to communicate with the device. You can enter multiple SNMP community strings separated with commas. **NOTE:** In addition to the **Set Community** name, an instrumentation password is required to perform an SNMP task on a device.
Timeout (seconds)	Specifies or edits the amount of time that OpenManage Essentials waits after issuing a **get** or **set** call before it considers the call failed. A valid range is from 1 to 15 seconds. The default is 4 seconds.
Retries (attempts)	Specifies or edits the number of times that OpenManage Essentials reissues a **get** or **set** call after the first call times out. A valid range is from 1 to 10 retries. The default is 2.

WMI Configuration

Use the WMI protocol for gathering discovery, inventory, and health information about Window-based servers. This protocol provides less information about devices than SNMP but is useful if SNMP is disabled on the network. Select these options to configure WMI parameters for Windows servers only.

Enable WMI discovery	Select to enable WMI discovery.
Domain \ User name	Provide the domain and user name.
Password	Provide password.

Storage Configuration

Enabling discovery of PowerVault MD or Dell|EMC arrays allows OpenManage Essentials to gather inventory and health information about the arrays. Set these options to discover PowerVault MD arrays or Dell|EMC devices.

Enable PowerVault MD array discovery	Select to discover PowerVault MD array. This discovery configuration does not require credentials.
Enable Dell/EMC array discovery	Select to discover Dell/EMC array.
Dell/EMC user name	Provide user name.
Dell/EMC password	Provide password.
Dell/EMC port	Increment or decrement the port number. Enter a TCP/IP port number ranging 1 to 65535. Default value is 443.

WS-Man Configuration

Use the WS-Man protocol to discover ESXi-based servers and gather inventory and health status from those servers. Select these options to configure WS-Man parameters for discovering ESXi installed devices.

Enable WS-Man Discovery	Select to discover ESXi installed devices.
User ID	Provide authenticated user ID.

Password	Provide password.
Timeout	Provide the time after which the discovery attempts must stop.
Retries	Provide the number of attempts to discover the devices.
Port	Provide the port information.
Secure Mode	Select to securely discovery devices and components.
Skip Common name check	Select to skip common name check.
Trusted Site	Select if the devices you are discovering is a trusted device.
Certificate file	Click **Browse** to traverse to the file location.

IPMI Configuration

Use the IPMI protocol for out of band discovery of RACs, DRACs, and iDRACs. This option is for Lifecycle controller enabled discovery and inventory. Ensure that the IP address of the DRAC and iDRAC is selected. To configure IPMI, see **support.dell.com**.

Select these options to configure the IPMI version 2.0 parameters. This configuration is required for discovery.

Enable IPMI Discovery	Enables or disables the IPMI protocol by discovery range.
User name	Enter the Baseboard Management Controller (BMC) or DRAC user name. **NOTE:** The default user name is **root**. It is recommended that you change it for security.
Password	Enter the BMC or DRAC password. **NOTE:** The default password is **calvin**. It is recommended that you change it for security.

KG Key	Enter the KG key value. DRAC also supports IPMI KG key value. Each BMC or DRAC is configured to require an access key in addition to user credentials. **NOTE:** The KG key is a public key that is used to generate an encryption key for use between the firmware and the application. The KG key value is an even number of hexadecimal characters.
Timeout	Specifies or edits the amount of time that OpenManage Essentials waits after issuing a **get** or **set** call before it considers the call failed. A valid range is from 1 to 60 seconds. The default is 5 seconds.
Retries	Specifies or edits the number of times that OpenManage Essentials reissues a **get** or **set** call after the first call times out. A valid range is from 0 to 10 retries. The default is 1.

NOTE: The retries and time-out parameters are used for both the Remote Management Control Protocol (RMCP) ping and the IPMI connection.

Discovery Range Action

Select these options to discover or inventory devices, components, and servers.

Do not perform discovery or inventory	Select this option set up a schedule to perform discovery and inventory (at a later time) using the discovery configuration scheduling options in the Discovery and Inventory Portal.
Perform only discovery	Select this option to perform discovery.
Perform both discovery and inventory	Select this option to perform both discovery and inventory.

Summary

View the configuration selections. To change configurations, click **Back.**

Add Exclude Range

From **Discovery Range Summary**, right-click **Exclude Ranges** and select **Add Exclude Range**. Register new ranges to exclude from discovery or to remove a previously set exclude range.

IP Address/Range	Register a device to exclude from the discovery process by specifying the device's IP address or IP address range. The following are examples of valid discovery range type address specifications (* is the wildcard character, meaning all possible addresses in the specified range): • Exclude range — 193.109.112.* • 193.104.20-40.* • 192.168.*.* • 192.168.2-51.3-91 • Exclude range — 193.109.112.45-99 • System IP address — 193.109.112.99
Host name	Register to exclude from the discovery process by specifying the device's host name, for example: **mynode.mycompany.com**. **NOTE:** OpenManage Essentials does not check for invalid characters in the host name. If the host name you specify contains invalid characters, the name is accepted. However, the device with that name is not found during the discovery cycle.

Configuration

The Configuration page contains the following information:

- Discovery Schedule
- Inventory Schedule
- Status Configuration

Discovery Schedule

You can configure OpenManage Essentials to discover devices and display them in the **Device** tree.

1. Enable device discovery.
2. Initiate device discovery.
3. Set the discovery speed.
4. Specify how devices are discovered.
5. For failed discovery attempts, use the Troubleshooting Tool.

To view discovery configuration, click **Manage→ Discovery and Inventory→ Configuration→ Discovery Schedule.**

Configure OpenManage Essentials to discover new devices on a network. The settings apply to all discovery ranges. OpenManage Essentials records all agents, IP addresses, and the health of the devices.

Enable Discovery	Select to schedule device discovery.
Configure Global Device Discovery interval	Set the frequency of discovery in weekly or daily intervals. • **Every Week On**—Specify the day or days to schedule discovery and the time for the discovery to begin. • **Every <n> Days <n> Hours interval**—Specify the intervals between discovery cycles. The maximum discovery interval is 365 days and 23 hours.
Discovery Speed	Specify the amount of resources (system and network) available for accelerating the discovery speed. The faster the speed, more resources are required to perform discovery, but less time is required.

Discover	Specify how the devices are discovered. • **All Devices**—Select to discover all devices that respond to an Internet Control Message Protocol (ICMP) ping. • **Instrumented Devices**—Select to discover only devices that have instrumentation (such as Dell OpenManage Server Administrator, Dell OpenManage Array Manager, and Dell PowerConnect) for Simple Network Management Protocol (SNMP), Windows management Instrumentation WMI), Intelligent Platform Management Interface (IPMI) management, or WS-Management (WS-Man). See agents supported for more information about systems management instrumentation agents.
Name Resolution	Specify how the device names are resolved. If you are managing a cluster, use the NetBIOS name resolution to discern each independent system. If you are not managing a cluster, a DNS name resolution is recommended. • **DNS**—Select to resolve names using the Domain Naming Service. • **NetBIOS**—Select to resolve names using system names.

Inventory Schedule

Use **Inventory Polling** to specify the default inventory settings for OpenManage Essentials. OpenManage Essentials collects inventory information such as software and firmware versions, as well as device-related information about memory, processor, power supply, Peripheral Component Interconnect (PCI) cards, and embedded devices, and storage.

Enable Inventory	Select to schedule inventory.
Configure Global Inventory Polling Interval	Set the frequency of the inventory in weekly or daily intervals. **NOTE:** OpenManage Essentials performs inventory only on devices that have already been discovered. • **Every Week On**—Specify the day or days of the week that you want to schedule the inventory and the time that you want it to begin. • **Every <n> Days <n> Hours interval**—Specify the intervals between inventory cycles. The maximum discovery interval is 365 days and 23 hours.
Inventory Polling Speed	Set the amount of resources available for accelerating the inventory poll speed. The faster you set the inventory poll speed, the more resources are required, but less time is required to perform the inventory. After changing the speed, OpenManage Essentials may take several minutes to adjust to the new speed.

Status Configuration

Use this window to specify the default status polling settings for OpenManage Essentials. Status polling performs a health and power check for all discovered devices. For example, this poll determines if discovered devices are healthy or powered down.

Enable Status Polling	Select to schedule device status polling.
Device Status Interval	Set frequency of the device status poll in intervals of days, hours, and minutes. The status polling does not begin until the previous polling has completed. **Days**—Specify the number of days between device status polling. **Hours**—Specify the number of hours between device status polling cycles. **Minutes**—Specify the number of minutes between device status polling cycles. The maximum discovery interval is 365 days, 23 hours, and 59 minutes.
Status Polling Speed	Set the amount of resources available for accelerating the device status polling speed. The faster you set the status speed, the more resources are required, but less time is required to perform the status polling.

7

Managing Devices

OpenManage Essentials lists devices based on their types. For example, Dell PowerEdge servers are listed under the device type **Servers**. OpenManage Essentials contains a defined list of device types. The devices you discover and inventory are included under these device types. Unclassified devices are listed under the device type **Unknown**. You can create device groups with combinations of the defined device types. However, you cannot create a new device types.

In the **Devices** page, you can:

- View devices types that are discovered on the network.
- View the inventory information for the devices.
- View all the alerts that were generated for a device.
- View the hardware logs for a device.
- Create device groups and include devices to that group based on your grouping preference. For example, you can create a group and include all devices present at a geographical location.

Viewing Devices

You can view a device that is discovered. For more information on discovering and inventorying a device, see Discovering and Inventorying Devices.

To view devices, click **Manage→ Devices**.

In the device summary page, expand the device types to view devices. The following device types are displayed.

- High Availability (HA) clusters
- KVM
- Microsoft Virtualization
- Modular systems
- Network devices
  - Switches

- OOB unclassified devices
  - IPMI unclassified devices
- Printers
- RAC
- Servers
- Storage Devices
  - Dell|EMC Arrays
  - EqualLogic arrays
  - PowerVault MD Arrays
  - Tape Devices
- Unknown
- VMware ESX servers

Use the refresh button to update the device tree with the current data. To update the device tree, right-click **Devices** and select **Refresh**.

NOTE: The device tree auto-updates when changes are made. Some changes to the tree may show after a brief delay depending on the managed servers' performance because the information propogates from the SQL database to the user interface.

Nodes and Symbols Description

Node Symbol	Description
❌	Denotes that a device is critical and requires attention. This information is rolled up to the parent device type. For example if a server is in critical state and requires attention the same symbol is assigned to the parent device type. Among server states, critical state is given the highest priority; That is, in a group, if different devices are in different states, and if one device is in critical state, then the state of the parent device type is set to critical.
⊘	Denotes that a device of this type is not discovered on the network or classified in the device tree.
⚠	Denotes that there is a deviation from the expected behavior, but the device is still manageable.

Node Symbol	Description
✓	Denotes that the device is working as expected.
?	Denotes either the device type is unknown and it is classified as an unknown device or that the health status cannot be determined, because the device does not have proper instrumentation or the proper protocol was not used to discover the device.

Device Details

The device details, depending on the device type, can contain the following information:

- Device Summary
- OS Information
- Software Agent Information
- NIC Information
- Virtual Machine Host Product Information
- RAC Device Information
- Processor Information
- Memory Device Information
- Firmware Information
- Power Supply Information
- Embedded Device Information
- Device Card Information
- Controller Information
- Controller Battery Information
- Enclosure Information
- Physical Disk Information
- Virtual Disk Information
- Contact Information
- Software Inventory Information
- Trusted Platform Module Information

- FRU Information
- Acquisition Information
- Depreciation Information
- Extended Warranty Information
- Ownership Information
- Outsource Information

Viewing Device Inventory

To view inventory, click **Manage→ Devices**, expand the device type and click the device.

Viewing Alerts Summary

You can view all the alerts generated for a device. To view alert summary:

1. Click **Manage→ Devices**.
2. Expand the device type and click the device.
3. In the details page, select **Alerts**.

Viewing System Event Logs

1. Click **Manage→ Devices.**
2. Expand the device type and select **Hardware Logs**.

Searching for Devices

Right-click **All Devices** at the top of the device tree and click **Search Devices**. You can also search for devices using logical arguments and save the queries for later.

For example, to create a query to search for a server in critical state with an IP address containing values 10.35, and the power status as Power Up:

1. Click **Manage→ Device Search**, then select **Create New Query**, in the adjacent text field enter a query name.
2. From the first line after **Where**, select **Device Type**, **Is**, and then **Server**.

3. In the next line select the check box, then select **AND**, **Device Health**, **Is**, and then select **Critical**.
4. In the next line select the check box, then select **AND, IP Address, Contains**, and then in the adjacent field enter **10.35**.
5. In the next line select the check box, then select **AND, Power Status, Is**, and then select **Power Up**.
6. Click **Save Query**.

   NOTE: You can click **Run Query** to run the query immediately.

To run an existing query, select the query from the drop-down list and click **Run Query**. You can filter the results and export it to an HTML, TXT, or CSV file.

8

Devices - Reference

This page provides the following information:

- List of devices based on the device type, for example, HA clusters, servers, and so on.
- Summary of devices and alerts.
- Alerts generated for a particular device.
- Health of devices based on the Normal, Critical, Unknown, and Warning types.

  NOTE: For Dell 12 Generation PowerEdge servers [denoted as *yx2x*, where *y* denotes alphabets, for example M (modular), R (rack), or T (tower) and *x* denotes numbers] discovered using WMI and SNMP protocols, the DRAC health status is displayed (under Servers) even if OpenManage Server Administrator is not installed on the server.

  NOTE: Based on the severity of the agents of a discovered device, the overall health is the most critical of the severity. For example, in the device tree, for server types, if there are two servers with status **Warning** and **Critical**, then the parent Server's status is set to **Critical**.

- Inventory information for devices.
- View hardware logs for servers.
- Filtering capabilities of the grid:
  - The grouping bar
  - Filter icon options
  - Sorting by clicking on the column
  - Re-ordering the columns

  NOTE: None of these are saved if the console is closed and restarted.

Viewing Inventory

To view inventory, from **All Devices**, traverse to the device and click the device.

The device details and the alerts link are displayed.

Viewing Alerts

To view alerts, from the inventory details page, click **Alerts**.

Severity	Alert severity based on Normal, Critical, Warning, and Unknown.
Acknowledged	Flagged status for an alert.
Time	Time at which the alert was generated in date and time format.
Device	IP address of the device.
Details	Lists the alert information. For example, **System is down: <IP Address of the device>.**
Category	Lists the alert category type, for example System Events.
Source	Lists the alert source name.

Viewing Hardware Logs

You can view hardware logs for servers. To view hardware logs, from the inventory details page, click **Hardware Logs**.

Severity	Alert severity based on Normal, Critical, Warning, and Unknown.
Local Time	The system time at which this alert was generated in date and time format.
UTC Time	Coordinated Universal Time (abbreviated UTC) at which the log was generated.
Details	Lists the details of the hardware log. For example, power supply redundancy is lost.

Alert Filters

You can apply these filters to Alerts. Select **Continuous Updates** to enable the user interface to update automatically when new alerts are received.

Severity	Select from these alerts: **All, Normal, Critical, Warning,** and **Unknown**.
Acknowledged	Flagged status for an alert.
Time	Time at which this alert was generated in date and time format.
Device	The IP address or host name of this device.
Details	The alert information. For example, **System is down: <IP Address of the device>.**
Category	The alert category type, for example System Events.
Source	The Alert Source.

Device Search

You can do the following devices search options:

- Run an existing query
- Create a new query
- Delete a query

Run Existing Query	Select this option and then select a query from the drop-down list.
Delete Query	Select to delete a query after you complete the following action. Select the **Run Existing Query** option, then from the drop down list select the query that you want to delete.
Create New Query	Select this option to create a query and then enter a name for the query in the adjoining field.
Query logic	Select from the query logic options to create multiple query options. Select the check box to enable and include an argument.

Run Query	Select to run the selected query.
Save Query	Select to save a query.

Query Results

The device search lists these options:

Health Status	Displays the health status of the device. The status options are **Normal, Warning, Critical,** and **Warning**.
Connection Status	Displays the connection status of the device. The connection status are **On** or **Off**.
Name	Displays the name of the device.
OS Name	Displays the operating system installed on the device.
OS Revision	Displays the version of the operating system installed on the device.
Service Tag	Displays a unique identifier, that provides the service lifecycle information.
Asset Tag	Displays the defined asset tag for the device.
Device Model	Displays the system's model name. For example, PowerEdge R710.
Device type	Displays the type of device. For example, for the Device Model PowerEdge R710, the Device Type value is Server.
System Revision Number	Displays the revision history of the device.

Creating Device Group

Device Group Configuration

Name	Provide name of the new group.
Parent	The device under which this group is created.
Description	Provide description for the device group.

Device Selection

You can select predefined groups (device types), custom groups, specific devices, or a device query.

To use device query, select a query from the list.

Click **New** to create a new device query to search and assign the devices to the alert action.

Click **Edit** to change the query logic.

Select groups or devices from the tree, you can use the query option to create very specific criteria for the selection.

All Devices	Select to include all the Devices that are managed in OpenManage Essentials.
HA Clusters	Select to include High Availability server clusters.
KVM	Select to include keyboard video mouse devices.
Microsoft Virtualization Servers	Select to include Microsoft virtualization servers.
Modular Systems	Select to include modular systems.
Network Devices	Select to include network devices.
OOB Unclassified Devices	Select to include out of band Unclassified Devices like Lifecycle controller enabled devices.
Printers	Select to include printers.
RAC	Select to include devices with remote access controllers.
Servers	Select to include Dell servers.
Storage Devices	Select to include storage devices.
Unknown	Select to include unknown devices.
VMware ESX Servers	Select to include VMware ESX servers.

Summary - Group Configuration

View and edit selections.

9

Viewing Inventory Reports

OpenManage Essentials provides pre-defined reports for all discovered and inventoried devices. With these reports, you can:

- Consolidate information about devices in your environment.
- Filter report data per your needs.
- Export data for use in another application in the `XML` file format.

NOTE: You cannot create new reports.

Choosing Predefined Reports

To view predefined reports, click **Reports**.

The Managed Systems Reports displays the predefined reports. Select from the available reports to view particular information about the devices in your environment. See table for more information.

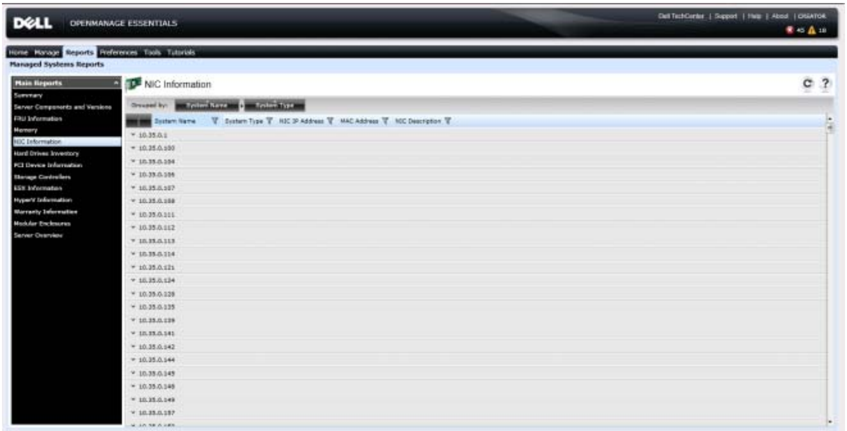
Report	Description
Summary	Identifies the OpenManage Server Administrator versions installed on devices in your environment and allows you to identify the devices generating the most alerts. • The upper left web part identifies the OpenManage Server Administrator versions in your environment. • Clicking the OpenManage Server Administrator version in the OpenManage Server Administrator pie chart in the top right web part shows you the list of servers with that version installed. • The lower left web part lists in descending order the devices generating the most alerts since initial discovery and inventory. • The top five event generating devices are identified in the lower right web part. Click on a specific device to view the events associated with it.

Report	Description
Server Components and Versions	Identifies BIOS, driver, and firmware versions on all discovered and inventoried servers
FRU Information	The Field Replaceable Unit (FRU) provides details on replaceable server components.
Memory	Provides details on DIMMs and identifies the slot a particular DIMM occupies within a server.
NIC Information	Identifies the NIC model-IP address, MAC address, manufacturer and part and serial numbers for NICs.
Hard Drives Inventory	Identifies serial number, revision, manufacturer, and bus type for hard drives.
PCI Device Information	Identifies model, manufacturer, and slot for PCI and PCIe controllers in each server.
Storage Controllers	Identifies the storage controllers on the server and provides the controller name, vendor, controller type, and controller state: **Ready:** The storage controller is ready for use. **Degraded:** There is a potential problem with the controller. Investigation is required.
ESX Information	Identifies ESX and ESXi virtual machine hosts and associated virtual machines.
HyperV Information	Identifies the HyperV virtual machine hosts and associated virtual machines.
Warranty Information	See Viewing Warranty Reports for details on how to run the warranty report and the information it provides.
Modular Enclosures	Provides information about the enclosure type, firmware version, enclosure Service Tag, and so on.
Server Overview	Provides information about the servers such as the system name, operating system installed on the server, processors, and memory.

Filtering Report Data

You can filter the results by dragging and dropping column headers to the top of reports. You can choose one or more attributes when revising the view to meet your specific needs.

For example, in the NIC Information report, drag the **System Type** and **System Name** to the top of the report. The view immediately changes to a nesting of information based on your preference. In this example, you can view nested data for NICs; NIC IP Address, MAC Address, and NIC description.



```
System Name   System Type   NIC IP Address   MAC Address   NIC Description
▾ 10.35.0.1
▾ 10.35.0.100
▾ 10.35.0.104
▾ 10.35.0.106
▾ 10.35.0.107
▾ 10.35.0.108
▾ 10.35.0.111
▾ 10.35.0.112
▾ 10.35.0.113
▾ 10.35.0.114
▾ 10.35.0.121
▾ 10.35.0.124
▾ 10.35.0.128
▾ 10.35.0.135
▾ 10.35.0.139
▾ 10.35.0.141
▾ 10.35.0.142
▾ 10.35.0.144
▾ 10.35.0.145
▾ 10.35.0.148
▾ 10.35.0.149
▾ 10.35.0.157
```

Exporting Reports

Exporting a report enables you to manipulate and reformat the data.

In the Reports list, right-click on any report to display the **Export** option. Scroll over the **Export** option to display supported formats. Choose your preferred format (CSV, HTML, or XML) and provide a file name for the exported report.

10

Reports - Reference

From Reports you can view the following:

- Summary
- Server components and versions
- FRU Information
- Memory
- NIC Information
- Hard Drives Inventory
- PCI Device Information
- Storage Controllers
- ESX Information
- HyperV Information
- Warranty Information
- Modular Enclosures
- Server Overview

The summary page lists the following:

- Systems using specific Server Administrator agent
- Summary of Server Administrator agents and systems
- Active systems based on event occurrence
- Top five systems with most event

Server Components and Versions

System Name	Host name of the system.
Service Tag	Unique identification number assigned to the system.
Model Type	The system’s model name. For example PowerEdge R710.
Description	The software information.

Software Type	The type of software that is available on the system. For example, firmware.
Software Version	The version number of the software that is available on the system.

Field Replaceable Unit (FRU) Information

System Name	The user provided name of the system.
Model Type	The system's model name. For example PowerEdge R710.
Service Tag	Unique identification number assigned to the system.
FRU Device Name	The standard FRU name assigned to the device.
FRU Manufacturer	The name of the FRU manufacturer.
FRU Serial Number	The manufacturer specified FRU's identification number.
FRU Part Number	The industry specific number that differentiates the type of FRU.

Memory

System Name	Provide a name for this server power options task.
Service Tag	Unique identification number assigned to the system.
System Type	The system's model name. For example PowerEdge R710.
Memory Device Name	The device's named assigned by the manufacturer. For example, DIMMI_A.
Memory Device Size (MB)	The size of the memory device in GB.
Memory Device Manufacturer	The name of the device's manufacturer.
Memory Device Part Number	The industry specific number assigned to the device.
Memory Device Serial Number	The roll number assigned to the device by the manufacturer.

NIC Information

System Name	The name of the system.
System Type	The system's model name. For example, PowerEdge R710.
NIC IP Address	The unique IP address assigned to the NIC device.
MAC Address	A unique Media Access Control address (MAC address) identifier assigned to network interfaces for communications on the physical network segment.
NIC Description	Information on the NIC device.

Hard Drives Inventory

System Name	The unique system's name that identifies it on the network.
System Type	The system's model information.
Service Tag	A Dell specific unique bar code label identifier on the system.
Channel	The number of channels
Enclosure ID	The enclosure ID is assigned to the enclosure by Storage Management. Storage Management numbers the enclosures attached to the controller starting with zero.
Target ID	The SCSI ID of the backplane (internal to the server) or the enclosure to which the controller connector is attached. The value is usually 6.
LUN ID	In computer storage, a logical unit number or LUN number used to identify a logical unit, which is a device addressed by the SCSI protocol or similar protocols such as Fibre Channel or iSCSI.
Size (GB)	The size of the hard drive in gigabytes.
Bus Type	The type of bus connection used. Buses are information pathways between components of a system.
Serial Number	The roll number assigned to the device by the manufacturer.
Revision	The hard disk's revision history.
Vendor	The organization that supplies the hard drive.

PCI Device Information

System Name	The unique system's name that identifies it on the network.
Service Tag	A Dell specific unique bar code label identifier for a system.
System Type	The system's model information.
Device Card Description	The type of Peripheral Component Interconnect card used. For example, 82546GB Gigabit Ethernet Controller.
Device Card Manufacturer	The manufacturer's information.
Device Card Slot Type	The type of slot on the mother board into which the card is inserted.

Storage Controllers

System Name	The unique system's name that identifies it on the network. The storage controller is present on this system.
System Type	The system's model information.
Controller Name	The name of the storage controller. For example, SAS 6/iR Integrated.
Vendor	The supplier's information. For example, SAS 6/iR Integrated is supplied by Dell.
Controller Type	The type of controller. For example, SAS 6/iR Integrated is of type SAS.
Controller State	The state of the controller. For example, ready to use.

ESX Information

Host Name	The unique system's name that identifies it on the network and the system in which embedded bare metal product is installed.
System Type	The system's model information.

VM Type	The type of embedded bare-metal product installed on the system. For example, VMware ESX.
Version	The version of the embedded bare-metal that is installed on the system.
Guest Name	The name of the guest virtual machine.
Guest OS Type	The operating system that is installed on the virtual machine.
Guest Memory Size (MB)	The size of the virtual machine's RAM.
Guest State	The state of the virtual machine, if the machine is powered off or powered on.

HyperV Information

Host Name	The unique system's name that identifies it on the network. and the system in which the HyperV is installed.
System Type	The system's model information.
Guest Name	The name of the guest virtual machine.
Guest Memory Size (MB)	The size of the virtual machine's RAM.
Guest State	The state of the virtual machine, if the machine is powered off or powered on.

Warranty Information

System Name	The unique system's name that identifies it on the network. Enable the proxy setting for the warranty to Warranty data from **support.dell.com**.
Device Model Type	The system's model information.
Device Type	The type of device, for example, server, Remote Access Controller.
Shipped Date	The date on which the device was sent from the factory.
Service Tag	A Dell specific unique bar code label identifier for a system.

Service Level Code	Displays the service level code such as parts only warranty (POW), next business day onsite (NBD), and so on for a particular system.
Service Provider	The name of the organization that will provide the warranty service support for the device.
Start Date	The date from which the warranty is available.
End Date	The date on which the warranty will expire.
Days Remaining	The number of days the warranty is available for the device.
Warranty Description	The warranty details applicable for the device.

Modular Enclosures

Enclosure Model Type	The enclosure's model name. For example, PowerEdge M1000e.
Slot Number	The slot number on the enclosure.
Slot Name	The slot name of the enclosure.
Slot Availability	Displays if the slot is available or occupied in the modular enclosure.
Firmware Version	The firmware version installed on the enclosure.
Enclosure Service Tag	A Dell specific unique bar code label identifier for the enclosure.
Enclosure Name	The unique enclosure name that identifies it on the network.
Blade Model Type	The blade's model information.
Blade Service Tag	A Dell specific unique bar code label identifier for the blade.
Blade Host Name	The blade's model name. For example, PowerEdge M710.
Blade OS	The operating system installed on the blade.

Server Overview

System Name	The unique system's name that identifies it on the network.
System Type	The system's model information.
Operating System	The operating system installed on the system.
Processor Count	The number of processors installed on the system.
Processor Family	The type of processor installed on the system.
Processor Cores	The number of processor cores.
Processor Speed	The speed of the processor
Total Cores	The total number of cores present in the system.
Total Memory	The total memory installed on the system

11

Viewing Warranty Reports

Warranty information is available for devices with valid Service Tags, including servers, switches, storage, and so on. Warranty information is automatically retrieved at the time devices are discovered.

The Warranty Information report is unique among OpenManage Essentials reports as it requires internet access to pull warranty information from the Dell warranty database. If you do not have internet access, no warranty information is populated. It is downloaded the next time you connect to the internet and open the Warranty Report.

To extend support for the devices, right-click a device and click **View and Renew Warranty**. This option opens **support.dell.com** with the device selected. Alternately you can click the **View and Renew Warranty** button to open the warranty site. If you log in to the warranty site with the company account you will see all their devices with warranty information.

12

Managing Alerts

With OpenManage Essentials you can:

- View alerts and alert categories
- Manage alert actions
- Configure alert log settings

To view the alerts page, from OpenManage Essentials, click **Manage→ Alerts**.

Viewing Alerts and Alert Categories

Viewing Alert Logs

To view alert logs, click **Manage→ Alerts→ Alert Logs**.

Understanding the Alert Types

The following alert log types are displayed.

Icon	Alert	Description
✓	Normal Alerts	An event from a server or a device that describes the successful operation of a unit, such as a power supply turning on or a sensor reading returning to normal.
⚠	Warning Alerts	An event that is not necessarily significant, but may indicate a possible future problem, such as crossing a warning threshold.
✖	Critical Alerts	A significant event that indicates actual or imminent loss of data or loss of function, such as crossing a failure threshold or a hardware failure.
?	Unknown Alerts	An event has occurred but there is insufficient information to classify it.
i	Information Alerts	Provides information only.

Viewing Alert Categories

To view alert categories, click **Manage**→ **Alerts**→ **Alert Categories**.

The predefined alert categories are listed in alphabetical order.

Viewing Alert Source Details

To view an alert category, in the alert categories list, expand an alert category, and then select an alert source.

NOTE: You cannot create a new event source.

For example, expand **Environmental** alert category and then select the **alertCoolingDeviceFailure** alert source.

Table 1. Alert Source Values and Descriptions for alertCoolingDeviceFailure

Name	Value	Description
Name	alertCoolingDeviceFailure	
Type	SNMP	An SNMP alert based source.
Catalog	MIB - 10892	
Severity	Critical	If this alert is received then the system is in critical state and immediate action is required.
Format String	$3	
SNMP Enterprise OID	.1.3.6.1.4.1.674.10892.1	
SNMP Generic Trap OID	6	
SNMP Specific Trap OID	1104	

Viewing Previously Configured Alert Actions

To view the application launch alert action:

1. Select **Manage**→ **Alerts**→ **Alert Actions**.
2. In Alert Actions, select **Application Launch**.

To view the e-mail alert action:

1 Select **Manage→ Alerts→ Alert Actions**.
2 In **Alert Actions**, select **Email**.

To view the alert ignore action:

1 Select **Manage→ Alerts→ Alert Actions**.
2 In **Alert Actions**, select **Ignore**.

To view the alert trap forward action:

1 Select **Manage→ Alerts→ Alert Actions**.
2 In **Alert Actions**, select **Trap Forwarding**.

Handling Alerts

Flagging an Alert

After you have completed action on an alert, flag the alert as acknowledged.

Acknowledging an alert indicates it is resolved or does not require further action as a reminder to yourself. To acknowledge alerts:

1 Select **Manage→ Alerts→ Alert Logs**.
2 Click the alert you want to acknowledge.

   NOTE: You can acknowledge multiple alerts simultaneously. Use <Ctrl> or <Shift> to select multiple alerts.

3 Right-click and click **Acknowledge→ Set→ Selected Alerts or Filtered Alerts**.

   If you choose **Selected Alerts**, the highlighted alerts are acknowledged.

   If you choose **Filtered Alerts**, all alerts in the current filter/view are acknowledged.

To remove an acknowledged flag, right-click and select **Acknowledge→ Clear→ Selected Alerts or Filtered Alerts**.

Creating and Editing a New View

To personalize the way you view alerts, create a new view or modify an existing view. To create a new view:

1. Select **Manage→ Alerts→ Alert Logs→ Alert View Filters**.
2. Right click and select **New Alert View Filter**.
3. In **Name and Severity Association**, enter a name for the new filter, and then check one or more severities. Click **Next**.
4. In **Categories and Sources Association**, assign the alert category or source to which you want to associate with this view filter and click **Next**.
5. In **Device Association**, create query for searching devices or assign the device or device groups, which you want to associate to this view filter and then click **Next**.
6. (Optional) By default the alert view filter is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.
7. (Optional) In **Acknowledged Association**, set duration when this alert action is active, and then click **Next**. The default is always active.
8. In **Summary**, review inputs and click **Finish**.

Configuring Alert Actions

NOTE: Alert actions occur on all alerts received by the OpenManage Essentials console. The alert is received and processed by the OpenManage Essentials console whether or not OpenManage Essentials has discovered the device so long as OpenManage Essentials is listed in the device's SNMP trap forward destinations list. To prevent this, remove OpenManage Essentials from the SNMP trap forward destinations list on the device.

Setting Up E-mail Notification

You can create e-mail notifications when an alert is received. For example, an e-mail is sent if a critical temperature alert is received from a server.

To configure an e-mail notification when an alert(s) is received:

1. Select **Manage→ Alerts→ Alert Actions**.
2. In **Alert Actions**, right-click **Email** and select **New Alert Email Action**.

3 In **Name and Description**, provide e-mail alert action name and description and then click **Next**.

4 In **E-mail Configuration**, do the following and then click **Next**.

   a Provide e-mail information for the **To:** and **From:** recipients and provide the substitution information.

   Separate each recipient or distribution list with a semi-colon.

   b Customize the e-mail message format with any of the following substitution parameters:

   $n = Device

   $ip = Device IP

   $m = Message

   $d = Date

   $t = Time

   $sev = Severity

   $st = Service Tag

   $e = Enterprise OID

   $sp = Specific Trap OID

   $g = Generic Trap OID

   $cn = Alert Category Name

   $sn = Alert Source Name

   $pkn = Package Name

   $at = Asset Tag

   c Click **Email Settings** and provide SMTP server name or IP Address, to test e-mail settings and click **OK**.

   d Click **Test Action** to send test e-mail.

5 In **Severity Association**, assign the alert severity to which you want to associate this e-mail alert and then click **Next**.

6 In **Categories and Sources Association**, assign the alert categories or alert sources to which you want to associate this e-mail alert and then click **Next**.

7 In **Device Association**, assign the device or device groups to which you want to associate this e-mail alert and then click **Next**.

8 By default the Email Notification is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.

9 In **Summary**, review the inputs and click **Finish**.

Ignoring Alerts

Sometimes you will receive alerts you might want to ignore. For example, you may want to ignore multiple alerts generated when **Send authentication trap** is selected within the SNMP service on the managed node. To ignore an alert:

1. From OpenManage Essentials, select **Manage→ Alerts→ Alert Actions**.
2. In **Alert Actions**, right-click **Ignore** and select **New Alert Ignore Action**.
3. In **Name and severity Association**, provide a name, assign the alert severity to which you want to associate this ignore alert action, and then click **Next**.
4. In **Categories and Sources Association**, assign the alert categories source to which you want to associate this alert ignore action and then click **Next**.
5. In **Device Association**, assign the device or device groups to which you want to associate this alert ignore action and then click **Next**.
6. By default the Ignore Alert is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.
7. In **Duplicate Alert Correlation**, select **yes** to exclude duplicate alerts received within the set time limit, and then click **Next**.
8. In **Summary**, review inputs and click **Finish**.

Running a Custom Script

In response to a specific alert received, you can run custom scripts or launch a specific application. This file must be present on the OpenManage Essentials service tier system (where OpenManage Essentials is installed) and not on the client browser system. For example:

- If you received a temperature warning, you can use a custom script to create an incident ticket for your internal Help Desk.
- If you received an MD Array storage alert, you can launch the Modular Disk Storage Manager (MDSM) application to view the status of the array.

To create a custom script:

1. Select **Manage→ Alerts→ Alert Actions**.
2. In **Alert Actions**, right-click **Application Launch** and select **New Alert Application Launch Action**.
3. In **Name and Description**, provide an application launch name and description and then click **Next**.
4. In **Application Launch Configuration**, provide an executable name (provide an absolute file path, for example, `C:\ProgramFiles\Dell\Application.exe`) and provide the substitution information, and then click **Next**.

   If you are running a `.bat` file, provide `> null` in the parameters.

   To test this script, click **Test Action** before you click **Next**.
5. In **Severity Association**, assign the alert severity to which you want to associate this alert application launch and then click **Next**.
6. In **Categories and Sources Association**, assign the alert categories or alert sources to which you want to associate this alert application launch and then click **Next**.
7. In **Device Association**, assign the device or device groups to which you want to associate this alert application launch and then click **Next**.
8. By default the Application Launch Action is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.
9. In **Summary**, review inputs and click **Finish**.

Forwarding Alerts

You may want to consolidate alerts from multiple management stations to one management station. For example, you have management stations in multiple locations and you want to view status and take action from one central location. To create alert forwards:

1. Select **Manage→ Alerts→ Alert Actions**.
2. In **Alert Actions**, select **Trap Forwarding** and right-click **New Alert Trap Forward Action**.

3 In **Name and Description**, provide Trap Forward name and description and then click **Next**.

4 In **Trap Forwarding Configuration**, provide destination host name or IP address, provide community information, to send a test trap to the destination management station, click **Test Action**, and then click **Next**.

5 In **Severity Association**, assign the alert severity to which you want to associate this trap forwarding alert and then click **Next**.

6 In **Categories and Sources Association**, assign the alert categories source to which you want to associate this trap forwarding alert and then click **Next**.

7 In **Device Association**, assign the device or device groups to which you want to associate this trap forwarding alert and then click **Next**.

8 By default the Trap Forward Action is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.

9 In **Summary**, review inputs and click **Finish**.

The severity status for any trap is set to normal and for a successful alert action, combination of severity, category, and device has to confer with the selections in the preceding steps.

Working With Sample Alert Action Use Cases

Sample alert actions are available for **Application Launch, E-mail, Ignore,** and **Trap Forwarding** alert actions. Sample alert action use cases are disabled by default. Click the sample alert actions to enable the sample alert action.

To enable a sample use case, right-click the use case and select **Enable**.

Use Cases in Alert Actions

Application Launch

Sample - Run Script on Server Critical Alert—Enable this use case to run a custom script when a critical alert is received.

Email

- **Sample - Email Alerts to Service Desk**—Enable this use case to send an e-mail to the service desk account from the OpenManage Essentials server when an alert criteria is matched.
- **Sample - Email Critical Server Alerts to Admin**—Enable this use case to send an e-mail to an administrator from the OpenManage Essentials server when an alert criteria is matched.

Ignore

- **Sample - Ignore Alerts During Maintenance Window**—Enable this use case to ignore alerts during a specified time interval.
- **Sample - Ignore Duplicate Alerts with 15s**—Enable this use case to ignore duplicate alerts from the same system.
- **Sample - Ignore Non-Critical Alerts from Printers**—Enable this use case to ignore non-critical alerts related to printers.

Trap Forwarding

Sample - Forward Critical Server Alerts to Other Monitoring Console - Enable this use case to forward SNMP alerts another monitoring console.

Configuring Alert Log Settings

You can configure alert log settings to set the maximum size of alert logs; to generate a warning alert when the alert log reaches a set threshold, and to purge the alert logs. To modify the default settings:

1. Select **Manage→ Alerts→ Alert Log Settings**.
2. Enter a value or use the increment/decrement arrow buttons to increase or decrease the value.

   NOTE: The default maximum size of alert logs is 20,000 alerts. Once that value is reached, the older alerts are purged.

Renaming Alert Categories and Alert Sources

1. Click **Manage**→ **Alerts**→ **Alert Categories**.
2. In **Alert Categories**, right-click any of the **alert categories** (under the Alert Category heading in the left pane) and select **Rename**.
3. Provide a name for the alert category and click **OK**.

You can also rename an alert source.

13

Alerts - Reference

This page provides the following information:

- Alert Logs
  - Alert Log Settings
  - Alert View Filters
    - All Alerts
    - Critical Alerts
    - Normal Alerts
    - Unknown Alerts
    - Warning Alerts
- Alert Actions
  - Application Launch
  - E-mail
  - Ignore
  - Trap Forwarding
- Alert Categories

Alert Logs

You can view alerts from **Alerts Logs**. The Alert Logs allow you to view all alerts filtered by the active view filter.

The criteria for matching the alerts in the view filter includes:

- Alert severity. See Severity.
- Alert category or source. See Category and Sources Association.
- Alert device or device group source. See Device Association.
- Alert date, time, or day of week. See Date and Time Range.
- Alert acknowledged flag. See Acknowledgement.

There are several ways to view alerts:

- **Filter to very specific criteria**—Use the predefined view filters or create Alert View Filter tree under **Manage→ Alerts**. Then set this to the active view by clicking the view filter in the tree or selecting it from the drop down when on the home portal.
- **Quick view for a specific device or device group**—Navigate to the device or device group in the device tree. Then select the Alerts link in the right pane or right click the device and select 'Alerts' to see all the alerts specific to the device.
- **Quick filter for severity**—From the Alerts by Severity chart, click on a region of the chart for the alerts with that severity.
- **Quick filter**—Any view using grid filtering options.

The following table lists the predefined alert view filters.

All Alerts	Select to view all the alerts.
Critical Alerts	Select to view all the systems that are critical.
Normal Alerts	Select to view normal alerts.
Unknown Alerts	Select to view alerts that OpenManage Essentials cannot categorize.
Warning Alerts	Select to view all the warnings.

Select **Continuous Updates** to enable the user interface to update automatically when new alerts are received.

Alert Logs Fields

Severity	The alert severity
Acknowledged	Whether the alert has been acknowledged or not by the user.
Time	The date and time the alert was generated.
Device	The device which generated the alert.
Details	The message contained in the alert.
Category	The categorization of the alert.
Source	The name of the alert source definition.

Group By Column

To group by in **All Alerts**, drag the All Alert column that you want to group by and drop it in **Drag a column header and drop it here to group by that column**.

For example, In **All Alerts**, if you want to group by severity, select **Severity** and drag and drop it in the **Drag a column header and drop it here to group by that column** bar.

The alerts are displayed by severity.

Alert Details

Severity	The alert severity
Acknowledged	Whether the alert has been acknowledged or not by the user
Device	The device which generated the alert
Time	The date and time the alert was generated
Category	The categorization of the alert
Source	The name of the alert source definition
Description	The message contained in the alert
SNMP Enterprise OID	Provides the enterprise OID (SNMP OID prefix) of the management information base (MIB) file that defines the event source that you want to monitor.
SNMP Generic Trap OID	Provides the generic trap ID of the SNMP trap that you want to monitor from the desired event source. See the *Dell OpenManage Server Administrator SNMP Reference Guide* for more information on SNMP traps.
SNMP Specific Trap OID	Provides the specific trap ID of the SNMP trap that you want to monitor from the desired event source. See the *Dell OpenManage Server Administrator SNMP Reference Guide* for more information on SNMP traps.

Alert Log Settings

Configure settings which control the size, messaging, and purge settings of the Alert Logs.

Maximum size of Alert Logs	Determines the max number of alerts the alert logs can have before purging occurs.
Log a warning when the Alert Log size reaches	A warning alert is sent to the application log when this size is reached.
When the Alert Logs reach the Maximum size, purge	Purges the specified number of alerts when the max size is reached.

Alert View Filters

Alert Filter Name

In OpenManage Essentials, you use alert filters that are associated with alert actions to implement alerting capabilities. For example:

- You can create alert action associations to trigger actions, such as sending e-mails, when an alert condition is met.
- You can create ignore, exclude, or both associations to ignore SNMP traps and CIM indications when they are received. You use these associations to suppress alert floods.
- You can create alert view filters to customize the **Alert Logs** view.

For more information about creating alert action associations, see Managing Alerts.

Use this window to perform the following tasks:

- Create new alert action associations, ignore/exclude filters, and alert view associations.
- View summary information for alert action associations, ignore/exclude associations, and alert view filters.
- Edit, delete, rename, and copy alert action associations, ignore/exclude associations, and alert view filters.

Severity

This page provides a list of alert severity.

Name	Name of the item (applicable only for ignore action and view filter).
Enabled	Select to enable the alert action (applicable only for ignore action).
Severity	The alert types available.
All	Select to include all types of alerts.
Unknown	Select to include unknown alerts.
Normal	Select to include normal alerts.
Warning	Select to include warning alerts.
Critical	Select to include critical alerts.

Acknowledgement

Limit alerts based on the acknowledge flag.	Associations alerts by whether they have been acknowledged or not. This option is disabled by default.
Match only acknowledged alerts	Select to track acknowledged alerts only.
Match only unacknowledged alerts	Select to track unacknowledged alerts only.

Summary - Alert View Filter

The view filter summary screen is shown on the final page of the alert view filter wizard or when clicking on the view summary right-click option in the tree.

Name	The name of the alert action.
Type	The alert action type - App Launch, Email, Ignore, Trap, and Forward.
Description	The description of the alert action.
Associated Severity	The alert severity criteria used when matching alerts.

Associated Alert Categories	The alert category criteria used when matching alerts.
Associated Alert Sources	The alert source criteria used when matching alerts.
Associated Device Groups	The alert source device group criteria used when matching alerts.
Associated Devices	The alert source device criteria used when matching alerts.
Associated Date Range	The alert date range criteria used when matching alerts.
Associated Time Range	The alert time range criteria used when matching alerts.
Associated Days	The alert days criteria used when matching alerts.
Associate Acknowledge	If enabled, uses the alert acknowledged flag when matching alerts.

Alert Actions

Alert actions are triggered when an incoming alert matches the specific criteria defined in the alert action.

The criteria for matching the alert includes:

- Alert severity. See Severity Association.
- Alert category or source. See Category and Sources Association.
- Alert device or device group source. See Device Association.
- Alert date, time, or day of week. See Date and Time Range.

There are four types of alert actions:

- **Alert Application Launch Action**—Launch a script or batch file when the alert action criteria is matched.
- **Alert Email Action**—Send an e-mail when the alert action criteria is matched.
- **Alert Ignore Action**—Ignore the alert when the alert action criteria is matched.
- **Alert Trap Forward Action**—Forward the SNMP Trap to another management console when the alert action criteria is matched.

By default, new alert actions are enabled. If you wish to turn off the alert action without deleting it, you can disable it either through the right-click menu or the edit wizard for the alert action.

Several common alert action use cases are pre-installed in the disabled state to illustrate common usage. When using these pre-installed actions, it is recommended to Clone the example to a new action specific to your needs. Make sure to enable and test the new action during this process.

Name and Description

Name	The name of the alert action.
Description	The description of the e-mail action.
Enabled	Select to activate the alert action.

Severity Association

Severity	The alert types available.
All	Select to include all types of alerts.
Unknown	Select to include unknown alerts.
Normal	Select to include normal alerts.
Warning	Select to include warning alerts.
Critical	Select to include critical alerts.

Application Launch Configuration

Use this window to configure the application that you want to launch and to test the launch.

NOTE: Alert actions are run when a matching alert is received so the alert application launch action is a script or batch file that does not require user interaction.

Executable Name	Specifies the fully qualified path name and file name of the executable file that launches the application program.

Arguments	Specifies or edits any required or desired command line parameters to be used in launching the application program. You can use the following variable substitutions to specify information in the **Arguments** field:
	`$n = system name`
	`$ip = IP address`
	`$m = message`
	`$d = date`
	`$t = time`
	`$sev = severity`
	`$st = Service Tag`
	`$e = enterprise OID`
	`$sp = specific trap ID`
	`$g = generic trap ID`
	`$cn = alert category name`
	`$sn = alert source name`
	`$pkn = package name`
	`$at = asset tag`
	If you have an executable or a batch file with the parameter /f in a file name, you might have an application launch that looks like the following:
	Executable Name value is c:\temp\your_script.bat and **Arguments** is /f output.txt>null. When the alert action is triggered, it runs your_script.bat /f output.txt.
	To use batch files in Application Launch for alert actions, in the Executable Name field, enter the path and name of batch file. In the Arguments field enter > null and ensure that you enter a space between > and null for the batch file to execute properly.
	See the sample alert action under **Application Launch** alert action for more information.

Test Action	Allows you to test the application launch. **NOTE:** Alert actions are run when a matching alert is received; so the alert application launch action is a script or batch file that does not require user interaction.

E-Mail Configuration

You can configure Essentials so that you receive e-mail each time the alert associations for your devices meet specific alert criteria. For example, you may want to receive an e-mail message for all warning and critical alerts.

Use this window to specify the parameters for configuring the e-mail alert action.

To	Specifies a valid e-mail address served by the company's SMTP server of the person who is to receive the e-mail.
From	Specifies the originating e-mail address.
Subject	Specify the e-mail subject using text or the available alert tokens.
Message	Specify the e-mail message using text or the available alert tokens.
Email Settings	Select to provide the SMTP server name or IP address.
Test Action	Allows you to test the e-mail action. **NOTE:** After sending the test e-mail, verify that the e-mail was received successfully and has the expected content.

NOTE: Alert tokens are substituted at the time the alert action occurs. They are not substituted for a test action.

NOTE: Certain paging vendors support alphanumeric paging through e-mail. OpenManage Essentials supports paging through the e-mail option.

Trap Forwarding

Simple Network Management Protocol (SNMP) traps are generated in response to changes in the status of sensors and other monitored parameters on a managed device. In order to correctly forward these traps, you must configure an SNMP trap destination, defined either by IP address or host name.

For example, you may want to use trap forwarding if you are in a multi tiered enterprise environment using OpenManage Essentials to create associations and forward traps to the enterprise manager.

If the trap is being processed locally and then forwarded to the destination or it is just forwarded to the destination.

Use this window to specify the parameters for configuring trap forwarding.

Destination	Provide the IP address or host name for the system that is hosting the enterprise management application.
Community	Provide the SNMP community to which the destination IP address or host name belongs.
Test Action	Forwards a test trap to the specified destination using the specified community string.

Category and Sources Association

OpenManage Essentials has many alert categories and sources that are predefined and prepopulated for Dell management agents. Select any of the predefined alert categories or sources to associate it with the alert action or filter. For more information and the complete list of categories and alert sources, see Alert Categories.

Device Association

You can select predefined groups (device types), custom groups, specific devices, or a device query. Device association currently only covers predefined groups.

For custom groups, create a custom group using the **New Custom Group Wizard**. The custom group shows up in the tree.

To use device query, select a query from the list.

Click **New** to create a new device query to search and assign the devices to the alert action.

Click **Edit** to change the query logic.

Select groups or devices from the tree, you can use the query option to create a specific criteria for the selection.

Select a query	Select a query from the drop-down list.
New	Add a new query.
Edit	Edit an existing query.
All Devices	Select to include all the Devices that is managed in OpenManage Essentials.
HA Clusters	Select to include High Availability server clusters.
KVM	Select to include keyboard video mouse devices.
Microsoft Virtualization Servers	Select to include Microsoft Virtualization Servers.
Modular Systems	Select to include Modular Systems.
Network Devices	Select to include Network Devices.
OOB Unclassified Devices	Select to include out of band Unclassified Devices like Lifecycle controller enabled devices.
Printers	Select to include Printers.
RAC	Select to include devices with Remote Access controllers.
Servers	Select to include Dell servers.
Storage Devices	Select to include storage devices.
Unknown	Select to include unknown devices.
VMware ESX Servers	Select to include VMware ESX servers.

Date and Time Range

Limit Date Range	Specifies a specific date range to match alerts.
Limit Time Range	Specifies a specific time range to match alerts.
Limit Days	Select to specify the days on which to enable the alert association. If you do not enable this option, the association is applied continuously within the time frame that you specify. Each of these fields are exclusive of the other, so selecting date 8/1/11- 10/1/11, 1am to 4 AM, Friday, will match alerts on only Fridays from 1-4 AM only within that date range. **NOTE:** It is possible to input a date range and days selection that will never produce a result. For example, 9/1/11 and Monday - since 9/1/11 was a Thursday, it will never match. If none of these are checked, it means the alert selection will have no date/time filter.

Alert Action - Duplicate Alert Correlation

Yes. Only duplicate alerts that match this filter will be executed.	Enabling this option deletes duplicate alerts (with the same ID and from the same device) received within the specified interval. Use this option to prevent a device from sending an overabundance of alerts to the console.
Ignore duplicate alerts that are received during the interval (1-600 seconds)	Select to set time.
No	Select this option if you do not want duplicate alerts to run at increased duration.

Summary- Alert Action Details

View and edit selections.

The alert action details screen is shown on the final page of the alert action wizards or when clicking on any alert action in the tree.

The alert action will have a subset of the following properties, depending on alert action type and filter criteria chosen (this probably should be a table):

Name	The name of the alert action.
Action Enabled	Specifies if the alert action is enabled or disabled.
Type	The alert action type - App Launch, Email, Ignore, and Trap Forward.
Description	The description of the alert action.
To	The e-mail address(es) to whom the e-mail is sent.
From	The e-mail address from whom the e-mail originates.
Subject	The subject of the e-mail which may include alert tokens.
Message	The message of the e-mail which may include alert tokens.
Destination	The destination name or IP address used for trap forwarding.
Community	The community string used for trap forwarding.
Executable Name	The name of the executable, script, or batch file to be used by the alert action.
Arguments	The command line arguments used when invoking the alert action.
Associated Severity	The alert severity criteria used when matching alerts.
Associated Alert Categories	The alert category criteria used when matching alerts.
Associated Alert Sources	The alert source criteria used when matching alerts.
Associated Device Groups	The alert source device group criteria used when matching alerts.
Associated Devices	The alert source device criteria used when matching alerts.
Associated Date Range	The alert date range criteria used when matching alerts.
Associated Time Range	The alert time range criteria used when matching alerts.
Associated Days	The alert days criteria used when matching alerts.
Minimum Repeat Time	If enabled, specifies the minimum time in seconds between two of the same alerts from the same device.

Alert Categories

OpenManage Essentials has many alert categories and sources that are predefined and pre populated for Dell management agents.

Alert categories are organizational levels of the **Alert Categories** tree. Alert sources specify the low level details of each alert. To monitor the alert categories and sources, apply an alert action association to the alert source or to its parent category.

This page provides a list of categories and the alerts sources within that category. Use this page to configure alerts based on categories.

Brocade-Switch	Select this category to include alerts for Brocade-Switch.
Dell Advanced Infrastructure Management	Select this category to include alerts for Advanced Infrastructure Management.
Environmental	Select this category to include alerts for temperature, fan enclosure, fan speed, thermal, and cooling.
EqualLogic Storage	Select this category to include alerts for EqualLogic storage.
FC-Switch	Select this category to include alerts for Fibre Channel switches.
General Redundancy	Select this category to include alerts for General Redundancy.
HyperV Server	Select this category to include alerts for HyperV Server.
iDRAC	Select this category to include alerts for iDRAC.
Juniper-Switch	Select this category to include alerts for Juniper switches.
Keyboard-Video-Mouse (KVM)	Select this category to include alerts for KVMs.
Memory	Select this category to include alerts for **memory.**
Network	Select this category to include alerts related to network**.**
Other	Select this category to include alerts for other devices.
PDU	Select this category to include alerts for PDUs.
Performance Monitoring	Select this category to include alerts for Performance Monitoring.
Physical Disk	Select this category to include alerts for physical disks.

Power	Select this category to include alerts for power.
Power Center	Select this category to include alerts for power center.
Power Management	Select this category to include alerts for power management.
Printers	Select this category to include alerts for printers.
Processor	Select this category to include alerts for processor.
Removable Flash Media	Select this category to include alerts for removable flash media.
Security	Select this category to include alerts for security.
Storage Enclosure	Select this category to include alerts for storage enclosures.
Storage Peripheral	Select this category to include alerts for storage peripherals.
Storage Software	Select this category to include alerts for storage software.
System Events	Select this category to include alerts for system events.
Tape	Select this category to include alerts for tape drives.
Test Events	Select this category to include alerts for **test events**.
Unknown	Select this category to include unknown alerts related statuses.
UPS	Select this category to include alerts for UPS.
Virtual Disk	Select this category to include alerts for virtual disks.
VMware ESX Server	Select this category to include alerts for VMware ESX servers.

Alert Source

Each Alert Category contains alert sources. Click an alert category to view alert sources. Expand a category to view the list of alert sources, and select an alert source.

Name	The name of the new alert source, for example, myFanAlert.
Type	The protocol information.
Catalog	Provides the catalog information.
Severity	Specifies the severity assigned to the alert that is triggered if the alert source generates the specified SNMP trap.

Format string	Provides the message string that appears in the **Alert Logs** if the alert source generates an alert of sufficient severity to trigger the alert. You can use formatting commands to specify parts of the message string. For SNMP, the valid formatting commands are: $n = system name $d = date $t = time $s = severity $e = enterprise object identifier (OID) $sp = specific trap OID $g = generic trap OID $1 - $# = varbind values
SNMP Enterprise OID	Provides the enterprise OID (SNMP OID prefix) of the management information base (MIB) file that defines the event source that you want to monitor.
SNMP Generic Trap OID	Provides the generic trap ID of the SNMP trap that you want to monitor from the desired event source. See the *Dell OpenManage Server Administrator SNMP Reference Guide* at **support.dell.com/manuals** for more information on SNMP traps.
SNMP Specific Trap OID	Provides the specific trap ID of the SNMP trap that you want to monitor from the desired event source. See the *Dell OpenManage Server Administrator SNMP Reference Guide* for more information on SNMP traps.

14

Updating Server BIOS, Firmware, Drivers, and Applications

With the System Update feature in OpenManage Essentials, you can:

- Upgrade and downgrade firmware, drivers, BIOS, application, and OpenManage Server Administrator.
- Compare the drivers and firmware on the inventoried servers and modular blade enclosures with a source catalog and update them if needed.

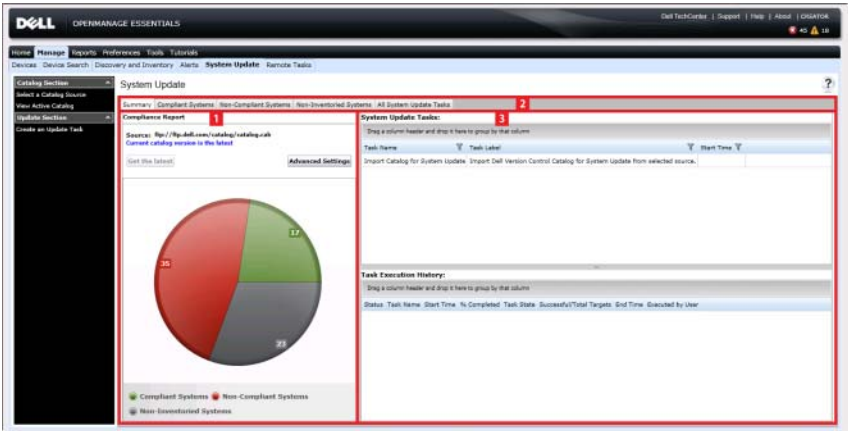
NOTE: Inventory automatically starts after the updates are applied to a target server.

NOTE: OpenManage Essentials does not support system updates through Lifecycle Controller.

Check for these prerequisites before you update systems:

- Internet is accessible and you can access **dell.com** and **ftp.dell.com** if you are using online catalog source.
- DNS is resolved.

To view the System Update page, click **Manage→ System Update**.


DELL
OPENMANAGE ESSENTIALS
Dell TechCenter | Support | Help | About | OSIATOR
45 18
Home Manage Reports Preferences Tools Tutorials
Devices Device Search Discovery and Inventory Alerts System Update Remote Tasks
Catalog Section
Select a Catalog Source
View Active Catalog
Update Section
Create an Update Task
System Update
?
Summary Compliant Systems Non-Compliant Systems Non-Inventoried Systems All System Update Tasks
1
2
3
Compliance Report
Get the latest
Advanced Settings
17
35
23
● Compliant Systems ● Non-Compliant Systems
● Non-Inventoried Systems

Source: ftp://ftp.dell.com/catalog/catalog.cab
Current catalog version is the latest

System Update Tasks:

Drag a column header and drop it here to group by that column

Task Name	Task Label	Start Time
Import Catalog for System Update	Import Dell Version Control Catalog for System Update from selected source.	

Task Execution History:

Drag a column header and drop it here to group by that column

Status	Task Name	Start Time	% Completed	Task State	Successful/Total Targets	End Time	Executed by User

1 Compliance report. See Compliance Report.

2 Tabbed systems information. See Compliant Systems, Non-Compliant Systems, and Non-Inventoried Systems.

3 System update tasks. See All System Update Tasks.

Understanding Server BIOS Firmware and Drivers Sources

There are multiple sources for obtaining firmware and drivers for the servers.

- **Online source**—Default option which obtains latest driver and firmware versions from ftp.dell.com.

  NOTE: OpenManage Essentials automatically checks for updates and displays a message if a newer version is available.

- **File system source**—Drivers and firmware from the Dell OpenManage Server Update Utility (SUU) media.
- **Repository Manager file**—Customized selection of specific drivers and firmware generated from the Dell Repository Manager tool.

Choosing the Right Source for Updates

- **Recommended Option**—Use the online source to ensure that you consistently have the latest drivers and firmware available from Dell or use the Dell Server Update Utility (SUU) option for a qualified set of drivers and firmware.
- **Create Custom Catalog**—Using this option gives you maximum control over driver and firmware revisions in your environment because you select them individually from either the SUU media or online source using the Dell Repository Manager. You can install Repository Manager, a separate tool, from the OpenManage Essentials installation package.

Selecting an Update Catalog Source

1. From OpenManage Essentials, click **Manage**→ **System Update**→ **Select a Catalog Source**.
2. In **Select a Catalog Source**, select an option, and click **Import now**.

   The catalog is downloaded and a set of reports are generated.

Viewing Comparison Results

To view compliant servers:

1. Click **Manage**→ **System Update**.
2. In **System Update**, select the **Compliant Systems** tab.

   The servers with drivers and firmware at the same version as the catalog are displayed.

To view non-compliant servers:

1. Click **Manage**→ **System Update**.
2. In **System Update**, select the **Non-Compliant Systems** tab.

   The servers with drivers and firmware versions that are different from the catalog are displayed.

To view non-inventoried servers:

1. Click **Manage**→ **System Update**.
2. In **System Update**, select the **Non-Inventoried Systems** tab.

   The servers that are not inventoried are displayed.

NOTE: CMC firmware updates (CMC active controller only) are also displayed in these results.

Applying System Updates

To apply system updates, first select the non-compliant systems and then schedule the update.

Selecting Non-Compliant Systems

1. Click **Manage**→ **System Update**.
2. In **System Update**, select the **Non-Compliant Systems** tab.
3. In **Non-Compliant systems**, select the systems you want to update.

   NOTE: You can update multiple systems at the same time.
4. Click **Apply Selected Updates**.

   A window is displayed to schedule the updates.

NOTE: Chassis and blades are not associated for updates. They are treated as individual components and you must manually select them.

NOTE: Chassis, blade server BIOS, and iDRAC version interdependency management is not available.

Scheduling Updates

You can set a schedule to update servers. For example, you might want to make updates during a specific maintenance time frame. To schedule updates:

1. Click **Manager**→ **System Update**→ **Update Section**→ **Create an Update Task**.
2. Provide a task name.
3. Review the selected updates.
4. Set the task schedule to **Run Now** or set a specific date and time.
5. If you do not want to apply the changes immediately, clear **After update, if required, reboot the device**. Changes are not activated until the next time you reboot.
6. Enter the operating system administrative credentials for the managed server.

   Examples:

   In a Windows domain environment, enter `<Domain\Administrator>` and the password.

   In a Windows workgroup environment, enter `<LocalHost\Administrator>` and the password.

   In a Linux environment, enter root and Password.

7 Click **Finish**.

> **NOTE:** You cannot schedule Windows and Linux updates to occur using the same task. Create a separate task for each.

8 Click **View All Software Update Tasks** for a list of all scheduled updates.

Viewing Updated Status

To view and confirm that updates were applied successfully, click **Manage→ System Update→ Summary.** The **Task Execution History** pane displays if the updates were applied successfully.

Viewing Active Catalog

1 From OpenManage Essentials, click **Manage→ System Update→ View Active Catalog**.

2 In **Active Catalog**, if new version is available and the source is the Dell FTP site, click **Update**.

15

System Update - Reference

You can access the following:

- System Update page
  - Summary
    - Compliance Report
    - System Update Tasks
    - Tasks Execution History
  - Compliant Systems
  - Non Compliant Systems
  - Non-Inventoried Systems
  - All System Update Tasks
- Catalog Section
  - Select a Catalog Source
  - View Active Catalog
- Update Section
  - Create an Update Task

Filter Options

1. Click the funnel icon to filter search.
2. After selecting a filter option from the drop-down list, and providing the alphanumeric characters in the field, click the **aA** button to make the filter search case independent.
3. After you set the filter logic, click **Filter** to run the filter logic.

Click **Clear Filter** to clear a search.

Is equal to	Select to create the *same as* logic.
Is not equal to	Select to create the *different from* logic.

Starts with	Select to filter search based on a text chunk's initial alphanumeric character(s). Provide the starting alphanumeric character(s) in the field.
Ends with	Select to filter search based on a text chunk's final alphanumeric character(s). Provide the ending alphanumeric character(s) in the field.
Contains	Select to filter search based on alphanumeric characters present in a text chunk. Provide the alphanumeric character(s) in the field.
Does not contain	Select to include the *not present* logic in search based on alphanumeric characters present in a text chunk.
Is contained in	Select to include the *is present* logic in an alphanumeric character string.
Is not contained in	Select to include the *not present* logic in an alphanumeric character string.

System Update

This page provides the following information:

- Summary
- Compliant Systems
- Non Compliant Systems
- Non-Inventoried System
- All System Update Tasks

Compliance Report

The compliance report provides a pie chart distribution of software update tasks. Click a pie chart portion to view more information on the systems.

Compliance Report lists this information:

Source	Report source
Get the latest	This option is disabled if the catalog version is the latest. Else, it is active. Click this option to get the latest catalog version.

Advanced Settings	Using these options you can set preferences for upgrading and downgrade firmware and BIOS versions: • **Enable Downgrades**—Select this option to install versions of firmware and BIOS that are earlier than the versions installed on the systems. • **Disable Downgrades**—This option is set by default, selecting this option enables you to install versions of firmware and BIOS that are later than the versions installed on the systems.
Systems information - pie chart format	The pie chart lists the systems status compared with the existing catalog file. The systems listed are as follows: • Compliant Systems • Non-Compliant Systems • Non-Inventoried Systems
Compliant Systems	Systems with software that is up to date when compared with versions available in the software updates active catalog. Click compliant systems portion to view more information in the **Compliant Systems** tab.
Non-Compliant Systems	Systems with software that requires updates when compared with versions available in the software updates active catalog. Click the non-compliant systems portion to view more information in the **Non-Compliant Systems** tab.
Non-Inventoried Systems	Discovered systems pending inventory when compared with available software in the active catalog. Click non-inventoried portion to view more information in the **Non-Inventoried Systems** tab.

Compliant Systems

The Compliant Systems tab provides this information:

System Name	System's domain name.
Model Type	Devices model information
Operating System	The operating system that is running on the server.
Service Tag	A unique identifier, that provides the service lifecycle.

Discovered Time	Time and date of discovery.
Inventory Time	Time and date of inventory.
Server Subnet Location	IP address range information.

Non-Compliant Systems

The Non-Compliant Systems tab provides this information:

System Name	System's domain name.
Model Type	The systems model name. For example, Dell PowerEdge.
Operating System	The operating system that is installed on the system.
Service Tag	A unique identifier, that provides the service lifecycle information.
Discovered Time	Time and date of discovery.
Inventory Time	Time and date of inventory.

Select non-compliant systems to select updates to apply and click **Apply Selected Updates**.

System Name	System's domain name.
Importance	The requirement of this software update for the system.
Component	The software information.
Type	The type of software update.
Installed Version	The installed version number.
Upgrade/Downgrade	A green arrow indicates and upgrade.
Available Version	The available version number.
Package Name	The name of the software update.

Non-Inventoried Systems

The **Non-Inventoried Systems** tab provides a list of systems that require inventory, select the systems you want to inventory and click **Inventory**.

System Name	System's domain name.
Discovered Time	Time and date of discovery.
Inventory Time	Time and date of inventory.
Server Subnet Location	IP address range information.

Inventory Systems

To inventory systems, select Systems To Inventory and click **Run Inventory**.

All System Update Tasks

This page provides more information on the software update tasks.

Task Name	The name of the task.
Task Label	Provides information on what the task does.
Start Time	Time and date of inventory.

Task Execution History

Lists the details of the system update tasks.

Status	Information on the task if enabled or disabled.
Task Name	The name of the task.
Start Time	Time and date at which the system update task started.
% Completed	The task's progress information.
Task State	Provides these task states: **Running** **Stopped** **Completed**
Success / Total Targets	The number of target systems on which the task is successfully executed.

End Time	Time and date at which the system update task ends.
Executed by User	The user information.

Select a Catalog Source

For updating software, select from these options to use a default catalog file present on the Dell FTP site or provide an alternate software update package file.

Use file system source (SUU)	Select to update software using Server Update Utility. Click **Browse** to traverse to the file location. The **catalog.cab** file is located in the repository folder.
Use repository manager file	Select to update software using repository manager file. Click **Browse** to traverse to file location. The **catalog.cab** file is located in the repository folder.
Use an online source	Select to update software using the software update package present on the Dell FTP site.

A Dell Update Package (DUP) is a self-contained executable in a standard package format that updates a single software element on the system. DUPs are software utilities provided by Dell to update specific software components on Dell PowerEdge systems, Dell desktops, and Dell laptops. The customized bundles and repositories are made up of DUPs based on operating systems supported, update types, form factor, and line of business.

Dell OpenManage Server Update Utility (SUU) is a DVD-based application for identifying and applying updates to your system. SUU displays a comparison report of the versions and provides various options for updating the components.

Repository Manager is an application that allows you to create repositories of customized bundles and updates, and groups of related updates for systems running supported Microsoft Windows or Linux operating systems. This facilitates generating comparison reports and establishing update baselines of repositories. By using Repository Manager, you can ensure that your Dell PowerEdge system, Dell desktop or Dell laptop is equipped with the latest BIOS, driver, firmware, and software updates.

View Active Catalog

Select to view the catalog file that is currently in use for doing software updates.

Source	Displays the source. The source is either System Update Utility, FTP, or Repository Manager.
Source Type	The type for source from which the catalog file is taken. For example Dell ftp site.
Release ID	The unique identification number assigned to the released catalog file.
Release Date	The date on which the catalog file was released.
Newer version available	Displays if a newer version is available.

Create an Update Task

Select to create a software update task and set a task schedule to run the task.

Task Name	Provide a name for the software update task.
Select System to Update	Select the system that you want to update.
System Name	System's domain name.
Importance	The requirement of this software update for the system.
Component	The software information.
Type	The type of software update.
Installed Version	The installed version number.
Upgrade/Downgrade	A green arrow indicates an upgrade.
Available Version	The available version number.
Package Name	The name of the software update.
Set the Task Schedule	
Run Now	Select this option if you want to run the task when you click **Finish**.

After update if required, reboot the device.	Select to reboot after the software update task is complete.
Set Schedule	Select to schedule a task at a required date and time. Click the icon to set date and time.
Enter Credentials for the task execution	
SSH Port Number	Provide the SSH port number
User name	Provide the user name for the selected target.
Password	Provide password for the selected target.

16

Managing Remote Tasks

About Remote Tasks

With the Remote Tasks feature in OpenManage Essentials, you can:

- Run commands on local and remote systems, run batch files and executable files on the local systems, and schedule local and remote tasks.

  NOTE: The files must be located on the system with OpenManage Essentials installed and not on the remote system.

- Change power status for a system.
- Deploy OpenManage Server Administrator on systems.
- View the remote tasks.
- Make changes to any task by right-clicking it.

Managing Command Line Task

You can create custom command line tasks to run CLI commands on local and remote systems, and run batch files and executables on local systems.

For example, you can create a custom command line task to run a security audit and gather information on the systems' security status.

To create command line tasks:

1. From OpenManage Essentials, click **Manage**→ **Remote Tasks**→ **Create Remote Tasks**. Right-click **Command Line** and click **Create Command Line Task**.
2. On **General**, provide a task name.
3. Select one of the following options:
   - **Remote Server Administrator Command**—Select to run the server administrator command on remote servers.
   - **Generic Command**—Select to run the command, executable file, or batch file.

- **IPMI Command**—Select to run the IPMI commands on the remote system.
- **RACADM Command Line**—Select to run the RACADM commands on the remote system.

4 Based on your selection in the preceding step, provide the following:

- If you selected **Remote Server Administrator Command**, then provide command, SSH port number, and select **Generate Trusted Key for Linux** if you want to generate a trusted key.
- If you selected **Generic Command, RACADM Command Line,** or **IPMI Command** then provide command and append output information. Providing the append output information is optional.

5 On **Task Target,** do one of the following:

- Select a query from the drop-down list or create a new query by clicking the **New** button.
- Select server targets for running the commands.

6 On **Schedule and Credentials**, provide user credentials, and set schedule for the tasks from available options, and then click **Finish**:

For more information, see Command Line Task.

Managing RACADM Command Line Tasks

RACADM command line tasks are used to run commands on remote DRACs and iDRACs. For example, run a RACADM task to configure iDRAC through out of band (OOB) channel. To manage RACADM Command line tasks:

1 From OpenManage Essentials, click **Manage→ Remote Tasks→ Create Remote Tasks**. Right-click **Command Line** and click **Create Command Line Task**.

2 On **General**, choose **RACADM Command Line** and enter a name for the task.

3 Enter the RACADM sub-command (for example, **getsysinfo.**) For a list of RACADM commands, go to **support.dell.com**.

4 (Optional) Choose **Output to file** to capture task output from multiple targets. Enter path and file name.

a To log the information from all selected targets, select **Append** b To write all the detected errors to the log file, select **Include errors**.

5 On **Task Target,** do one of the following:

- Select a query from the drop-down list or create a new query by clicking the **New** button.
- Choose target servers or DRACs/iDRACs.

6 On **Schedule and Credentials**, set the schedule parameters, provide target credentials and then click **Finish**.

Make changes to any task by right-clicking the task.

Managing Server Power Options

You can create tasks to manage power on servers. To create a remote task:

1 From OpenManage Essentials, select **Manage**→ **Remote Tasks**→ **Create Remote Tasks**. Right-click **Server Power Options** and select **Create Power Task**.

2 In **Create a Power Task**, on **General**, do the following:

- Provide task name.
- Select power options. If required, select **Shutdown OS first** to shut the operating system down before starting the power tasks.

3 On **Task Target,** do one of the following:

- Select a query from the drop-down list or create a new query by clicking the **New** button.
- Select server targets for running the commands.

4 On **Schedule and Credentials**, set the schedule parameters, provide target credentials, and then click **Finish**.

For more information, see Server Power Options.

Deploying Server Administrator

You can create tasks to deploy OpenManage Server Administrator on servers installed with Windows or Linux operating systems. You can also plan a date and time to schedule the OpenManage Server Administrator deploy task.

To create an OpenManage Server Administrator deployment task:

1. Select **Manage**→ **Remote Tasks**→ **Create Remote Tasks.** Right-click **Deploy Server Administrator** and click **Create Deployment Task.**
2. On **General**, provide task name. If you want to deploy OpenManage Server Administrator on Windows-based servers, then select **Windows**, provide installer path and, if required, provide arguments. If you want to deploy OpenManage Server Administrator on Linux-based servers, select **Linux** and provide the installer path and, if required, provide arguments. Select **Generate Trusted Key** and select **Allow reboot**.

   NOTE: Install Server Administrator prerequisites before deploying Server Administrator on Linux.

3. On **Task Target,** do one of the following:
   - Select a query from the drop-down list or create a new query by clicking the **New** button.
   - Select servers on which you want to run this task and click Next.
4. On **Schedule and Credentials**, set the schedule parameters, provide user credentials; to enable the task, and then click **Finish**.

For more information, see Deploy Server Administrator Task.

Working With Sample Remote Tasks Use Cases

Sample remote tasks are available for Server Power Options, Deploy Server Administrator, and Command Line. Sample remote tasks use cases are disabled by default. To enable a sample use case:

1. Right-click the use case and select **Clone**.
2. Enter the **Cloned Task Name** and click **Ok**.
3. Right-click the cloned task and select **Edit**.
4. Enter the required information and assign targets to the tasks. For information about the options, see Remote Tasks - Reference.

Use Cases in Remote Tasks

Server Power Options

Sample-Power On Device—Enable this use case to turn on the server. The system must have RAC/DRAC configured.

Deploy Server Administrator

Sample-OMSA Upgrade Windows—Enable this use case to upgrade OpenManage Server Administrator on a Windows-based system.

Command Line

- **Sample-Generic Command Remote**—Enable this use case to use tokens to receive the IP address or name of inventories systems.

  NOTE: To use this command, you must enter the local system credentials.

- **Sample-Generic Command Local**—Enable this use case to run a command or script on system with OpenManage Essentials.

  NOTE: To use this command, you must enter the local system credentials.

- **Sample-IPMI Command**—Enable this use case to receive information about the power status of a server.
- **Sample-Remote Command**—Enable this use case to view the system summary through Server Administrator.
- **Sample RACADM-Clear SEL Log**—Enable this use case to clear the SEL log of RAC.
- **Sample-RACADM-Reset**—Enable this use case to reset the RAC.

17

Remote Tasks - Reference

From Remote Tasks you can:

- Run commands on local and remote systems, batch files and executable files on the local systems, and schedule local and remote tasks.
- Change power status for a system.
- Deploy OpenManage Server Administrator on systems.
- View the remote tasks.

Remote Tasks:

- Create Remote Tasks
  - Server Power Options
  - Deploy Server Administrator
  - Command Line

Remote Tasks Home

To view Remote Tasks page, in OpenManage Essentials, click **Manage→ Remote Tasks**.

Remote Tasks

Remote Tasks page lists this information:

- All Tasks
- Server Power Options
- Server Administrator Deployment
- Command Line

All Tasks

Scheduled State	Displays if the task is enabled.
Task Name	Names of the task.
Task Label	Type of task that is run, for example; for a command line task the options displayed are Remote Server Administrator Command, Generic Command, IPMI Command, and RACADM Command Line.
Last Run	The last time and date information when the task was run.
Created On	The time and date on which the task was created.
Updated On	The time and date information when the task was run.
Updated By	The name of the user.

Task Execution History

Status	Displays the status of the task.
Task Name	Schedule information of the task.
Start Time	The date and time on which the task was run.
% Completed	Progress of the task.
Task State	Status information of the task.
Successful/Total Targets	Number of target servers accessed.
End Time	The date and time on which the task ends.
Executed by User	Name of the user who ran this task.

Server Power Options

Select this option to change the power state or reboot systems.

General	
Task Name	Provide a name for this server power options task
Select the type	Select from the following options: • **Reboot**—Reboots the system without powering off. • **Power Cycle**—Powers off and then reboots the system. **NOTE:** Make sure that the shutdown option is configured for the operating system before you perform a graceful shutdown using this option. If you use this option without configuring it on the operating system, it reboots the managed system instead of performing a shutdown operation. • **Power Off**—Powers off the system. • **Power On**—Powers on the system. This option works only on target systems that contain RAC.
Shutdown OS first	Select to shut down the operating system before executing the server power options task.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click **New**.
Select the server(s) for this task to target	Select the severs to which you want to assign this task.
Schedule and Credentials	

Set Schedule	Select from these options: • **Activate Schedule**—Select this option to activate a schedule for the task. • **Run now**—Select this option to run the task immediately. • **Set schedule**—To set a date and time for the task to run. • **Run Once** —Select this option to run the task on the planned schedule only once. • **Periodic** —Select this option to run the task frequently at specified intervals. – **Hourly**—Select this option to run the task once every hour. – **Daily**—To run the task once every day. – **Weekly**—To run the task once every week. – **Monthly**—To run the task once every month. **Range of Recurrence**: – **Start**—To specify the date and time at which the task should begin. – **No End Date**—To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. – **End By**—To stop the task at the specified date and time.

Enter User Name and Password	**User Name —**Provide credentials in the format domain\user name or local host\user name. **Password—**Provide the password for the target server. **Power On** works only on targets systems with iDRAC; use the IPMI credentials to perform **Power On** task. If you selected **Power On** then provide KG Key. **KG Key** - Enter the KG Key. DRAC also supports IPMI KG Key. Each BMC is configured to require an access key in addition to user credentials. The KG key is prompted only for power-on task and not other power tasks because it is an IPMI task. **NOTE:** The KG key is a public key that is used to generate an encryption key for use between the firmware and the application; and is available only on Dell PowerEdge *y9xx* and later systems. The KG key value is an even number of hexadecimal characters. In the format, *yxxx*, *y* denotes alphanumeric characters and x denotes numbers.

Deploy Server Administrator Task

Select this option to create tasks to deploy Server Administrator on selected servers.

General	
Task Name	Provide a name for the task.
Select the type	Select from the following options: • Windows • Linux

Installer Path	The location where the Server Administrator installer is available. For Windows, packages with **.dup, .msi,** and **.msp**. file extensions are available. Msi packages enable Server Administrator installation and upgrades while dup and msp packages enable only Server Administrator upgrades. For Linux, packages with the tar.gz file extensions are available. For Linux, the**.sign** file is required for verification. The .sign file must reside in the same folder as the tar.gz file.
Installer Arguments	(Optional) Provide arguments. For example, in Windows, the parameters are as follows: • `ADDLOCAL = IWS`—Server Administrator web server only • `ADDLOCAL = SSA`—Server instrumentation only For example, in Linux, the parameters are as follows: • `–w` - Server administrator web server only • `–d` - Server instrumentation only See the *Dell OpenManage Installation and Security User's Guide* at **support.dell.com/manuals** for a complete list of arguments.
Generate Trusted Key	This option is available if you selected Linux. Select this option to generate a trusted key.
Allow reboot (if required)	Select this option to reboot the server once you deploy Server Administrator on the server.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click **New**.
Select the server(s) for this task to target	Select the severs to which you want to assign this task.

Schedule and Credentials	
Set schedule	Select from these options: • **Activate Schedule**—Select this option to activate a schedule for the task. • **Run now—**Select this option to run the task immediately. • **Set schedule—**Select this option to set a date and time for the task to run.
Enter User Name and Password	**User Name—**Provide in the format domain\user name or local host\user name. **Password—**Provide the password.

Command Line Task

Select this option to create command line tasks.

General	
Task Name	Provide name of the task.
Remote Server Administrator Command	Select this option to run Remote Server Administrator Command on selected servers.
Generic Command	Select this option to run executable and commands on the system with OpenManage Essentials.
IPMI Command	Select this option to run IPMI commands on selected servers.
RACADM Command Line	Select this option to run RACADM commands on selected servers.

Remote Server Administrator Command

Command	Provide command, for example. `omereport system summary`
SSH Port number	Provide the Secure Shell (SSH) port number on the managed Linux system. The default value for the port number is 22.

Generate Trusted Key for Linux	Select this option to generate a trusted device key for communicating with devices. This option is disabled by default. **NOTE:** The first time that OpenManage Essentials communicates with a managed device with Linux operating system, a key is generated and stored on both the devices. This key is generated per device and enables a trust relationship with the managed device.
Output to file	Select to enable output to a log file. This option captures standard output and writes it to the log file. If you select this option, enter the path name and file name of the log file. This option is disabled by default.
Append	Select to append output from the completed command to the specified file. If the file does not exist, it is created.
Include errors	Select to write all OpenManage Essentials-detected errors to the log file. For example, if no response is received to a ping request before the execution of the command, an error is written to the log file.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click **New**.
Select the servers	Select the severs to which you want to assign this task.

Schedule and Credentials	
Set schedule	Select from these options: • **Activate Schedule**—Select this option to activate a schedule for the task. • **Run now**—Select this option to run the task immediately. • **Set schedule**—Select this option to set a date and time for the task to run. • **Run Once**—Select this option to run the task on the planned schedule only once. • **Periodic**—Select this option to run the task frequently at specified intervals. – **Hourly**—Select this option to run the task once every hour. – **Daily**—To run the task once every day. – **Weekly**—To run the task once every week. – **Monthly**—To run the task once every month. **Range of Recurrence**: – **Start**—To specify the date and time at which the task should begin. – **No End Date**—To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. – **End By**—To stop the task at the specified date and time.
Enter User Name and Password	**User Name**—Provide in the format domain\user name or local host\user name. **Password**—Provide the password.

Generic Command

Command	Provide the fully qualified path name and file name of the executable, command, or script file that launches the application program.
Arguments	Provide the supporting arguments for the launching the application, script, or command. These arguments are case sensitive. To view and select from the list of inventoried systems, In Arguments, include **$IP** or **$NAME**. The returned value includes information of the IP address and the system name.
Output to file	Select to enable output to a log file. This option captures standard output from the running application and writes it to the log file. If you select this option, you must enter the pathname and file name of the log file. This option is disabled by default.
Append	Select to append output from the completed command to the specified file. If the file does not exist, it is created.
Include errors	Select to write all OpenManage Essentials-detected errors to the log file. For example, if no response is received to a ping request before the execution of the command, an error is written to the log file.

Schedule and Credentials	
Set schedule	Select from these options: • **Activate Schedule**—Select this option to activate a schedule for the task. • **Run now**—Select this option to run the task immediately. • **Set schedule**—Select this option to set a date and time for the task to run. • **Run Once**—Select this option to run the task on the planned schedule only once. • **Periodic**—Select this option to run the task frequently at specified intervals. – **Hourly**—Select this option to run the task once every hour. – **Daily**—To run the task once every day. – **Weekly**—To run the task once every week. – **Monthly**—To run the task once every month. **Range of Recurrence**: – **Start**—To specify the date and time at which the task should begin. – **No End Date**—To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. – **End By**—To stop the task at the specified date and time.
Enter User Name and Password	**User Name**—Provide OpenManage Essentials user credentials in the format domain\user name or local host\user name. **Password**—Provide the password.

IPMI Command

Arguments	Provide the supporting arguments. These arguments are case-sensitive. Provide the corresponding IPMI commands to run the task on selected targets.
Output to file	Select to enable output to a log file. This option captures standard output from the running application and writes it to the log file. If you select this option, you must enter the path name and file name of the log file. This option is disabled by default.
Append	Select to append output from the completed command to the specified file. If the file does not exist, it is created.
Include errors	Select to write all OpenManage Essentials-detected errors to the log file. For example, if no response is received to a ping request before the execution of the command, an error is written to the log file.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click **New**.
Select the server(s) for this task to target	Select the severs to which you want to assign this task.

Schedule and Credentials	
Set schedule	Select from these options: • **Activate Schedule**—Select this option to activate a schedule for the task. • **Run now**—Select this option to run the task immediately. • **Set schedule**—Select this option to set a date and time for the task to run. • **Run Once** —Select this option to run the task on the planned schedule only once. • **Periodic**—Select this option to run the task frequently at specified intervals. – **Hourly**—Select this option to run the task once every hour. – **Daily**—To run the task once every day. – **Weekly**—To run the task once every week. – **Monthly**—To run the task once every month. **Range of Recurrence**: – **Start**—To specify the date and time at which the task should begin. – **No End Date**—To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. – **End By**—To stop the task at the specified date and time.
Enter User Name and Password for accessing remote system	**User Name**—Provide the IPMI (or DRAC/iDRAC) credentials. **Password**—Provide the password. **KG Key**—Enter the KG Key. DRAC also supports IPMI KG Key. Each BMC is configured to require an access key in addition to user credentials.

RACADM Command Line

Command	Provide the RACADM command you want to run on the servers.
Output to file	Select to enable output to a log file. This option captures standard output from the running application and writes it to the log file. If you select this option, you must enter the path name and file name of the log file. This option is disabled by default.
Append	Select to append output from the completed command to the specified file. If the file does not exist, it is created.
Include errors	Select to write all OpenManage Essentials-detected errors to the log file. For example, if no response is received to a ping request before the execution of the command, an error is written to the log file.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click **New**.
Select the server(s) for this task to target	Select the severs to which you want to assign this task.

Schedule and Credentials	
Set schedule	Select from these options: • **Activate Schedule**—Select this option to activate a schedule for the task. • **Run now**—Select this option to run the task immediately. • **Set schedule**—Select this option to set a date and time for the task to run. • **Run Once**—Select this option to run the task on the planned schedule only once. • **Periodic**—Select this option to run the task frequently at specified intervals. – **Hourly**—Select this option to run the task once every hour. – **Daily**—To run the task once every day. – **Weekly**—To run the task once every week. – **Monthly**—To run the task once every month. **Range of Recurrence**: – **Start**—To specify the date and time at which the task should begin. – **No End Date**—To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. – **End By**—To stop the task at the specified date and time.
Enter User Name and Password	**User Name**—The RACADM task requires IPMI credentials. Provide IPMI credentials to run the task. **Password**—Provide the password.

18

Managing Security Settings

Using Security Roles and Permissions

OpenManage Essentials provides security through role-based access control (RBAC), authentication, and encryption. RBAC manages security by determining the operations run by persons in particular roles. Each user is assigned one or more roles, and each role is assigned one or more user privileges that are permitted to users in that role. With RBAC, security administration corresponds closely to an organization's structure.

OpenManage Essentials roles and associated permissions are as follows:

- OpenManage Essentials Guests is a default role assigned to all users at initial log in. No permissions are associated with this role, and it is not displayed in the Windows user groups list. It enables administrators to monitor unauthorized users attempting to access the console.
- OpenManage Essentials Users have read only access and cannot perform other operations. They can log in to the console, run discovery and inventory tasks, view settings, and acknowledge events. The Windows Users group is a member of this group.
- OpenManage Essentials Administrators have full access to all the operations within OpenManage Essentials. Windows Administrators group is member of this group.

Microsoft Windows Authentication

For supported Windows operating systems, OpenManage Essentials authentication is based on the operating system's user authentication system using Windows NT LAN Manager (NTLM) modules to authenticate. For the network, this underlying authentication system allows you to incorporate OpenManage Essentials security in an overall security scheme.

Assigning User Privileges

You do not have to assign user privileges to OpenManage Essentials users before installing OpenManage Essentials. The following procedures provide step-by-step instructions for creating OpenManage Essentials users and assigning user privileges for Windows operating system.

NOTE: Log in with administrator privileges to perform these procedures.

NOTE: For questions about creating users and assigning user group privileges or for more detailed instructions, see the operating system documentation.

1 From Windows desktop, click **Start→ All Programs→ Administrative Tools→ Computer Management**.

2 In the console tree, expand **Local Users and Groups**, and click **Groups**.

3 Double-click either the **OmeAdministrators** or **OmeUsers** group to add the new user.

4 Click **Add** and type the user name that you are adding. Click **Check Names to validate** and then click **OK**.

New users can log on to OpenManage Essentials with the user privileges for their assigned group.

Using Custom SSL Certificates (Optional)

OpenManage Essentials default settings ensure that a secure communication is established within your environment. However, some users may prefer to utilize their own SSL certificate for encryption.

To create a new domain certificate:

1 Open Internet Information Services (IIS) Manager by clicking **Start→ All Programs→ Administrative Tools→ Internet Information Services (IIS) Manager**.

2 Expand the ***<server name>*** and click **Server Certificates→ Sites**.

3 Click **Create Domain Certificate** and enter the required information.

To use a custom SSL certificate, you must configure IIS Services on the system where OpenManage Essentials is installed:

1 Open Internet Information Services (IIS) Manager by clicking **Start**→ **All Programs**→ **Administrative Tools**→ **Internet Information Services (IIS) Manager**.

2 Expand the ***<server name>*** → **Sites**.

3 Right-click on **DellSystemEssentials** and select **Edit Bindings**.

4 In **Site Bindings**, select the **https binding** and click **Edit**.

5 In **Edit Site Binding**, from the **SSL certificate** drop-down list select your custom SSL certificate and click **OK**.

Supported Protocols and Ports in OpenManage Essentials

Management Stations

Table 1. Supported Protocols and Ports on Management Stations

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
25	SMTP	TCP	None	In/Out	Optional e-mail alert action	No
162	SNMP	UDP	None	In	Event reception through SNMP	No
1433	Proprietary	TCP	None	In/Out	Optional remote SQL server access	Yes
2607	HTTPS	TCP	128-bit SSL	In/Out	Web GUI	Yes

Managed Nodes

Table 2. Supported Protocols and Ports on Managed Nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
22	SSH	TCP	128 bit	In/Out	Contextual application launch—SSH client Remote software updates to Server Administrator— for systems supporting Linux operating systems Performance monitoring in Linux systems	Yes
80	HTTP	TCP	None	In/Out	Contextual application launch— PowerConnect console	No
135	RPC	TCP/ UDP	None	In/Out	Remote software update transfer to Server Administrator—for systems supporting Windows operating systems Remote Command Line— for systems supporting Windows operating systems	No
161	SNMP	UDP	None	In/Out	SNMP query management	No
623	RMCP	UDP	None	In/Out	IPMI access through LAN	No
1433	Proprietary	TCP	None	In/Out	Optional remote SQL server access	Yes
443	Proprietary / WSMAN	TCP	None	In/Out	EMC storage discovery and inventory.	No
3389	RDP	TCP	128-bit SSL	In/Out	Contextual application launch—Remote desktop to Windows terminal services	Yes

Table 2. Supported Protocols and Ports on Managed Nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
6389	Proprietary	TCP	None	In/out	EMC storage discovery and inventory. Enables communication between a host system (through NaviCLI/NaviSec CLI or Navisphere host agent) and a Navisphere Array Agent on a Storage system	No

19

Troubleshooting

OpenManage Essentials Troubleshooting Tool

The OpenManage Essentials troubleshooting tool is a standalone tool that installs along with OpenManage Essentials. You can use the troubleshooting tool for a wide array of protocol related problems that are often at the root of discovery and alert issues.

This tool provides the following protocol-specific diagnostics to identify the problem with the remote node:

- Database—Fetches all the user defined databases present on the remote box.
- Dell|EMC—Verifies the connection to the Dell|EMC storage devices.
- ICMP—Verifies whether you can ping the remote device from the local box.
- IPMI—Verifies the IPMI protocol to connect to BMC/iDRAC.
- Name Resolution—Verifies whether you can get the resolved name from the local box.
- OpenManage Server Administrator Remote Enablement—This test helps you to verify that Dell OpenManage Server Administrator's remote enablement feature is working on the managed node (Dell OpenManage Server administrator installed with the remote enablement component). This tool behaves like a Server Administrator Distributed Web server (DWS) and connects to Server Administrator managed node instrumentation agent using the WSMAN protocol.

  To connect successfully, the Managed Node must have OpenManage Server Administrator installed with the Remote Enablement feature working.
- Port—Verifies whether managed node is listening to the specified port. You can specify 1-65,535 port numbers.
- PowerVault Modular Disk Arrays—Verifies that PowerVault modular disk storage array protocol is used to connect to PowerVault Storage devices.
- Services—Uses SNMP protocol to fetch the running services on the managed node.

- SNMP—Verifies SNMP connection to the remote node, using the required SNMP community string, retries, and time out. First it tries to connect to MIB-II agent and then various other agents to find out the type of device. Troubleshooting Tool also gathers other agent specific information from that device.
- SSH—Verifies that the SSH protocol is used to connect to managed node.
- WMI—Verifies WMI/CIM connection to the remote node. Default retries and time out values are used internally.
- WSMAN—Attempts to connect to WSMAN client on the remote node. Use this test to verify connectivity problems with iDRAC, ESX, and other devices, which support WSMAN specification. This test will connect to such devices and will also list the exposed WSMAN profiles enabled on the remote device.

Troubleshooting Procedures

Troubleshooting Inventory

Inventoried Linux servers are listed under Non-Inventoried systems, numerous retries does not resolve this.

To resolve this issue for the Red Hat Enterprise Linux 5.5, SUSE Linux Enterprise Server version 10 and version 11 installed servers:

1. Mount the *Dell Systems Management Tools and Documentation DVD* (version 6.5 or later) on the Linux server.
2. Install **srvadmin-cm** rpm.
3. Restart **OpenManage Server Administrator 6.5**.
4. Make sure the OpenManage Server Administrator inventory collector is working from the location **/opt/dell/srvadmin/sbin/invcol**, run **./invcol -outc=/home/inv.xml**.
5. Perform server inventory.

Troubleshooting Device Discovery

If a device discovery is not successful, perform the following steps to troubleshoot and fix the problem:

1. If the device assigned for discovery is a Dell PowerEdge system, ensure that Dell OpenManage Server Administrator is installed on it.
2. To discover Windows devices successfully, configure the SNMP services appropriately. For detailed information on configuring SNMP services on Windows, see Configuring SNMP Services on Windows.
3. To discover Linux devices successfully, configure the SNMP services appropriately. For detailed information on configuring SNMP services on Linux, see Configuring SNMP Services on Linux.
4. After configuring the SNMP services, verify whether the SNMP services are responding correctly.
5. If the device assigned for discovery is Microsoft Windows and you want to use WMI, ensure that the user name and password used in the WMI credentials has the local administrator permissions on the machine that you want to discover. You can use the Microsoft **wbemtest** utility to ensure that WMI connectivity to the Windows Server is correct.
6. If the device assigned for discovery is a non-server network device, such as a printer, Dell PowerConnect switch, and so on, ensure that SNMP is enabled on the device. You can do this by accessing the Web interface for a device.

Configuring SNMP Services on Windows

1. Open a command run prompt and type **services.msc** to open the Services MMC.
2. Right-click **SNMP Service** and select **Properties**. If you cannot locate SNMP Service, you need to install it using **Add/Remove Windows Components**.
3. Click **Security** and ensure that **Accept SNMP packets from any host** is selected.
4. Under **Accepted Community Names**, ensure that **public** (or a community string of your choice) is set. If not set by default, click **Add**, and type a community string in **Community Name**. Also select community rights as **READ ONLY** or **READ WRITE**.

5. Click **Traps** and ensure that the community string field has a valid name.
6. In **Trap destination**, click **Add** and enter the Open Manage Essential Console IP address.
7. Start the service.

Configuring SNMP Services on 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, enter the Open Manage Essentials Console IP address in the following format:

   ```
   trapsink <OPEN MANAGE ESSENTIALS CONSOLE IP>
   <community string>
   ```

   For example, trapsink 10.94.174.190 public
6. Start the SNMP services (service snmpd restart).

Troubleshooting Receiving SNMP Traps

If you encounter a problem receiving SNMP traps, perform the following steps to troubleshoot and fix the problem:

1. Check for network connectivity between the two systems. You can do this by pinging one system from another using the ping <IP address> command.
2. Check the SNMP configuration on the managed node. Ensure that you have specified the OpenManage Essential console IP address and the community string name in the SNMP services of the managed node.

   For information on setting SNMP on a Windows system, see Configuring SNMP Services on Windows.

   For information on setting SNMP on a Linux system, see Configuring SNMP Services on Linux.

3. Ensure that the SNMP Trap service services are running in the Open Manage Essentials system.
4. Check firewall settings to allow UDP 161, 162 ports.

Troubleshooting Discovery of Windows Server 2008-Based Servers

You also have to allow the server discovery. By default, the option is disabled in Windows Server 2008.

1. Click **Start**→ **Control Panel**→ **Network and Internet**→ **Network and Sharing Center**→ **Advanced Sharing Setting**.
2. Choose the drop-down arrow for the applicable network profile (Home or Work / Public)→ Under **Network Discovery** section select the **Turn on network discovery**.

Troubleshooting SNMP Traps for ESX or ESXi Versions 3.5, 4.x, or 5.0

Details

To generate virtual machine and environmental traps from ESX or ESXi 3.5 or 4.*x* hosts, configure and enable the embedded SNMP agent. You cannot use the Net-SNMP-based agent to generate these traps, although it can receive GET transactions and generate other types of traps.

This represents a change in behavior from ESX 3.0.x, in which the configuration file for the Net-SNMP-based agent controlled the generation of virtual machine traps.

Solution

Use the `vicfg-snmp` command from the Remote CLI or vSphere CLI to enable the SNMP agent and configure trap destinations. Each time you specify a target with the vicfg-snmp command, the settings you specify overwrite all previously specified settings. To specify multiple targets, specify them in a single command, separated by commas.

To enable and configure SNMP traps:

NOTE: Ensure that the SNMP protocol is open in the ESX firewall. For ESX 3.5, use the Remote CLI. For ESX 4.x, use the vSphere CLI. The commands for both are same.

1 Run the vicfg-snmp.pl command to see if SNMP is enabled:

```
vicfg-snmp --show
```

NOTE: By default, vicfg-snmp.pl is located in the C:\Program Files\VMware\VMware vSphere CLI\bin directory after the VMware vSphere CLI installation. Run the vicfg-snmp --help command for a full list of options.

2 Specify the communities and trap targets using the following command:

```
vicfg-snmp.pl --server <hostname> --username
<username> --password <password> -t <target
hostname>@<port>/<community>
```

NOTE: In ESX 4.*x*, you may need to use the -c <community> flag.

For example, to send SNMP traps from the host host.example.com, to port 162 on target.example.com, using the public community, use the following command:

```
vicfg-snmp.pl --server host.example.com --username
root --password password -t
target.example.com@162/public
```

NOTE: To prevent clear text display of the user password, remove the --password portion. You are then prompted to enter the password, and the entry is hidden.

3 To enable the SNMP service, run the following command:

```
vicfg-snmp.pl --server <hostname> --username
<username> --password <password> --enable
```

To verify SNMP settings, run the following command:

```
vicfg-snmp.pl --server <hostname> --username
<username> --password <password> --show
```

4 Optionally, send a test trap to verify that the agent is configured correctly using the following command:

```
vicfg-snmp.pl --server <hostname> --username
<username> --password <password> --test
```

The test trap generated is a warmStart trap.

For additional information, see SNMP trap information incorrectly displays in third party monitoring software (1007483).

The VMware Infrastructure Remote CLI can be downloaded from the VMware Download Center.

20

Frequently Asked Questions

Installation

Question: How do I install OpenManage Essentials using a remote SQL database named instance?

Answer: To connect remotely, the SQL Server with named instances requires a running **SQL Server Browser** service.

Question: Will OpenManage Essentials support SQL Server evaluation edition?

Answer: No, SQL Server **evaluation** edition is not supported.

Tasks

Question: What troubleshooting can I do if a software update task or remote task fails to create or run?

Answer: Ensure that the DSM Essentials Task Manager service is running in Windows services.

Question: How do I use command line features while deploying OpenManage Server Administrator?

Answer: Unattended installation provides the following features:

- A set of optional command line settings to customize an unattended installation.
- Customization parameters to designate specific software features for installation.

Optional Command Line Settings

Table 1 shows the optional settings available for the **msiexec.exe** MSI installer. Type the optional settings on the command line after **msiexec.exe** with a space between each setting.

NOTE: See **support.microsoft.com** for full details about all the command line switches for the Windows Installer Tool.

Table 1. Command Line Settings for MSI Installer

Setting	Result
`/i <Package|Product Code>`	This command installs or configures a product. **`/i SysMgmt.msi`** – Installs the Server Administrator software.
`/i SysMgmt.msi /qn`	This command carries out a fresh installation of version 6.1.
`/x <Package|Product Code>`	This command uninstalls a product. **`/x SysMgmt.msi`** – Uninstalls the Server Administrator software.
`/q[n|b|r|f]`	This command sets the user interface (UI) level. **`/q`** or **`/qn`** – no UI. This option is used for silent and unattended installation. **`/qb`** – basic UI. This option is used for unattended but not silent installation. **`/qr`** – reduced UI. This option is used for unattended installation while displaying a modal dialog box showing install progress. **`/qf`** – full UI. This option is used for standard attended installation.

Table 1. Command Line Settings for MSI Installer *(continued)*

Setting	Result
`/f[p|o|e|d|c|a|u|m|s|v]<Package|ProductCode>`	This command repairs a product. **`/fp`** – This option reinstalls a product only if a file is missing. **`/fo`** – This option reinstalls a product if a file is missing or if an older version of a file is installed. **`/fe`** – This option reinstalls a product if a file is missing or an equal or older version of a file is installed. **`/fd`** – This option reinstalls a product if a file is missing or a different version of a file is installed. **`/fc`** – This option reinstalls a product if a file is missing or the stored checksum value does not match the calculated value. **`/fa`** – This option forces all files to reinstall. **`/fu`** – This option rewrites all required user-specific registry entries. **`/fm`** – This option rewrites all required system-specific registry entries. **`/fs`** – This option overwrites all existing shortcuts. **`/fv`** – This option runs from the source and re-caches the local package. Do not use the **`/fv`** reinstall option for the first installation of an application or feature.
INSTALLDIR=<path>	This command installs a product to a specific location. If you specify an install directory with this switch, it must be created manually prior to executing the CLI install commands or they fail with no error or message. **`/i SysMgmt.msi INSTALLDIR=c:\OpenManage /qn`** – installs a product to a specific location using **`c:\OpenManage`** as the install location.

For example, running `msiexec.exe /i SysMgmt.msi /qn` installs Server Administrator features on each remote system based on the system's hardware configuration. This installation is done silently and unattended.

Customization Parameters

NOTE: Type the REINSTALL, and REMOVE CLI parameters in upper case, as they are case-sensitive.

REINSTALL and **REMOVE** customization CLI parameters provide a way to customize the exact software features to install, reinstall, or uninstall when running silently or unattended. With the customization parameters, you can selectively install, reinstall, or uninstall software features for different systems using the same unattended installation package. For example, you can choose to install Server Administrator, but not Remote Access Controller service on a specific group of servers, and choose to install Server Administrator, but not Storage Management Service, on another group of servers. You can also choose to uninstall one or multiple features on a specific group of servers.

NOTE: The software feature IDs mentioned in Table 2 are case-sensitive.

Table 2. Software Feature IDs

Feature ID	Description
ALL	All features
BRCM	Broadcom NIC Agent
INTEL	Intel NIC Agent
IWS	Dell OpenManage Server Administrator Web Server
OMSM	Server Administrator Storage Management Service
RmtMgmt	Remote Enablement
RAC4	Remote Access Controller (DRAC 4)
RAC5	Remote Access Controller (DRAC 5)
iDRAC	Integrated Dell Remote Access Controller
SA	Server Administrator

NOTE: Only iDRAC6 is supported on *xx*1*x* systems.

You can include the **REINSTALL** customization parameter on the command line and assign the feature ID (or IDs) of the software feature that you would like to reinstall. An example is:

```
msiexec.exe /i SysMgmt.msi REINSTALL=BRCM /qb.
```

This command runs the installation for Dell OpenManage Systems Management and reinstall only the Broadcom agent, in an unattended but not silent mode.

You can include the **REMOVE** customization parameter on the command line and assign the feature ID (or IDs) of the software feature that you would like to uninstall. For example:

```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb.
```

This command runs the installation for Dell OpenManage Systems Management and uninstalls only the Broadcom agent, in an unattended but not silent mode.

You can also choose to install, reinstall, and uninstall features with one execution of the **msiexec.exe** program. For example:

```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb
```

This command runs the installation for managed system software, and uninstalls the Broadcom agent. This execution is in an unattended but not silent mode.

NOTE: A Globally Unique Identifier (GUID) is 128 bits long, and the algorithm used to generate a GUID guarantees each GUID to be unique. The product GUID uniquely identifies the application. In this case, the product GUID for Server Administrator is {54C04D53-C3C3-46EA-A75F-7AFF4BEB727C}.

MSI Return Code

An application event log entry is recorded in the **SysMgmt.log** file. Table 3 shows some of the error codes returned by the **msiexec.exe** Windows Installer Engine.

Table 3. Windows Installer Return Codes

Error Code	Value	Description
ERROR_SUCCESS	0	The action is completed successfully.
ERROR_INVALID_PARAMETER	87	One of the parameters was invalid.

Table 3. Windows Installer Return Codes *(continued)*

Error Code	Value	Description
`ERROR_INSTALL_USEREXIT`	`1602`	The user canceled the installation.
`ERROR_SUCCESS_REBOOT_REQUIRED`	`3010`	A restart is required to complete the installation. This message is indicative of a successful installation.

NOTE: See **support.microsoft.com** for full details on all the error codes returned by the **msiexec.exe** and **InstMsi.exe** Windows installer functions.

E-mail Alert Action

Question: Why am I not receiving e-mails after setting up e-mail alert action?

Answer: If you have an Antivirus Client installed on the system, then configure it to allow e-mails.

Discovery

Question: What troubleshooting can I do if a discovery task fails to create or run?

Answer: Ensure that the DSM Essentials Task Manager service is running in Windows services.

Question: Why are my ESX virtual machines not correlated with their ESX host server?

Answer: You must discover the ESXi host server using SNMP and WSMan or the guest virtual machine will not correlate correctly when discovered using SNMP.

Question: Why are devices discovered with WMI getting classified as Unknown?

Answer: WMI discovery classifies a device as unknown when the credentials for a user account in the Administrators group (not Administrator) is supplied for the discovery range in some cases.

If you are seeing this issue, read the KB article at **support.microsoft.com/?scid=kb;en-us;951016** and apply the registry work as described. This resolution applies to managed nodes with Windows Server 2008 R2.

Question: What are SNMP authentication traps?

Answer: An authentication trap is sent when an SNMP agent is hit with an enquiry that contains a community name it does not recognize. The community names are case-sensitive.

The traps are useful to find if someone is probing a system, although its better nowadays to just sniff packets and find out the community name.

If you use multiple community names on the network, and some management might overlap, users may want to turn these off as they become false positives (annoyances).

For more information, see **technet.microsoft.com/en-us/library/cc959663.aspx**.

When an SNMP agent receives a request that does not contain a valid community name or the host that is sending the message is not on the list of acceptable hosts, the agent can send an authentication trap message to one or more trap destinations (management systems). The trap message indicates that the SNMP request failed authentication. This is a default setting.

Question: Why does OpenManage Essentials not support entering host names with underscore in the discovery wizard?

Answer: Per RFC 952, underscores are not valid in DNS names. A *name* (net, host, gateway, or domain name) is a text string up to 24 characters drawn from the alphabet (A-Z), digits (0-9), minus sign (-), and period (.). Periods are only allowed when they serve to delimit components of domain style names.

For more information see, **ietf.org/rfc/rfc952.txt and zytrax.com/books/dns/apa/names.html**

Question: What is On-demand?

Answer: On-demand is an operation where a managed system is checked for status/health by OpenManage Essentials when an SNMP trap is received. There are no settings to be changed to enable the on-demand feature. However, the IP address of the management system must be available in the trap destination of SNMP service. An SNMP trap is received from the managed system when there is an issue or failure of a server component. These traps can be viewed under the alert logs.

Inventory

Question: What troubleshooting can I do if an inventory task fails to create or run?

Answer: Ensure that DSM Essentials Task Manager service is running in Windows services.

System Update

Question: How do I load a Dell catalog for software update? or What do I do when I get errors when trying to run software update tasks?

Answer:

1. Download the catalog to the OpenManage Essentials system directly or use an System Update Utility DVD in the local system drive.
2. Browse for **catalog.xml** file on the local system or DVD (not on a file share, it is possible to use a file share, but for troubleshooting, do not use file share.)

   Load catalog and verify that it shows as loaded in OpenManage Essentials. You can also try using the FTP download to get the latest catalog for troubleshooting purposes if you cannot load other catalogs.
3. Now, create software update tasks. If tasks fail, more information is found in the task details.
4. Try setting all internet explorer security settings to LOW if tasks do not run.

Question: What order are packages installed on a system?

Answer: Packages are applied in the following order:

1. Driver
2. Firmware
3. Firmware ES
4. BIOS

5 Application

Question: When performing a catalog import task, what do I do when I see this error - Attempted to perform an unauthorized operation?

Answer: Modify the permissions of the folder on the network share to allow the close user access.

Question: How do I configure Internet Explorer with Enhanced Security Configuration to ensure that OpenManage Essentials can utilize all features that use resources from Dell online?

Answer: To ensure that these features work in the Dell Open Manage Essentials console on an environment with Internet Explorer Enhanced Security Configuration enabled. The user needs to add ***.dell.com** to the **Trusted sites** zone.

Import Catalog and *System Update* require internet access when the user selects Dell Online as the source.

The warranty report also uses Dell online resources to retrieve information and also will not return data without it.

Question: What if IPMI is disabled after installing BMC Utility?

Answer: Try restarting DSM Essentials Network Monitor Service, DSM Essentials Task Manager service and restart IIS.

Question: What is Omremote?

Answer: Omremote enables you to execute remote Server Administrator command line tasks (inband) and also helps you to deploy Server Administrator on remote Dell servers. Omremote is an executable file that is located at C:\Program Files\Dell\SystMgt\Essentials\bin folder. It uses WMI connection for the Windows-based devices and SSH for the Linux-based devices. Ensure that the required ports are opened. Omremote commands require a Server Administrator supported operating system with Server administrator installed. To install/update Server administrator on the remote system, you must use an operating system preinstall package.

21

Preferences - Reference

In the Preferences page, you can configure the OpenManage Essentials console. Set the SMTP and proxy server information, adjust session timeout, database maintenance schedules, restart services, and enable or disable the ActiveX features.

NOTE: After modifying the console settings, click **Apply** to save the changes. Navigating to another portion of the console without clicking **Apply** resets the settings to the previously saved preferences.

SMTP Server Name or IP Address	The SMTP server host name or IP address used for sending e-mail alerts.
Console Session Timeout	Amount of user-inactive time that passes before the console automatically logs the user out.
Database Maintenance Execution Schedule	The date and time when the database maintenance activity will begin. The console is less responsive during the maintenance.
Restart Network Monitor and Task Manager Services	Restarts the Windows Services associated with OpenManage Essentials.
Security Settings (ActiveX)	
Allow Remote Desktop Launch	Installs and runs an ActiveX component on the client machine to launch remote desktop sessions.
Allow Troubleshooting Tool Launch	Installs and runs an ActiveX component on the client machine to launch the Dell Troubleshooting Tool.
Allow OpenManage Power Center Installation Verification	Installs and runs an ActiveX component on the client machine to verify and launch OpenManage Power Center.
Proxy Settings (used for System Update and Warranty)	
User Proxy Settings	Enable the use of proxy settings for internet access for System Update and Warranty.
Domain \ User name	The domain and user name of the proxy user.

Password	User's proxy password.
Proxy Server Address or Name	The IP address or server name of the proxy server. Check the browser's proxy LAN settings or ask your network administrator if unsure.
Proxy Port Number	The port number to access the proxy server. Check the browser's proxy LAN settings or ask your network administrator if unsure.
Test Connection	Click to test connection to the internet with the proxy credentials.

22

Tools- Reference

From tools you can:

- View User Interface Logs
- View Application Logs
- Export Discovery Logs to File System—Export the logs that were generated while discovering devices.
- Launch OpenManage Power Center—If installed, will launch the OpenManage Power Center.
- Launch Troubleshooting Tool—If installed, will launch the troubleshooting tool application which is used to run tests and configure devices.

User Interface Logs

Enabled	Enable or disable logging of User Interface. Disable to increase performance.
Log Asynchronous Calls	Enable or disable logging for threading and asynchronous update method calls. Turn on both **Log Asynchronous Calls** and **Informational** to view update calls.
Informational	Enable or disable logging of behaviors that are marked with a severity of **General Information**.
Warning	Enable or disable logging of behaviors that are marked with a severity of **Warning**.
Critical	Enable or disable logging of behaviors that are marked with a severity of **Critical**.
Clear	Clear the user interface log grid.
Export	Export the user interface log to file (.CSV, .HTML, .TXT, and .XML supported).
Severity	The severity of the recorded deviation in user interface behavior.

Start Time	The time at which this behavior occurred.
Source	The source of the behavior.
Description	More information on the behavior.

Application Logs

Severity	The severity of the recorded deviation in application's behavior.
Time	The time at which this behavior occurred.
Message	Information on the behavior.

23

Tutorials

You can refer the tutorials for the setup options you need to complete when configuring OpenManage Essentials for the first time.

In Tutorials click **First Time Setup** to view the configuration information for the following:

- SNMP Configuration
- SNMP - Open Services Console
- SNMP - Open SNMP Properties
- SNMP Security Settings
- SNMP Trap Settings
- Install OpenManage Server Administrator
- Windows Server 2008 Configuration
- Discover Devices

You can view tutorials for the following:

- Linux configuration for SNMP and OpenManage Server Administrator
- SNMP configuration using group policies
- Configuring ESX 4.*x* for discovery and inventory
- Configuring ESXi 4.*x* and 5.0 for discovery and inventory

A

Appendix—Right-Click Actions

The following tables lists all the right-click actions that are available in OpenManage Essentials.

NOTE: The right-click options displayed in OpenManage Essentials are dependent on your access privilege. You must have administrator access to see all the options.

Devices

IP Address or iDRAC name	Right-click to view the iDRAC console.
Details	Select to view device details.
Alerts	Select to view the alerts generated for this device.
Application Launch	Select to launch an application.
Troubleshoot	If the Troubleshooting Tool is installed, then select this option to launch the Troubleshooting Tool. **NOTE:** The Troubleshooting Tool is disabled by default. To enable the Troubleshooting Tool, see Preferences - Reference.
Refresh Inventory	Select to run inventory on the device.
Refresh Status	Select to run a status check on the device.
Add to New Group	Select to add the device to a group.
Exclude Range	Select to remove the device from the discovery and inventory range.
Remove	Select to remove the device information.
Export	Select to export the device information.

Device Search

Details	Displays the device summary information. For example, NIC Information.
Alerts	Displays the alerts generated for this device.
Show Associated IP/MAC	Displays the IP address, MAC address, NIC, and manufacturer's information for the selected device.
Show Associated Agents	Displays the agents present on the selected device. The agent's name, version, and manufacturer related information is listed.
Export	Select to export the device information.

Discovery Range Summary

Managing Include Ranges

Right-click the IP address to view the following options:

Edit	Select to edit discovery range configuration.
Rename	Select to rename the range.
Delete	Select to disable a range.
Enable	Select to enable a disabled range. This options toggles.
Perform Discovery Now	Select to do the discovery.
Perform Discovery and Inventory Now	Select to do the discovery and inventory.
Perform Status Polling Now	Select to start the status polling task for the discovered server or device.
Perform Inventory Now	Select to perform the inventory.

Managing Exclude Ranges

Right-click **Exclude Ranges** and select **Add Exclude Range** to add a range that you want to exclude from discovery and inventory.

View Filters

Edit	Select to edit the alert action or alert filter.
View Summary	Select to view all the systems that are critical.
Rename	Select to rename action or alert filter.
Clone	Select to create a copy of an action or alert filter.
Delete	Select the alert to delete the alerts.

Alerts

Details	Select to view the details of alerts.
Acknowledge	Select to set or clear alerts.
Delete	Select to delete alerts.
Enable or Disable	Select to enable or disable an alert action.
Ignore	Select to ignore alert filter action on the selected devices.
Export	Select to export alert information in CSV or HTML formats.

Remote Tasks

Edit	Select to edit the task.
Delete	Select to delete the task.
Run	Select to run the task immediately.
View	Select to view the task.
Activate Task Schedule	Select to activate the task schedule.
Clone	Select to create a copy of a task.

Index