Dell OpenManage Server Administrator Version 6.4

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 either potential damage to hardware or loss of data and tells you how to avoid the problem.

Information in this publication is subject to change without notice.
© 2010 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, PowerEdge™, PowerVault™, and OpenManage™ are trademarks of Dell Inc. Microsoft®, Windows®, Internet Explorer®, Active Directory®, Windows Server®, and Windows NT® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. EMC® is a registered trademark of EMC Corporation. Java® is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. and other countries. Novell® and SUSE® are registered trademarks of Novell, Inc. in the United States and other countries. Red Hat® and Red Hat Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and other countries. VMware® is a registered trademark and ESX Server™ is a trademark of VMware Inc in the United States and/or other jurisdictions. Mozilla® and Firefox® are registered trademarks of the Mozilla Foundation. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries.

Server Administrator includes software developed by the Apache Software Foundation (**www.apache.org**). Server Administrator utilizes the OverLIB JavaScript library. This library can be obtained from **www.bosrup.com**.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

December 2010

Contents

1 Introduction 9

Overview **9**

Installation 9

Updating Individual System Components 10

Storage Management Service 10

Instrumentation Service 11

Remote Access Controller 11

Logs 11

What's New in Version 6.4 . . . . . **11**

Systems Management Standards Availability **13**

Availability on Supported Operating Systems 13

Server Administrator Home Page **14**

Other Documents You May Need **15**

Obtaining Technical Assistance **17**

2 Setup and Administration 19

Security Management **19**

Role-Based Access Control 19

Authentication 21

Microsoft Windows Authentication 21

Red Hat Enterprise Linux and SUSE Linux Enterprise Server Authentication 21

VMware ESX Server 4.X 21
VMware ESXi Server 4.X 22
Encryption 22

Assigning User Privileges **22**

Creating Server Administrator Users for Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems 23
Editing Server Administrator User Privileges on Linux Operating Systems 25
Creating Server Administrator Users for VMware ESX 4.X and ESXi 4.X 26

Disabling Guest and Anonymous Accounts in Supported Windows Operating Systems **27**

Configuring the SNMP Agent **27**

Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems 29
Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux . . . 32
Configuring the SNMP Agent on Systems Running Supported SUSE Linux Enterprise Server 36
Configuring the SNMP Agent on Systems Running Supported VMware ESX 4.X Operating Systems to Proxy VMware MIBs 39
Configuring the SNMP Agent on Systems Running Supported VMware ESXi 4.X Operating Systems 41

Firewall Configuration on Systems Running Supported Red Hat Enterprise Linux Operating Systems and SUSE Linux Enterprise Server **43**

3 Using Server Administrator 45

Starting Your Server Administrator Session **45**

Logging In and Out **45**

Server Administrator Local System Login 45

Server Administrator Managed System Login 46

Central Web Server Login 47

Single Sign-On 48

Configuring Security Settings on Systems Running a Supported Microsoft Windows Operating System 49

The Server Administrator Home Page **51**

Server Administrator User Interface Differences Across Modular and Non-Modular Systems 54

Global Navigation Bar 55

System Tree 55

Action Window 55

Using the Online Help **58**

Using the Preferences Home Page **58**

Managed System Preferences 59

Server Administrator Web Server Preferences 60

Server Administrator Web Server Action Tabs **64**

Managing Server Administrator **64**

Starting Server Administrator 65

Stopping Server Administrator 65

Restarting Server Administrator 66

Using the Server Administrator Command Line Interface **66**

4 Server Administrator Services 69

Overview **69**

Managing Your System **70**

Managing System/Server Module Tree Objects **70**

Server Administrator Home Page System Tree Objects **71**

Unsupported Features in OpenManage Server Administrator 71

Modular Enclosure 72

System/Server Module 73

Managing Preferences: Home Page Configuration Options **91**

General Settings 91

Server Administrator 92

5 Working With Remote Access Controller 93

Overview **93**

Viewing Basic Information **95**

Configuring the Remote Access Device to use a LAN Connection **96**

Configuring the Remote Access Device to use a Serial Port Connection **98**

Configuring the Remote Access Device to use a Serial Over LAN Connection **100**

Additional Configuration for iDRAC **100**

Configuring Remote Access Device Users **101**

Setting Platform Event Filter Alerts **102**
Setting Platform Event Alert Destinations 103

6 Server Administrator Logs 105

Overview **105**

Integrated Features **105**
Log Window Task Buttons 105

Server Administrator Logs **106**
Hardware Log 106
Alert Log 107
Command Log 108

7 Setting Alert Actions 109

Setting Alert Actions for Systems Running Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems . . . **109**

Setting Alert Actions in Microsoft Windows Server 2003 and Windows Server 2008 . . . . . **110**

Setting Alert Action Execute Application in Windows Server 2008 . . . . . **111**

BMC/iDRAC Platform Events Filter Alert Messages **112**

Understanding Service Names **114**

A Troubleshooting 115

Connection Service Failure **115**

Login Failure Scenarios **115**

Fixing a Faulty Server Administrator Installation on Supported Windows Operating Systems **116**

OpenManage Server Administrator Services **117**

B Frequently Asked Questions 121

Index 125

1

Introduction

Overview

Dell OpenManage Server Administrator (OMSA) provides a comprehensive, one-to-one systems management solution in two ways: from an integrated, Web browser-based graphical user interface (GUI) and from a command line interface (CLI) through the operating system. Server Administrator is designed for system administrators to manage systems locally and remotely on a network. It allows system administrators to focus on managing their entire network by providing comprehensive one-to-one systems management.

In the context of Server Administrator, a system refers to a stand-alone system, a system with attached network storage units in a separate chassis, or a modular system consisting of one or more server modules in a modular enclosure.

Server Administrator provides information about:

- Systems that are operating properly and systems that have problems
- Systems that require remote recovery operations.

Server Administrator provides easy-to-use management and administration of local and remote systems through a comprehensive set of integrated management services. Server Administrator is the sole installation on the system being managed and is accessible both locally and remotely from the **Server Administrator** home page. Remotely monitored systems may be accessed by dial-in, LAN, or wireless connections. Server Administrator ensures the security of its management connections through role-based access control (RBAC), authentication, and secure socket layer (SSL) encryption.

Installation

You can install Server Administrator using the *Dell Systems Management Tools and Documentation* DVD (OpenManage DVD). The DVD provides a setup program to install, upgrade, and uninstall Server Administrator, managed

system and management station software components. Additionally, you can install Server Administrator on multiple systems through an unattended installation across a network.

The Dell OpenManage installer provides installation scripts and RPM packages to install and uninstall Dell OpenManage Server Administrator and other managed system software components on your managed system. For more information, see the *Dell OpenManage Server Administrator Installation Guide* and the *Dell OpenManage Management Station Software Installation Guide*. You can access these documents at **support.dell.com/manuals.**

NOTE: When you install the opensource packages from the OpenManage DVD, the corresponding license files are automatically copied to the system. When you remove these packages, the corresponding files are removed.

If you have a modular system, you must install Server Administrator on each server module installed in the chassis.

Updating Individual System Components

To update individual system components, use component-specific Dell Update Packages. Use the *Dell Server Updates* DVD to view the complete version report and to update an entire system. The Server Update Utility is a DVD-ROM–based application for identifying and applying updates to your system. The Server Update Utility can be downloaded from **support.dell.com**.

See the *Server Update Utility User's Guide* for more information about obtaining and using the Server Update Utility (SUU) to update your Dell Systems or to view the updates available for any systems listed in the Repository.

Storage Management Service

The Storage Management Service provides storage management information in an integrated graphical view.

For detailed information on the Storage Management Service, see the *Dell OpenManage Server Administrator Storage Management User's Guide* at **support.dell.com/manuals**.

Instrumentation Service

The Instrumentation Service provides rapid access to detailed fault and performance information gathered by industry-standard systems management agents and allows remote administration of monitored systems, including shutdown, startup, and security.

Remote Access Controller

The Remote Access Controller provides a complete remote system management solution for systems equipped with Dell Remote Access Controller (DRAC) or Baseboard Management Controller (BMC)/Integrated Dell Remote Access Controller (iDRAC) solution. The Remote Access Controller provides remote access to an inoperable system, allowing you to get the system up and running as quickly as possible. The Remote Access Controller also provides alert notification when a system is down and allows you to remotely restart a system. Additionally, the Remote Access Controller logs the probable cause of system crashes and saves the most recent crash screen.

Logs

Server Administrator displays logs of commands issued to or by the system, monitored hardware events, and system alerts. You can view logs on the home page, print or save them as reports, and send them by e-mail to a designated service contact.

What's New in Version 6.4

The release highlights of OpenManage Server Administrator 6.4:

- Dell OpenManage Server Administrator user interface redesign that improves the overall customer experience, which includes:
  - If there is an error condition, such as wrong username or password, in the login page, the error message is displayed for 30 seconds and then the login prompt is displayed. To get to the login prompt before 30 seconds, click **Try Again**.
  - The **Back to Server Administrator** button is renamed as **Home**.
  - The **OK** button is renamed as **Submit** button in the login page.
  - The **Email**, **Export**, **Refresh** buttons are now represented as icons.

  - The **Help** icon is available with the **Email**, **Export**, and **Refresh** icons in the top right corner of the page.
  - The custom buttons like **Save as**, **Clear Log**, **Restart**, and **Reset to Default** are grouped under the **Options** section.
  - The **User Rights** and **Host Name** buttons are now available on the top left corner of the page instead of the top right corner.
  - The **Manage Remote Node**, **About** and **Support** links are available at the bottom of the login page.
  - All the buttons such as **Print**, **Export** and so on are displayed in all the OMSA pages. Only the buttons applicable to a particular page are enabled while the rest are grayed out.
  - Tooltip feature for buttons and links in the data area is active.
  - In the **System Summary** and **Summary of Asset Information** page, the **Jump to** and **Back to top** links are not available. Instead, you can expand and collapse each section in the page.
  - The **Details** button in the **About** page no longer exists. All details are displayed in the same page.
- Express service code (ESC) attribute added.
- Added support for the following operating systems:
  - Microsoft Windows 2008 HPC Edition Server R2
  - Red Hat Enterprise Linux 6
  - VMware ESX 4.0 U2
  - VMware ESXi 4.0 U2
- Deprecated the following operating systems:
  - Red Hat Enterprise Linux 4.8
  - VMware ESX 4.0 U1
  - VMware ESXi 4.0 U1
- Skins preference feature is deprecated.
- Page level health status icon feature is deprecated.

For the supported operating systems list, see the *Dell Systems Software Support Matrix* located at **support.dell.com/manuals**.

See the Server Administrator context-sensitive online help for more information on features introduced in this release.

Systems Management Standards Availability

Dell OpenManage Server Administrator supports the following major systems management protocols:

- HyperText Transfer Protocol Secure (HTTPS)
- Common Information Model (CIM)
- Simple Network Management Protocol (SNMP)

If your system supports SNMP, you must install and enable the service on your operating system. If SNMP services are available on your operating system, the Server Administrator installation program installs the supporting agents for SNMP.

HTTPS is supported on all operating systems. Support for CIM and SNMP is operating system dependent and, in some cases, operating system-version dependent.

For information on SNMP security concerns, see the Dell OpenManage Server Administrator **readme** file (packaged with the Server Administrator application) or at **support.dell.com/manuals**. You must apply updates from your operating system's master SNMP agents to ensure that Dell's SNMP subagents are secure.

Availability on Supported Operating Systems

On supported Microsoft Windows operating systems, Server Administrator supports two systems management standards: CIM/WMI (Windows Management Instrumentation) and SNMP, while on supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, Server Administrator supports the SNMP systems management standard.

Server Administrator adds considerable security to these systems management standards. All attributes set operations (for example, changing the value of an asset tag) must be performed with Dell OpenManage IT Assistant while logged in with the required authority.

Table 1-1 shows the systems management standards that are available for each supported operating system.

Table 1-1. Systems Management Standards Availability

Operating System	SNMP	CIM
Windows Server 2008 family and Windows Server 2003 family	Available from the operating system installation media	Always installed
Red Hat Enterprise Linux	Available in the **net-snmp** package from the operating system installation media	Unavailable
SUSE Linux Enterprise Server	Available in the **net-snmp** package from the operating system installation media	Unavailable
VMware ESX	Available in the net-snmp package installed by the operating system	Available
VMware ESXi	SNMP trap support available **NOTE:** While ESXi supports SNMP traps, it does not support hardware inventory through SNMP.	Available
Citrix XenServer 5.6.	Available in the **net-snmp** package from the operating system installation media	Unavailable

Server Administrator Home Page

The **Server Administrator** home page provides easy-to-set up and easy-to-use Web browser-based system management tasks from the managed system or from a remote host through a LAN, dial-up service, or wireless network. When the Dell Systems Management Server Administrator Connection Service (DSM SA Connection Service) is installed and configured on the managed system, you can perform remote management functions from any system that has a supported Web browser and connection. Additionally, the **Server Administrator** home page provides extensive, context-sensitive online help.

Other Documents You May Need

In addition to this guide, you can access the following guides available at **support.dell.com/manuals**. On the **Manuals** page, click **Software → Systems Management**. Click on the appropriate product link on the right-side to access the documents.

- The *Dell Systems Software Support Matrix* provides information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage components that can be installed on these systems.
- The *Dell OpenManage Server Administrator Installation Guide* contains instructions to help you install Dell OpenManage Server Administrator.
- The *Dell OpenManage Management Station Software Installation Guide* contains instructions to help you install Dell OpenManage management station software that includes Baseboard Management Utility, DRAC Tools, and Active Directory Snap-In.
- The *Dell OpenManage Server Administrator SNMP Reference Guide* documents the Simple Network Management Protocol (SNMP) management information base (MIB). The SNMP MIB defines variables that extend the standard MIB to cover the capabilities of systems management agents.
- The *Dell OpenManage Server Administrator CIM Reference Guide* documents the Common Information Model (CIM) provider, an extension of the standard management object format (MOF) file. The CIM provider MOF documents supported classes of management objects.
- The *Dell OpenManage Server Administrator Messages Reference Guide* lists the messages that are displayed in your **Server Administrator** home page Alert log or on your operating system's event viewer. This guide explains the text, severity, and cause of each Instrumentation Service Alert message that Server Administrator issues.
- The *Dell OpenManage Server Administrator Command Line Interface User's Guide* documents the complete command line interface for Server Administrator, including an explanation of CLI commands to view system status, access logs, create reports, configure various component parameters, and set critical thresholds.
- The *Integrated Dell Remote Access Controller User's Guide* provides detailed information on configuring and using the iDRAC.

- The *Dell Chassis Management Controller User's Guide* provides detailed information on installing, configuring and using CMC.
- The *Dell Online Diagnostics User's Guide* provides complete information on installing and using Online Diagnostics on your system.
- The *Dell OpenManage Baseboard Management Controller Utilities User Guide* provides additional information about using Server Administrator to configure and manage your system's BMC.
- The *Dell OpenManage Server Administrator Storage Management User's Guide* is a comprehensive reference guide for configuring and managing local and remote storage attached to a system.
- The *Dell Remote Access Controller Racadm User's Guide* provides information about using the racadm command-line utility.
- The *Dell Remote Access Controller 5 User's Guide* provides complete information about installing and configuring a DRAC 5 controller and using DRAC 5 to remotely access an inoperable system.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.
- The *Dell OpenManage Server Update Utility User's Guide* provides information about obtaining and using the Server Update Utility (SUU) to update your Dell systems or to view the updates available for any systems listed in the Repository.
- The *Dell Management Console User's Guide* has information about installing, configuring, and using Dell Management Console. Dell Management Console is a Web-based systems management software that enables you to discover and inventory devices on your network. It also provides advanced functions, such as health and performance monitoring of networked devices and patch management capabilities for Dell systems.

- The *Dell Lifecycle Controller User Guide* provides information on setting up and using the Unified Server Configurator to perform systems and storage management tasks throughout your system's lifecycle. You can use the Unified Server Configurator to deploy an operating system, configure a Redundant Array of Independent Disks (RAID), and run diagnostics to validate the system and attached hardware. Remote Services capabilities enable automated system platform discovery by management consoles and enhance remote operating system deployment capabilities. These capabilities are exposed through the web services based hardware management interface provided by the Lifecycle Controller firmware.
- The *Glossary* for information on terms used in this document.

Obtaining Technical Assistance

If at any time you do not understand a procedure described in this guide or if your product does not perform as expected, help tools are available to assist you. For more information about these help tools, see "Getting Help" in your system's *Hardware Owner's Manual*.

Additionally, Dell Enterprise Training and Certification is available; see **dell.com/training** for more information. This service may not be offered in all locations.

2

Setup and Administration

Security Management

Dell OpenManage Server Administrator provides security through Role-Based Access Control (RBAC), authentication, and encryption for both the Web-based and command line interfaces.

Role-Based Access Control

RBAC manages security by determining the operations that can be executed 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.

User Privileges

Server Administrator grants different access rights based on the user's assigned group privileges. The four user levels are: User, Power User, Administrator, and Elevated Administrator.

- *Users* can view most information.
- *Power Users* can set warning threshold values and configure which alert actions are to be taken when a warning or failure event occurs.
- *Administrators* can configure and perform shutdown actions, configure Auto Recovery actions in case a system has a non-responsive operating system, and clear hardware, event, and command logs. *Administrators* can also configure the system to send e-mails.
- *Elevated Administrators* can view and manage information.

Server Administrator grants read-only access to users logged in with *User* privileges, read and write access to users logged in with *Power User* privileges, and read, write, and administrator access to users logged in with *Administrator* and *Elevated Administrator* privileges. See Table 2-1.

Table 2-1. User Privileges

User Privileges	Access Type	
	View	Manage
User	Yes	No
Power User	Yes	Yes
Administrator	Yes	Yes
Elevated Administrator (Linux only)	Yes	Yes

Privilege Levels to Access Server Administrator Services

Table 2-2 summarizes the users who have privileges to access and manage Server Administrator services.

Table 2-2. Server Administrator User Privilege Levels

Service	User Privilege Level Required	
	View	Manage
Instrumentation	U, P, A, EA	P, A, EA
Remote Access	U, P, A, EA	A, EA
Storage Management	U, P, A, EA	A, EA

Table 2-3 defines the user privilege level abbreviations used in Table 2-2.

Table 2-3. Legend for Server Administrator User Privilege Levels

U	User
P	Power User
A	Administrator
EA	Elevated Administrator

Authentication

The Server Administrator authentication scheme ensures that the correct access types are assigned to the correct user privileges. Additionally, when the command line interface (CLI) is invoked, the Server Administrator authentication scheme validates the context within which the current process is running. This authentication scheme ensures that all Server Administrator functions, whether accessed through the **Server Administrator** home page or CLI, are properly authenticated.

Microsoft Windows Authentication

For supported Microsoft Windows operating systems, Server Administrator authentication uses Integrated Windows Authentication (formerly called NTLM) to authenticate. This authentication system allows Server Administrator security to be incorporated in an overall security scheme for your network.

Red Hat Enterprise Linux and SUSE Linux Enterprise Server Authentication

For supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, Server Administrator uses various authentication methods based on the Pluggable Authentication Modules (PAM) library. Users can log in to Server Administrator either locally or remotely using different account management protocols, such as LDAP, NIS, Kerberos, and Winbind.

VMware ESX Server 4.X

VMware ESX Server uses the Pluggable Authentication Modules (PAM) structure for authentication when users access the ESX Server host. The PAM configuration for VMware services is located in /etc/pam.d/vmware-authd, which stores paths to authentication modules.

The default installation of ESX Server uses /etc/passwd authentication, just as Linux does, but you can configure ESX Server to use another distributed authentication mechanism.

NOTE: On systems running VMware ESX Server 4.1 operating system, to login to the Server Administrator, all users require Administrator privileges. For information on assigning roles, see the VMware documentation.

VMware ESXi Server 4.X

ESXi Server authenticates users accessing ESXi hosts using the vSphere/VI Client or Software Development Kit (SDK). The default installation of ESXi uses a local password database for authentication. ESXi authentication transactions with Server Administrator are also direct interactions with the **vmware-hostd** process. To make sure that authentication works efficiently for your site, perform basic tasks such as setting up users, groups, permissions, and roles, configuring user attributes, adding your own certificates, and determining whether you want to use SSL.

NOTE: On systems running VMware ESXi Server 4.1 operating system, to login to Server Administrator, all users require Administrator privileges. For information on assigning roles, see the VMware documentation.

Encryption

Server Administrator is accessed over a secure HTTPS connection using secure socket layer (SSL) technology to ensure and protect the identity of the system being managed. Java Secure Socket Extension (JSSE) is used by supported Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems to protect the user credentials and other sensitive data that is transmitted over the socket connection when a user accesses the **Server Administrator** home page.

Assigning User Privileges

To ensure critical system component security, assign user privileges to all Dell OpenManage software users before installing Dell OpenManage software. New users can log into Dell OpenManage software using their operating system user privileges.

CAUTION: To protect access to your critical system components, assign a password to every user account that can access Dell OpenManage software. Users without an assigned password cannot log into Dell OpenManage software on a system running Windows Server 2003 due to the operating system design.

CAUTION: Disable guest accounts for supported Windows operating systems to protect access to your critical system components. Consider renaming the accounts so that remote scripts cannot enable the accounts using the name.

NOTE: For instructions on assigning user privileges for each supported operating system, see your operating system documentation.

NOTE: Add new users to the operating system if you want to add users to OpenManage software. You do not have to create new users from within the OpenManage software.

Adding Users to a Domain on Windows Operating Systems

NOTE: You must have Microsoft Active Directory installed on your system to perform the following procedures. See "Using the Active Directory Login" on page 48 for more information about using Active Directory.

1. Navigate to **Control Panel**→ **Administrative Tools**→ **Active Directory Users and Computers**.
2. In the console tree, right-click **Users** or right-click the container in which you want to add the new user, and then point to **New**→ **User**.
3. Type the appropriate user name information in the dialog box, and then click **Next**.
4. Click **Next**, and then click **Finish**.
5. Double-click the icon representing the user that you just created.
6. Click the **Member of** tab.
7. Click **Add**.
8. Select the appropriate group and click **Add**.
9. Click **OK**, and then click **OK** again.

   New users can log into Dell OpenManage software with the user privileges for their assigned group and domain.

Creating Server Administrator Users for Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

Administrator access privileges are assigned to the user logged in as `root`. To create users with User and Power User privileges, perform the following steps.

NOTE: You must be logged in as `root` or an equivalent user to perform these procedures.

NOTE: You must have the **useradd** utility installed on your system to perform these procedures.

Creating Users

NOTE: For information about creating users and user groups, see your operating system documentation.

Creating Users With User Privileges

1. Run the following command from the command line:

   `useradd -d <home-directory> -g <group> <username>`

   where `<group>` is *not* `root`.

   NOTE: If `<group>` does not exist, create it by using the **groupadd** command.

2. Type `passwd <username>` and press <Enter>.
3. When prompted, enter a password for the new user.

NOTE: Assign a password to every user account that can access Server Administrator to protect access to your critical system components.

The new user can now log in to Server Administrator with User group privileges.

Creating Users With Power User Privileges

1. Run the following command from the command line:

   `useradd -d <home-directory> -g root <username>`

   NOTE: Set `root` as the primary group.

2. Type `passwd <username>` and press <Enter>.
3. When prompted, enter a password for the new user.

   NOTE: Assign a password to every user account that can access Server Administrator to protect access to your critical system components.

   The new user can now log in to Server Administrator with Power User group privileges.

Editing Server Administrator User Privileges on Linux Operating Systems

NOTE: Log in as `root` or an equivalent user to perform these procedures.

1. Open the **omarolemap** file located at **/opt/dell/srvadmin/etc/omarolemap**.
2. Add the following in the file:

   <User_Name>[Tab]*<Host_Name>*[Tab]*<Rights>*

   Table 2-4 lists the legends for adding the role definition to the *omarolemap* file

   Table 2-4. Legends for adding the role definition in OpenManage Server Administrator

<User_Name>	<Host_Name>	<Rights>
User Name	Host Name	Administrator
(+)Group Name	Domain	User
Wildcard (*)	Wildcard (*)	User
[Tab] = \t (tab character)		

   Table 2-5 lists the examples for adding the role definition to the *omarolemap* file.

   Table 2-5. Examples for adding the role definition in OpenManage Server Administrator

<User_Name>	<Host_Name>	<Rights>
Bob	Ahost	Poweruser
+root	Bhost	Administrator
+root	Chost	Administrator
Bob	*.aus.amer.com	Poweruser
Mike	192.168.2.3	Poweruser

3. Save and close the file.

Best Practices While Using the omarolemap File

The following lists the best practices to be considered while working with **omarolemap** file:

- Do not delete the following default entries in **omarolemap** file.
  - root * Administrator
  - +root * Poweruser
  - * * User
- Do not change the **omarolemap** file permissions or file format.
- Server Administrator uses the default operating system user privilege, if a user is degraded in the **omarolemap** file.
- Do not use the loop back address for *<Host_Name>*, for example: localhost or 127.0.0.1.
- After the connection services are restarted and the changes do not take effect for the **omarolemap** file, see the command log for the errors.
- When **omarolemap** file is copied from one machine to another machine, file permissions and the entries of the file needs to be rechecked.
- Prefix the *Group Name* with +.
- Server Administrator uses the default operating system user privileges, if there are duplicate entries of user names or user groups along with same *<Host_Name>*.
- You can also use *Space* as a delimiter for columns instead of `[Tab]`.

Creating Server Administrator Users for VMware ESX 4.X and ESXi 4.X

To add a user to the Users table:

1. Log in to the host using the vSphere Client.
2. Click the **Users & Groups** tab and click **Users**.
3. Right-click anywhere in the Users table and click **Add** to open the **Add New User** dialog box.
4. Enter a login, a user name, a numeric user ID (UID), and a password; specifying the user name and UID are optional. If you do not specify the UID, the vSphere Client assigns the next available UID.

5 To allow a user to access the ESX/ESXi host through a command shell, select **Grant shell access to this user**. Users that access the host only through the vSphere Client do not need shell access.

6 To add the user to a group, select the group name from the **Group** drop-down menu and click **Add**.

7 Click **OK**.

Disabling Guest and Anonymous Accounts in Supported Windows Operating Systems

NOTE: You must be logged in with Administrator privileges to perform this procedure.

1 Open the **Computer Management** window.

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

3 Double click **Guest** or **IUSR_system** name user account to see the Properties for those users, or right click the **Guest** or **IUSR_system** name user account and then choose **Properties**.

4 Select **Account is disabled** and click **OK**.

A red circle with an X appears over the user name. The account is disabled.

Configuring the SNMP Agent

Server Administrator supports the Simple Network Management Protocol (SNMP)—a systems management standard—on all supported operating systems. The SNMP support may or may not be installed depending on your operating system and how the operating system was installed. In most cases, SNMP is installed as part of your operating system installation. An installed supported systems management protocol standard, such as SNMP, is required before installing Server Administrator.

You can configure the SNMP agent to change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as the Dell OpenManage IT Assistant, perform the procedures described in the following sections.

NOTE: The default SNMP agent configuration usually includes a SNMP community name such as **public**. For security reasons, change the SNMP community names from their default values. For information about changing SNMP community names, see the appropriate section below.

NOTE: SNMP Set operations are disabled by default in Server Administrator version 5.2 or later. Server Administrator provides support to enable or disable SNMP Set operations in Server Administrator. You can use the **Server Administrator SNMP Configuration** page under **Preferences** or the Server Administrator command line interface (CLI) to enable or disable SNMP Set operations in Server Administrator. For more information about the Server Administrator CLI, see the *Dell OpenManage Server Administrator Command Line Interface User's Guide*.

NOTE: For IT Assistant to retrieve management information from a system running Server Administrator, the community name used by IT Assistant must match a community name on the system running Server Administrator. For IT Assistant to modify information or perform actions on a system running Server Administrator, the community name used by IT Assistant must match a community name that allows Set operations on the system running Server Administrator. For IT Assistant to receive traps (asynchronous event notifications) from a system running Server Administrator, the system running Server Administrator must be configured to send traps to the system running IT Assistant.

The following procedures provide step-by-step instructions for configuring the SNMP agent for each supported operating system:

- "Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems"
- "Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux"
- "Configuring the SNMP Agent on Systems Running Supported SUSE Linux Enterprise Server"
- "Configuring the SNMP Agent on Systems Running Supported VMware ESX 4.X Operating Systems to Proxy VMware MIBs"
- "Configuring the SNMP Agent on Systems Running Supported VMware ESXi 4.X Operating Systems"

Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems

Server Administrator uses the SNMP services provided by the Windows SNMP agent. You can configure the SNMP agent to change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as IT Assistant, perform the procedures described in the following sections.

NOTE: See your operating system documentation for additional details on SNMP configuration.

Enabling SNMP Access By Remote Hosts

Windows Server 2003, by default, does not accept SNMP packets from remote hosts. For systems running Windows Server 2003, you must configure the SNMP service to accept SNMP packets from remote hosts if you plan to manage the system by using SNMP management applications from remote hosts.

To enable a system running the Windows Server 2003 operating system to receive SNMP packets from a remote host, perform the following steps:

1. Open the **Computer Management** window.
2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon and click **Services**.
4. Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and then click **Properties**.

   The **SNMP Service Properties** window appears.
5. Click the **Security** tab.
6. Select **Accept SNMP packets from any host**, or add the remote host to the **Accept SNMP packets from these hosts** list.

Changing the SNMP Community Name

Configuring the SNMP community names determines which systems are able to manage your system through SNMP. The SNMP community name used by management applications must match an SNMP community name configured on the Server Administrator system so that the management applications can retrieve management information from Server Administrator.

1. Open the **Computer Management** window.
2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon and click **Services**.
4. Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and then click **Properties**.

   The **SNMP Service Properties** window appears.
5. Click the **Security** tab to add or edit a community name.
   a. To add a community name, click **Add** under the **Accepted Community Names** list.

      The **SNMP Service Configuration** window appears.

   b. Type the community name of a system that is able to manage your system (the default is public) in the **Community Name** text box and click **Add**.

      The **SNMP Service Properties** window appears.

   c. To change a community name, select a community name in the **Accepted Community Names** list and click **Edit**.

      The **SNMP Service Configuration** window appears.

   d. Make all necessary edits to the community name of the system that is able to manage your system in the **Community Name** text box, and then click **OK**.

      The **SNMP Service Properties** window appears.
6. Click **OK** to save the changes.

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the Server Administrator system to change Server Administrator attributes using IT Assistant.

1. Open the **Computer Management** window.
2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon, and then click **Services**.
4. Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and click **Properties.**

   The **SNMP Service Properties** window appears.
5. Click the **Security** tab to change the access rights for a community.
6. Select a community name in the **Accepted Community Names** list, and click **Edit**.

   The **SNMP Service Configuration** window appears.
7. Set the **Community Rights** to **READ WRITE** or **READ CREATE**, and click **OK**.

   The **SNMP Service Properties** window appears.
8. Click **OK** to save the changes.

Configuring Your System to Send SNMP Traps to a Management Station

Server Administrator generates SNMP traps in response to changes in the status of sensors and other monitored parameters. You must configure one or more trap destinations on the Server Administrator system for SNMP traps to be sent to a management station.

1. Open the **Computer Management** window.
2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon and click **Services**.
4. Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and click **Properties**.

   The **SNMP Service Properties** window appears.
5. Click the **Traps** tab to add a community for traps or to add a trap destination for a trap community.

a To add a community for traps, type the community name in the **Community Name** box and click **Add to list**, which is located next to the **Community Name** box.

b To add a trap destination for a trap community, select the community name from the **Community Name** drop-down box and click **Add** under the **Trap Destinations** box.

c The **SNMP Service Configuration** window appears.

Type in the trap destination and click **Add**.

The **SNMP Service Properties** window appears.

6 Click **OK** to save the changes.

Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux

Server Administrator uses the SNMP services provided by the ***net-snmp*** SNMP agent. You can configure the SNMP agent to change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as IT Assistant, perform the procedures described in the following sections.

NOTE: See your operating system documentation for additional details on SNMP configuration.

SNMP Agent Access Control Configuration

The management information base (MIB) branch implemented by Server Administrator is identified by the Object Identifier (OID) 1.3.6.1.4.1.674. Management applications must have access to this branch of the MIB tree to manage systems running Server Administrator.

For Red Hat Enterprise Linux and VMware ESXi 4.0 operating systems, the default SNMP agent configuration gives read-only access for the *public* community only to the MIB-II *system* branch (identified by the 1.3.6.1.2.1.1 OID) of the MIB tree. This configuration does not allow management applications to retrieve or change Server Administrator or other systems management information outside of the MIB-II *system* branch.

Server Administrator SNMP Agent Install Actions

If Server Administrator detects the default SNMP configuration during installation, it attempts to modify the SNMP agent configuration to give read-only access to the entire MIB tree for the *public* community. Server Administrator modifies the **/etc/snmp/snmpd.conf** SNMP agent configuration file in two ways:

The first change is to create a view to the entire MIB tree by adding the following line if it does not exist:

```
view all included .1
```

The second change is to modify the default *access* line to give read-only access to the entire MIB tree for the *public* community. Server Administrator looks for the following line:

```
access notConfigGroup "" any noauth exact systemview
none none
```

If Server Administrator finds the line above, it modifies the line so that it reads:

```
access notConfigGroup "" any noauth exact all none none
```

These changes to the default SNMP agent configuration give read-only access to the entire MIB tree for the *public* community.

NOTE: To ensure that Server Administrator is able to modify the SNMP agent configuration for providing proper access to systems management data, it is recommended that any other SNMP agent configuration changes be made after installing Server Administrator.

Server Administrator SNMP communicates with the SNMP agent using the SNMP Multiplexing (SMUX) protocol. When Server Administrator SNMP connects to the SNMP agent, it sends an object identifier to the SNMP agent to identify itself as a SMUX peer. Because that object identifier must be configured with the SNMP agent, Server Administrator adds the following line to the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, during installation if it does not exist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Changing the SNMP Community Name

Configuring the SNMP community names determines which systems are able to manage your system through SNMP. The SNMP community name used by management applications must match an SNMP community name configured on the Server Administrator system so that the management applications can retrieve management information from Server Administrator.

To change the SNMP community name used for retrieving management information from a system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   com2sec publicsec default public
   ```

   or

   ```
   com2sec notConfigUser default public
   ```

2. Edit this line, replacing `public` with the new SNMP community name. When edited, the new line should read:

   ```
   com2sec publicsec default community_name
   ```

   or

   ```
   com2sec notConfigUser default community_name
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   service snmpd restart
   ```

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the system running Server Administrator in order to change Server Administrator attributes using IT Assistant.

To enable SNMP Set operations on the system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   access publicgroup "" any noauth exact all none
   none
   ```

or

```
access notConfigGroup "" any noauth exact all none
none
```

2 Edit this line, replacing the first `none` with `all`. When edited, the new line should read:

```
access publicgroup "" any noauth exact all all
none
```

or

```
access notConfigGroup "" any noauth exact all all
none
```

3 To enable SNMP configuration changes, restart the SNMP agent by typing:

```
service snmpd restart
```

Configuring Your System to Send Traps to a Management Station

Server Administrator generates SNMP traps in response to changes in the status of sensors and other monitored parameters. One or more trap destinations must be configured on the system running Server Administrator for SNMP traps to be sent to a management station.

To configure your system running Server Administrator to send traps to a management station, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, and perform the following steps:

1 Add the following line to the file:

```
trapsink IP_address community_name
```

where *IP_address* is the IP address of the management station and *community_name* is the SNMP community name

2 To enable SNMP configuration changes, restart the SNMP agent by typing:

```
service snmpd restart
```

Configuring the SNMP Agent on Systems Running Supported SUSE Linux Enterprise Server

Server Administrator uses the SNMP services provided by the ***net-snmp*** agent. You can configure the SNMP agent to enable SNMP access from remote hosts, change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as IT Assistant, perform the procedures described in the following sections.

NOTE: See your operating system documentation for additional details about SNMP configuration.

Sever Administrator SNMP Install Actions

Server Administrator SNMP communicates with the SNMP agent using the SMUX protocol. When Server Administrator SNMP connects to the SNMP agent, it sends an object identifier to the SNMP agent to identify itself as a SMUX peer. This object identifier must be configured with the SNMP agent, therefore, Server Administrator adds the following line to the SNMP agent configuration file (**/etc/snmp/snmpd.conf**) during installation if it does not exist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Enabling SNMP Access From Remote Hosts

The default SNMP agent configuration on SUSE Linux Enterprise Server operating systems gives read-only access to the entire MIB tree for the *public* community from the local host only. This configuration does not allow SNMP management applications such as IT Assistant running on other hosts to discover and manage Server Administrator systems properly. If Server Administrator detects this configuration during installation, it logs a message to the operating system log file, **/var/log/messages**, to indicate that SNMP access is restricted to the local host. You must configure the SNMP agent to enable SNMP access from remote hosts if you plan to manage the system by using SNMP management applications from remote hosts.

NOTE: For security reasons, it is advisable to restrict SNMP access to specific remote hosts if possible.

To enable SNMP access from a specific remote host to a system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edit or copy this line, replacing 127.0.0.1 with the remote host IP address. When edited, the new line should read:

   ```
   rocommunity public IP_address
   ```

   NOTE: You can enable SNMP access from multiple specific remote hosts by adding a `rocommunity` directive for each remote host.

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

To enable SNMP access from all remote hosts to a system running Server Administrator, edit the SNMP agent configuration file **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edit this line by deleting 127.0.0.1. When edited, the new line should read:

   ```
   rocommunity public
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

Changing the SNMP Community Name

Configuring the SNMP community name determines which management stations are able to manage your system through SNMP. The SNMP community name used by management applications must match the SNMP community name configured on the Server Administrator system, so the management applications can retrieve the management information from Server Administrator.

To change the default SNMP community name used for retrieving management information from a system running Server Administrator, edit the SNMP agent configuration file **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edit this line by replacing `public` with the new SNMP community name. When edited, the new line should read:

   ```
   rocommunity community_name 127.0.0.1
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the system running Server Administrator in order to change Server Administrator attributes using IT Assistant. To enable remote shutdown of a system from IT Assistant, SNMP Set operations must be enabled.

NOTE: Rebooting of your system for change management functionality does not require SNMP Set operations.

To enable SNMP Set operations on a system running Server Administrator, edit the SNMP agent configuration file **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edit this line by replacing `rocommunity` with `rwcommunity`. When edited, the new line should read:

   ```
   rwcommunity public 127.0.0.1
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

Configuring Your System to Send Traps to a Management Station

Server Administrator generates SNMP traps in response to changes in the status of sensors and other monitored parameters. One or more trap destinations must be configured on the system running Server Administrator for SNMP traps to be sent to a management station.

To configure your system running Server Administrator to send traps to a management station, edit the SNMP agent configuration file **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Add the following line to the file:

   ```
   trapsink IP_address community_name
   ```

   where `IP_address` is the IP address of the management station and `community_name` is the SNMP community name.

2. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

Configuring the SNMP Agent on Systems Running Supported VMware ESX 4.X Operating Systems to Proxy VMware MIBs

The ESX 4.X server can be managed through a single default port 161 using the SNMP protocol. To do this, `snmpd` is configured to use the default port 161 and `vmwarehostd` is configured to use a different (unused) port, for example, 167. Any SNMP request on the VMWare MIB branch is rerouted to the ***vmware-hostd*** using the proxy feature of the ***snmpd*** daemon.

The VMWare SNMP configuration file can be modified manually on the ESX server or by running VMWare Remote Command-Line Interface (RCLI) command ***vicfg-snmp*** from a remote system (Windows or Linux). The RCLI tools can be downloaded from the VMware website (**vmware.com/download/vi/drivers_tools.html**).

Below are the required steps for the configuration.

1. Edit the VMWare SNMP configuration file (**/etc/vmware/snmp.xml**) either manually or run the following vicfg-snmp commands to modify the SNMP configuration settings. This includes the SNMP listening port, community string, and the trap target ipaddress/port and trap community name and then enable the VMWare SNMP service.

a `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> -c <community name> -p X –t <DMC_IP_Address>@162/<community name>`

Where X represents an unused port. To find an unused port, check the **/etc/services** file for the port assignment for defined system services. Also, to make sure that the port selected is not currently being used by any application/service, run the following command on the ESX server: `netstat –a command`

NOTE: Multiple IP addresses can be entered using a comma-separated list.

b To enable VMWare SNMP service, run the following command:

```
vicfg-snmp.pl --server <ESX_IP_addr> --username
root --password <password>

-E
```

c To view the configuration settings, run the following command:

```
vicfg-snmp.pl --server <ESX_IP_addr> --username
root --password <password>

-s
```

After modification, the configuration file looks like this:

```
<?xml version="1.0">

<config>

<snmpSettings>

<enable>true</enable>

<communities>public</communities>

<targets>143.166.152.248@162/public</targets>

<port>167</port>

</snmpSettings>

</config>
```

2 Stop the SNMP service if it is already running on your system by entering the following command:

```
service snmpd stop
```

3 Add the following line at the end of the **/etc/snmp/snmpd.conf**:.

```
proxy -v 1 -c public udp:127.0.0.1:X
.1.3.6.1.4.1.6876
```

Where X represents the unused port specified above, while configuring SNMP.

4 Configure the trap destination using the following command:
`<Destination_IP_Address> <community_name>`

The trapsink specification is required to send traps defined in the proprietary MIBs.

5 Restart mgmt-vmware service with the following command:

```
service mgmt-vmware restart
```

6 Restart the snmpd service with the following command:

```
service snmpd start
```

NOTE: If the srvadmin is installed and the services are already started, restart the services as they depend on the ***snmpd*** service.

7 Run the following command so that the snmpd daemon starts on every reboot:

```
chkconfig snmpd on
```

8 Run the following command to ensure that the SNMP ports are open before sending traps to the management station.

```
esxcfg-firewall -e snmpd
```

Configuring the SNMP Agent on Systems Running Supported VMware ESXi 4.X Operating Systems

Server Administrator supports SNMP traps on VMware ESXi 4.X. The Server Administrator does not support SNMP Get and Set operations on VMWare ESXi 4.x as the required SNMP support is unavailable. The VMware vSphere Command-Line Interface (CLI) is used to configure a system running VMware ESXi 4.X to send SNMP traps to a management station.

NOTE: For more information about using the VMware vSphere CLI, see the VMware support site at vmware.com/support.

Configuring Your System to Send Traps to a Management Station

Server Administrator generates SNMP traps in response to changes in the status of sensors and other monitored parameters. One or more trap destinations must be configured on the system running Server Administrator for SNMP traps to be sent to a management station.

To configure your ESXi system running Server Administrator to send traps to a management station, perform the following steps:

1. Install the VMware vSphere CLI.
2. Open a command prompt on the system where the VMware vSphere CLI is installed.
3. Change to the directory where the VMware vSphere CLI is installed. The default location on Linux is **/usr/bin**. The default location on Windows is **C:\Program Files\VMware\VMware vSphere CLI\bin**.
4. Execute the following command:

   ```
   vicfg-snmp.pl --server <server> --username
   <username> --password <password> -c <community> -t
   <hostname>/<community>
   ```

   where `<server>` is the hostname or IP address of the ESXi system, `<username>` is a user on the ESXi system, `<password>` is the password of the ESXi user, `<community>` is the SNMP community name and `<hostname>` is the hostname or IP address of the management station.

NOTE: The extension .pl is not required on Linux.

NOTE: If you do not specify a user name and password, you are prompted.

The SNMP trap configuration takes effect immediately without restarting any services.

Firewall Configuration on Systems Running Supported Red Hat Enterprise Linux Operating Systems and SUSE Linux Enterprise Server

If you enable firewall security while installing Red Hat Enterprise Linux/SUSE Linux, the SNMP port on all external network interfaces is closed by default. To enable SNMP management applications such as IT Assistant to discover and retrieve information from Server Administrator, the SNMP port on at least one external network interface must be open. If Server Administrator detects that the SNMP port is not open in the firewall for any external network interface, Server Administrator displays a warning message and logs a message to the system log.

You can open the SNMP port by disabling the firewall, opening an entire external network interface in the firewall, or opening the SNMP port for at least one external network interface in the firewall. You can perform this action before or after Server Administrator is started.

To open the SNMP port on Red Hat Enterprise Linux using one of the previously described methods, perform the following steps:

1. At the Red Hat Enterprise Linux command prompt, type `setup` and press **<Enter>** to start the Text Mode Setup Utility.

   NOTE: This command is available only if you have performed a default installation of the operating system.

   The **Choose a Tool** menu appears.

2. Select **Firewall Configuration** using the down arrow and press **<Enter>**.

   The **Firewall Configuration** screen appears.

3. Press **<Tab>** to select **Security Level** and then press the spacebar to select the security level you want to set. The selected Security Level is indicated by an asterisk.

   NOTE: Press <F1> for more information about the firewall security levels. The default SNMP port number is **161**. If you are using the X Window System graphical user interface, pressing <F1> may not provide information about firewall security levels on newer versions of Red Hat Enterprise Linux.

   a. To disable the firewall, select **No firewall** or **Disabled** and go to step 7.

   b. To open an entire network interface or the SNMP port, select **High, Medium,** or **Enabled** and continue with step 4.

4 Press <Tab> to go to **Customize** and press <Enter>.

The **Firewall Configuration - Customize** screen appears.

5 Select whether to open an entire network interface or just the SNMP port on all network interfaces.

a To open an entire network interface, press <Tab> to go to one of the Trusted Devices and press the spacebar. An asterisk in the box to the left of the device name indicates that the entire interface is opened.

b To open the SNMP port on all network interfaces, press <Tab> to go to **Other ports** and type `snmp:udp`.

6 Press <Tab> to select **OK** and press <Enter>.

The **Firewall Configuration** screen appears.

7 Press <Tab> to select **OK** and press <Enter>.

The **Choose a Tool** menu appears.

8 Press <Tab> to select **Quit** and press <Enter>.

To open the SNMP port on SUSE Linux Enterprise Server, perform the following steps:

1 Configure SuSEfirewall2 by executing this on a console
```
a.# yast2 firewall
```

2 Use the arrow keys to navigate to **Allowed Services**.

3 Enter **Alt+d** to open the **Additional Allowed Ports** dialog box.

4 Enter **Alt+T** to move the cursor to the **TCP Ports** text box.

5 Enter **snmp** in the text box.

6 Enter **Alt-O** and '**Alt-N**' to go to the next screen.

7 Enter **Alt-A** to accept and apply the changes.

3

Using Server Administrator

Starting Your Server Administrator Session

To start a Server Administrator session, click the **Dell OpenManage Server Administrator** icon on your desktop.

The **Server Administrator Log in** screen displays. The default port for Dell OpenManage Server Administrator is 1311. You can change the port, if required. See "Dell Systems Management Server Administration Connection Service and Security Setup" for instructions on setting up your system preferences.

Logging In and Out

OpenManage Server Administrator provides three types of logins. These are:

- Server Administrator Local System Login
- Server Administrator Managed System Login
- Central Web Server Login

Server Administrator Local System Login

This login is available only if you install the Server Instrumentation and Server Administrator Web Server components on the local system.

Use this login window to log in to Server Administrator on a local system:

1. Type your preassigned **Username** and **Password** in the appropriate fields on the Systems Management **Log in** window.

   If you are accessing Server Administrator from a defined domain, you also must specify the correct **Domain** name.

2. If your system is running a Microsoft Windows operating system and is a member of the Windows domain, select a domain from the domain list.
3. Select the **Active Directory Login** check box to log in using Microsoft Active Directory. See "Using the Active Directory Login" on page 48.
4. Click **Submit**.

To end your Server Administrator session, click **Log Out** located in the upper-right corner of each **Server Administrator** home page.

NOTE: For information about Configuring Active Directory on Systems using CLI, see the *Dell OpenManage Management Station Software Installation Guide*.

Server Administrator Managed System Login

This login is available only when you install the Server Administrator Web Server component. To log in to Server Administrator to manage a remote system:

Method 1

1. Click on the **Dell OpenManage Server Administrator** icon on your desktop.
2. Type the managed system's IP Address or system name or Fully Qualified Domain Name (FQDN).

NOTE: If you have entered the system name or FQDN, Dell OpenManage Server Administrator Web Server host converts the system name or FQDN into the IP Address of the managed system. You can also enter the port number of the managed system. For example, Hostname:Port Number, or IP address:Port Number. If you are connecting to a Citrix XenServer 5.6 managed node, use port 5986 in the format Hostname:Port Number, or IP address:Port Number.

3. Select the **Ignore Certificate Warnings** check box, if you are using an Intranet connection.
4. Select the **Active Directory Login** check box. Check this option to log in using Microsoft Active Directory authentication. Do not check this box if Active Directory software is not used to control access to your network. See "Using the Active Directory Login" on page 48.
5. Click **Submit**.

Method 2

Open your Web browser and type one of the following in the address field and press <Enter>:

`https ://hostname:1311`

where `hostname` is the assigned name for the managed node system and `1311` is the default port number

or

`https ://IP address:1311`

where `IP address` is the IP address for the managed system and `1311` is the default port number. You should type `https ://` (and not `http://`) in the address field to receive a valid response in your browser.

NOTE: You must have preassigned user rights to log in to Server Administrator. See "Setup and Administration" on page 19 for instructions on setting up new users.

Central Web Server Login

This login is available only when you install the Server Administrator Web Server component. Use this login to manage the OpenManage Server Administrator Central Web Server:

1. Click on the **Dell OpenManage Server Administrator** icon on your desktop. The remote login page is displayed.

CAUTION: The login screen has an Ignore certificate warnings check box.You should use this option with discretion. It is highly recommended that you use it only in trusted Intranet environments.

2. Click on the **Manage Web Server** Link, located at the top right corner of the screen.
3. Enter the **User Name**, **Password** and **Domain name** (if you are accessing Server Administrator from a defined domain) and click **Submit**.
4. Select the **Active Directory Login** check box to log in using Microsoft Active Directory. See "Using the Active Directory Login" on page 48.
5. Click **Submit.**

To end your Server Administrator session, click **Log Out** on the "Global Navigation Bar." The **Log Out** button is located in the upper-right corner of each **Server Administrator** home page.

NOTE: When you launch Server Administrator using either Mozilla Firefox version 3.0 and 3.5 or Microsoft Internet Explorer version 7.0 or 8.0, an intermediate warning page may appear displaying the problem with security certificate. To ensure system security, it is strongly recommended that you generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from a Certification Authority (CA). To avoid encountering such warning messages about the certificate, the certificate used must be from a trusted CA. For more information on X.509 Certificate Management, see "X.509 Certificate Management."

To ensure system security, it is strongly recommended that you import a root certificate or certificate chain from a Certification Authority (CA). See the VMware documentation for details.

NOTE: If the certificate authority on the managed system is valid and if the Server Administrator web server still reports an untrusted certificate error, you can still make the managed system's CA as trusted by using the **certutil.exe**. See your operating system documentation for details on accessing this **.exe**. On supported Windows operating systems, you can also use the certificates snap in option to import certificates.

Using the Active Directory Login

You should select the **Active Directory Login** check box to log in using the Dell Extended Schema Solution in Active Directory.

This solution enables you to provide access to Server Administrator; allowing you to add/control Server Administrator users and privileges to existing users in your Active Directory software. For more information see *Using Microsoft Active Directory* in the *Dell OpenManage Installation and Security User's Guide*.

Single Sign-On

The Single Sign-On option in Windows operating systems enables all logged-in users to bypass the login page and access the Server Administrator Web application by clicking the **Dell OpenManage Server Administrator** icon on your desktop.

NOTE: For more information on Single Sign-On, see the Knowledge Base article at **support.microsoft.com/default.aspx?scid=kb;en-us;Q258063**.

For local machine access, you must have an account on the machine with the appropriate privileges (User, Power User, or Administrator). Other users are authenticated against the Microsoft Active Directory. To launch Server Administrator using Single Sign-On authentication against Microsoft Active Directory, the following parameters must also be passed in:

```
authType=ntlm&application=[plugin name]
```

Where *plugin name* = *omsa*, *ita*, etc.

For example:

```
https ://localhost:1311/?authType=ntlm&application=
omsa
```

To launch Server Administrator using Single Sign-On authentication against the local machine user accounts, the following parameters must also be passed in:

```
authType=ntlm&application=[plugin
name]&locallogin=true
```

Where *plugin name* = *omsa*, *ita*, etc.

For example:

```
https ://localhost:1311/?authType=ntlm&application=
omsa&locallogin=true
```

Server Administrator has also been extended to allow other products (such as Dell OpenManage IT Assistant) to directly access Server Administrator Web pages without going through the login page (if you are currently logged in and have the appropriate privileges).

Configuring Security Settings on Systems Running a Supported Microsoft Windows Operating System

You must configure the security settings for your browser to log in to Server Administrator from a remote management system that is running a supported Microsoft Windows operating system.

The security settings for your browser might prevent the execution of client-side scripts that are used by Server Administrator. To enable the use of client-side scripting, perform the following steps on the remote management system.

NOTE: If you have not configured your browser to enable the use of client-side scripting, you might receive a blank screen when logging in to Server Administrator. In this case, an error message is displayed instructing you to configure your browser settings.

Internet Explorer

1. In your Web browser, click **Tools**→ **Internet Options**→ **Security**.
2. Click the **Trusted Sites** icon.
3. Click **Sites**.
4. Copy the Web address used to access the remote managed system from the browser's address bar and paste it onto the **Add this Web Site to the Zone** field.
5. Click **Custom Level**.

   For Windows Server 2003:

   - Under **Miscellaneous**, select the **Allow Meta Refresh** radio button.
   - Under **Active Scripting**, select the **Enable** radio button.
   - Under **Active Scripting**, select the **Allow scripting of Internet Explorer web browser controls** radio button.
6. Click **OK** to save the new settings. Close the browser and log in to Server Administrator.

To allow Single Sign-On for Server Administrator without prompts for user credentials, perform the following steps:

1. In your Web browser click **Tools**→ **Internet Options**→ **Security**
2. Click the **Trusted Sites** icon.
3. Click **Sites**.
4. Copy the Web address used to access the remote managed system from the browser's address bar and paste it onto the **Add this Web Site to the Zone** field.
5. Click **Custom Level**.

6 Under **User Authentication**, select the **Automatic Logon with current username and password** radio button.

7 Click **OK** to save the new settings. Close the browser and log in to Server Administrator.

Mozilla Firefox

1 Start your browser.

2 Click **Edit→ Preferences**.

3 Click **Advanced→ Scripts and Plugins.**

4 Ensure that the **Navigator** check box is selected under **Enable JavaScript for**.

5 Click **OK** to save the new settings.

6 Close the browser.

7 Log in to Server Administrator.

The Server Administrator Home Page

NOTE: Do not use your Web browser toolbar buttons (such as **Back** and **Refresh**) while using Server Administrator. Use only the Server Administrator navigation tools.

With only a few exceptions, the **Server Administrator** home page has three main areas:

- The global navigation bar provides links to general services.
- The system tree displays all visible system objects based on the user's access privileges.
- The action window displays the available management actions for the selected system tree object based on the user's access privileges. The action window contains three functional areas:
  - The action tabs display the primary actions or categories of actions that are available for the selected object based on the user's access privileges.
  - The action tabs are divided into subcategories of all available secondary options for the action tabs based on the user's access privileges.
  - The data area displays information for the selected system tree object, action tab, and subcategory based on the user's access privileges.

Additionally, when logged in to the **Server Administrator** home page, the system model, the assigned name of the system, and the current user's user name and user privileges are displayed in the top-right corner of the window.

Table 3-1 lists the GUI field names and the applicable system, when Server Administrator is installed on the system.

Table 3-1. System Availability for the Following GUI Field Names

GUI Field Name	Applicable System
`Modular Enclosure`	Modular System
`Server module`	Modular System
`Main System`	Modular System
`System`	Non-Modular System
`Main system Chassis`	Non-Modular System

Figure 3-1 shows a sample Server Administrator home page layout for a user logged in with administrator privileges on a non-modular system.

Figure 3-1. Sample Server Administrator Home Page — Non-Modular System

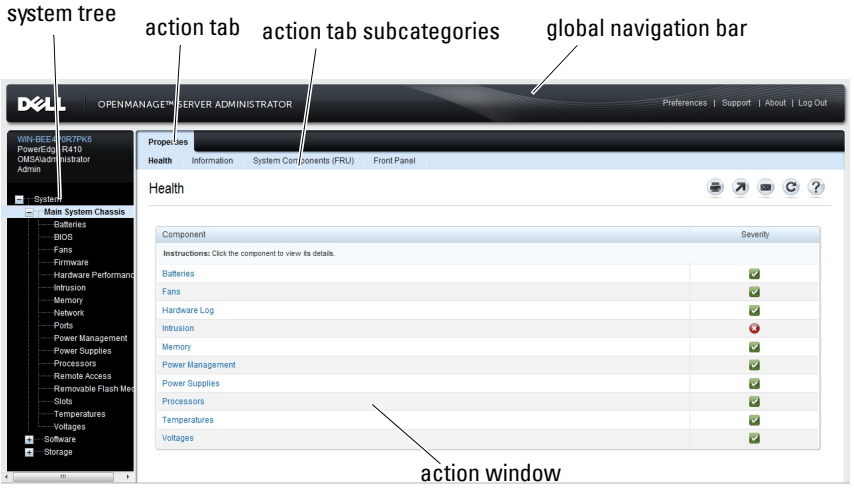
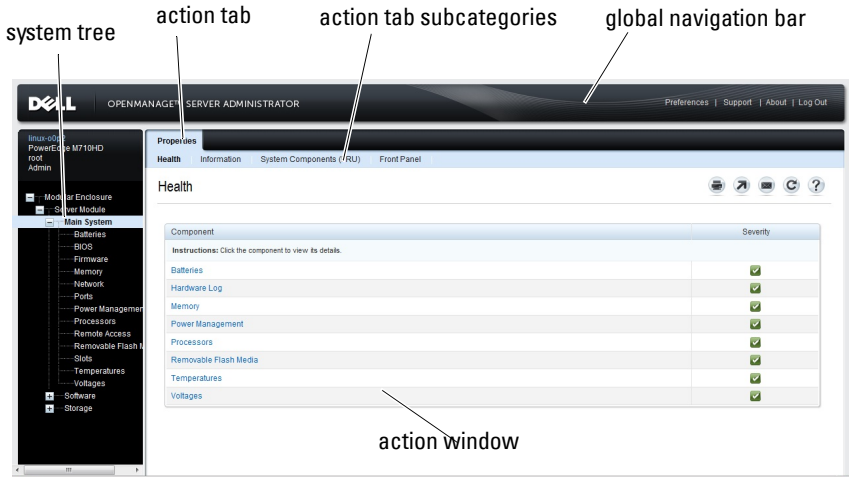


Figure 3-2 shows a sample Server Administrator home page layout for a user logged in with administrator privileges on a modular system.

Figure 3-2. Sample Server Administrator Home Page — Modular System



Clicking an object in the system tree opens a corresponding action window for that object. You can navigate in the action window by clicking action tabs to select major categories and clicking the action tab subcategories to access more detailed information or more focused actions. The information displayed in the data area of the action window can range from system logs to status indicators to system probe gauges. Underlined items in the data area of the action window indicate a further level of functionality. Clicking an underlined item creates a new data area in the action window that contains a greater level of detail. For example, clicking **Main System Chassis/Main System** under the **Health** subcategory of the **Properties** action tab lists the health status of all the components contained in the Main System Chassis/Main System object that are monitored for health status.

NOTE: Administrator or Power User privileges are required to view most of the system tree objects, system components, action tabs, and data area features that are configurable. Additionally, only users logged in with Administrator privileges can access critical system features such as the shutdown functionality included under the **Shutdown** tab.

Server Administrator User Interface Differences Across Modular and Non-Modular Systems

Table 3-2 lists the availability of Server Administrator features across modular and non-modular systems. A tick mark indicates availability, while a crossout indicates non-availability of the feature.

Table 3-2. Server Administrator User Interface Differences Across Modular and Non-Modular Systems

Features	Modular System	Non-Modular System
Batteries	✓	✓
Power Supplies	✗	✓
Fans	✗	✓
Hardware Performance	✗	✓ (*xx0x* system onwards)
Intrusion	✗	✓
Memory	✓	✓
Network	✓	✓
Ports	✓	✓
Power Management	✓	✓ (*xx0x* system onwards)
Processors	✓	✓
Remote Access	✓	✓
Removable Flash Media	✓	✓
Slots	✓	✓
Temperatures	✓	✓
Voltages	✓	✓
Modular Enclosure (Chassis Information and CMC Information)	✓	✗

Global Navigation Bar

The global navigation bar and its links are available to all user levels in the program.

- Click **Preferences** to open the **Preferences** home page. See "Using the Preferences Home Page."
- Click **Support** to connect to the Dell Support website.
- Click **About** to display Server Administrator version and copyright information.
- Click **Log Out** to end the current Server Administrator program session.

System Tree

The system tree appears on the left side of the Server Administrator home page and lists the components of your system that are viewable. The system components are categorized by component type. When you expand the main object known as **Modular Enclosure→ System/Server Module**, the major categories of system/server module components that may appear are **Main System Chassis/Main System**, **Software**, and **Storage**.

To expand a branch of the tree, click the plus sign ( ) to the left of an object, or double-click the object. A minus sign ( ) indicates an expanded entry that cannot be expanded further.

Action Window

When you click an item on the system tree, details about the component or object appear in the data area of the action window. Clicking an action tab displays all available user options as a list of subcategories.

Clicking an object on the system/server module tree opens that component's action window, displaying the available action tabs. The data area defaults to a preselected subcategory of the first action tab for the selected object. The preselected subcategory is usually the first option. For example, clicking the **Main System Chassis/Main System** object opens an action window in which the **Properties** action tab and **Health** subcategory are displayed in the window's data area.

Data Area

The data area is located below the action tabs on the right side of the home page. The data area is where you perform tasks or view details about system components. The content of the window depends on the system tree object and action tab that are currently selected. For example, when you select **BIOS** from the system tree, the **Properties** tab is selected by default and the version information for the system BIOS appears in the data area. The data area of the action window contains many common features, including status indicators, task buttons, underlined items, and gauge indicators.

The Server Administrator user interface displays the date in the <mm/dd/yyyy> format.

System/Server Module Component Status Indicators

The icons that appear next to component names show the status of that component (as of the latest page refresh).

Table 3-3. System/Server Module Component Status Indicators

	indicates that a component is healthy (normal).
	indicates that a component has a warning (noncritical) condition. A warning condition occurs when a probe or other monitoring tool detects a reading for a component that falls within certain minimum and maximum values. A warning condition requires prompt attention.
	indicates that a component has a failure (critical) condition. A critical condition occurs when a probe or other monitoring tool detects a reading for a component that falls within certain minimum and maximum values. A critical condition requires immediate attention.
	indicates that a component's health status is unknown.

Task Buttons

Most windows opened from the Server Administrator home page contain at least five task buttons: **Print**, **Export**, **Email**, **Help** and **Refresh**. Other task buttons are included on specific Server Administrator windows. Log windows, for example, also contain **Save As** and **Clear Log** task buttons.

- Clicking **Print** ( )prints a copy of the open window to your default printer.

- Clicking **Export** ( )generates a text file that lists the values for each data field on the open window. The export file is saved to a location you specify. See "Setting User and System Preferences" for instructions on customizing the delimiter separating the data field values.
- Clicking **Email** ( )creates an e-mail message addressed to your designated e-mail recipient. See "Setting User and System Preferences" for instructions on setting up your e-mail server and default e-mail recipient.
- Clicking **Refresh** ( )reloads the system component status information in the action window data area.
- Clicking **Save As** saves an HTML file of the action window in a **.zip** file.
- Clicking **Clear Log** erases all events from the log displayed in the action window data area.
- Clicking **Help** ( )provides detailed about the specific window or task button you are viewing.

NOTE: The **Export**, **Email**, **Save As**, and **Clear Log** buttons are only visible for users logged in with Power User or Administrator privileges.

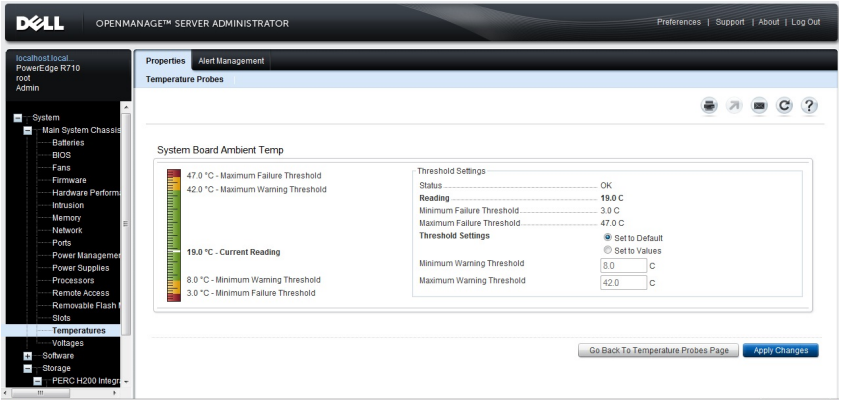
Underlined Items

Clicking an underlined item in the action window data area displays additional details about that item.

Gauge Indicators

Temperature probes, fan probes, and voltage probes are each represented by a gauge indicator. For example, Figure 3-3 shows readings from a system's CPU fan probe.

Figure 3-3. Gauge Indicator



Using the Online Help

Context-sensitive online help is available for every window of the Server Administrator home page. Clicking **Help** opens an independent help window that contains detailed information about the specific window you are viewing. The online help is designed to help guide you through the specific actions required to perform all aspects of the Server Administrator services. Online help is available for all windows you can view, based on the software and hardware groups that Server Administrator discovers on your system and your user privilege level.

Using the Preferences Home Page

The left-hand pane of the **Preferences** home page (where the system tree is displayed on the Server Administrator home page) displays all available configuration options in the system tree window.

The available Preferences home page configuration options are:

- General Settings
- Server Administrator

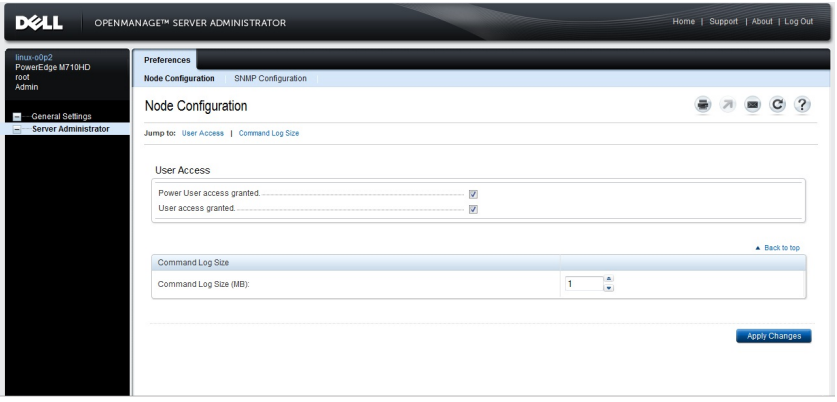
You can view the **Preferences** tab after you log in to manage a remote system. This tab is also available when you log in to manage the Server Administrator Web server or manage the local system.

Like the Server Administrator home page, the **Preferences** home page has three main areas:

- The global navigation bar provides links to general services.
  - Click **Home** to return to the Server Administrator home page.
- The left-hand pane of the **Preferences** home page (where the system tree is displayed on the Server Administrator home page) displays the preference categories for the managed system or the Server Administrator Web server.
- The action window displays the available settings and preferences for the managed system or the Server Administrator Web Server.

Figure 3-4 shows a sample Preferences home page layout.

Figure 3-4. Sample Preferences Home Page - Managed System



Managed System Preferences

When you log in to a remote system, the Preferences home page defaults to the Node Configuration window under the **Preferences** tab.

Click the Server Administrator object to enable or disable access to users with User or Power User privileges. Depending on the user's group privileges, the Server Administrator object action window can have the **Preferences** tab.

Under the Preferences tab, you can:

- Enable or disable access to users with User or Power User privileges.
- Configure the Command Log Size
- Configure SNMP

Server Administrator Web Server Preferences

When you log in to manage the Server Administrator Web server, the **Preferences** home page defaults to the **User Preferences** window under the Preferences tab.

Due to the separation of the Server Administrator Web server from the managed system, the following options are displayed when you log in to the Server Administrator Web server, using the Manage Web Server link:

- Web Server Preferences
- X.509 Certificate Management

For more information on accessing these features, see "Server Administrator Services."

Dell Systems Management Server Administration Connection Service and Security Setup

Setting User and System Preferences

You set user and secure port system preferences from the **Preferences** home page.

NOTE: You must be logged in with Administrator privileges to set or reset user or system preferences.

Perform the following steps to set up your user preferences:

1. Click **Preferences** on the global navigation bar.

   The **Preferences** home page appears.

2. Click **General Settings**.

3 To add a preselected e-mail recipient, type the e-mail address of your designated service contact in the **Mail To:** field, and click **Apply Changes**.

NOTE: Click **Email** in any window to send an e-mail message with an attached HTML file of the window to the designated e-mail address.

4 To change the home page appearance, select an alternative value in the **skin** or **scheme** fields and click **Apply Changes**.

Perform the following steps to set up your secure port system preferences:

1 Click **Preferences** on the global navigation bar.

The **Preferences** home page appears.

2 Click **General Settings**, and the **Web Server** tab.

3 In the **Server Preferences** window, set options as necessary.

- The **Session Timeout** feature can set a limit on the amount of time that a Server Administrator session can remain active. Select the **Enable** radio button to allow Server Administrator to time out if there is no user interaction for a specified number of minutes. Users whose session times out must log in again to continue. Select the **Disable** radio button to disable the Server Administrator session timeout feature.
- The **HTTPS Port** field specifies the secure port for Server Administrator. The default secure port for Server Administrator is 1311.

NOTE: Changing the port number to an invalid or in-use port number might prevent other applications or browsers from accessing Server Administrator on the managed system. See the *Dell OpenManage Installation and Security User's Guide* for the list of default ports.

- The **IP Address to Bind to** field specifies the IP address(es) for the managed system that Server Administrator binds to when starting a session. Select the **All** radio button to bind to all IP addresses applicable for your system. Select the **Specific** radio button to bind to a specific IP address.

NOTE: Changing the **IP Address to Bind to** value to a value other than **All** may prevent other applications or browsers from accessing Server Administrator on the managed system.

- The **SMTP Server name** and **DNS Suffix for SMTP Server** fields specify your company or organization's Simple Mail Transfer Protocol (SMTP) and domain name server (DNS) suffix. To enable Server Administrator to send e-mails, you must type the IP address and DNS suffix for the SMTP Server for your company or organization in the appropriate fields.

NOTE: For security reasons, your company or organization might not allow e-mails to be sent through the SMTP server to outside accounts.

- The **Command Log Size** field specifies the largest file size in MB for the command log file.

NOTE: This field appears only when you log in to manage the Server Administrator Web Server.

- The **Support Link** field specifies the URL for the business entity that provides support for your managed system.
- The **Custom Delimiter** field specifies the character used to separate the data fields in the files created using the **Export** button. The **;** character is the default delimiter. Other options are **!**, **@**, **#**, **$**, **%**, **^**, *****, **~**, **?**, **|**, and **,**.
- The **SSL Encryption** field specifies the encryption levels for the secured HTTPS sessions. The available encryption levels include **Auto Negotiate** and **128-bit or higher**.
  - **Auto Negotiate** — To allow connection from browser with any encryption strength. The browser auto negotiates with the Server Administrator web server and uses the highest available encryption level for the session. Legacy browsers with weaker encryption can connect to the Server Administrator.
  - **128-bit or higher** — To allow connections from browsers with 128-bit or higher encryption strength. One of the following cipher suites is applicable based upon the browser for any established sessions:

    SSL_RSA_WITH_RC4_128_SHA
    SSL_RSA_WITH_RC4_128_MD5
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    SSL_RSA_WITH_3DES_EDE_CBC_SHA
    TLS_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

- **Key Signing Algorithm** displays the supported signing algorithms. Select an algorithm from the drop down list. If you select either SHA 512 or SHA 256, ensure that your operating system/browser supports this algorithm. If you select one of these options without the requisite operating system/browser support, Server Administrator displays a `cannot display the webpage` error. This field is meant only for Server Administrator auto-generated self-signed certificates. The drop down list is grayed out if you import or generate new certificates into Server Administrator

NOTE: 128-bit or higher option does not allow connections from browsers with lower SSL encryption strength, such as 40 bit and 56 bit.

NOTE: Restart the Server Administrator web server for the changes to take effect.

NOTE: If the encryption level is set to **128-bit or higher**, you can access or modify the Server Administrator settings using a browser with the same or higher encryption levels.

4 When you finish setting options in the **Server Preferences** window, click **Apply Changes**.

X.509 Certificate Management

Web certificates are necessary to ensure the identity of a remote system and ensure that information exchanged with the remote system cannot be viewed or changed by others. To ensure system security, it is strongly recommended that:

- You generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from a Certification Authority (CA).
- All systems that have Server Administrator installed have unique host names.

NOTE: You must be logged in with Administrator privileges to perform certificate management.

To manage X.509 certificates through the Preferences home page, click **General Settings**, click the **Web Server** tab, and click **X.509 Certificate**.

You can use this option to:

- **Generate a new X.509 certificate** — Use this option to create a certificate for access to Server Administrator.
- **Certificate Maintenance** — This option selects an existing certificate that your company has title to, and uses this certificate to control access to Server Administrator.
- **Import a root certificate** — This option allows you to import the root certificate, as well as the certificate response (in PKCS#7 format), received from the trusted certificate authority.
- **Import certificate chain from a CA** — This option allows you to import the certificate response (in PKCS#7 format) from the trusted certificate authority. Some of the reliable certificate authorities are Verisign, Thawte, and Entrust.

Server Administrator Web Server Action Tabs

When you log in to manage Server Administrator Web Server, these are the action tabs that are displayed:

- Shutdown
- Logs
- Session Management

Managing Server Administrator

Server Administrator automatically starts each time you reboot the managed system. To manually start, stop, or restart Server Administrator, use the following instructions.

NOTE: To manage the Server Administrator, you must be logged in with administrator privileges (logged in as `root` for supported Citrix XenServer, Red Hat Enterprise Linux, or SUSE Linux Enterprise Server operating systems).

Starting Server Administrator

Supported Microsoft Windows Operating Systems

To start Server Administrator on systems running a supported Windows operating system, perform the following steps:

1. Open the **Services** window.
2. Right-click the **Dell Systems Management Server Administration (DSM SA) Connection Service** icon.
3. Click **Start**.

Supported Citrix XenServer, Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

To start Server Administrator on systems running a supported Citrix XenServer, Red Hat Enterprise Linux, or SUSE Linux Enterprise Server operating system, run the following command from the command line:

```
dsm_om_connsvc start
```

Stopping Server Administrator

Supported Microsoft Windows Operating Systems

To stop Server Administrator, perform the following steps:

1. Open the **Services** window.
2. Right-click the **DSM SA Connection Service** icon.
3. Click **Stop**.

Supported Citrix XenServer, Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

To stop Server Administrator on systems running a supported Citrix XenServer, Red Hat Enterprise Linux, or SUSE Linux Enterprise Server operating system, run the following command from the command line:

```
dsm_om_connsvc stop
```

Restarting Server Administrator

Supported Microsoft Windows Operating Systems

To restart Server Administrator, perform the following steps:

1. Open the **Services** window.
2. Right-click the **DSM SA Connection Service** icon.
3. Click **Restart**.

Supported Citrix XenServer, Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

To restart Server Administrator on systems running a supported Citrix XenServer, Red Hat Enterprise Linux, or SUSE Linux Enterprise Server operating system, run the following command from the command line:

```
dsm_om_connsvc restart
```

Using the Server Administrator Command Line Interface

The Server Administrator command line interface (CLI) allows users to perform essential systems management tasks from the operating system command prompt of a monitored system.

The CLI allows a user with a very well-defined task in mind to rapidly retrieve information about the system. Using CLI commands, for example, administrators can write batch programs or scripts to execute at specific times. When these programs execute, they can capture reports on components of interest, such as fan RPMs. With additional scripting, the CLI can be used to capture data during periods of high system usage to compare with the same measurements at times of low system usage. Command results can be routed to a file for later analysis. The reports can help administrators to gain information that can be used to adjust usage patterns, to justify purchasing new system resources, or to focus on the health of a problem component.

For complete instructions on the functionality and use of the CLI, see the *Dell OpenManage Server Administrator Command Line Interface User's Guide*.

4

Server Administrator Services

Overview

The Dell OpenManage Server Administrator Instrumentation Service monitors the health of a system and provides rapid access to detailed fault and performance information gathered by industry standard systems management agents. The reporting and viewing features allow retrieval of overall health status for each chassis that comprises your system. At the subsystem level, you can view information about the voltages, temperatures, fan rpm, and memory function at key points in the system. A detailed account of every relevant cost of ownership (COO) detail about your system can be seen in the summary view. Version information for BIOS, firmware, operating system, and all installed systems management software is easy to retrieve.

Additionally, system administrators can use the Instrumentation Service to perform the following essential tasks:

- Specify minimum and maximum values for certain critical components. The values, called thresholds, determine the range in which a warning event for that component occurs (minimum and maximum failure values are specified by the system manufacturer).
- Specify how the system responds when a warning or failure event occurs. Users can configure the actions that a system takes in response to notifications of warning and failure events. Alternatively, users who have around-the-clock monitoring can specify that no action is to be taken and rely on human judgment to select the best action in response to an event.
- Populate all of the user-specifiable values for the system, such as the name of the system, the phone number of the system's primary user, the depreciation method, whether the system is leased or owned, and so on.

NOTE: You must configure the Simple Network Management Protocol (SNMP) service to accept SNMP packets for both managed systems and network management stations running Microsoft Windows Server 2003. See "Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems" for details.

Managing Your System

The Server Administrator home page defaults to the **System** object of the system tree view. The default for the **System** object opens the **Health** components under the **Properties** tab.

The **Preferences** home page defaults to the **Access Configuration** window under the **Preferences** tab.

From the **Preferences** home page, you can restrict access to users with User and Power User privileges, set the SNMP password, and configure user settings and DSM SA Connection Service settings.

NOTE: Context-sensitive online help is available for every window of the Server Administrator home page. Click **Help** to open an independent help window that contains detailed information about the specific window you are viewing. The online help is designed to guide you through the specific actions required to perform all aspects of the Server Administrator services. Online help is available for all windows you can view, based on the software and hardware groups that Server Administrator discovers on your system and your user privilege level.

NOTE: You must have Administrator or Power User privileges to view many of the system tree objects, system components, action tabs, and data area features that are configurable. Additionally, only users logged in with Administrator privileges can access critical system features such as the shutdown functionality included under the **Shutdown** tab.

Managing System/Server Module Tree Objects

The Server Administrator system/server module tree displays all visible system objects based on the software and hardware groups that Server Administrator discovers on the managed system and on the user's access privileges. The system components are categorized by component type. When you expand the main object—"**Modular Enclosure**"—"**System/Server Module**"—the major categories of system components that may appear are, "**Main System Chassis/Main System**," "**Software**," and "**Storage**."

If Storage Management Service is installed, depending on the controller and storage attached to the system, the Storage tree object expands to display various objects.

For detailed information on the Storage Management Service component, see the *Dell OpenManage Server Administrator Storage Management User's Guide* at **support.dell.com/manuals**.

Server Administrator Home Page System Tree Objects

Unsupported Features in OpenManage Server Administrator

Due to the limitations of the VMware ESXi version 4.X operating system, some features available with earlier versions of OpenManage Server Administrator are not available in this release. These are:

Unsupported Features on ESXi 4.X

- Alert Management – Alert Actions
- Network Interface – Administrative Status
- Network Interface – DMA
- Network Interface – Internet Protocol (IP) Address
- Network Interface – Maximum Transmission Unit
- Network Interface – Operational Status
- Preferences – SNMP Configuration
- Remote Shutdown – Power Cycle System with Shutdown operating system First
- About Details - Server administrator component details not listed under Details tab
- Rolemap

NOTE: Server Administrator always displays the date in <mm/dd/yyyy> format.

NOTE: Administrator or Power User privileges are required to view many of the system tree objects, system components, action tabs, and data area features that are configurable. Additionally, only users logged in with Administrator privileges can access critical system features such as the shutdown functionality included under the **Shutdown** tab.

Modular Enclosure

NOTE: For the purposes of Server Administrator, *modular enclosure* refers to a system that may contain one or more modular systems that appear as a separate Server Module in the system tree. Like a stand-alone Server Module, a Modular Enclosure contains all of the essential components of a system. The only difference is that there are slots for at least two Server Modules within a larger container, and each of them is as complete a system as a Server Module.

To view the modular system's chassis information and Chassis Management Controller (CMC) information, click the **Modular Enclosure** object.

Properties

Subtabs: Information

Under the **Properties** tab, you can:

- View the chassis information for the modular system being monitored.
- View detailed Chassis Management Controller (CMC) information for the modular system being monitored.

Accessing and Using Chassis Management Controller

To link to the Chassis Management Controller **Log in** window from the Server Administrator home page:

1. Click the **Modular Enclosure** object
2. Click the **CMC Information** tab, and then click **Launch the CMC Web Interface**. The CMC **Log in** window is displayed.

You can monitor and manage your modular enclosure after connecting to the CMC.

System/Server Module

The **System/Server Module** object contains three main system component groups: "Main System Chassis/Main System," "Software," and "Storage." The Server Administrator home page defaults to the **System** object of the system tree view. Most administrative functions can be managed from the **System/Server Module** object action window. The **System/Server Module** object action window has the following tabs, depending on the user's group privileges: **Properties**, **Shutdown**, **Logs**, **Alert Management**, and **Session Management**.

Properties

Subtabs: Health | Summary | Asset Information | Auto Recovery

Under the **Properties** tab, you can:

- View the current health alert status for hardware and software components in the **Main System Chassis/Main System** object and the **Storage** object.
- View detailed summary information for all components in the system being monitored.
- View and configure asset information for the system being monitored.
- View and set the Automatic System Recovery (operating system watchdog timer) actions for the system being monitored.

NOTE: Automatic System Recovery options may not be available because the operating system watchdog timer is enabled in BIOS. To configure the auto recovery options, the operating system watchdog timer must be disabled.

NOTE: Automatic System Recovery actions may not execute exactly per the time-out period (n seconds) when the watchdog identifies a system that has stopped responding. The action execution time ranges from *n-h+1* to *n+1* seconds, where *n* is the time-out period and *h* is the heart beat interval. The value of the heart beat interval is 7 seconds when $n \leq 30$ and 15 seconds when $n > 30$.

NOTE: The functionality of the watchdog timer feature cannot be guaranteed when an uncorrectable memory event occurs in the system DRAM Bank_1. If an uncorrectable memory event occurs in this location, the BIOS code resident in this space may become corrupted. Because the watchdog feature uses a call to BIOS to effect the shutdown or reboot behavior, the feature may not work properly. If this occurs, you must manually reboot the system.

Shutdown

Subtabs: Remote Shutdown | Thermal Shutdown | Web Server Shutdown

Under the **Shutdown** tab, you can:

- Configure the operating system shutdown and remote shutdown options.
- Set the thermal shutdown severity level to shut down your system in the event that a temperature sensor returns a warning or failure value.

  NOTE: A thermal shutdown occurs only when the temperature reported by the sensor goes above the temperature threshold. A thermal shutdown does not occur when the temperature reported by the sensor goes below the temperature threshold.

- Shut down the DSM SA Connection Service (Web server).

  NOTE: Server Administrator is still available using the command line interface (CLI) when the DSM SA Connection Service is shut down. The CLI functions do not require the DSM SA Connection Service to be running.

Logs

Subtabs: Hardware | Alert | Command

Under the **Logs** tab, you can:

- View the Embedded System Management (ESM) log or the System Event Log (SEL) for a list of all events related to your system's hardware components. The status indicator icon next to the log name changes from normal status ( ) to noncritical status( ) when the log file reaches 80 percent capacity. On Dell PowerEdge *x8xx*, *x9xx* and *xx1x* systems, the status indicator icon next to the log name changes to critical status ( ) when the log file reaches 100 percent capacity.

  NOTE: It is recommended that you clear the hardware log when it reaches 80 percent capacity. If the log is allowed to reach 100 percent capacity, the latest events are discarded from the log.

- View the Alert log for a list of all events generated by the Server Administrator Instrumentation Service in response to changes in the status of sensors and other monitored parameters.

  NOTE: See the *Server Administrator Messages Reference Guide* for a complete explanation of each alert event ID's corresponding description, severity level, and cause.

- View the Command log for a list of each command executed from either the **Server Administrator** home page or from its command line interface.

NOTE: See "Server Administrator Logs" for complete instructions on viewing, printing, saving, and e-mailing logs.

Alert Management

Subtabs: Alert Actions | Platform Events | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a system component sensor returns a warning or failure value.
- View current Platform Event Filter settings and set the Platform Event Filtering actions to be performed in the event that a system component sensor returns a warning or failure value. You can also use the **Configure Destination** option to select a destination (IPv4 or IPv6 address) where an alert for a platform event is to be sent.

NOTE: Server Administrator does not display the scope ID of the IPv6 address in its graphical user interface.

- View current SNMP trap alert thresholds and set the alert threshold levels for instrumented system components. The selected traps are triggered if the system generates a corresponding event at the selected severity level.

NOTE: Alert actions for all potential system component sensors are listed on the **Alert Actions** window, even if they are not present on your system. Setting alert actions for system component sensors that are not present on your system has no effect.

Session Management

Subtabs: Session

Under the **Session Management** tab, you can:

- View session information for current users that have logged in to Server Administrator.
- Terminate user sessions.

NOTE: Only users with administrative privileges can view the Session Management page and terminate session(s) of logged-in users.

Main System Chassis/Main System

Click the **Main System Chassis/Main System** object to manage your system's essential hardware and software components.

The available components are:

- Batteries
- BIOS
- Fans
- Firmware
- Hardware Performance
- Intrusion
- Memory
- Network
- Ports
- Power Management
- Power Supplies
- Processors
- Remote Access
- Removable Flash Media
- Slots
- Temperatures
- Voltages

NOTE: Hardware performance is supported only on Dell *xx0x* and above systems.
Power supplies is not available on Dell PowerEdge 1900 system.
Power management is supported on limited Dell *xx0x* and above systems.

The system/server module may contain one main system chassis or several chassis. The main system chassis/main system contains the essential components of a system. The **Main System Chassis/Main System** object action window has the following tab: **Properties**.

Properties

Subtabs: Health | Information | System Components (FRU) | Front Panel

Under the **Properties** tab, you can:

- View the health or status of hardware components and sensors. Each listed component has a "System/Server Module Component Status Indicators" icon next to its name. indicates that a component is healthy (normal). indicates that a component has a warning (noncritical) condition and requires prompt attention. indicates a component has a failure (critical) condition and requires immediate attention. indicates that a component's health status is unknown. The available monitored components include:
  - Batteries
  - Fans
  - Hardware Log
  - Intrusion
  - Memory
  - Network
  - Power Management
  - Power Supplies
  - Processors
  - Temperatures
  - Voltages

  NOTE: Batteries are supported only on Dell PowerEdge *x9xx* and Dell *xx0x* systems.
  Power supplies is not available on Dell PowerEdge 1900 system.
  Power management is supported on limited Dell *xx0x* systems.
- View information about the main system chassis attributes such as the Host Name, iDRAC version, Lifecycle Controller version, Chassis Model, Chassis Lock, Chassis Service Tag, Express Service Code, and Chassis Asset Tag. The Express Service Code (ESC) attribute is an 11 digit numeric-only conversion of the Dell system Service Tag. You can key in

this attribute into a telephone while calling Dell Technical Support for auto call routing. Express Service Code attribute is not present for Storage (DAS).

- View detailed information about the field-replaceable units (FRUs) installed in your system (under the **System Components (FRU)** subtab.)
- Enable or disable the managed system's front panel buttons, namely Power button and Non-Masking Interrupt (NMI) button (if present on the system). Also, select the managed system's LCD Security Access level. The managed system's LCD information can be selected from the drop-down menu. You can also enable Indication of Remote KVM session from the **Front Panel** subtab.

Batteries

Click the **Batteries** object to view information about your system's installed batteries. Batteries maintain the time and date when your system is turned off. The battery saves the system's BIOS setup configuration, which allows the system to reboot efficiently. The **Batteries** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Information

Under the **Properties** tab, you can view the current readings and status of your system's batteries.

Alert Management

Under the **Alert Management** tab, you can configure the alerts that you want to take effect in case of a battery warning or critical/failure event.

BIOS

Click the **BIOS** object to manage key features of your system's BIOS. Your system's BIOS contains programs stored on a flash memory chip set that control communications between the microprocessor and peripheral devices, such as the keyboard and the video adapter, and other miscellaneous functions, such as system messages. The **BIOS** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Setup**.

Properties

Subtab: Information

Under the **Properties** tab, you can view BIOS information.

Setup

Subtab: BIOS

Under the **Setup** tab, you can set the state for each BIOS setup object.

You can modify the state of many BIOS setup features including but not limited to the Serial Port, Network Interface Controller cards, Boot Sequence, Hard Disk Drive Sequence, User Accessible USB Ports, CPU Virtualization Technology, CPU HyperThreading, AC Power Recovery Mode, Embedded SATA Controller, Console Redirection, and Console Redirection Failsafe Baud Rate. You can also configure internal USB device, optical drive controller settings, automatic system recovery (ASR) Watchdog Timer, embedded hypervisor and additional LAN network ports on motherboard information. You can view the settings of Trusted Platform Module (TPM) and Trusted Cryptographic Module (TCM).

Depending upon your specific system configuration, additional setup items may be displayed. However, some BIOS setup options may be shown on the F2 BIOS Setup screen that are not accessible in Server Administrator.

NOTE: The NIC configuration information within the Server Administrator **BIOS** setup may be inaccurate for embedded NICs. Using the **BIOS** setup screen to enable or disable NICs might produce unexpected results. It is recommended that you perform all configurations for embedded NICs through the actual **System Setup** screen that is available by pressing <F2> while a system is booting.

NOTE: The BIOS Setup tab for your system only displays the BIOS features that are supported on your system.

Fans

Click the **Fans** object to manage your system fans. Server Administrator monitors the status of each system fan by measuring fan rpms. Fan probes report rpms to the Server Administrator Instrumentation Service. When you select **Fans** from the device tree, details appear in the data area in the right-hand pane of the Server Administrator home page. The **Fans** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Fan Probes

Under the **Properties** tab, you can:

- View the current readings for your system's fan probes and configure minimum and maximum values for fan probe warning threshold.

  NOTE: Some fan probe fields differ according to the type of firmware your system has: BMC or ESM. Some threshold values are not editable on BMC-based systems.

- Select fan control options.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a fan returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for fans. The selected traps are triggered if the system generates a corresponding event at the selected severity level.

Firmware

Click the **Firmware** object to manage your system firmware.
Firmware consists of programs or data that have been written to ROM. Firmware can boot and operate a device. Each controller contains firmware that helps provide the controller's functionality. The **Firmware** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view your system's firmware information.

Hardware Performance

Click the **Hardware Performance** object to view the status and cause for the system's performance degradation. The **Hardware Performance** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Table 4-1 lists the possible values for status and cause of a probe:

Table 4-1. Possible Values for Status and Cause of a Probe

Status Values	Cause Values
Degraded	User Configuration
	Insufficient Power Capacity
	Unknown Reason
Normal	[N/A]

Properties

Subtab: Information

Under the **Properties** tab, you can view the details of system's performance degradation.

Intrusion

Click the **Intrusion** object to manage your system's chassis intrusion status. Server Administrator monitors chassis intrusion status as a security measure to prevent unauthorized access to your system's critical components. Chassis intrusion indicates that someone is opening or has opened the cover to the system's chassis. The **Intrusion** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Intrusion

Under the **Properties** tab, you can view the chassis intrusion status.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that the intrusion sensor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for the intrusion sensor. The selected traps are triggered if the system generates a corresponding event at the selected severity level.

Memory

Click the **Memory** object to manage your system's memory devices. Server Administrator monitors the memory device status for each memory module present in the monitored system. Memory device prefailure sensors monitor memory modules by counting the number of ECC memory corrections. Server Administrator also monitors memory redundancy information if your system supports this feature. The **Memory** object action window can have the following tabs, depending on the user's group privileges: **Properties and Alert Management**.

Properties

Subtab: Memory

Under the **Properties** tab, you can view memory attributes, memory device details, and memory device status.

NOTE: If a system with spare bank memory enabled enters a redundancy lost state, it may not be apparent which memory module is the cause. If you cannot determine which DIMM to replace, see the *switch to spare memory bank detected* log entry in the ESM system log to find which memory module failed.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a memory module returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for memory modules. The selected traps are triggered if the system generates a corresponding event at the selected severity level.

Network

Click the **Network** object to manage your system's NICs. Server Administrator monitors the status of each NIC present in your system to ensure continuous remote connection. Dell OpenManage Server Administrator reports NIC teaming details if it's already configured on the system. Two or more physical NICs can be teamed into a single logical NIC, to which an administrator can assign an IP address. Teaming can be configured using NIC vendor tools. For example, Broadcom - BACS. If one of the physical NICs fails, the IP address

remains accessible because it is bound to the logical NIC rather than to a single physical NIC. If Team Interface is configured, the detailed team properties are displayed. The relation between physical NICs and Team Interface and vice-versa is also reported, if these physical NICs are members of the Team Interface. The **Network** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view information about the physical NIC interfaces and also the team interfaces installed on your system.

NOTE: In the IPv6 Addresses section, Server Administrator displays only two addresses, in addition to the link-local address.

Ports

Click the **Ports** object to manage your system's external ports.
Server Administrator monitors the status of each external port present in your system. The **Ports** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view information about your system's internal and external ports.

Power Management

NOTE: Power Management features are only available for PowerEdge systems that have hot-swappable power supplies and not systems that have a fixed, non-redundant power supply installed.

Monitoring

Subtabs: Consumption | Statistics

Under the Consumption tab you can view and manage your system's Power Consumption information in Watts and BTU/hr.

BTU/hr=Watt X 3.413 (Value rounded off to the nearest whole number)

Server Administrator monitors power consumption status, amperage, and tracks power statistic details.

You can also view the System Instantaneous Headroom and System Peak Headroom. The values are displayed in both Watts and BTU/hr (British Thermal Unit). Power thresholds can be set in Watts and BTU/hr.

The Statistics tab allows you to view and reset your system's Power tracking statistics like energy consumption, system peak power, and system peak amperage.

Management

Subtabs: Budget | Profiles

The Budget tab allows you to view the Power Inventory attributes like System Idle Power and System Maximum Potential Power in Watts and BTU/hr. You can also use the Power Budget option to Enable Power Cap and set the Power Cap for your system.

The Profiles tab allows you to choose a power profile to maximize your system's performance and conserve energy.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Use the Alert Actions tab to set system alert actions for various system events like System Power Probe Warning and System Peak Power.

Use the SNMP Traps tab to configure SNMP traps for your system.

Certain Power Management features may be available only on systems enabled with the Power Management Bus (PMBus).

Power Supplies

Click the Power Supplies object to manage your system's power supplies. Server Administrator monitors power supply status, including redundancy, to ensure that each power supply present in your system is functioning properly. The Power Supplies object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Elements

Under the **Properties** tab, you can:

• View information about your power supply redundancy attributes.

• Check the status of individual power supply elements, including the Rated Input Wattage and Maximum Output Wattage. The Rated Input Wattage attribute are displayed only on PMBus systems starting *xx1x*.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a system power returns a warning or failure value.
- Configure Platform Event Alert destinations for IPv6 addresses.
- View current SNMP trap alert thresholds and set the alert threshold levels for system power watts. The selected traps are triggered if the system generates a corresponding event at the selected severity level.

NOTE: The System Peak Power trap generates events only for informational severity.

Processors

Click the **Processors** object to manage your system's microprocessor(s). A processor is the primary computational chip inside a system that controls the interpretation and execution of arithmetic and logic functions. The **Processors** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.
Properties

Subtab: Information

Under the **Properties** tab, you can view information about your system's microprocessor(s) and access detailed capabilities and cache information.

Alert Management

Subtabs: Alert Actions

Under the **Alert Management** tab, you can view current alert actions settings and set the alert actions that you want to be performed in the event that a processor returns a warning or failure value.

Remote Access

Click the **Remote Access** object to manage the Baseboard Management Controller (BMC) or Integrated Dell Remote Access Controller (iDRAC) features and Remote Access Controller features.

Selecting Remote Access tab allows you to manage the BMC/iDRAC features such as, general information on the BMC/iDRAC. You can also manage the configuration of the BMC/iDRAC on a local area network (LAN), serial port for the BMC/iDRAC, terminal mode settings for the serial port, BMC/iDRAC on a serial over LAN connection, and BMC/iDRAC users.

NOTE: BMC is supported in Dell PowerEdge *x8xx* and *x9xx* systems and iDRAC is supported in Dell *xx0x* and *xx1x* systems only.

NOTE: If an application other than Server Administrator is used to configure the BMC/iDRAC while Server Administrator is running, the BMC/iDRAC configuration data displayed by Server Administrator may become asynchronous with the BMC/iDRAC. It is recommended that Server Administrator be used to configure the BMC/iDRAC while Server Administrator is running.

DRAC allows you to access your system's remote system management capabilities. The Server Administrator DRAC provides remote access to inoperable systems, alert notification when a system is down, and the ability to restart a system.

The **Remote Access** object action window can have the following tabs, depending on the user's group privileges: **Properties**, **Configuration**, and **Users**.

Properties

Subtab: Information

Under the **Properties** tab, you can view general information on the remote access device. You can also view the attributes of the IPv4 and IPv6 addresses.

Click **Reset to Defaults** to reset all the attributes to their system default values.

Configuration

Subtabs: LAN | Serial Port | Serial Over LAN |Additional Configuration

Under the **Configuration** tab when BMC/iDRAC is configured, you can configure the BMC/iDRAC on a LAN, serial port for BMC/iDRAC, and BMC/iDRAC on a serial over LAN connection.

NOTE: The **Additional configuration** tab is available only on systems with iDRAC.

Under the **Configuration** tab, when DRAC is configured, you can:

Configure network properties

NOTE: The **Enable NIC**, **NIC Selection**, and **Encryption Key** fields display only on Dell PowerEdge *x9xx* systems.

Under the Additional Configuration tab you can either enable or disable IPv4/IPv6 properties.

NOTE: Enabling/disabling IPv4/IPv6 is possible only in a dual stack environment (where both the IPv4 and IPv6 stacks are loaded).

Users

Subtab: Users

Under the **Users** tab, you can modify the remote access user configuration. You can add, configure, and view information about Remote Access Controller users.

NOTE: On the Dell PowerEdge *x9xx* systems:
- Ten user IDs are displayed. If a DRAC card is installed, sixteen user IDs are displayed.
- Serial Over LAN Payload column is displayed.

Removable Flash Media

Click the **Removable Flash Media** object to view the health and redundancy status of the Internal SD Modules and vFlash media. The Removable Flash Media action window has the **Properties** tab.

Properties

Subtab: Information

Under the **Properties** tab, you can view information about the Removable Flash Media and Internal SD Modules. This includes details about the Connector Name, its state and storage size.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that the removable flash media probe returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for removable flash media probes. The selected traps are triggered if the system generates a corresponding event at the selected severity level.

Alert management is common for Internal SD modules and vFlash. Configuring alert actions/SNMP/PEF for either the SD modules or vFlash automatically configures it for the other.

Slots

Click the **Slots** object to manage the connectors or sockets on your system board that accept printed circuit boards, such as expansion cards. The **Slots** object action window has a **Properties** tab.

Properties

Subtab: Information

Under the **Properties** tab, you can view information about each slot and installed adapter.

Temperatures

Click the **Temperatures** object to manage your system temperature in order to prevent thermal damage to your system's internal components. Server Administrator monitors the temperature in a variety of locations in your system's chassis to ensure that temperatures inside the chassis do not become too high. The **Temperatures** object action window displays the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Temperature Probes

Under the **Properties** tab, you can view the current readings and status for your system's temperature probes and configure minimum and maximum values for temperature probe warning threshold.

NOTE: Some temperature probe fields differ according to the type of firmware your system has: BMC or ESM. Some threshold values are not editable on BMC-based systems. When assigning probe threshold values, Server Administrator sometimes rounds the minimum or maximum values you enter to the closest assignable value.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a temperature probe returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for temperature probes. The selected traps are triggered if the system generates a corresponding event at the selected severity level.

NOTE: You can set minimum and maximum temperature probe threshold values for an external chassis to whole numbers only. If you attempt to set either the minimum or maximum temperature probe threshold value to a number that contains a decimal, only the whole number before the decimal place is saved as the threshold setting.

Voltages

Click the **Voltages** object to manage voltage levels in your system. Server Administrator monitors voltages across critical components in various chassis locations in the monitored system. The **Voltages** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Voltage Probes

Under the **Properties** tab, you can view the current readings and status for your system's voltage probes and configure minimum and maximum values for voltage probe warning threshold.

NOTE: Some voltage probe fields differ according to the type of firmware your system has: BMC or ESM. Some threshold values are not editable on BMC-based systems.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a system voltage sensor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for voltage sensors. The selected traps are triggered if the system generates a corresponding event at the selected severity level.

Software

Click the **Software** object to view detailed version information about the managed system's essential software components, such as the operating system and the systems management software. The **Software** object action window has the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Summary

Under the **Properties** tab, you can view a summary of the monitored system's operating system and system management software.

Operating System

Click the **Operating System** object to view basic information about your operating system. The **Operating System** object action window has the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view basic information about your operating system.

Storage

Server Administrator provides the Storage Management Service:

The Storage Management Service provides features for configuring storage devices. In most cases, the Storage Management Service is installed using **Typical Setup**. The Storage Management Service is available on Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems.

When the Storage Management Service is installed, click the **Storage** object to view the status and settings for various attached array storage devices, system disks, and so on.

In the case of Storage Management Service, the **Storage** object action window has the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Health

Under the **Properties** tab, you can view the health or status of attached storage components and sensors such as array subsystems and operating system disks.

Managing Preferences: Home Page Configuration Options

The left pane of the Preferences home page (where the system tree is displayed on the Server Administrator home page) displays all available configuration options in the system tree window. The options displayed are based on the systems management software installed on the managed system.

The available Preferences home page configuration options are:

- General Settings
- Server Administrator

General Settings

Click the **General Settings** object to set user and DSM SA Connection Service (Web server) preferences for selected Server Administrator functions. The **General Settings** object action window has the following tabs, depending on the user's group privileges: **User** and **Web Server**.

User

Subtab: Properties

Under the **User** tab, you can set user preferences, such as the home page appearance and the default e-mail address for the **Email** button.

Web Server

Subtabs: Properties | X.509 Certificate

Under the **Web Server** tab, you can:

- Set DSM SA Connection Service preferences. See "Dell Systems Management Server Administration Connection Service and Security Setup" for instructions on configuring your server preferences.
- Configure the SMTP server address and Bind IP address in either the IPv4 or IPv6 addressing mode.
- Perform X.509 certificate management by generating a new X.509 certificate, reusing an existing X.509 certificate, or importing a root certificate or certificate chain from a Certification Authority (CA). For more information about certificate management, see "X.509 Certificate Management" on page 63.

Server Administrator

Click the **Server Administrator** object to enable or disable access to users with User or Power User privileges and to configure the SNMP root password. The **Server Administrator** object action window can have the following tab, depending on the user's group privileges: **Preferences**.

Preferences

Subtabs: Access Configuration | SNMP Configuration

Under the **Preferences** tab, you can:

- Enable or disable access to users with User or Power User privileges.
- Configure the SNMP root password.

NOTE: The default SNMP configuration user is `root` and the password is `calvin`.

- Configure the SNMP Set Operations.

NOTE: The defAfter configuring SNMP Set Operations, services must be restarted for the change to take effect. On systems running supported Microsoft Windows operating systems, the Windows SNMP Service must be restarted. On systems running supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, Server Administrator services must be restarted by running the `srvadmin-services.sh` restart command.

5

Working With Remote Access Controller

NOTE: *Baseboard Management Controller (BMC)* is supported on Dell PowerEdge *x8xx* and *x9xx* systems and the *Integrated Dell Remote Access Controller (iDRAC)* is supported on Dell *xx0x* and *xx1x* systems.

Overview

This chapter provides information on accessing and using the remote access features of BMC/iDRAC and DRAC.

The Dell systems baseboard management controller (BMC)/Integrated Dell Remote Access Controller (iDRAC) monitors the system for critical events by communicating with various sensors on the system board and sends alerts and log events when certain parameters exceed their preset thresholds. The BMC/iDRAC supports the industry-standard Intelligent Platform Management Interface (IPMI) specification, enabling you to configure, monitor, and recover systems remotely.

The DRAC is a systems management hardware and software solution designed to provide remote management capabilities, crashed system recovery, and power control functions for Dell systems.

By communicating with the system's baseboard management controller (BMC)/ Integrated Dell Remote Access Controller (iDRAC), the DRAC can be configured to send you e-mail alerts for warnings or errors related to voltages, temperatures, and fan speeds. The DRAC also logs event data and the most recent crash screen (available only on systems running Microsoft Windows operating system) to help you diagnose the probable cause of a system crash.

The Remote Access Controller provides remote access to an inoperable system, allowing you to get the system up and running as quickly as possible. The Remote Access Controller also provides alert notification when a system is down and allows you to remotely restart a system. Additionally, the Remote Access Controller logs the probable cause of system crashes and saves the *most recent crash screen*.

You can log in to the Remote Access Controller through the Server Administrator home page or by directly accessing the controller's IP address using a supported browser.

When using the Remote Access Controller, you can click **Help** for more detailed information about the specific window you are viewing. Remote Access Controller help is available for all windows accessible to the user based on user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed system.

NOTE: See the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* for more information about the BMC.

NOTE: See the *Dell Remote Access Controller 4 User's Guide* for more information on using DRAC 4 or *Dell Remote Access Controller 5 User's Guide* for more information on using DRAC 5.

NOTE: See the *Integrated Dell Remote Access Controller User's Guide* for detailed information on configuring and using the iDRAC.

Table 5-1 lists the GUI field names and the applicable system, when Server Administrator is installed on the system.

Table 5-1. System Availability for the following GUI Field Names

GUI Field Name	Applicable System
`Modular Enclosure`	Modular System
`Server Modules`	Modular System
`Main System`	Modular System
`System`	Non-Modular System
`Main System Chassis`	Non-Modular System

See the *Dell Systems Software Support Matrix* for more information on the systems support for remote access devices.

Server Administrator allows remote, in-band access to event logs, power control, and sensor status information and provides the ability to configure the BMC/iDRAC. To manage BMC/iDRAC and DRAC through the Server Administrator graphical user interface, click the **Remote Access** object, which is a subcomponent of the **Main System Chassis/Main System** group.

You can perform the following tasks:

- View basic information
- Configure the remote access device on a LAN connection
- Configure the remote access device on a serial over LAN connection
- Configure the remote access device on a serial port connection
- Configure Additional remote access device properties
- Configure users on the remote access device
- Set platform event filter alerts

You can view BMC/iDRAC or DRAC information based on which hardware is providing the remote access capabilities for the system.

The reporting and configuration of BMC/iDRAC and DRAC can also be managed using the `omreport/omconfig chassis remoteaccess` CLI command.

In addition, the Server Administrator Instrumentation Service allows you to manage the Platform Event Filters (PEF) parameters and alert destinations.

NOTE: You can view BMC data on Dell PowerEdge *x8xx* and *x9xx* systems only.

Viewing Basic Information

You can view basic information about the BMC/iDRAC, IPv4 Address, and DRAC. You can also reset the Remote access controller settings to their default values. To do this:

NOTE: You must be logged in with Administrator privileges to reset the BMC settings.

Click the **Modular Enclosure→ System/Server Module→ Main System Chassis/Main System→ Remote Access**.

The **Remote Access** page displays the following base information of the system's BMC:

Remote Access Device

- Device type
- IPMI Version
- System GUID
- Number of Possible Active Sessions

- Number of Current Active Sessions
- LAN Enabled
- SOL Enabled
- MAC Address

IPv4 Address

- IP Address Source
- IP Address
- IP Subnet
- IP Gateway

IPv6 Address

- IP Address Source
- IPv6 Address 1
- Default Gateway
- IPv6 Address 2
- Link Local Address
- DNS Address Source
- Preferred DNS Server
- Alternate DNS Server

NOTE: You can view IPv4 and IPv6 address details only if you enable the IPv4 and IPv6 address properties under **Additional Configuration** in the **Remote Access** tab.

Configuring the Remote Access Device to use a LAN Connection

You can configure the remote access device for communication over a LAN connection.

1. Click the **Modular Enclosure→ System/Server Module→ Main System Chassis/Main System→ Remote Access** object.
2. Click the **Configuration** tab.

3 Click **LAN**.

The **LAN Configuration** window appears.

NOTE: BMC/iDRAC management traffic does not function properly if the LAN on motherboard (LOM) is teamed with any network adapter add-in-cards.

4 Configure the following NIC configuration details:

– Enable NIC (this option is available on Dell PowerEdge *x9xx* systems and when DRAC is installed. Select this option for NIC teaming. In Dell PowerEdge *x9xx* systems, you can team NICs for added redundancy.)

NOTE: Your DRAC contains an integrated 10BASE-T/100BASE-T Ethernet NIC and supports TCP/IP. The NIC has a default address of 192.168.20.1 and a default gateway of 192.168.20.1.

NOTE: If your DRAC is configured to the same IP address as another NIC on the same network, an IP address conflict occurs. The DRAC stops responding to network commands until the IP address is changed on the DRAC. The DRAC must be reset even if the IP address conflict is resolved by changing the IP address of the other NIC.

NOTE: Changing the IP address of the DRAC causes the DRAC to reset. If SNMP polls the DRAC before it initializes, a temperature warning is logged because the correct temperature is not transmitted until the DRAC is initialized.

– NIC Selection

NOTE: **NIC Selection** cannot be configured on modular systems.

– Enable IPMI Over LAN

– IP Address Source

– IP Address

– Subnet Mask

– Gateway Address

– Channel Privilege Level Limit

– New Encryption Key (This option is available on Dell PowerEdge *x9xx* systems.)

5 Configure the following optional VLAN configuration details:

NOTE: VLAN configuration is not applicable for systems with iDRAC

- Enable VLAN ID
- VLAN ID
- Priority

6 Configure the following IPv4 Properties:

- IP Address Source
- IP Address
- Subnet Mask
- Gateway Address

7 Configure the following IPv6 Properties:

- IP Address Source
- IP Address
- Prefix Length
- Default Gateway
- DNS Address Source
- Preferred DNS Server
- Alternate DNS Server

NOTE: You can configure the IPv4 and IPv6 address details only if you enable the IPv4 and IPv6 properties under **Additional Configuration**.

8 Click **Apply Changes**.

Configuring the Remote Access Device to use a Serial Port Connection

You can configure the BMC for communication over a serial port connection. To do this:

1 Click the **Modular Enclosure→ System/Server Module→ Main System Chassis/Main System→ Remote Access**.

2 Click the **Configuration** tab.

3 Click **Serial Port**.

The **Serial Port Configuration** window appears.

4 Configure the following details:

- Connection Mode Setting
- Baud Rate
- Flow Control
- Channel Privilege Level Limit

5 Click **Apply Changes.**

6 Click **Terminal Mode Settings**.

In the **Terminal Mode Settings** window, you can configure terminal mode settings for the serial port.

Terminal mode is used for Intelligent Platform Interface Management (IPMI) messaging over the serial port using printable ASCII characters. Terminal mode also supports a limited number of text commands to support legacy, text-based environments. This environment is designed so that a simple terminal or terminal emulator can be used.

7 Specify the following customizations to increase compatibility with existing terminals:

- Line Editing
- Delete Control
- Echo Control
- Handshaking Control
- New Line Sequence
- Input New Line Sequence

8 Click **Apply Changes**.

9 Click **Back To Serial Port Configuration Window** to go to back to the **Serial Port Configuration** window.

Configuring the Remote Access Device to use a Serial Over LAN Connection

You can configure the BMC/iDRAC for communication over a serial over LAN (SOL) connection. To do this:

1. Click the **Modular Enclosure→ System/Server Module→ Main System Chassis/Main System→ Remote Access**.
2. Click the **Configuration** tab.
3. Click **Serial Over LAN**.

   The **Serial Over LAN Configuration** window appears.
4. Configure the following details:
   - Enable Serial Over LAN
   - Baud Rate
   - Minimum Privilege Required
5. Click **Apply Changes.**
6. Click **Advanced Settings** to further configure BMC.
7. In the **Serial Over LAN Configuration Advanced Settings** window, you may configure the following information:
   - Character Accumulate Interval
   - Character Send Threshold
8. Click **Apply Changes.**
9. Click **Go Back to Serial Over LAN Configuration** to return to the **Serial Over LAN Configuration** window.

Additional Configuration for iDRAC

You can configure the IPv4 and IPv6 properties using the **Additional Configuration** tab. To do this:

1. Click the **Modular Enclosure→ System/Server Module→ Main System Chassis/Main System→ Remote Access** object.
2. Click the **Configuration** tab.
3. Click **Additional Configuration.**

4 Configure the IPv4 and IPv6 properties as **Enabled** or **Disabled**.

5 Click **Apply Changes.**

Configuring Remote Access Device Users

Remote access device users can be configured using the **Remote Access** page. To access this page:

1 Click the **Modular Enclosure→ System/Server Module→ Main System Chassis/Main System→ Remote Access** object.

2 Click the **Users** tab.

The **Remote Access Users** window displays information about users that can be configured as BMC/iDRAC users.

3 Click **User ID** to configure a new or existing BMC/iDRAC user.

The **Remote Access User Configuration** window allows you to configure a specific BMC/iDRAC user.

4 Specify the following general information:

- Select **Enable User** to enable the user.
- Enter the name for the user in the **User Name** field.
- Select the **Change Password** check box.
- Enter a new password in the **New Password** field.
- Re-enter the new password in the **Confirm New Password** field.

5 Specify the following user privileges:

- Select the maximum LAN user privilege level limit.
- Select the maximum serial port user privilege granted.
- On Dell PowerEdge *x9xx* systems, select **Enable Serial Over LAN** to enable Serial Over LAN.

6 Specify the User group for DRAC/iDRAC user privileges.

7 Click **Apply Changes** to save changes.

8 Click **Back to Remote Access User Window** to go back to the **Remote Access Users** window.

NOTE: Six additional user entries are configurable when DRAC is installed. This results in a total of 16 users. The same username and password rules apply to BMC/iDRAC and RAC users. When DRAC/iDRAC6 is installed, all the 16 users entries are allocated to DRAC.

Setting Platform Event Filter Alerts

You can use the Server Administrator Instrumentation Service to configure the most relevant BMC features, such as Platform Event Filter (PEF) parameters and alert destinations. To do this:

1 Click the **System** object.

2 Click the **Alert Management** tab.

3 Click **Platform Events**.

The **Platform Events** window allows you to take individual action on specific platform events. You can select those events for which you want to take shutdown actions and generate alerts for selected actions. You can also send alerts to specific IP address destinations of your choice.

NOTE: You must be logged in with Administrator privileges to configure the BMC PEF Alerts.

NOTE: The **Enable Platform Event Filters Alerts** setting disables or enables PEF alert generation. It is independent of the individual platform event alert settings.

NOTE: **System Power Probe Warning** and **System Power Probe Failure** are not supported on Dell systems without PMBus support although Server Administrator allows you to configure them.

NOTE: On Dell PowerEdge 1900 systems, the **PS/VRM/D2D Warning, PS/VRM/D2D Failure,** and **Power Supply Absent** Platform Event Filters are not supported even though Server Administrator allows you to configure these Event Filters.

4 Choose the platform event for which you want to take shutdown actions or generate alerts for selected actions and click **Set Platform Events**.

The **Set Platform Events** window allows you to specify the actions to be taken if the system is to be shut down in response to a platform event.

5 Select one of the following actions:

- **None**
  Takes no action when the operating system is hung or has crashed.
- **Reboot System**
  Shuts down the operating system and initiates system startup, performing BIOS checks and reloading the operating system.
- **Power Cycle System**
  Turns the electrical power to the system off, pauses, turns the power on, and reboots the system. Power cycling is useful when you want to reinitialize system components such as hard drives.
- **Power Off System**
  Turns off the electrical power to the system.
- **Power Reduction**
  Throttles the CPU.

NOTE: Power reduction is not supported on all systems.

CAUTION: If you select a Platform Event shutdown action other than None or Power Reduction, your system shuts down forcefully when the specified event occurs. This shutdown is initiated by firmware and is done without first shutting down the operating system or any running applications.

6 Select the **Generate Alert** check box for the alerts to be sent.

NOTE: To generate an alert, you must select both **Generate Alert** and the **Enable Platform Events Alerts** settings.

7 Click **Apply Changes**.

8 Click **Go Back to Platform Events Page** to go back to the **Platform Event Filters** window.

Setting Platform Event Alert Destinations

You can also use the **Platform Event Filters** window to select a destination where an alert for a platform event is to be sent. Depending on the number of destinations that are displayed, you can configure a separate IP address for each destination address. A platform event alert is sent to each destination IP address that you configure.

1 Click **Configure Destinations** in the **Platform Event Filters** window.

The **Configure Destinations** window displays a number of destinations.

2 Click the number of the destination you want to configure.

NOTE: The number of destinations that you can configure on a given system may vary.

3 Select the **Enable Destination** check-box.

4 Click **Destination Number** to enter an individual IP address for that destination. This IP address is the IP address to which the platform event alert is sent.

5 Enter a value in the **Community String** field to act as a password to authenticate messages sent between a management station and a managed system. The community string (also called the community name) is sent in every packet between the management station and a managed system.

6 Click **Apply Changes**.

7 Click **Go Back to Platform Events Page** to go back to the **Platform Event Filters** window.

6

Server Administrator Logs

Overview

Server Administrator allows you to view and manage hardware, alert, and command logs. All users can access logs and print reports from either the Server Administrator home page or from its command line interface. Users must be logged in with Administrator privileges to clear logs or must be logged in with Administrator or Power User privileges to e-mail logs to their designated service contact.

See the *Dell OpenManage Server Administrator Command Line Interface User's Guide* for information about viewing logs and creating reports from the command line.

When viewing Server Administrator logs, you can click **Help** for more detailed information about the specific window you are viewing. Server Administrator log help is available for all windows accessible to the user based on user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed system.

Integrated Features

Click a column heading to sort by the column or change the sort direction of the column. Additionally, each log window contains several task buttons that can be used for managing and supporting your system.

Log Window Task Buttons

- Click **Print** to print a copy of the log to your default printer.
- Click **Export** to save a text file containing the log data (with the values of each data field separated by a customizable delimiter) to a destination you specify.
- Click **Email** to create an e-mail message that includes the log content as an attachment.
- Click **Clear Log** to erase all events from the log.

- Click **Save As** to save the log content in a **.zip** file.
- Click **Refresh** to reload the log content in the action window data area.

See "Task Buttons" for additional information about using the task buttons.

Server Administrator Logs

Server Administrator provides the following logs:

- "Hardware Log"
- "Alert Log"
- "Command Log"

Hardware Log

Use the hardware log to look for potential problems with your system's hardware components. On Dell PowerEdge *x8xx*, *x9xx*, and *xx1x* systems, the hardware log status indicator changes to critical status ( ) when the log file reaches 100 percent capacity. There are two available hardware logs, depending on your system: the Embedded System Management (ESM) log and the System Event Log (SEL). The ESM log and SEL are each a set of embedded instructions that can send hardware status messages to systems management software. Each component listed in the logs has a status indicator icon next to its name. A green check mark ( ) indicates that a component is healthy (normal). A yellow triangle containing an exclamation point ( ) indicates that a component has a warning (noncritical) condition and requires prompt attention. A red X ( ) indicates that a component has a failure (critical) condition and requires immediate attention. A blank space ( ) indicates that a component's health status is unknown.

To access the hardware log, click **System**, click the **Logs** tab, and click **Hardware**.

Information displayed in the ESM and SEL logs includes:

- The severity level of the event
- The date and time that the event was captured
- A description of the event

Maintaining the Hardware Log

The status indicator icon next to the log name on the Server Administrator homepage changes from normal status ( ) to noncritical status ( ) when the log file reaches 80 percent capacity. Be sure to clear the hardware log when it reaches 80 percent capacity. If the log is allowed to reach 100 percent capacity, the latest events are discarded from the log.

Alert Log

NOTE: If the Alert log displays invalid XML data (for example, when the XML data generated for the selection is not well formed), click **Clear Log** and then redisplay the log information.

Use the Alert log to monitor various system events. The Server Administrator generates events in response to changes in the status of sensors and other monitored parameters. Each status change event recorded in the Alert log consists of a unique identifier called the event ID for a specific event source category and an event message that describes the event. The event ID and message uniquely describe the severity and cause of the event and provide other relevant information such as the location of the event and the monitored component's previous state.

To access the Alert log, click **System**, click the **Logs** tab, and click **Alert**.

Information displayed in the Alert log includes:

- The severity level of the event
- The event ID
- The date and time that the event was captured
- The category of the event
- A description of the event

NOTE: The log history may be required for future troubleshooting and diagnostic purposes. Therefore, it is recommended that you save the log files.

See the *Server Administrator Messages Reference Guide* for detailed information about alert messages.

Command Log

NOTE: If the Command log displays invalid XML data (for example, when XML data generated for the selection is not well formed), click **Clear Log** and then redisplay the log information.

Use the Command log to monitor all of the commands issued by Server Administrator users. The Command log tracks logins, logouts, systems management software initialization, and shutdowns initiated by systems management software, and records the last time the log was cleared. The size of the command log file can be specified as per your requirement.

To access the Command log, click **System**, click the **Logs** tab, and click **Command**.

Information displayed in the Command log includes:

- The date and time that the command was invoked
- The user that is currently logged in to the Server Administrator home page or the CLI
- A description of the command and its related values

NOTE: The log history may be required for future troubleshooting and diagnostic purposes. Therefore, it is recommended that you save the log files.

7

Setting Alert Actions

Setting Alert Actions for Systems Running Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

When you set alert actions for an event, you can specify the action to display an alert on the server. To perform this action, Server Administrator sends a message to **/dev/console**. If the Server Administrator system is running an X Window System, you do not see that message by default. To see the alert message on a Red Hat Enterprise Linux system when the X Window System is running, you must start **xconsole** or **xterm -C** before the event occurs. To see the alert message on a SUSE Linux Enterprise Server system when the X Window System is running, you must start **xterm -C** before the event occurs.

When you set Alert Actions for an event, you can specify the action to **Broadcast a message.** To perform this action, Server Administrator executes the **wall** command, which sends the message to everybody logged in with their message permission set to **Yes.** If the Server Administrator system is running an X Window System, you do not see that message by default. To see the broadcast message when the X Window System is running, you must start a terminal such as **xterm** or **gnome-terminal** before the event occurs.

When you set Alert Actions for an event, you can specify the action to **Execute application.** There are limitations on the applications that Server Administrator can execute. Follow these guidelines to ensure proper execution:

- Do not specify X Window System based applications because Server Administrator cannot execute such applications properly.
- Do not specify applications that require input from the user because Server Administrator cannot execute such applications properly.

- Redirect **stdout** and **stderr** to a file when specifying the application so that you can see any output or error messages.
- If you want to execute multiple applications (or commands) for an alert, create a script to do that and put the full path to the script in the **Absolute path to the application** box.

  Example 1:

  ```
  ps -ef >/tmp/psout.txt 2>&1
  ```

  The command in Example 1 executes the application **ps**, redirects **stdout** to the file **/tmp/psout.txt**, and redirects **stderr** to the same file as **stdout**.

  Example 2:

  ```
  mail -s "Server Alert" admin </tmp/alertmsg.txt
  >/tmp/mailout.txt 2>&1
  ```

  The command in Example 2 executes the mail application to send the message contained in the file **/tmp/alertmsg.txt** to Red Hat Enterprise Linux user or SUSE Linux Enterprise Server user, and Administrator, with the subject **Server Alert.** The file **/tmp/alertmsg.txt** must be created by the user before the event occurs. In addition, **stdout** and **stderr** are redirected to the file **/tmp/mailout.txt** in case an error occurs.

Setting Alert Actions in Microsoft Windows Server 2003 and Windows Server 2008

When specifying alert actions, Visual Basic scripts are not automatically interpreted by the Execute Application feature, although you can run a `.cmd`, `.com`, `.bat`, or `.exe` file by only specifying the file as the alert action.

To resolve this issue, first call the command processor `cmd.exe` to start your script. For example, the alert action value to execute an application can be set as follows:

```
c:\winnt\system32\cmd.exe /c d:\example\example1.vbs
```

where `d:\example\example1.vbs` is the full path to the script file.

Do not set a path to an interactive application (an application that has a Graphical User Interface or which requires user input) in the Absolute path to the application field. The interactive application may not work as expected on some operating systems.

NOTE: The full path to both the cmd.exe file and your script file should be specified.

Setting Alert Action Execute Application in Windows Server 2008

For security reasons, Windows Server 2008 is configured to not allow interactive services. When a service is installed as an interactive service on Windows Server 2008, the operating system logs an error message to the Windows System log about the service being marked as an interactive service.

When you use Server Administrator to configure Alert Actions for an event, you can specify the action to *execute an application*. In order for interactive applications to execute properly for an Alert Action, the Dell Systems Management Server Administrator (DSM SA) Data Manager service must be configured as an interactive service. Examples of interactive applications are applications with a Graphical User Interface (GUI) or that prompt the user for input in some way such as the *pause* command in a batch file.

When Server Administrator is installed on Microsoft Windows Server 2008, the DSM SA Data Manager service is installed as a non-interactive service which means that it is configured to not be allowed to interact with the desktop by default. This means that interactive applications are not executed properly when executed for an Alert Action. If an interactive application is executed for an Alert Action in this situation, the application is suspended and waits for an input. The application interface/prompt is not visible to you and remains invisible even after the Interactive Services Detection service is started. The **Processes** tab in the **Task Manager** displays an application process entry for each execution of the interactive application.

If you need to execute an interactive application for an Alert Action on Microsoft Windows Server 2008, you must configure the DSM SA Data Manager service to be allowed to interact with the desktop.

To allow interaction with the desktop:

1. Right-click on the DSM SA Data Manager service in the **Services control** panel and select Properties.
2. In the **Log On** tab, enable **Allow service to interact with desktop** and click **OK**.
3. Restart the DSM SA Data Manager service for the change to take effect.

When the DSM SA Data Manager service is restarted with this change, the Service Control Manager logs the following message to the System log: `The DSM SA Data Manager service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly`. This change allows the DSM SA Data Manager service to execute interactive applications properly for an Alert Action. Also ensure that the Interactive Services Detection service is running in order to see the interface/prompt displayed by the interactive application. Once these changes are made, the **Interactive services dialog detection** dialog box is displayed by the operating system to provide access to the interactive application interface/prompt.

BMC/iDRAC Platform Events Filter Alert Messages

All possible Platform Event Filter (PEF) messages along with a description of each event is listed in Table 7-1.

Table 7-1. PEF Alert Events

Event	Description
Fan Probe Failure	The fan is running too slow or not at all.
Voltage Probe Failure	The voltage is too low for proper operation.
Discrete Voltage Probe Failure	The voltage is too low for proper operation.
Temperature Probe Warning	The temperature is approaching excessively high or low limits.
Temperature Probe Failure	The temperature is either too high or too low for proper operation.

Table 7-1. PEF Alert Events *(continued)*

Event	Description
Chassis Intrusion Detected	The system chassis has been opened.
Redundancy (PS or Fan) Degraded	Redundancy for the fans and/or power supplies has been reduced.
Redundancy (PS or Fan) Lost	No redundancy remains for the system's fans and/or power supplies.
Processor Warning	A processor is running at less than peak performance or speed.
Processor Failure	A processor has failed.
PPS/VRM/DCtoDC Warning	The power supply, voltage regulator module, or DC to DC converter is pending a failure condition.
Power Supply/VRM/D2D Failure	The power supply, voltage regulator module, or DC to DC converter has failed.
Hardware log is full or emptied	Either an empty or a full hardware log requires administrator attention.
Automatic System Recovery	The system is hung or is not responding and is taking an action configured by Automatic System Recovery.
System Power Probe Warning	The power consumption is approaching the failure threshold.
System Power Probe Failure	The power consumption has crossed the highest acceptable limit and has resulted in a failure.
Removable Flash Media Present	The removable flash media is present.
Removable Flash Media Failure	The removable flash media is pending a failure condition.
Removable Flash Media Warning	The removable flash media is present.

Understanding Service Names

The service executable and display names of the following services have changed:

Table 7-2. Service Names

Purpose	Service Name	Previous Release (prior to 5.0)	Current Release
Web Server	Display Name	Secure Port Server	DSM SA Connection Service
	Executable Name	Omaws[32|64]	dsm_om_connsvc
			dsm_om_connsvc
Scheduling or Notification	Display Name	OM Common Services	DSM SA Shared Services
	Executable Name	Omsad[32|64]	dsm_om_shrsvc
			dsm_om_shrsvc

A

Troubleshooting

Connection Service Failure

On Red Hat Enterprise Linux, when `SELinux` is set to `enforced` mode, the Dell Systems Management Server Administrator (DSM SA) Connection service fails to start. Perform any one of the following steps and start this service:

- Set `SELinux` to `Disabled` mode or to `Permissive` mode.
- Change the SELinux **allow_execstack** property to **ON** state. Run the following command:

  ```
  setsebool   allow_execstack   on
  ```

- Change the security context for the DSM SA connection service. Run the following command:

  ```
  chcon -t unconfined_execmem_t
  /opt/dell/srvadmin/sbin/dsm_om_connsvcd
  ```

Login Failure Scenarios

You may not be able to login to the Managed System if:

- You enter an invalid/incorrect IP address.
- You enter incorrect credentials (user name and password).
- The Managed System is OFF.
- The Managed System is not reachable due to an invalid IP address or a DNS error.
- The Managed System has an untrusted certificate and you do not select the **Ignore Certificate Warning** in the login page.
- Server Administrator services are not enabled on the VMware ESX/ESXi system. See the *Dell OpenManage Server Administrator Installation Guide* for information on how to enable Server Administrator Services on the VMware ESX/ESXi system.

- The small footprint CIM broker daemon (SFCBD) service on the VMware ESX/ESXi system is not running.
- The Web Server Management Service on the managed system is not running.
- You enter the IP address of the managed system and not the hostname, when you don't check the **Ignore Certificate Warning** Check box.
- The WinRM Authorization feature (Remote Enablement) is not configured in the managed system. For information on this feature, see the *Dell OpenManage Server Administrator Installation Guide*.
- There is an authentication failure while connecting to a VMware ESXi 4.1/ESX 4.1 operating system, which may occur due to any of the following reasons:
  - The `lockdown` mode is enabled either while you are logging to the server or while you are logged into the Server Administrator. For more information on `lockdown` mode, see VMware documentation.
  - The password is changed while you are logged into Server Administrator.
  - You log in to Server Administrator as a normal user without administrator privileges. For more information, see the VMware documentation on assigning the role.

Fixing a Faulty Server Administrator Installation on Supported Windows Operating Systems

You can fix a faulty installation by forcing a reinstall and then performing an uninstall of Server Administrator.

To force a reinstall:

1. Check the version of Server Administrator that was previously installed.
2. Download the installation package for that version from **support.dell.com.**
3. Locate **SysMgmt.msi** in the **srvadmin\windows\SystemsManagement** directory.
4. Type the following command at the command prompt to force a reinstall

   ```
   msiexec /i SysMgmt.msi REINSTALL=ALL
   REINSTALLMODE=vamus
   ```

5 Select **Custom Setup** and choose all the features that were originally installed. If you are not sure which features were installed, select all features and perform the installation.

NOTE: If you have installed Server Administrator in a non-default directory, ensure to change it in the **Custom Setup** as well.

6 After the application is installed, you can uninstall Server Administrator using **Add/Remove Programs**.

OpenManage Server Administrator Services

This table lists the services used by Server Administrator to provide systems management information and the impact of these services failing.

Table A-1. OpenManage Server Administrator Services

Service Name	Description	Impact of failure	Recovery Mechanism	Severity
Windows: DSM SA Connection Service Linux: dsm_om_connsvc (This service is installed with the Server Administrator Web server.)	Provides remote/local access to Server Administrator from any system with a supported Web browser and network connection.	Users are not able to login to Server Administrator and perform any operation through the Web user interface. However, CLI can still be used.	Restart Service	Critical

Table A-1. OpenManage Server Administrator Services *(continued)*

Service Name	Description	Impact of failure	Recovery Mechanism	Severity
Common Service				
Windows: DSM SA Shared Services Linux: dsm_om_shrsvc (This service runs on the Managed system.)	Runs inventory collector at startup to perform a software inventory of the system to be consumed by Server Administrator's SNMP and CIM providers to perform a remote software update using Dell System Management Console and Dell IT Assistant (ITA).	Software updates are not possible using ITA. However, the updates can still be done locally and outside of Server Administrator using individual Dell Update packages. Updates can still be performed using 3rd party tools (for example, MSSMS, Altiris and Novell ZENworks).	Restart Service	Warning

NOTE: If the 32-bit compatibility libraries are not installed on a 64-bit Linux system, the shared services fail to start the inventory collector and display the error message `libstdc++.so.5 is required to run the Inventory Collector.` The srvadmin-cm.rpm provides the binaries for the inventory collector. For the list of RPMs that srvadmin-cm depends on, see the *Dell OpenManage Server Administrator Installation Guide*.

Table A-1. OpenManage Server Administrator Services *(continued)*

Service Name	Description	Impact of failure	Recovery Mechanism	Severity
		Instrumentation Services		
Windows: DSM SA Data Manager Linux: dsm_sa_datamgrd (hosted under dataeng service) (This service runs on the Managed system.)	Monitors the system, provides rapid access to detailed fault and performance information and allows remote administration of monitored systems, including shutdown, startup, and security.	Users are not able to configure/view the hardware level details on GUI/CLI without these services running.	Restart Service	Critical
DSM SA Event Manager (Windows) Linux: dsm_sa_eventmgrd (hosted under dataeng service) (This service runs on the Managed system.)	Provides operating system and file event logging service for systems management and is also used by event log analyzers.	If this service is stopped, event logging features do not function properly.	Restart Service	Warning
Linux: dsm_sa_snmpd (hosted under dataeng service) (This service runs on the Managed system.)	Data Engine Linux SNMP Interface	SNMP get/set /trap request is not functional from a management station.	Restart Service	Critical

Table A-1. OpenManage Server Administrator Services *(continued)*

Service Name	Description	Impact of failure	Recovery Mechanism	Severity
	Storage Management Service			
Windows: mr2kserv (This service runs on the Managed system.)	The Storage Management Service provides storage management information and advanced features for configuring a local or remote storage attached to a system.	User are not able to perform storage functions for all supported RAID and non-RAID controllers.	Restart Service	Critical

B

Frequently Asked Questions

This section lists the frequently asked questions about Dell OpenManage Server Administrator:

NOTE: These questions are not specific to this release of Server Administrator.

1 **Why does ESXi 4.0.x (4.0 U1/U2) host rebooting functionality fail from OpenManage Server Administrator?**

This issue is due to VMware stand-alone license (SAL) key. See the Knowledge Base article at kb.vmware.com/kb/1026060 for more information.

2 **What are the tasks that need to be performed after adding a VMware ESX 4.1 operating system to the active directory domain?**

After adding a VMware ESX 4.1 operating system to the Active Directory domain, an Active Directory user must do the following:

- Log in to the Server Administrator while using the VMware ESX 4.1 operating system as a Server Administrator and restart the DSM SA Connection Service.
- Log in to the Remote Node while using the VMware ESX 4.1 operating system as a Remote Enablement Agent. Wait for approximately 5 minutes for the sfcbd process to add the permission to the new user.

3 **What is the minimum permission level a user would need to install Server Administrator?**

You need to have a minimum permission level of **Administrator** to install Server Administrator. Power Users and Users do not have permissions to install Server Administrator.

4 **Is there an upgrade path required to install Server Administrator?**

For systems that have version Server Administrator 4.3, an upgrade path is not required. For systems that have a version older than 4.3, you need to

first upgrade to version 4.3, and then again upgrade to a 6.x version (x indicates the version of Server Administrator you want to upgrade to).

5 How do I determine what is the latest version of Server Administrator available for my system?

Log on to: **support.dell.com→ Enterprise IT→ Manuals→ Software→ Systems Management → Dell OpenManage Server Administrator**

The latest documentation version reflects the version of OpenManage Server Administrator available for you.

6 How do I know what version of Server Administrator is running on my system?

After logging in to Server Administrator, navigate to **Properties→ Summary**. You can find the version of Server Administrator installed on your system in the **Systems Management** column.

7 Are there other ports users can use apart from 1311?

Yes, you can set your preferred https port. Navigate to **Preferences→ General Settings→Web Server→HTTPS Port**

Instead of **Use default**, click on the **Use radio button to set your preferred port**.

NOTE: Changing the port number to an invalid or in-use port number might prevent other applications or browsers from accessing Server Administrator on the managed system. See the *Dell OpenManage Installation and Security User's Guide* for the list of default ports.

8 Can I install Server Administrator on Fedora, College Linux, Mint, Ubuntu, Sabayon or PClinux?

No, Server Administrator does not support any of these Operating Systems.

9 Can Server Administrator send e-mails when there is a problem?

No, Server Administrator is not designed to send e-mails when there is a problem.

10 Is SNMP Required for ITA Discovery, inventory and software updates on PowerEdge systems? Can CIM be used by itself for discovery, inventory, and updates or is SNMP required?

ITA communicating with Linux systems:

SNMP is required on the Linux system for discovery, status polling and inventory.

Dell software updates are done through an SSH session and secure FTP and root level permissions/credentials are required for this discrete action and asked for when the action is setup or requested. Credentials from the discovery range are not assumed.

ITA *communicating with Windows systems:*

For servers (systems running Windows Server operating systems), the system may be configured with either or both of SNMP and CIM for discovery by ITA. Inventory requires CIM.

Software updates, as in Linux, are not related to discovery and polling and the protocols used.

Using Administrator level credentials asked for at the time the update is scheduled or performed, an administrative (drive) share is established to a drive on the target system, and file(s) copying from somewhere (possibly another network share) is done to the target system. WMI functions are then invoked to execute the software update.

As Server Administrator is not installed on Clients/Workstations, so CIM discovery is used when the target is running the OpenManage Client Instrumentation.

For many other devices such as network printers, the standard is still SNMP to communicate with (primarily discover) the device.

Devices such as EMC storage have proprietary protocols. Some information about this environment can be gathered from looking at the ports used tables in the OpenManage documentation.

11 Are there any plans for SNMP v3 support?

No, there are no plans for SNMP v3 support.

12 Does an Underscore character in the domain name cause Server Admin login issues?

Yes, an underscore character in the domain name is invalid. All other special characters (except the hyphen) are invalid too. Use only case-insensitive alphabets and numerals.

13 How does checking/unchecking the 'Active Directory' on the login page of Server Administrator impact privilege levels?

If you do not select the Active Directory check box, you will only have access that is configured in the Microsoft Active Directory. You cannot log in using the Dell Extended Schema Solution in Microsoft Active Directory. This solution enables you to provide access to Server Administrator; allowing you to add/control Server Administrator users and privileges to existing users in your Active Directory software. For more information see "Using Microsoft Active Directory" in the *Dell OpenManage Server Administrator Installation Guide*.

14 What actions do I follow while performing Kerberos authentication and trying to login from Web Server?

For authentication, the contents of the files **/etc/pam.d/openwsman** and **/etc/pam.d/sfcb**, on the managed node, must be replaced with:

For 32-bit:

```
auth required pam_stack.so service=system-auth
auth required /lib/security/pam_nologin.so
account required pam_stack.so service=system-auth
```

For 64-bit:

```
auth required pam_stack.so service=system-auth
auth required /lib64/security/pam_nologin.so
account required pam_stack.so service=system-auth
```

Index

A

about
server, 9

action window, of home page, 55

administer, Server Administrator, 19

alert, 75-82, 85-86, 89-90

alert actions, Red Hat Enterprise Linux, 116

alert messages, BMC, 112

assign, user privileges, 22

authentication
for Red Hat Enterprise Linux, 21
for Windows, 21
Server Administrator, 21
single sign-on, 48-49

B

Bind IP address, 92

BIOS, manage, 78

BMC, 86, 93
about, 93
alert messages, 112
configuring users, 101
filter alerts, 102
viewing basic details, 95
working with, 93

BMC, manage, 86

browser setting, Windows, 50-51

C

certificate management
X.509, 63

chassis, 76

chassis, intrusion, 81

command line interface (CLI), 66

components of home page
action window, 55
data area, 56-57
navigation bar, 55
system tree, 55

configuring SNMP Agent, 27
for Red Hat Enterprise Linux, 32, 34-35
for Windows, 29-31

configuring, BMC users, 101

configuring, firewalls
for Red Hat Enterprise Linux, 43

configuring, SNMP Agent, 27, 29-32, 34-35

connectors, manage, 88

creating users
Red Hat Enterprise Linux, 24

creating users, Red Hat Enterprise Linux, 23-24
current, manage, 79

D

data area, of home page, 56-57
disabling users, for Windows, 27
documentation, related, 15

E

enabling SNMP
by remote hosts, 29
encryption, 22
Server Administrator, 22
Express Service Code, 12, 77

F

fans, manage, 79
firewalls, configuring for Red Hat Enterprise Linux, 43
firmware, manage, 80

G

gauge indicator, home page, 57

H

help, using, 58
home page
components, 55-57
gauge indicator, 57
preferences, 58
server, 14
status indicator, 56
system tree objects, 71
task button, 56
underlined item, 57
home page, managing
configuration options, 91
general settings, 91
Server Administrator, preferences, 92
user preferences, 91
Web server, 92
home page, Server Administrator, 51

I

installing, server, 9
instrumentation
server, 11
instrumentation service, 69
intrusion, manage, 81

L

Local Login, 47

logging in, Server Administrator, 45
logging out, Server Administrator, 45
logs, 74
about, 105-106, 109
alert log, 107
command log, 108
features, 105
hardware log, 106
server, 11

M

manage
current, 79
intrusion, 81
memory devices, 82
ports, 83
processors, 85
system, 70
temperatures, 88
management
alert, 75-82, 85-86, 89-90
certificate, X.509, 63, 92
security, 19
storage, 10
storage, enhanced, 91
X.509 certificate, 63
management information base, 32
Managing a Remote System, 46
memory devices, manage, 82
MIB, 32

N

navigation bar, of home page, 55
network properties, RAC, 102
network, managing, 82
Non-Masking Interrupt, 78

O

online help, using, 58
operating system
basic information, 90

P

port, 60
port, managing, 83
preferences of home page, 58
preferences, setting up, 60
privilege levels, Server Administrator, 20
privileges, types of
for Red Hat Enterprise Linux, 24
processors, manage, 85

R

RAC users
configuring existing user, 102

RAC, network properties, 102
Red Hat Enterprise Linux, 32
Red Hat Enterprise Linux, alert actions, 116
remote access, 11
  server, 11
remote access controller, managing, 86
Remote Login, 46
remote shutdown, 74
restarting, Server Administrator, 66

S

secure port, 60
security, 19, 48-49, 60
  access control, 19
  Server Administrator, 19
  user privileges, 19
security, management, 19
server
  home page, 14
  install, 9
  instrumentation, 11
  logs, 11
Server Administrator, 9
  about, 9
  adding users, 23
  authentication, 21
  controlling, 64
  disabling users, Windows, 27
  encryption, 22
  logs, 105, 109
  restarting, 66
  security, 19
  uses, 9
Server Administrator, logging in, 45
Server Administrator, logging out, 45
Server Administrator, logs, 105-108
Server Administrator, restarting, 66
  on Red Hat Enterprise Linux, 66
  on Windows, 66
Server Administrator, starting, 65
  on Red Hat Enterprise Linux, 65-66
  on Windows, 65
Server Administrator, stopping, 65
  on Red Hat Enterprise Linux, 65
  on Windows, 65
Server Administrator, using, 45
server features, integrated
  home page, 14
  installation, 9
  instrumentation, 11
  logs, 11
server port, 60
server preferences, 60
server storage management, 10

service, instrumentation, 69
session, Server Administrator, 45
setting, BMC filter alerts, 102
setup, Server Administrator, 19
Sever Administrator, CLI, 66
Sever Administrator, home page, 51
components, 55-57
preferences, 58
shutdown, 74
single sign-on, 48
Windows, 49
slots, manage, 88
SNMP
agent configuration, 33
SNMP Agent, configuring, 27, 29-32, 34-35
SNMP community name, changing, 30
SNMP community name, for Red Hat Enterprise Linux, 34
SNMP set operations, enabling, 31
SNMP set operations, Red Hat Enterprise Linux, 34
SNMP tables
reference guide content, 28
SNMP traps, configuring
for Red Hat Enterprise Linux, 35
for Windows, 31
sockets, manage, 88
software, 90
software details, view, 90
status indicator, home page, 56
stopping, Server Administrator, 65
storage, 91
Storage Management Service
about, 121
storage management service
enhanced, 91
storage, manage, 90
system, 73
managing, 70-71
system chassis, 76
system component, 56
system tree objects, 55, 70-71
system, managing, 70

T

task button, home page, 56
temperature, manage, 88
thermal, shutdown, 74
tree objects, home page, 71

U

underlined item, home page, 57
user preferences, 60

user privileges
  creating, for Red Hat Enterprise Linux, 24
  security, 19
user privileges, assigning, 22
users
  adding, 23
  creating, for Red Hat Enterprise Linux, 23-24
  disabling, for Windows, 27
uses of server, 9

V

viewing, BMC basic details, 95
voltage, manage, 89

W

Web server shutdown, 74