Dell OpenManage Server Administrator Version 7.4 User's Guide

Notes, Cautions, and Warnings

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

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

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Introduction

Server Administrator 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 enables system administrators to manage systems locally and remotely on a network. It enables 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 through 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*. 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 Server Administrator installer provides installation scripts and RPM packages to install and uninstall Server Administrator and other managed system software components on your managed system. For more information, see the *Server Administrator Installation Guide* and the *Management Station Software Installation Guide* at **dell.com/opemanagemanuals**.

NOTE: When you install the open source packages from the *Dell Systems Management Tools and Documentation* DVD, the corresponding license files are automatically copied to the system. When you remove these packages, the corresponding license files are also removed.

NOTE: 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 Update Utility* DVD to view the complete version report and to update an entire system. The Server Update Utility (SUU) identifies and applies the required updates to your system. SUU can also be downloaded from **support.dell.com.**

NOTE: 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, see the *Dell Server Update Utility User's Guide* at **dell.com/openmanagemanuals**.

Storage Management Service

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

NOTE: For more information about the Storage Management Service, see the *Server Administrator Storage Management* User's Guide at **dell.com/openmanagemanuals**.

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 the 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 an alert notification when a system is down and allows you to remotely restart the 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 Is New In This Release

The release highlights of Server Administrator are:

- Added support for the following operating systems:

  - Microsoft Windows Server 2012 R2 Datacenter, Foundation, Essentials, and Standard editions
  - Novell SUSE Linux Enterprise Server 11 SP3 (64-bit)
  - Red Hat Enterprise Linux 6.5 (64-bit)
  - VMware ESXi 5.0 U3 and ESXi 5.1 U2
  - VMware vSphere 5.5
- Added support for the following browsers:

  - Mozilla Firefox 22 and 23
  - Internet Explorer 11

- – Safari 6.0
- – Google Chrome 27, 28, and 30
- Support for a new license format for Citrix XenServer 6.1.
- Added support for the following adapter cards:

  - – Mellanox ConnectX-3 Dual Port 40 GbE QSFP+ Network Adapter
  - – Mellanox ConnectX-3 Dual Port 10 GbE DA/SFP+ Network Adapter
  - – Mellanox ConnectX-3 Dual Port 10 GbE KR Blade Mezzanine Card
  - – Emulex OCe14102-UX-D Dual Port 10Gb SFP+ CNA
  - – Emulex OCm14102-U3-D Dual Port 10Gb KR Blade Mezz
  - – Emulex OCm14102-U2-D Dual Port 10Gb KR Blade NDC
  - – Emulex OCm14104-UX-D Quad Port 10Gb DA/SFP+ Rack NDC

- Support for displaying and setting the JRE version. See [Secure Port System](#).
- Support for displaying Node Id in System/Server Module Summary information. See *Server Administrator Command Line Interface Guide* or online help.
- Support for new values for form factor aligning to iDRAC values. See *Server Administrator Command Line Interface Guide* or online help.
- Added support for Software RAID controllers (PERC S110) on systems running the Windows Server 2012 R2 operating system.
- Added support for Non-Volatile Memory Express (NVMe) Peripheral Component Interconnect Express (PCIe) solid-state drives (SSDs). See the *Server Administrator Storage Management* guide at **dell.com/ openmanagemanuals**.

  > **NOTE:** Management of Dell PowerEdge Express Flash NVMe PCIe SSD devices is supported only through Dell-provided Windows Server 2012 R2 (64-bit) drivers.

- Added support for Dell PERC 9 controllers (H730P Adapter) on R920 with the following features:

  - – RAID 10 virtual disk with uneven span.
  - – Advanced 4KB sector hard disk drives.
  - – T10 Protection Information (PI) for data integrity.

  > **NOTE:** For more information, see the *Server Administrator Storage Management* guide at **dell.com/openmanagemanuals**.

- Added support for the following LSI Serial Attached SCSI (SAS) Host Bus Adapters (HBAs) on supported 12G systems:

  - – LSI SAS 9207-8e
  - – LSI SAS 9300-8e
  - – LSI SAS 9206-16e

- Added support for the following Dell PowerEdge servers:

  - – R920
  - – R220
  - – M820VRTX

- Deprecated support for the following operating systems:

  - – SUSE Linux Enterprise Server 10 SP4
  - – SUSE Linux Enterprise Server 11 SP2

- Red Hat Enterprise Linux 6.4 (64-bit)
- VMware ESXi 5.1 U1 HDD and Flash
- VMware ESXi 5.0 U2 HDD and Flash

> **NOTE:** For the list of supported operating systems and Dell servers, see the *Dell Systems Software Support Matrix* in the required version of OpenManage Software at **dell.com/openmanagemanuals**.

> **NOTE:** For more information about the features introduced in this release, see the Server Administrator context-sensitive online help.

Systems Management Standards Availability

Server Administrator supports the following 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.

> **NOTE:** For information on SNMP security concerns, see the Server Administrator readme file (packaged with the Server Administrator application) or at **dell.com/openmanagemanuals**. 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/Windows Management Instrumentation (WMI) 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 Essentials while logged in with the required privileges.

The following table shows the systems management standards that are available for each supported operating system.

Table 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

Operating System	SNMP	CIM
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 6.0	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 an extensive, context-sensitive online help.

Other Documents You May Need

In addition to this guide, you can access the following guides available at **dell.com/ softwaresecuritymanuals** .

- The *Dell Systems Software Support Matrix* provides information about the various Dell systems, the operating systems supported by these systems, and the components that can be installed on these systems.
- The *Server Administrator Installation Guide* contains instructions to help you install Dell OpenManage Server Administrator.
- The *Management Station Software Installation Guide* contains instructions to help you install Dell OpenManage management station software.
- The *OpenManage SNMP Reference Guide* documents the Simple Network Management Protocol (SNMP) management information base (MIB).
- 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 *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.
- The*Server Administrator Command Line Interface Guide* documents the complete command line interface for Server Administrator.
- The *Dell Remote Access Controller 5 User's Guide* provides comprehensive information about using the RACADM command line utility to configure a DRAC 5.
- The *Dell Chassis Management Controller User's Guide* provides comprehensive information about using the controller that manages all modules in the chassis containing your Dell system.
- The *Command Line Reference Guide for iDRAC6 and CMC* provides information about the RACADM subcommands, supported interfaces, property database groups and object definitions for iDRAC6 and CMC.
- The *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide* provides information about configuring and using iDRAC7 for 12G rack, tower, and blade servers to remotely manage and monitor your system and its shared resources through a network.

- The *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide* provides information about configuring and using an iDRAC6 for 11G blade servers to remotely manage and monitor your system and its shared resources through a network.
- The *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide* provides complete information about configuring and using an iDRAC6 for 11G tower and rack servers to remotely manage and monitor your system and its shared resources through a network.
- 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's 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* provides information about installing, configuring, and using Dell Management Console.
- The *Dell Lifecycle Controller User's Guide* provides information on setting up and using the Unified Server Configurator to perform systems and storage management tasks throughout your system's lifecycle.
- The *Dell License Manager User's Guide* provides information about managing component server licenses for Dell 12G servers.
- The *Glossary* for information on terms used in this document.

Accessing Documents From Dell Support Site

You can access the required documents in one of the following ways:

- From the following links:

  - For all Systems Management documents — **dell.com/softwaresecuritymanuals**
  - For Enterprise Systems Management documents — **dell.com/openmanagemanuals**
  - For Remote Enterprise Systems Management documents — **dell.com/esmmanuals**
  - For Serviceability Tools documents — **dell.com/serviceabilitytools**
  - For Client Systems Management documents — **dell.com/OMConnectionsClient**
  - For OpenManage Connections Enterprise Systems Management documents — **dell.com/ OMConnectionsEnterpriseSystemsManagement**
  - For OpenManage Connections Client Systems Management documents — **dell.com/ OMConnectionsClient**

- From Dell Support site as follows:

  - Go to **dell.com/support/manuals**.
  - In the **Tell us about your Dell system** section, under **No**, select **Choose from a list of all Dell products** and click **Continue**.
  - In the **Select your product type** section, click **Software and Security**.

- In the **Choose your Dell Software** section, click the required link from the following:

  * **Client System Management**
  * **Enterprise System Management**
  * **Remote Enterprise System Management**
  * **Serviceability Tools**

- To view the document, click the required product version.
- Using search engines as follows:

  - Type the name and version of the document in the **Search** box.

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.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to **dell.com/contactdell**.
2. Verify your country or region from the drop-down menu at the top left corner of the page.
3. Select your support category: **Technical Support**, **Customer Support**, **Sales**, or **International Support Services**.
4. Select the appropriate service or support link based on your requirement.

NOTE: If you have purchased a Dell system, you may be asked for the Service Tag.

Setup And Administration

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 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 privilege levels are: User, Power User, Administrator, and Elevated Administrator.

Table 2. User Privileges

User Privilege Level	Access Type		Description
	View	**Manage**	
User	Yes	No	*Users* can view most information.
Power User	Yes	Yes	*Power Users* can set warning threshold values and configure which alert actions are to be performed when a warning or failure event occurs.
Administrator	Yes	Yes	*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 Administrator (Linux only)	Yes	Yes	*Elevated Administrators* can view and manage information.

Privilege Levels to Access Server Administrator Services

The following table summarizes the users who have privileges to access and manage Server Administrator services.

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.

Table 3. Privileges Required To Manage Server Administrator Services

Service	User Privilege Level Required	
	View	**Manage**
Instrumentation	User, Power User, Administrator, Elevated Administrator	Power User, Administrator, Elevated Administrator
Remote Access	User, Power User, Administrator, Elevated Administrator	Administrator, Elevated Administrator
Storage Management	User, Power User, Administrator, Elevated Administrator	Administrator, 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

On supported Microsoft Windows operating systems, Server Administrator 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

On 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 Authentication

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 stores paths to the authentication modules and is located at **/etc/pam.d/vmware-authd**.

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

> **NOTE:** On systems running VMware ESX Server 4.x operating system, to login to Server Administrator, all users require Administrator privileges. For information on assigning roles, see the VMware documentation.

VMware ESXi Server 5.X Authentication

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 5.0 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 in to 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 the Dell OpenManage software. Users without an assigned password cannot log in to 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 guest accounts so that remote scripts cannot enable the accounts using the default guest account names.

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

> NOTE: To add users to OpenManage software, add new users to the operating system. 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 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 in to 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 the following procedures.

> **NOTE:** You must have the **useradd** utility installed on your system to perform the following 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 <group> <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: You must be logged in as root or an equivalent user to perform the following 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>`

   The following table lists the legend for adding the role definition to the `omarolemap` file

   Table 4. Legend for adding the role definition in Server Administrator

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

   The following table lists the examples for adding the role definition to the omarolemap file.

   Table 5. Examples for adding the role definition in 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 are the best practices to be considered while working with the omarolemap file :

- Do not delete the following default entries in the **omarolemap** file.

root	* Administrator
+root	* Poweruser
*	* User

- Do not change the **omarolemap** file permissions or file format.
- 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 the **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 :

  - a user is degraded in the **omarolemap** file

- 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, ESXi 4.X, And ESXi 5.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 login, user name, a numeric user ID (UID), and password; specifying that 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 select **Properties**.
4. Select **Account is disabled** and click **OK**.

A red circle with an X appears over the user name to indicate that 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 and to send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as the Dell OpenManage Essentials, 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, you must rename the default SNMP community names. For information about renaming the SNMP community names, see Changing The SNMP Community Name.

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 and ESXi 5.X Operating Systems](#)

Configuring The SNMP Agent On 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 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: For additional details on SNMP configuration, see the operating system documentation.

Enabling SNMP Access On Remote Hosts (Windows Server 2003 Only)

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:

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 system running Server Administrator 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.

   To add a community name:
   a) 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** box and click **Add**.

      The **SNMP Service Properties** window appears.

   To edit a community name:
   a) Select a community name in the **Accepted Community Names** list and click **Edit**.

      The **SNMP Service Configuration** window appears.
   b) Edit the community name in the **Community Name** box, and then click **OK** .

      The **SNMP Service Properties** window appears.
6. 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 system running Server Administrator 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 then 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.

      The **SNMP Service Configuration** window appears.
   c) In the **Host name**, **IP or IPX address box**, type the trap destination, **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: For additional details on SNMP configuration, see the operating system documentation.

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 SNMP agent configuration file **/etc/snm, p/snmpd.conf** by:

- Creating a vew to the entire MIB tree by adding the following line if it does not exist: `view all included`
- Modifying 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 above line, it modifies the line as: `access notConfigGroup "" any noauth exact all none none`

    > 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 name 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 system running Server Administrator, 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:

1. Open the SNMP agent configuration file, **/etc/snmp/snmpd.conf**.
2. Find the line that reads: `com2sec publicsec default public` or `com2sec notConfigUser default public`.

    > NOTE: For IPv6, find the line `com2sec6 notConfigUser default public`. Also, add the text `agentaddress udp6:161` in the file.

3. 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`.
4. 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: For additional details on SNMP configuration, see the operating system documentation.

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:

4. Find the line that reads: `rocommunity public 127.0.0.1`.
5. Edit this line by deleting 127.0.0.1. When edited, the new line should read: `rocommunity public`.

6. 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 system running Server Administrator,, 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:

1. Open the SNMP agent configuration file, **/etc/snmp/snmpd.conf**.
2. Find the line that reads: `rocommunity public 127.0.0.1.`
3. 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.`
4. 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 162 using the SNMP protocol. To do this, `snmpd` is configured to use the default port 162 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 VMWware SNMP configuration file can be modified manually on the ESX server or by running the 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 at **vmware.com/download/vi/drivers_tools.html.**

To configure the SNMP agent:

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 <Destination_IP_Address> @162/ <community name>`

   Where 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 or service, run the following command on the ESX server: `netstat -a command`

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

   To enable VMWare SNMP service, run the following command:

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

   To view the configuration settings, run the following command:

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

   The following is an example of the configuration file, after modification:

   `<?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** file: `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 the 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 And ESXi 5.X Operating Systems

Server Administrator supports SNMP traps on VMware ESXi 4.X and ESXi 5.X. If a stand-alone license is only present, SNMP configuration fails on VMware ESXi operating systems. Server Administrator does not support SNMP Get and Set operations on VMWare ESXi 4.X and ESXi 5.X as the required SNMP support is unavailable. The VMware vSphere Command- Line Interface (CLI) is used to configure systems running VMware ESXi 4.X and ESXi 5.X to send SNMP traps to a management station.

✎ **NOTE:** For more information about using the VMware vSphere CLI, see **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:

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. Run the following command: `vicfg-snmp.pl --server <server> --username <username> --password <password> -c <community> -t <hostname> @162/<community>`

   where `<server>` is the hostname or IP address of the ESXi system, `<username>` is a user on the ESXi system, `<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:

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:** For more information about the firewall security levels, press <F1>. 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 Step7.
   b) To open an entire network interface or the SNMP port, select **High, Medium,** or **Enabled** and proceed to 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**>.

Firewall Configuration
To open the SNMP port on SUSE Linux Enterprise Server:

1. Configure SuSEfirewall2 by running the following command on a console: `a.# yast2 firewall`
2. Use the arrow keys to navigate to **Allowed Services**.
3. Press <Alt><d> to open the **Additional Allowed Ports** dialog box.
4. Press <Alt><T> to move the cursor to the **TCP Ports** text box.
5. Type **snmp** in the text box.
6. Press <Alt><O> <Alt><N> to go to the next screen.
7. Press <Alt><A> to accept and apply the changes.

Using Server Administrator

To start a Server Administrator session, double-click the **Server Administrator** icon on your desktop.

The **Server Administrator Log in** screen is displayed. The default port for Server Administrator is 1311. You can change the port, if required. For instructions on setting up your system preferences, see Dell Systems Management Server Administration.

> **NOTE:** Servers running on XenServer 6.0 can be managed using Command Line Interface (CLI) or a central web server installed on a separate machine

Logging In And Out

Server Administrator provides the following types of logins:

- Server Administrator Local System Login
- Server Administrator Managed System Login — Using the Desktop Icon
- Server Administrator Managed System Login — Using The Web Browser
- Central Web Server Login

Server Administrator Local System Login

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

This option is unavailable for servers running on XenServer 6.0.

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 must also specify the correct Domain name.

2. Select the **Active Directory Login** check box to log in using Microsoft Active Directory. See Using the Active Directory Login.

3. 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 *Management Station Software Installation Guide* at **dell.com/openmanagemanuals**.

Server Administrator Managed System Login — Using the Desktop Icon

This login is available only if the Server Administrator Web Server component is installed on the system. To log in to Server Administrator to manage a remote system:

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

   ![NOTE icon] **NOTE:** If you have provided the system name or FQDN, the Server Administrator Web Server host converts the system name or FQDN to the IP address of the managed system. You can also connect by providing the port number of the managed system in the following format: Hostname:Port number, or IP address:Port number. If you are connecting to a Citrix XenServer, Server Administrator Web Server automatically selects the default port (5986) or you can specify an alternative port.

3. If you are using an Intranet connection, select **Ignore Certificate Warnings**.
4. Select **Active Directory Login** to log in using Microsoft Active Directory authentication. If Active Directory software is not used to control access to your network, , do not select **Active Directory Login**. See Using the Active Directory Login.
5. Click **Submit.**

Server Administrator Managed System Login — Using The Web Browser

![NOTE icon] **NOTE:** You must have preassigned user rights to log in to Server Administrator. See Setup and Administration for instructions on setting up new users.

1. Open the Web browser.
2. In the address field, type one of the following:

   - `https://hostname:1311`, where hostname is the assigned name for the managed system and 1311 is the default port number.
   - `https://IP address:1311`, where IP address is the IP address for the managed system and 1311 is the default port number.

   ![NOTE icon] **NOTE:** Make sure that you type `https://` (and not `http://`) in the address field.

3. Press <Enter>.

Central Web Server Login

This login is available only if the Server Administrator Web Server component is installed on the system. Use this login to manage the Server Administrator Central Web Server:

1. Double-click the **Server Administrator** icon on your desktop. The remote login page is displayed.

   ![CAUTION icon] **CAUTION: The login screen displays an Ignore certificate warnings check box. You should use this option with discretion. It is recommended that you use it only in trusted Intranet environments.**

2. Click 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 **Active Directory Login** to log in using Microsoft Active Directory. See Using the Active Directory Login.

5. Click **Submit** .

To end your Server Administrator session, click **Log Out** on the <u>Global Navigation Bar</u>.

> 📝 **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 a problem with security certificate. To ensure system security, it is recommended that you generate a new X.509 certificate, reuse an existing X.509 certificate, or import a 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 about X.509 Certificate Management, see <u>X.509 Certificate Management</u>.

> 📝 **NOTE:** To ensure system security, it is recommended that you import a certificate chain from a Certification Authority (CA). For more information, see the VMware documentation.

> 📝 **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** file. For information about accessing this .exe file, see your operating system documentation. 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 **Active Directory Login** 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 *Server Administrator Installation Guide* at **dell.com/openmanagemanuals**.

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 **Server Administrator** icon on your desktop.

> 📝 **NOTE:** For more information about 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:

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

where `plugin name = omsa, ita,` and so on.

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:

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

Where `plugin name = omsa, ita,` and so on.

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 Essentials) 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 may 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 may see a 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.

Enabling The Use Of Client-Side Scripts On Internet Explorer

1. In your Web browser, click **Tools → Internet Options → Security**.
   The **Internet Options** window is displayed.
2. Under **Select a zone to view or change security settings**, click **Trusted Sites**, and then click **Sites**.
3. In the **Add this website to the zone** field, paste the Web address used to access the remote managed system.
4. Click **Add** .
5. 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**.
6. Under **Security level for this zone**, click **Custom** level
   For Windows Server 2003:
   a) Under **Miscellaneous**, select **Allow Meta Refresh**.
   b) Under **Active Scripting**, select **Enable**.
   c) Under **Active Scripting**, select **Allow scripting of Internet Explorer web browser controls**.
7. Click **OK** to save the new settings.
8. Close the browser and log in to Server Administrator.

Enabling Single Sign-On For Server Administrator On Internet Explorer
To allow Single Sign-On for Server Administrator without prompts for user credentials:

1. In your Web browser, click **Tools → Internet Options → Security**
2. Under **Select a zone to view or change security settings**, click **Trusted Sites**, and then click **Sites**.
3. In the **Add this website to the zone** field, paste the Web address used to access the remote managed system.
4. Click **Add**.
5. Click **Custom Level** .
6. Under **User Authentication**, select **Automatic Logon with current username and password**.
7. Click **OK** to save the new settings.
8. Close the browser and log in to Server Administrator.

Enabling The Use Of Client-Side Scripts On Mozilla Firefox

1. Open your browser.
2. Click **Edit → Preferences**.
3. Click **Advanced → Scripts and Plugins**.
4. Under Enable Javascript for, make sure that Navigator is selected. 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.

The following table lists the **GUI** field names and the applicable system, when Server Administrator is installed on the system.

Table 6. GUI Field Names And The Applicable Systems

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

The following figure shows a sample Server Administrator home page layout for a user logged in with administrator privileges on a non-modular system.

system tree   action tab   action tab subcategories   global navigation bar

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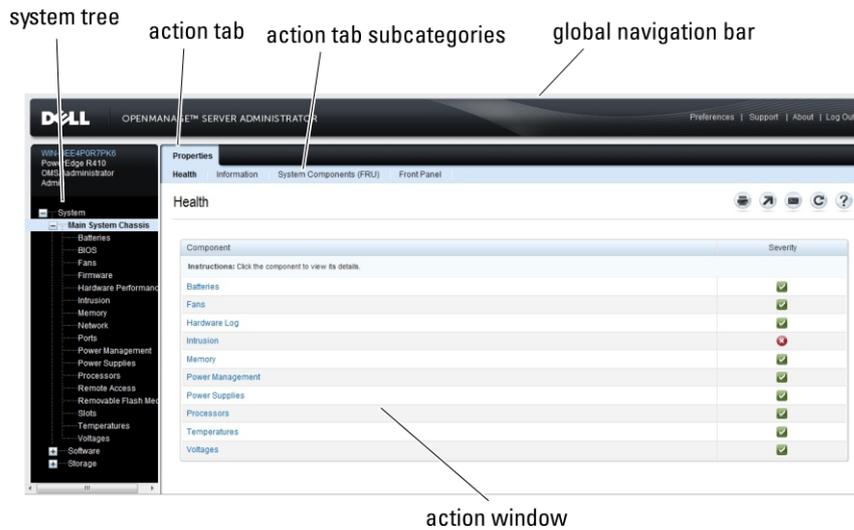
Figure 1. Sample Server Administrator Home Page — Non-Modular System

The following figure shows a sample Server Administrator home page layout for a user logged in with administrator privileges on a modular system.

system tree   action tab   action tab subcategories   global navigation bar
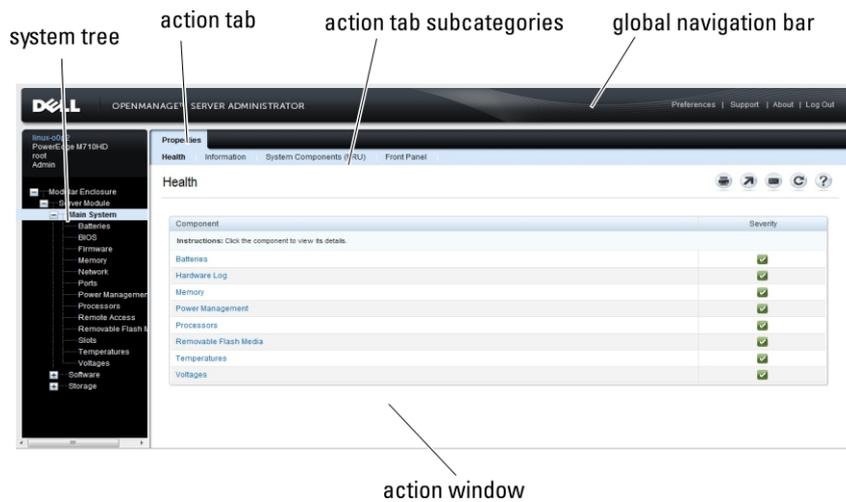
action window

Figure 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 the 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.

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

The following table lists the availability of Server Administrator features across modular and non-modular systems.

Table 7. Server Administrator User Interface Differences Across Modular and Non- Modular Systems

Features	Modular System	Non-Modular System
Batteries	✔	✔
Power Supplies	✘	✔
Fans	✘	✔
Hardware Performance	✘	✔ (10G onwards)
Intrusion	✘	✔
Memory	✔	✔
Network	✔	✔
Ports	✔	✔
Power Management	✔	✔ (10G onwards)
Processors	✔	✔
Remote Access	✔	✔
Removable Flash Media	✔	✔
Slots	✔	✔
Temperatures	✔	✔
Voltages	✔	✔
Modular Enclosure (Chassis Information	✔	✘

Features	Modular System	Non-Modular System
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 is 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).

36

Table 8. System/Server Module Component Status Indicators

Description	Icon
	The component is healthy (normal).
	The component has a warning (non-critical) 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.
	The component has a failed or 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.
	The 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. The **Log** window, 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. For information about customizing the delimiter separating the data field values see, "Setting User"and "System Preferences."

- Clicking **Email** ( ) creates an e-mail message addressed to your designated e-mail recipient. For instructions on setting up your e-mail server and default e-mail recipient, see "Setting User"and "System Preferences."

- 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 information about the specific window or task button you are viewing.

  NOTE: The **Export**, **Email**, and **Save As** buttons are only visible for users logged in with Power User or Administrator privileges. The **Clear Log** button is visible only for users with 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, the following figure shows readings from a system's CPU fan probe.
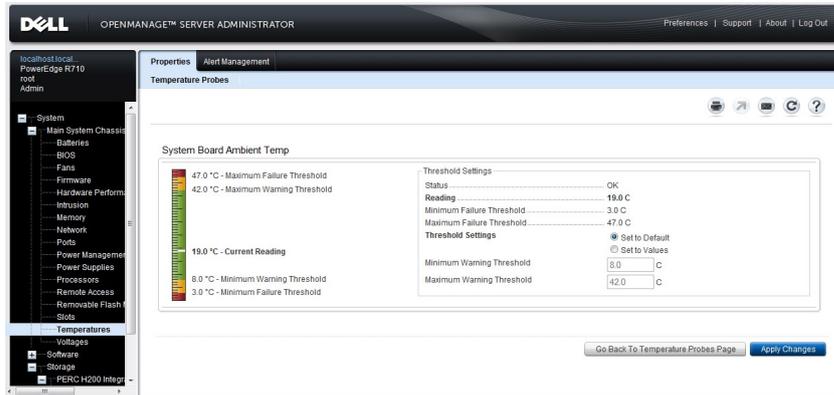
Figure 3. Gauge Indicator

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 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.

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 may have the **Preferences** tab.

Under the Preferences tab, you can:

- Enable or disable access to users with User or Power User privileges
- Select the format of alert messages

  📝 NOTE: The possible formats are **traditional** and **enhanced**. The default format is **traditional**, which is the legacy format.

- 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 about accessing these features, see [Server Administrator Services Overview](#).

Dell Systems Management Server Administration Connection Service And Security Setup

Setting User And System Preferences
You can 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.

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**.

   📝

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

   📝 NOTE: The Web Server URL is not retained if you restart Server Administrator service or the system where Server Administrator is installed. Use the omconfig command to reenter the URL.

Secure Port System

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**.

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

– The **Session Timeout (minutes)** feature can be used to set a limit on the amount of time that a Server Administrator session can remains active. Select **Enable** 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 **Disable** to disable the Server Administrator **Session Timeout (minutes)**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 may prevent other applications or browsers from accessing Server Administrator on the managed system. For a list of default ports, see the *Server Administrator Installation Guide*.

– 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 **All**to bind to all IP addresses applicable for your system. Select **Specific** 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 **Mail To** field specifies the e-mail address(es) to which you want to send e-mails about updates by default. You can configure multiple e-mail address(es) and use a comma to separate each one.

– The **SMTP Server Name (or IP Address)** 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** — Allows 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 also connect to the Server Administrator.

* **128-bit or Higher** — Allows connections from browsers with 128-bit or higher encryption strength. One of the following cipher suites is applicable based on 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
```

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

- **Key Signing Algorithm (For Self Signed Certificate)** — Allows you to select a supported signing algorithm. 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.

- **The Java Runtime Environment** — Allows you to select the one of the following options:
- **Bundled JRE** — Enables use of the JRE provided along with the System Administrator.
- **System JRE** — Enables use of the JRE installed on the system. Select the required version from the drop-down list.

> NOTE: If the JRE does not exist on the system on which Server Administrator is running, the JRE provided with the Server Administrator is used.

> 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**.

> NOTE: You must restart the Server Administrator web server for the changes to take effect.

X.509 Certificate Management

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

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

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

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

The following are the available options:

- **Generate a new certificate** — Generates a new self-signed certificate used for SSL communication between the server running Server Administrator and the browser.

> NOTE: When using a self-signed certificate, most web browsers display an *untrusted* warning as the self-signed certificate is not signed by a Certificate Authority (CA) trusted by the operating system. Some secure browser settings can also block the self-signed SSL certificates. The OMSA web GUI requires a CA-signed certificate for such secure browsers.

- **Certificate Maintenance** — Allows you to generate a Certificate Signing Request (CSR) containing all the certificate information about the host required by the CA to automate the creation of a trusted SSL web certificate. You can retrieve the necessary CSR file either from the instructions on the Certificate Signing Request (CSR) page or by copying the entire text in the text box on the CSR page and pasting it in the CA submit form. The text must be in the Base64−encoded format.

> NOTE: You also have an option to view the certificate information and export the certificate that is being used in the Base64−encoded format, which can be imported by other web services.

- **Import certificate chain** — Allows you to import the certificate chain (in PKCS#7 format) signed by a trusted CA. The certificate can be in DER or Base64-encoded format.

Server Administrator Web Server Action Tabs

The following are the action tabs that are displayed when you log in to manage the Server Administrator web server:

- Properties
- Shutdown
- Logs
- Alert Management
- Session Management

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 *Server Administrator Command Line Interface Guide* at **dell.com/openmanagemanuals**.

4

Server Administrator Services

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 the 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 can also be retrieved.

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 systems running Microsoft Windows Server 2003. For more information about configuring SNMP, see, Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems.

Managing Your System

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

By default, the **Preferences** home page, opens the **Node Configuration**.

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 SM 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 *Storage Management User's Guide* at **dell.com/openmanagemanuals**.

Server Administrator Home Page System Tree Objects

This section provides information about the objects in the System tree on the Server Administrator's home page. Due to the limitations of the VMware ESX and ESXi version 4.X and 5.X operating systems, some features available in earlier versions of Server Administrator are not available in this release. These include:

- Fibre Channel over Ethernet (FCoE) Capable and iSCSI over Ethernet (iSoE) capable information

- FCoE-capable and iSoE-capable information.
- Alert Management — Alert Actions
- Network Interface — Administrative Status, DMA, Internet Protocol (IP) Address,
- Network Interface — Operational Status
- 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.

- **Tab: Properties**
- **Subtab : 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 launch 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 appears.

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

System/Server Module Properties

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: **Licensing**, **Properties**, **Shutdown**, **Logs**, **Alert Management**, and **Session Management**

Licensing

Subtabs: Information | Licensing

Under the Licensing sub tab, you can:

- Set preferences to use Integrated Dell Remote Access Controller (iDRAC) to import, export, delete, or replace the digital license of the hardware.
- View details of the device used. The details include status of the license, description of the license, entitlement ID and date of expiry of the license.

   > **NOTE:** Server Administrator supports the licensing feature on PowerEdge 12G system onwards. The feature is available only if the required minimum version of iDRAC, iDRAC 1.30.30, is installed.

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 if 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≤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. The watchdog timer can be set to a maximum of 720 seconds.

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 through 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 9G and 11G 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: For more information about each alert event ID and its corresponding description, severity level, and cause, see the *Server Administrator Messages Reference Guide* at **dell.com/ openmanagemanuals**.

- 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: For instructions to view, print, save, and e-mail logs, see "Server Administrator 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.

    NOTE: On any Microsoft Windows operating system, the **Advanced System Settings → Advanced Recovery** option in the operating system must be disabled to make sure that Server Administrator Automatic System Recovery alerts are generated.

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 Administrator 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 PowerEdge 10G and later systems. The **Power Supplies** option is not available on Dell PowerEdge 1900. Power management is supported on limited Dell PowerEdge 10G and later systems. Power Supply Monitoring and Power Monitoring features are available only for systems that have two or more redundant, hot-swappable power supplies installed. These features are unavailable for permanently installed, non-redundant power supplies that lack power management circuitry.

Main System Chassis/Main System Properties

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 includes the following:

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 that 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](#)
- [Network](#)
- [Power Management](#)
- [Power Supplies](#)
- [Processors](#)
- [Temperatures](#)
- [Voltages](#)

> **NOTE:** Batteries are supported only on Dell PowerEdge 9G and Dell PowerEdge 10G systems. The **Power supplies** is not available on Dell PowerEdge 1900. Power management is supported on limited Dell PowerEdge 10G systems. **Power Supply Monitoring** and **Power Monitoring** features are available only for systems that have two or more redundant, hot-swappable power supplies installed. These features are unavailable for permanently installed, non-redundant power supplies that lack power management circuitry.

NOTE: If the QLogic QLE2460 4Gb Single-Port Fibre Channel HBA, QLogic QLE2462 4Gb Dual-Port Fibre Channel HBA, Qlogic QLE2562 Dual Port FC8 Adapter, or Qlogic QLE2560 Single Port FC8 Adapter cards are installed on 12G systems, the **System Components (FRU)** screen is not displayed.

- 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 a 11-digit numeric-only conversion of the Dell system Service Tag. When calling Dell Technical Support, you can key in the ESC for auto call routing.
- View detailed information about the field-replaceable units (FRUs) installed in your system (under the **System Components** (**FRU**) sub tab).
- 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** sub tab.

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 chipset 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

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

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, Hard Disk Drive Sequence, User Accessible USB Ports, CPU Virtualization Technology, CPU HyperThreading, AC Power Recovery Mode, Embedded SATA Controller, System Profile, 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 also view the Trusted Platform Module (TPM) and Trusted Cryptographic Module (TCM) settings.

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

For 12G systems, the configurable BIOS features are grouped as specific categories. The categories include System Information, Memory Settings, System Profile Settings, Unified Extensible Firmware Interface (UEFI) Boot Settings, Network Interface Controller cards, One-Time Boot, and Slot Disablement. For example, on the **System BIOS Settings** page, when you click the **Memory Settings** link , the features pertaining to the system memory appear. You can view or modify the settings by navigating to the respective categories.

You can set a BIOS Setup password, on the**BIOS Setup - System Security** page. You must enter the password to enable and modify the BIOS settings. Else, the BIOS settings appear in a read-only mode. You must restart the system after setting the password.

When pending values from the previous session exist or the inband configuration is disabled from an out-of-band interface, Server Administrator does not allow BIOS Setup configuration.

> **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.

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-side 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, such as 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**.

The following table lists the possible values for status and cause of a probe:

Table 9. 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 of 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 the 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 the 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 the memory redundancy status, memory array attributes, total capacity of the memory arrays, details of memory arrays, memory device details, and memory device status. The memory device details provides the details of a memory device on a connector such as the status, device name, size, type, speed, rank, and failures. A rank is a row of dynamic random access memory (DRAM) devices comprising 64 bits of data per Dual Inline Memory Module (DIMM). The possible values of rank are `single`, `dual`, `quad`, `octal`, and `hexa`. The rank displays the rank of the DIMM and helps in the easy service of DIMMs on the server.

> 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 the 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 the 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. Server Administrator reports FCoE and iSoE capabilities of the NICs. Also, NIC teaming details are reported if they are 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.

On Windows 2008 Hypervisor operating system, Server Administrator does not report the IP addresses of the physical NIC ports that are used to assign an IP to a virtual machine.

> NOTE: The order in which devices are detected is not guaranteed to match the physical port ordering of the device. Click the hyperlink under Interface Name to view NIC information.

In case of ESX and ESXi operating systems, the network device is considered a group. For example, the virtual ethernet interface that is used by the Service Console (vswif) and virtual network interface that is used by VMKernel (vmknic) devices on ESX and vmknic device on ESXi.

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.

> **NOTE:** CMC USB ports attached with Blade Servers are not enumerated by OMSA.

The **Ports** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Subtab: Information

Properties

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

Power Management

> **NOTE:** Power Supply Monitoring and Power Monitoring features are available only for systems that have two or more redundant, hot-swappable power supplies installed. These features are unavailable for permanently installed, non-redundant power supplies that lack power management circuitry.

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**.

NOTE: Power Supply Monitoring and Power Monitoring features are available only for systems that have two or more redundant, hot-swappable power supplies installed. These features are unavailable for permanently installed, non-redundant power supplies that lack power management circuitry.

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 Firmware Version of the power supply, Rated Input Wattage, and Maximum Output Wattage. The Rated Input Wattage attribute is displayed only on PMBus systems starting 11G.

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**.

Subtab: Information

Properties

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 on Dell PowerEdge 9G systems and iDRAC is supported on Dell PowerEdge 10G and 11G 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**.

Subtab: Information

Properties

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.

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

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 are displayed only on Dell PowerEdge 9G 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 Dell PowerEdge 9G 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**.

Subtab: Temperature Probes

Under the **Properties** tab, you can view the current readings and status of 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 such as 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 the 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 the 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 of 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, such as 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 the 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 the 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**.

Subtab: Summary

Properties

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**.

Subtab: Properties

User

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

- **Web Server**
- **Subtabs: Properties | X.509 Certificate**

Under the Web Server tab, you can:

- Set DSM SA Connection Service preferences. For instructions on configuring your server preferences, see Dell Systems Dell Systems Management Server Administration Connection Service and Security Setup.
- 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 certificate chain from a Certification Authority (CA). For more information about certificate management, see X.509 Certificate Management.

Server Administrator

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

Subtabs: Access Configuration

Preferences

Under the **Preferences** tab, you can enable or disable access to users with User or Power User privileges.

5

Working With Remote Access Controller

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.

> **NOTE:** Baseboard management controller (BMC) is supported on Dell PowerEdge 9G systems and the Integrated Dell Remote Access Controller (iDRAC) is supported on Dell PowerEdge 10G and 11G systems.

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 the user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed system.

> **NOTE:** For more information about the BMC, see the *Dell OpenManage Baseboard Management Controller User's Guide* at **dell.com/systemsecuritymanuals**.

> **NOTE:** For more information on using DRAC 5, see the *Dell Remote Access Controller 5 User's Guide* at **dell.com/systemsecuritymanuals**.

> **NOTE:** For detailed information on configuring and using the iDRAC, see the *Integrated Dell Remote Access Controller User's Guide* at **dell.com/systemsecuritymanuals**.

The following table lists the graphical user interface (GUI) field names and the applicable system, when Server Administrator is installed on the system.

Table 10. GUI Field Names And The Applicable System

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

For more information on the systems support for remote access devices, see the *Dell Systems Software Support Matrix* available at **dell.com/openmanagemanuals**.

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 (GUI), click the **Remote Access** object, which is a subcomponent of the **Main System Chassis/Main System** group.

You can perform the following tasks:

- [Viewing Basic Information](#)
- [Configuring The Remote Access Device To Use A LAN Connection](#)
- [Configuring The Remote Access Device To Use A Serial Over LAN Connection](#)
- [Configuring The Remote Access Device To Use A Serial Port Connection](#)
- [Additional Configuration For iDRAC](#)
- [Configuring Remote Access Device Users](#)
- [Setting 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` command-line interface (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 9G 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

To 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 9G systems when DRAC is installed. Select this option for NIC teaming. In Dell PowerEdge 9G 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

> **NOTE:** The NIC Selection option is available only on 11G systems and earlier.

– Primary and Failover Network options

For 12G systems, the Primary Network options for Remote Management (iDRAC7) **NIC** are: **LOM1**, **LOM2**, **LOM3**, **LOM4**, and **Dedicated**. The Failover Network options are: **LOM1**, **LOM2**, **LOM3**, **LOM4**, **All LOMs**, and **None**.

The dedicated option is available when the iDRAC7 Enterprise License is present and valid.

> **NOTE:** The number of LOMs varies based on the system or hardware configuration.

– 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 9G 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

To configure the BMC for communication over a serial port connection:

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

To configure the BMC/iDRAC for communication over a serial over LAN (SOL) connection:

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

To configure the IPv4 and IPv6 properties using the **Additional Configuration** tab:

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**.

   > **NOTE:** For information about license management, see the *Dell License Manager User's Guide* available at **dell.com/openmanagemanuals**.

Configuring Remote Access Device Users

To configure Remote Access Device users using the Remote Access 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 9G 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] **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

To configure the most relevant BMC features, such as Platform Event Filter (PEF) parameters and alert destinations using Server Administrator Instrumentation Service:

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

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

   ![note] **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**
   – **Reboot System**

   Shuts down the operating system and initiates system startup, performing BIOS checks and reloading the operating system.

   – **Power Off System**

   Turns off the electrical power to the 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 Reduction**

   Throttles the CPU.

   ⚠ **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.**

   📝 NOTE: Power reduction is not supported on all systems. Power Supply Monitoring and Power Monitoring features are available only for systems that have two or more redundant, hot-swappable power supplies installed. These features are unavailable for permanently installed, non-redundant power supplies that lack power management circuitry.

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**.
8. Click **Apply 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.
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.

   📝 NOTE: On 12G systems with iDRAC7 specific versions, you can set Platform Event Destination as IPv4, IPv6, or FQDN.

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

6

Server Administrator Logs

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.

For information about viewing logs and creating reports from the command line, see the *Server Administrator Command Line Interface Guide* at **dell.com/openmanagemanuals**.

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

The following table lists the Log window task buttons.

Table 11. Log Window Task Buttons

Name	Description
Print	To print a copy of the log to your default printer.
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.
Email	To create an e-mail message that includes the log content as an attachment.
Clear Log	To erase all events from the log.
Save As	To save the log content in a **.zip** file.
Refresh	To reload the log content in the action window data area.

NOTE: For additional information about using the task buttons, see Task Buttons .

Server Administrator Logs

Server Administrator provides the following logs:

Hardware Log

On Dell PowerEdge 9G and 11G systems, use the hardware log to look for potential problems with your

system's hardware components. 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. The following table lists the status indicators.

Table 12. Hardware Log Status Indicators

Status	Description
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 question mark ( )	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. Make sure 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.

To clear a hardware log, on the **Hardware Log** page, click the **Clear Log** link.

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.

> **NOTE:** OMSA may send duplicate SNMP traps or log duplicate events in the Alert Log page or in the operating system log file. The duplicate traps and events are logged either when OMSA services are manually restarted or when the device sensor still indicates a non-normal state when OMSA services starts after an operating system reboot.

For detailed information about alert messages, see the *Server Administrator Messages Reference Guide* at **dell.com/openmanagemanuals**.

Command Log

> **NOTE:** If the Command 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 Command log to monitor all of the commands issued by Server Administrator users. The Command log tracks logins, logouts, systems management software initialization, 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, the messsage is not displayed. 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 a terminal such as **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, the message is not displayed 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. 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 insert 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 the 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:** You must specify the full path for both the **cmd.exe** and script files.

> **NOTE:** Microsoft Windows 2003 is not supported on 12G systems.

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 and enable interactive services.

To allow interaction with the desktop:

- Right-click the DSM SA Data Manager service in the **Services** control panel and select **Properties**.
- In the **Log On** tab, select **Allow service to interact with desktop** and click **OK**.
- Restart the DSM SA Data Manager service for the change to take effect.
- Ensure that the **Interactive Services Detection** service is running.

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. Enabling
the Interactive Services Detection service allows the DSM SA Data Manager
service to execute interactive applications properly for an Alert Action.
```

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

The following table lists all possible Platform Event Filter (PEF) messages along with a description of each event.

Table 13. 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.
Battery Probe Warning	The battery is operating below the recommended charge level.
Battery Probe Failure	The battery has failed.
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.
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.
Processor Absent	A processor has been removed.
PS/VRM/D2D Warning	The power supply, voltage regulator module, or DC to DC converter is pending a failure condition.
PS/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 Absent	The removable flash media is removed.
Removable Flash Media Failure	The removable flash media is pending a failure condition.

Event	Description
Removable Flash Media Warning	The removable flash media pending a failure condition.
Internal Dual SD Module Card Critical	The internal dual SD module card has failed.
Internal Dual SD Module Card Warning	The internal dual SD module card is pending a failure condition.
Internal Dual SD Module Card Redundancy Lost	The internal dual SD module card has no redundancy.
Internal Dual SD Module Card Absent	The internal dual SD module card is removed.

Troubleshooting

Connection Service Failure

On Red Hat Enterprise Linux, when `SELinux is set to enforced mode`, the Dell Systems Management Server Administrator (SM SA) Connection service fails to start. Perform 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 SM 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 turned 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. For information on how to enable Server Administrator Services on the VMware ESX/ESXi system, see the *Server Administrator Installation Guide*, at **dell.com/openmanagemanuals**.
- 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 do not 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 *Server Administrator Installation Guide* available at **dell.com/openmanagemanuals**.
- There is an authentication failure while connecting to a VMware ESXi 4.1/5.0 operating system, which may occur due to any of the following reasons:

  a. The `lockdown` mode is enabled either while you are logging to the server or while you are logged in to the Server Administrator. For more information on `lockdown` mode, see the VMware documentation.

  b. The password is changed while you are logged in to Server Administrator.

  c. 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.

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

Server Administrator Services

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

Table 14. Server Administrator Services

Service Name	Description	Impact of Failure	Recovery Mechanism	Severity
Windows: SM 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 the service	Critical
Windows: SM 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 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	Restart the service	Warning

Service Name	Description	Impact of Failure	Recovery Mechanism	Severity
	software update using Dell System Management Console and Dell IT Assistant (ITA).	performed using 3rd party tools (for example, MSSMS, Altiris and Novell ZENworks).		

📝 **NOTE:** OMSA may send duplicate SNMP traps or log duplicate events in the Alert Log page or in the operating system log file. The duplicate traps and events are logged either when OMSA services are manually restarted or when the device sensor still indicates a non-normal state when OMSA services starts after an operating system reboot.

📝 **NOTE:** Inventory Collector is required to update Dell consoles using Dell Update packages.

📝 **NOTE:** Some of the Inventory Collector features are not supported on OMSA (64–bit).

Service Name	Description	Impact of Failure	Recovery Mechanism	Severity
Windows: SM SA Data Manager Linux: `dsm_sa_datamgr d` (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 the service	Critical
SM SA Event Manager (Windows) Linux: `dsm_sa_eventmg rd` (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 the 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 the service	Critical
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	Users are unable to perform storage functions for all supported RAID and non-RAID controllers.	Restart the service	Critical

Service Name	Description	Impact of Failure	Recovery Mechanism	Severity
	storage attached to a system.			

Frequently Asked Questions

This section lists the frequently asked questions about Server Administrator.

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

1. **Why does ESXi 4.x (4.0 U3) and ESXi 5.x host rebooting functionality fail from Server Administrator?**

   This issue is due to VMware stand-alone license (SAL) key. For more information, see the knowledge base article at **kb.vmware.com/kb/kb1026060**.

2. **What are the tasks to be performed after adding a VMware ESX 4.0 U3 or ESX 4.1 U2 operating system to the Active Directory domain?**

   After adding a VMware ESX 4.0 U3 and ESX 4.1 U2 operating system to the Active Directory domain, an Active Directory user must:

   a. Log in to Server Administrator on the system running the VMware ESX 4.0 U3 and ESX 4.1 U2 operating system and restart the DSM SA Connection Service.

   b. Log in to the Remote Node while using the VMware ESX 4.0 U3 and ESX 4.1 U2 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 required to install Server Administrator?**

   To install Server Administrator, you must have Administrator level privileges. Power Users and Users do not have permission to install Server Administrator.

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

   For systems that are running Server Administrator version 4.3, upgrade to a 6.x version and then to version 7.x. For systems running a version prior to 4.3, upgrade to version 4.3, then to a 6.x version, and then to version 7.x (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** → Software & Security → Enterprise System Management → OpenManage Server Administrator.

   All the available versions of Server Administrator is displayed on the page.

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**, select the **Use** radio button to set your preferred port.

   NOTE: Changing the port number to an invalid or in-use port number may prevent other applications or browsers from accessing Server Administrator on the managed system. For the list of default ports, see the *Server Administrator Installation Guide* available at **dell.com/ openmanagemanuals**.

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 emails when there is a problem?**

No, Server Administrator is not designed to send emails 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.

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 set up 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 files 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, SNMP is the standard 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.

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 case-sensitive alphabets and numerals only.

13. **How does selecting/deselecting '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 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 *Server Administrator Installation Guide* available at **dell.com/openmanagemanuals**.

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
```

15. **Why is the Red Hat Enterprise Linux 5.9 (32-bit) operating system not able to detect the Emulex card after installing the Emulex drivers?**

    On systems running Red Hat Enterprise Linux 5.9 (32-bit) operating system, the Emulex driver is dependent on the following RPMs:

    – kernel-headers-2.6.18-346.el5.i386.rpm
    – glibc-headers-2.5-107.i386.rpm
    – glibc-devel-2.5-107.i386.rpm
    – gcc-4.1.2-54.el5.i386.rpm

    If any of the RPMs are missing, the system has issues in detecting the Emulex network adapters.