

Dell OpenManage™
Server Administrator Version 1.8.3
User's Guide

Notes and Notices



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



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

Information in this document is subject to change without notice.

© 2004 Dell Inc. All rights reserved.

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

Trademarks used in this text: *Dell*, the *DELL* logo, *Dell OpenManage*, and *PowerEdge* are trademarks of Dell Inc.; *Microsoft*, *Windows*, and *Windows NT* are registered trademarks of Microsoft Corporation; *Intel* is a registered trademark of Intel Corporation; *Red Hat* is a registered trademark of Red Hat, Inc.

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

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

May 2004

Contents

1	Introduction	
	Overview	7
	Integrated Features	7
	Installation	7
	Server Administrator Home Page	7
	Instrumentation Service	8
	Logs	8
	Other Documents You Might Need	8
	Obtaining Technical Assistance	9
2	Setup and Administration	
	Security Management	11
	Role-Based Access Control	11
	Authentication	12
	Encryption	13
	Assigning User Privileges	13
	Creating Server Administrator Users for Windows Server 2003 64–Bit Operating Systems	13
	Creating Server Administrator Users for Red Hat Linux 64–Bit Operating Systems	15
	Disabling Guest and Anonymous Accounts in Windows Server 2003 64–Bit Operating Systems	16
	Configuring the SNMP Agent	16
	Configuring the SNMP Agent for Systems Running Windows Server 2003 64–Bit Operating Systems	17
	Configuring the SNMP Agent on Systems Running Supported Red Hat Linux 64–Bit Operating Systems	19
	Firewall Configuration on Systems Running Red Hat Linux 64–Bit Operating Systems	22

3 Installing Server Administrator

Overview	25
Systems Management and Documentation CD	25
Before You Begin	25
Installation Requirements	25
Supported Operating Systems	25
System Requirements	26
Installation Procedures	27
Installing/Uninstalling on Systems Running Windows Server 2003 64–Bit Operating Systems	27
Prerequisites for Installing Server Administrator	28
Performing a Scripted Installation of Managed System Software	28
Uninstalling Server Administrator	28
Installing/Uninstalling on Systems Running Red Hat Linux 64–Bit Operating Systems	29
Dynamic Kernel Support	29
Prerequisites for Installing Server Administrator	32
Installing Server Administrator From the Red Hat Linux 64–Bit Command Line	33
Uninstalling Server Administrator	34

4 Using Server Administrator

Starting Your Server Administrator Session	35
Logging In and Out	35
Systems Running Windows Server 2003 64–Bit Operating Systems	36
The Server Administrator Home Page	37
Global Navigation Bar	39
System Tree	39
Action Window	39
Using the Online Help	41
Using the Preferences Home Page	41
Using the Server Administrator Command Line Interface	42

Secure Port Server and Security Setup	42
Setting User and Server Preferences.	43
X.509 Certificate Management	44
Controlling Server Administrator	44
Starting Server Administrator	44
Stopping Server Administrator.	45
Restarting Server Administrator	45
5 Instrumentation Service	
Overview	47
Managing Your System.	48
Managing System Tree Objects.	49
Server Administrator Home Page System Tree Objects	50
System	50
Managing Preferences Home Page Configuration Options.	58
Server Administrator	59
General Settings	59
6 Server Administrator Logs	
Overview	61
Integrated Features	61
Log Window Task Buttons	61
Server Administrator Logs	62
Hardware Log.	62
Alert Log	62
Command Log.	63
7 Appendix	
Overview	65
Setting Alert Actions for Systems Running a Supported Red Hat Linux Operating System	65

Figures

Figure 4-1.	Sample Server Administrator Home Page	38
Figure 4-2.	Sample Preferences Home Page	42
Figure 5-1.	Sample Server Administrator Home Page	48
Figure 5-2.	Server Administrator Home Page System Tree Objects	49
Figure 5-3.	Preferences Home Page Configuration Options	59

Tables

Table 2-1.	User Privileges	11
Table 2-2.	Server Administrator User Privilege Levels	12
Table 2-3.	Legend for Server Administrator User Privilege Levels	12
Table 3-1.	Availability of Systems Management Protocol by Operating Systems	27

Introduction

Overview

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

Server Administrator provides information about systems that are operating properly and systems that have problems.

Integrated Features

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

The following sections describe the Server Administrator integrated services and features:

Installation

The *Dell PowerEdge 7250 Systems Management and Documentation* CD provides scripts to install and uninstall Server Administrator on your managed system.

Server Administrator Home Page

The Server Administrator home page provides easy to set up and easy-to-use Web browser-based system management from the managed system or from a remote host through a LAN, dial-up service, or wireless network. When the Server Administrator secure port server is installed and configured on the managed system, you can perform remote management functions from any system that has a supported Web browser and connection. Additionally, the Server Administrator home page provides extensive, context-sensitive online help.

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.

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.

Other Documents You Might Need

Besides this *User's Guide*, you can find the following guides either on the Dell Support website at support.dell.com or on the *Systems Management and Documentation CD*:

- The *Dell OpenManage Software Quick Installation Guide* provides an overview of applications that you can install on your Dell™ PowerEdge™ 7250 system running supported operating systems.
- The *Dell OpenManage Server Administrator SNMP Reference Guide* documents the Simple Network Management Protocol (SNMP) management information base (MIB). The SNMP MIB defines variables that extend the standard MIB to cover the capabilities of systems management agents.
- The *Dell OpenManage Server Administrator CIM Reference Guide* documents the Common Information Model (CIM) provider, an extension of the standard management object format (MOF) file. The CIM provider MOF documents supported classes of management objects.
- The *Dell OpenManage Server Administrator Messages Reference Guide* lists the messages that are displayed in your Server Administrator home page Alert log or on your operating system's event viewer. This guide explains the text, severity, and cause of each Instrumentation Service Alert message that Server Administrator issues.
- The *Dell OpenManage Server Administrator Command Line Interface User's Guide* documents the complete command line interface for Server Administrator, including an explanation of CLI commands to view system status, access logs, create reports, configure various component parameters, and set critical thresholds.
- The *Dell PowerEdge 7250 Systems Product Guide* includes information about configuring, servicing, and troubleshooting your system.

The *Systems Management and Documentation CD* contains a readme file for Server Administrator.

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 *Installation and Troubleshooting Guide*.

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

Setup and Administration

Security Management

Server Administrator provides security through role-based access control (RBAC), authentication, and encryption for both the Web-based and command line interfaces.

Role-Based Access Control

RBAC manages security by determining the operations that can be executed by persons in particular roles. Each user is assigned one or more roles, and each role is assigned one or more user privileges that are permitted to users in that role. With RBAC, security administration corresponds closely to an organization's structure.

User Privileges

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

Users can view most information.

Power Users can set warning threshold values and configure which alert actions to take when a warning or failure event occurs.

Administrators can configure and perform shutdown actions, configure Auto Recovery actions in case a system has a hung operating system, and clear hardware, event, and command logs. Administrators can also send e-mail.

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 admin access to users logged in with Admin privileges. See Table 2-1.

Table 2-1. User Privileges

User Privileges	Access Type		
	Admin	Write	Read
User			X
Power User		X	X
Admin	X	X	X

Read access allows viewing of data reported by Server Administrator. Read access does not allow changing or setting values on the managed system.

Write access allows values to be changed or set on the managed system.

Admin access allows shutdown of the managed system.

Privilege Levels to Access Server Administrator Services

Table 2-2 summarizes which user levels have privileges to access and manage Server Administrator Services.

Table 2-2. Server Administrator User Privilege Levels

Service	User Privilege Level Required	
	View	Manage
Instrumentation	U, P, A	P, A

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

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

U	User
P	Power User
A	Administrator
NA	Not Applicable

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 Server 2003 for 64-Bit Itanium 2–based Systems Authentication



NOTE: All other references in this chapter to Microsoft® Windows® Server 2003 for 64-bit Itanium 2–based Systems use a shortened form of the operating system’s name: Windows Server 2003 64-bit.

For Windows Server 2003 64–bit operating systems, Server Administrator authentication is based on the operating system’s user authentication system using Windows NT® LAN Manager (NTLM) modules to authenticate. This underlying authentication system allows Server Administrator security to be incorporated in an overall security scheme for your network.

Red Hat Enterprise Linux (AS), Version 3, for 64–Bit Systems Authentication

 **NOTE:** All other references in this chapter to Red Hat® Enterprise Linux (AS), version 3, for 64-bit systems use a shortened form of the operating system's name: Red Hat Linux 64-bit.

For supported Red Hat® Linux 64-bit operating systems, Server Administrator authentication is based on the Red Hat Linux Pluggable Authentication Modules (PAM) library. This documented library of functions allows an administrator to determine how individual applications authenticate users.

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 and Red Hat Linux 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

You must properly assign user privileges to all Server Administrator users before installing Server Administrator in order to ensure critical system component security.


The following procedures provide step-by-step instructions for creating Server Administrator users and assigning user privileges for each supported operating system:

- Creating Server Administrator Users for Windows Server 2003 64–Bit Operating Systems
- Creating Server Administrator Users for Red Hat Linux 64–Bit Operating Systems


 **NOTICE:** You must assign a password to every user account that can access Server Administrator to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Server Administrator on a system running Windows Server 2003 64-bit due to operating system constraints.

 **NOTICE:** You should disable guest accounts for supported Microsoft Windows operating systems in order to protect access to your critical system components. See "Disabling Guest and Anonymous Accounts in Windows Server 2003 64–Bit Operating Systems" for instructions.

Creating Server Administrator Users for Windows Server 2003 64–Bit Operating Systems

 **NOTE:** You must be logged in with Admin privileges to perform these procedures.

Creating Users and Assigning User Privileges for Windows Server 2003 64–Bit Operating Systems

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

- 1 Click the **Start** button, right-click **My Computer**, and point to **Manage**.
- 2 In the console tree, expand **Local Users and Groups**, and then click **Users**.

- 3 Click **Action**, and then click **New User**.
 - 4 Type the appropriate information in the dialog box, select or clear the appropriate check boxes, and then click **Create**.
 - ➔ **NOTICE:** You must assign a password to every user account that can access Server Administrator to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Server Administrator on a system running Windows Server 2003 64-bit due to operating system constraints.
 - 5 In the console tree, under **Local Users and Groups**, click **Groups**.
 - 6 Click the group to which you want to add the new user: **Users**, **Power Users**, or **Administrators**.
 - 7 Click **Action**, and then click **Properties**.
 - 8 Click **Add**.
 - 9 Type the user name that you are adding and click **Check Names** to validate.
 - 10 Click **OK**.
- New users can log into Server Administrator with the user privileges for their assigned group.

Adding Users to a Domain

- ✍ **NOTE:** For questions about creating users and assigning user group privileges or for more detailed instructions, see your operating system documentation.
 - ✍ **NOTE:** You must have Active Directory installed on your system to perform the following procedures.
- 1 Click the **Start** button, and then point 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**.
 - ➔ **NOTICE:** You must assign a password to every user account that can access Server Administrator to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Server Administrator on a system running Windows Server 2003 64-bit due to operating system constraints.
 - 4 Click **Next**, and then click **Finish**.
 - 5 Double-click the icon representing the user you just created.
 - 6 Click the **Member of** tab.
 - 7 Click **Add**.
 - 8 Select the appropriate group and click **Add**.

- 9 Click **OK**, and then click **OK** again.

New users can log into Server Administrator with the user privileges for their assigned group and domain.

Creating Server Administrator Users for Red Hat Linux 64-Bit Operating Systems

Admin 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` to perform these procedures.



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

Creating Users



NOTE: For questions about creating users and assigning user group privileges or for more detailed instructions, 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, you must create it by using the `groupadd` command.

- 2 Type `passwd <username>` and press `<Enter>`.
 - 3 When prompted, enter a password for the new user.
- ➔ **NOTICE:** You must assign a password to every user account that can access Server Administrator to protect access to your critical system components.

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

Creating Users With Power User Privileges

- 1 Run the following command from the command line:

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




NOTE: You must set `root` as the primary group.

- 2 Type `passwd <username>` and press `<Enter>`.
 - 3 When prompted, enter a password for the new user.
- ➔ **NOTICE:** You must 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.

Disabling Guest and Anonymous Accounts in Windows Server 2003 64–Bit Operating Systems

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


- 1 If your system is running Windows Server 2003 64–bit, click the **Start** button, right-click **My Computer**, and point to **Manage**.
- 2 In the console tree, expand **Local Users and Groups** and click **Users**.
- 3 Click the **Guest** or **IUSR_***system name* user account.
- 4 Click **Action** and point to **Properties**.
- 5 Select **Account is disabled** and click **OK**.

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

Configuring the SNMP Agent

Server Administrator supports the Simple Network Management Protocol (SNMP) systems management standard on all supported operating systems. For Windows Server 2003 64-bit, you must manually install SNMP as part of your operating system installation. For Red Hat Linux 64-bit, SNMP is installed if the default package list is selected during installation. If you customize the package list during Red Hat Linux 64-bit installation, you may need to manually install SNMP after Red Hat Linux 64-bit is installed. An installed supported systems management protocol standard, such as SNMP, is required before installing Server Administrator. See "Installation Requirements" for more information.

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

 **NOTE:** 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 Windows Server 2003 64–Bit Operating Systems
- Configuring the SNMP Agent on Systems Running Supported Red Hat Linux 64–Bit Operating Systems

Configuring the SNMP Agent for Systems Running Windows Server 2003 64–Bit Operating Systems

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

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

Enabling SNMP Access By Remote Hosts

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

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

- 1 Click the **Start** button, right-click **My Computer**, and point to **Manage**.
The **Computer Management** window appears.
- 2 Expand the **Computer Management** icon in the window, if necessary.
- 3 Expand the **Services and Applications** icon and click **Services**.
- 4 Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and then click **Properties**.
The **SNMP Service Properties** window appears.
- 5 Click the **Security** tab.
- 6 Select **Accept SNMP packets from any host**, or add the remote host to the **Accept SNMP packets from these hosts** list.

Changing the SNMP Community Name

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

- 1 If your system is running Windows Server 2003 64–bit, click the **Start** button, right-click **My Computer**, and point to **Manage**.
The **Computer Management** window appears.
- 2 Expand the **Computer Management** icon in the window, if necessary.
- 3 Expand the **Services and Applications** icon and click **Services**.

- 4 Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and then click **Properties**.
The **SNMP Service Properties** window appears.
- 5 Click the **Security** tab to add or edit a community name.
 - a To add a community name, click **Add** under the **Accepted Community Names** list.
The **SNMP Service Configuration** window appears.
 - b Type the community name of a system that is able to manage your system (the default is public) in the **Community Name** text box and click **Add**.
The **SNMP Service Properties** window appears.
 - c To change a community name, select a community name in the **Accepted Community Names** list and click **Edit**.
The **SNMP Service Configuration** window appears.
 - d Make all necessary edits to the community name of the system that is able to manage your system in the **Community Name** text box, and then click **OK**.
The **SNMP Service Properties** window appears.
- 6 Click **OK** to save the changes.

Enabling SNMP Set Operations

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

- 1 If your system is running Windows Server 2003 64-bit, click the **Start** button, right-click **My Computer**, and point to **Manage**.
The **Computer Management** window appears.
- 2 Expand the **Computer Management** icon in the window, if necessary.
- 3 Expand the **Services and Applications** icon, and then click **Services**.
- 4 Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and click **Properties**.
The **SNMP Service Properties** window appears.
- 5 Click the **Security** tab to change the access rights for a community.
- 6 Select a community name in the **Accepted Community Names** list, and then click **Edit**.
The **SNMP Service Configuration** window appears.
- 7 Set the **Community Rights** to **READ WRITE** or **READ CREATE**, and click **OK**.
The **SNMP Service Properties** window appears.
- 8 Click **OK** to save the changes.

Configuring Your System to Send SNMP Traps to a Management Station

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

- 1 If your system is running Windows Server 2003 64-bit, click the **Start** button, right-click **My Computer**, and point to **Manage**.

The **Computer Management** window appears.

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

The **SNMP Service Properties** window appears.

- 5 Click the **Traps** tab to add a community for traps or to add a trap destination for a trap community.
 - a To add a community for traps, type the community name in the **Community Name** box and click **Add to list**, which is located next to the **Community Name** box.
 - b To add a trap destination for a trap community, select the community name from the **Community Name** drop-down menu and click **Add** under the **Trap Destinations** box.
 - c The **SNMP Service Configuration** window appears.

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

The **SNMP Service Properties** window appears.

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

Configuring the SNMP Agent on Systems Running Supported Red Hat Linux 64-Bit Operating Systems

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



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

SNMP Agent Access Control Configuration

The management information base (MIB) branch implemented by the Instrumentation Service is identified by the OID 1.3.6.1.4.1.674.10892.1. Management applications must have access to this branch of the MIB tree to manage systems running the Instrumentation Service. For Red Hat Linux 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 OID 1.3.6.1.2.1.1) of the MIB tree. This configuration does not allow management applications to retrieve or change Instrumentation Service and other systems management information outside of the MIB-II "system" branch.

If Server Administrator detects this 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 does this by changing the SNMP agent configuration file, `/etc/snmp/snmpd.conf`, in two ways:

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

```
view all included .1
```

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

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

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

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

These changes to the default SNMP agent configuration give read-only access to the entire MIB tree for the "public" community. To ensure that Server Administrator is able to modify the SNMP agent configuration to provide proper access to systems management data, it is recommended that any other SNMP agent configuration changes be made after the installation of Server Administrator.

Changing the SNMP Community Name

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

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

- 1 Find the line that reads:

```
com2sec publicsec default public
```

or

```
com2sec notConfigUser default public
```

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

```
com2sec publicsec default community_name
```

or

```
com2sec notConfigUser default community_name
```

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

```
service snmpd restart
```

Enabling SNMP Set Operations

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

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

- 1 Find the line that reads:

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

or

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

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

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

or

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

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

```
service snmpd restart
```

Configuring Your System to Send Traps to a Management Station

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

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

- 1 Add the following line to the file:

```
trapsink IP_address community_name
```

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

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

```
service snmpd restart
```

Firewall Configuration on Systems Running Red Hat Linux 64-Bit Operating Systems

If you enable firewall security when installing Red Hat Linux 64-bit, 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 using one of the previously described methods, perform the following steps:

- 1 At the Red Hat Linux 64-bit 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 Select the Security Level by tabbing to it and pressing the spacebar. The selected Security Level is indicated by an asterisk.



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

- a To disable the firewall, select **No firewall** or **Disabled** and go to step 7.
 - b To open an entire network interface or the SNMP port, select **High**, **Medium**, or **Enabled** and continue with step 4.
- 4 Tab 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, tab 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 will be opened.

- b** To open the SNMP port on all network interfaces, tab to **Other ports** and type `snmp:udp`.
- 6** Tab to **OK** and press <Enter>. The **Firewall Configuration** screen appears.
- 7** Tab to **OK** and press <Enter>. The **Choose a Tool** menu appears.
- 8** Tab to **Quit** and press <Enter>.

Installing Server Administrator

Overview

The *Systems Management and Documentation* CD provides an HTML Browser interface as well as scripts to install and uninstall Server Administrator on your managed system.

Systems Management and Documentation CD

Using the scripts on the *Systems Management and Documentation* CD, you can install and uninstall Server Administrator on Microsoft® Windows® Server 2003 64-bit and Red Hat® Linux 64-bit operating systems.

Before You Begin

- Read and follow the applicable instructions in "Setup and Administration."
- Read the installation requirements to ensure that your system meets or exceeds the minimum requirements.
- Read the Server Administrator readme file on the *Systems Management and Documentation* CD. The file contains the latest information about software, firmware, and driver versions, in addition to information about known issues.
- Read the installation instructions for your operating system.

Installation Requirements

The following sections describe the Server Administrator general requirements. Operating system-specific installation prerequisites are listed as part of the installation procedures.


- Supported Operating Systems
- System Requirements


Supported Operating Systems

Server Administrator supports each of the following operating systems:

- Microsoft Windows Server 2003 for 64-Bit Itanium 2-based Systems, referred to in this document as Windows Server 2003 64-bit.

- Red Hat Enterprise Linux (AS), version 3, for 64-Bit Systems, referred to in this document as Red Hat Linux 64-bit.

 **NOTE:** Support for updated kernels released by Red Hat and for later versions of Red Hat Linux 64-bit may require the use of Dynamic Kernel Support (see "Dynamic Kernel Support" for an explanation of this feature).

 **NOTE:** See the Server Administrator readme file on the *Systems Management and Documentation* CD for the latest detailed list of the Server Administrator Services that are supported on each supported operating system.

System Requirements

Server Administrator must be installed on each system to be managed. You can then manage each system running Server Administrator locally or remotely through a supported Web browser.

Managed System Requirements

- One of the supported operating systems.
- A minimum of 512 MB of RAM.
- A minimum of 256 MB of free hard-drive space.
- Administrator rights.
- A TCP/IP connection on the monitored system and the remote system to facilitate remote system management.
- One of the supported Web browsers.
- One of the supported systems management protocol standards.
- A mouse, keyboard, and monitor to manage a system locally. The monitor requires a minimum screen resolution of 800 x 600. The recommended setting for the screen resolution is 1024 x 768.

Remote Management System Requirements

- One of the supported Web browsers to manage a system remotely from the Server Administrator home page.
- A TCP/IP connection on the managed system and the remote system to facilitate remote system management.
- A minimum screen resolution of 800 x 600. The recommended screen resolution setting is 1024 x 768.

Supported Web Browsers

A supported Web browser is required to manage a system locally from the Server Administrator home page.

- Microsoft Internet Explorer 5.5 (with Service Pack 2) and 6.0

- Netscape Navigator 7.02 and 7.1
- Mozilla 1.5 and 1.6

Supported Systems Management Protocol Standards

A supported systems management protocol standard must be installed on the managed system before installing Server Administrator. On Windows Server 2003 64-bit operating systems, Server Administrator supports these two systems management standards: Common Information Model/Windows Management Instrumentation (CIM/WMI) and Simple Network Management Protocol (SNMP). On Red Hat Linux 64-bit operating systems, Server Administrator supports the SNMP systems management standard.



NOTE: For information about installing a supported system management protocol standard on your managed system, see your operating system documentation.

Table 3-1 shows the availability of the systems management standards for each supported operating system.

Table 3-1. Availability of Systems Management Protocol by Operating Systems

Operating System	SNMP	CIM/WMI
Windows Server 2003 64-bit operating systems.	Available from the operating system installation media.	Always installed.
Red Hat Linux 64-bit operating systems.	You must install the SNMP package provided with the operating system.	Unavailable.

Installation Procedures

The following installation procedures provide step-by-step instructions for installing and uninstalling Server Administrator for each supported operating system:

- Installing/Uninstalling on Systems Running Windows Server 2003 64-Bit Operating Systems
- Installing/Uninstalling on Systems Running Red Hat Linux 64-Bit Operating Systems

Installing/Uninstalling on Systems Running Windows Server 2003 64-Bit Operating Systems

This section explains how to install and uninstall Server Administrator on a system that is running the Windows Server 2003 64-bit operating system. This section includes the following topics:


- Prerequisites for Installing Server Administrator
- Installing Server Administrator
- Uninstalling Server Administrator

Prerequisites for Installing Server Administrator

- You must have administrator privileges.
- If you want to use supporting agents for SNMP, you must install the operating system support for the SNMP standard before you install Server Administrator. For more information about installing SNMP, see the installation instructions for the operating system you are running on your system.

Installing Server Administrator from the Systems Management and Documentation CD

- 1 Log on with administrator privileges to the system where you want to install Server Administrator.
- 2 Exit any open application programs and disable any virus-scanning software.
- 3 Insert the *Systems Management and Documentation* CD into your system's CD drive.
If the CD does not automatically start the setup program, go to your system's desktop, double-click **My Computer**, double-click the CD drive icon, and double-click the **autorun.exe** file.
- 4 In the left pane, click **Install Dell OpenManage Server Administrator**.
- 5 Select **Open**, and then click **OK** to start the installation process.
Installation messages are displayed in a text file while Server Administrator is being installed.
Server Administrator files are copied to the default installation directory:
`%Windows%\Program Files\Dell\OpenManage`
- 6 Close the text file.

 **NOTICE:** You do not need to reboot your system after installing Server Administrator.

Performing a Scripted Installation of Managed System Software

You can perform a scripted installation from the *Systems Management and Documentation* CD. A scripted installation can be performed by executing **omsa_install.bat** from the root directory. When the installation completes, it displays installation results in Notepad. It also sets an exit status of 0 for success and non-zero for failure.

Scripted unattended installation can be performed by specifying the **-q** option on the command line. This suppresses the display of installation results within Notepad.

Uninstalling Server Administrator

You can uninstall Server Administrator by using the uninstallation script on the *Systems Management and Documentation* CD or where Server Administrator was installed.

Uninstalling Server Administrator By Using the Systems Management and Documentation CD

- 1 Log on with administrator privileges to the system where you want to uninstall Server Administrator.
- 2 Exit any open application programs and disable any virus-scanning software.
- 3 Insert the *Systems Management and Documentation* CD into your system's CD drive. If the CD automatically starts the setup program, exit it.
- 4 Run the following command from the CD's root directory:

```
omsa_install -u
```

➡ **NOTICE:** You do not need to reboot your system after uninstalling Server Administrator.

Uninstalling Server Administrator From Disk

- 1 Go to the following directory: %Windows%\Program Files\Dell\OpenManage.
- 2 Run the following command:

```
omsa_uninstall -u
```

➡ **NOTICE:** You do not need to reboot your system after uninstalling Server Administrator.

Installing/Uninstalling on Systems Running Red Hat Linux 64-Bit Operating Systems

This section explains how to install and uninstall Server Administrator on a system that is running the Red Hat Linux 64-bit operating system.

Additionally, Server Administrator includes Dynamic Kernel Support, a feature that automatically builds a device driver for a running kernel if Server Administrator detects that none of its prebuilt device drivers support that kernel. This section includes the following topics:

- Dynamic Kernel Support
- Prerequisites for Installing Server Administrator
- Installing Server Administrator
- Uninstalling Server Administrator

Dynamic Kernel Support


Server Administrator provides prebuilt device drivers for the precompiled kernels listed in the Server Administrator readme file on the *Systems Management and Documentation* CD. If the running kernel is not one of the precompiled kernels listed in the readme file, or if the running kernel is reconfigured and recompiled in such a way that none of the prebuilt Server Administrator device drivers support the recompiled kernel, Server Administrator may need to use its Dynamic Kernel Support feature to support the running kernel.

For example, if you see either of the following messages during Server Administrator installation or startup, Server Administrator attempted to use its Dynamic Kernel Support feature, but was unable to use the feature because certain prerequisites were not met:

```
Server Administrator is unable to build a device driver for the
running kernel because the needed kernel source files are not
installed.
```

or

```
Building device driver for running kernel... [FAILED]
Needed kernel source files are not installed.
```


 **NOTE:** Server Administrator logs messages to the Red Hat Linux system log file, `/var/log/messages`.

Determining the Running Kernel

- 1 Log in as root.
- 2 To determine the kernel that is running on your system, type the following string and press <Enter>:

```
uname -r
```

The system displays a message about the running kernel.

 **NOTE:** If the running kernel is not one of those listed in the Server Administrator readme file, Server Administrator may need to use Dynamic Kernel Support to support the running kernel.

Dynamic Kernel Support Prerequisites

For Server Administrator to use its Dynamic Kernel Support feature, the following Dynamic Kernel Support prerequisites must be met before installing or restarting Server Administrator:

- The running kernel must be installed from an RPM package file released by Red Hat.
- The running kernel must have loadable module support enabled.
- The `kernel-source` RPM for the running kernel must be installed.
- The GNU make utility must be installed. The `make` RPM provides this utility.
- The GNU C compiler (`gcc`) must be installed. The `gcc` RPM provides this compiler.
- The GNU linker (`ld`) must be installed. The `binutils` RPM provides this linker.

When these prerequisites have been met, Server Administrator's Dynamic Kernel Support automatically builds a device driver when needed during Server Administrator installation or startup. For example:

- If Server Administrator is not installed when an unsupported kernel is booted, Server Administrator builds a device driver for the kernel during installation.

- If Server Administrator is already installed when an unsupported kernel is booted, Server Administrator builds a device driver for the kernel the first time that it starts after the kernel is loaded.



NOTE: *Unsupported kernels* are kernels that are not supported by a prebuilt device driver. You may proceed to the installation instructions if you are running a supported kernel.

Using Dynamic Kernel Support During Server Administrator Installation

To install Server Administrator on a system running a kernel that is not supported by a prebuilt device driver, perform the following steps:

- 1 Ensure that the Dynamic Kernel Support Prerequisites are met on the system to be managed.
- 2 Install Server Administrator on the system.

During installation, Server Administrator builds a device driver for the kernel running on the system.

Using Dynamic Kernel Support After Server Administrator Installation

To enable Server Administrator to support a kernel that is not supported by a prebuilt device driver and is loaded after Server Administrator has been installed, perform the following steps:

- 1 Ensure that the Dynamic Kernel Support Prerequisites are met on the system to be managed.
- 2 Boot the new kernel on the system.

Server Administrator builds a device driver for the kernel running on the system the first time that Server Administrator starts after the kernel is loaded. By default, Server Administrator starts during system startup.


Copying a Dynamically Built Device Driver to Systems Running the Same Kernel


When Server Administrator dynamically builds a device driver for the running kernel, it installs the device driver into the directory `/lib/modules/<kernel>/misc`, where `<kernel>` is the kernel name returned by typing `uname -r`. If you have a system running the same kernel for which a device driver was built, you can copy the newly built device driver to the directory `/var/omsa/dks/<kernel>` on the other system for use by Server Administrator. This action allows Server Administrator to use its Dynamic Kernel Support feature on multiple systems without having to install the kernel source on every system.

For example: System A is running a kernel that is not supported by one of the Server Administrator prebuilt device drivers. System B is running the same kernel. Perform the following steps to build a device driver on system A and copy the device driver to system B for use by Server Administrator:

- 1 Ensure that the Dynamic Kernel Support prerequisites are met on system A.
- 2 Install Server Administrator on system A.
- 3 Server Administrator builds a device driver for the kernel running on system A during installation.


- 4 Type `uname -r` on system A to determine the name of the running kernel.
- 5 Copy any `dcd*.o` files present in the directory `/lib/modules/<kernel>/misc` on system A to the directory `/var/omsa/dks/<kernel>` on system B, where `<kernel>` is the kernel name returned by typing `uname -r` in step 4.

 **NOTE:** The `/lib/modules/<kernel>/misc` directory will contain two or more of the following files: `dcdbas.o`, `dcdesm.o`, `dcdipm.o`, and `dcdtvm.o`.

 **NOTE:** You may have to create the directory `/var/omsa/dks/<kernel>` on system B. For example, if the kernel name is `1.2.3-4smp`, type `mkdir -p /var/omsa/dks/1.2.3-4smp`.

- 6 Install Server Administrator on system B.

Server Administrator detects that the device driver you copied to the directory `/var/omsa/dks/<kernel>` supports the running kernel and uses that device driver.

 **NOTE:** When Server Administrator is uninstalled from system B, the `/var/omsa/dks/<kernel>/dcd*.o` files that you copied to system B are not removed. You must remove the files if they are no longer needed.

Prerequisites for Installing Server Administrator

- You must be logged in with Admin privileges.
- The running kernel must have loadable module support enabled.
- Your `/usr` partition must have at least 200 MB of free space and your `/tmp` and `/var` partitions must have at least 20 MB of free space.
- The `ucd-snmp` or `net-snmp` package that is provided with the operating system must be installed. If you want to use supporting agents for the `ucd-snmp` or `net-snmp` agent, you must install the operating system support for the SNMP standard before you install Server Administrator. For more information about installing SNMP, see the installation instructions for the operating system you are running on your system.

Installing Server Administrator Using the Systems Management and Documentation CD

- 1 Log on with Admin privileges to the system running Red Hat Linux 64-bit where you want to install Server Administrator.
- 2 Exit any open application programs and disable any virus-scanning software.
- 3 Start the X Windows graphical user interface (GUI) using the `startx` command.
- 4 Insert the *Systems Management and Documentation* CD into the CD drive on your system. When the installation completes, it will display installation results in "more." It will also set an exit status of 0 for success and non-zero for failure. Scripted unattended installation can be performed by specifying the `-q` option in the command line. This will suppress the display of installation results within "more."

If the CD mounts automatically, go to step 6.

- 5 Type the following commands if the CD did not mount automatically:

```
mount /mnt/cdrom  
cd /mnt/cdrom  
./autorun
```

- 6 In the left pane, click **Install Dell OpenManage Server Administrator**.
- 7 Click **Open With** to proceed with the installation process, and then type the following command:

```
bin/bash
```

Installation messages are displayed while Server Administrator is being installed.

Server Administrator is installed at `/usr/lib/dell/openmanage` on your system's hard drive.

 **NOTICE:** You do not need to reboot your system to make Server Administrator available for use.

Installing Server Administrator From the Red Hat Linux 64-Bit Command Line

This section describes how to install Server Administrator from the Red Hat Linux 64-bit command line.

Prerequisites for Installing Server Administrator

- You must be logged in with Admin privileges.
- The running kernel must have loadable module support enabled.
- The `ucd-snmp` or `net-snmp` package that is provided with the operating system must be installed.

Installing Server Administrator

- 1 Insert the *Systems Management and Documentation* CD into the CD drive on your system.
- 2 If the CD does not mount automatically, type `mount /mnt/cdrom`.
- 3 Change to the directory that contains the installation shell script by typing the following command:

```
cd /mnt/cdrom
```

- 4 Run the installation script by typing the following command:

```
./omsa_install.sh
```

Installation messages are displayed while Server Administrator is being installed.

Server Administrator is installed at `/usr/lib/dell/openmanage` on your system's hard drive.

 **NOTICE:** You do not need to reboot your system to make Server Administrator available for use.

Uninstalling Server Administrator

This section describes how to uninstall Server Administrator from the Red Hat Linux 64-bit command line.

Prerequisites for Uninstalling Server Administrator

You must be logged in with Admin privileges.


Uninstalling Server Administrator Using the Systems Management and Documentation CD

- 1 Log on with Admin privileges to the system running Red Hat Linux 64-bit where you want to uninstall the managed system components.
- 2 Exit any open application programs and disable any virus-scanning software.
- 3 Insert the *Systems Management and Documentation* CD into the CD drive on your system. If the CD does not automatically mount, type `mount /mnt/cdrom`.

Change to the directory that contains the uninstallation shell script by typing the following command:


```
cd /mnt/cdrom
```

- 4 Run the uninstallation script by typing the following command:
`./omsa_install -u`

 **NOTICE:** You do not need to reboot your system after uninstalling Server Administrator.

Uninstalling Server Administrator From Disk

- 1 Change to the directory that contains the uninstallation shell script by typing the following command:
`cd /usr/lib/dell/openmanage/uninstall`
- 2 Run the uninstallation script by typing the following command:
`./omsa_install.sh`

 **NOTICE:** You do not need to reboot your system after uninstalling Server Administrator.

Using Server Administrator

Starting Your Server Administrator Session

To start a Server Administrator session on a local system running Windows Server 2003 64-bit, click the **Dell OpenManage** icon on your desktop. Clicking the **Dell OpenManage** icon causes the **Log in** window to be displayed.

To start a Server Administrator session on a local or remote system running Windows or Red Hat Linux operating systems, open your Web browser and type one of the following in the address field and press <Enter>:

```
https://hostname:1311
```


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


or

```
https://IP address:1311
```

where *IP address* is the IP address for the managed system and 1311 is the default port


The Dell OpenManage **Log in** window appears.


 **NOTE:** You must type `https://` (instead of `http://`) in the address field to receive a valid response in your browser.


 **NOTE:** The default port for Dell OpenManage is 1311. You can change the port, if necessary. See "Secure Port Server and Security Setup" for instructions on setting up your server preferences.


Logging In and Out

To log into Server Administrator, type your preassigned **Username** and **Password** in the appropriate fields on the Systems Management **Log in** window.

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

 **NOTE:** When logging into Server Administrator from a system running the Microsoft® Windows® Server 2003 64-bit operating system, you cannot use a blank password due to operating system constraints.

 **NOTE:** If you are accessing Server Administrator from a defined domain, you will also need to specify the correct **Domain** name.


 **NOTE:** The **Application** drop-down menu will appear as a nonselectable field for systems that can only access one Dell OpenManage component. The drop-down menu is only functional when two or more Dell OpenManage components are available on the managed system.

To end your Server Administrator session, click **Log Out** on the global navigation bar. The **Log Out** button is located in the upper-right corner of each Server Administrator home page.

Systems Running Windows Server 2003 64-Bit Operating Systems

You must configure the security settings for your browser to log into Server Administrator from a remote management system that is running the Windows Server 2003 64-bit operating system.

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

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


Internet Explorer

- 1 Start your browser.
- 2 Click **Tools**→ **Internet Options**→ **Security**.
- 3 Click the **Local Intranet** icon.
- 4 Click **Sites**→ **Advanced**.
- 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** box.
- 6 Click **OK** to save the new settings.
- 7 Close the browser.
- 8 Log into Server Administrator.

Netscape and Mozilla

- 1 Start your browser.
- 2 Click **Edit**→ **Preferences**.
- 3 Click **Advanced**→ **Scripts and Plugins**.
- 4 Ensure that the Navigator check box is checked under **Enable JavaScript for**.
- 5 Click **OK** to save the new settings.
- 6 Close the browser.
- 7 Log into Server Administrator.

The Server Administrator Home Page

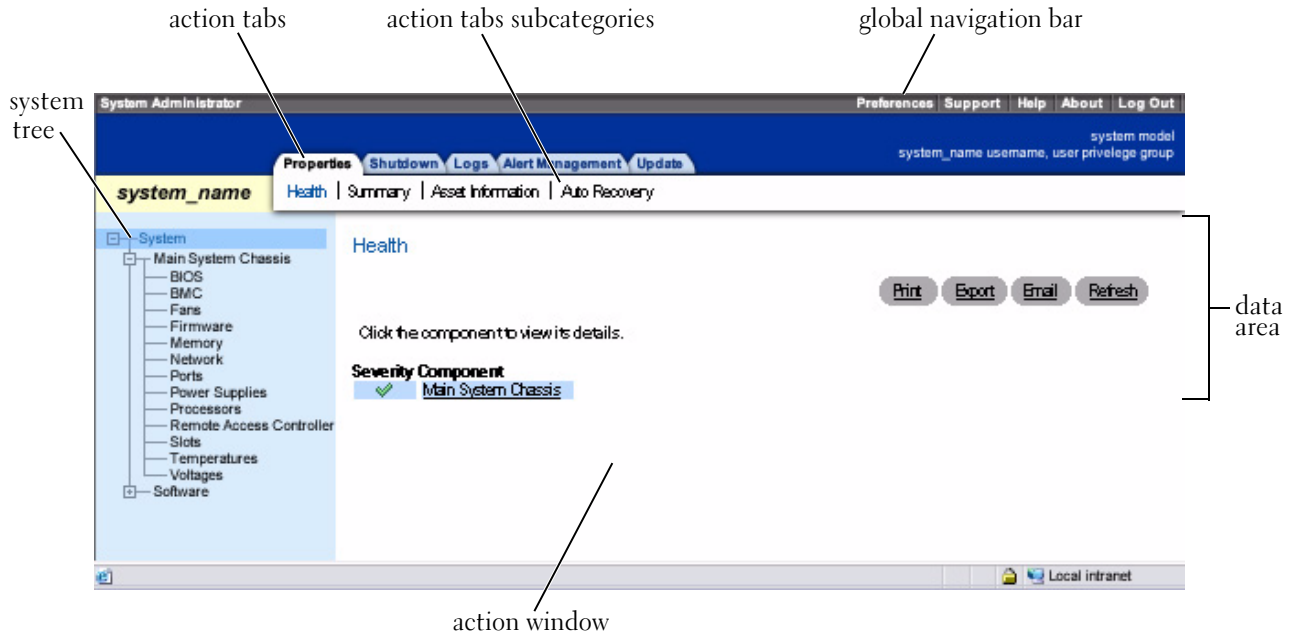
 **NOTE:** Do not use your Web browser toolbar buttons (such as **Back** and **Refresh**) while using Server Administrator. Use only the Server Administrator navigation tools.

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 into 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.

Figure 4-1 shows a sample Server Administrator home page layout for a user logged in with administrator privileges.

Figure 4-1. Sample Server Administrator Home Page

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

NOTE: Many of the system tree objects, system components, action tabs, or data area features are not available to users logged in with only User privileges. Admin 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 Admin privileges have access to the shutdown functionality included under the **Shutdown** tab.



Global Navigation Bar

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

- Clicking **Preferences** opens the **Preferences** home page. See "Using the Preferences Home Page."
- Clicking **Support** connects you to the Dell Support website.
- Clicking **Help** opens the context-sensitive online help window. See "Using the Online Help."
- Clicking **About** displays Server Administrator version and copyright information.
- Clicking **Log Out** ends your 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 **System**, the major categories of system components that may appear are **Main System Chassis** and **Software**.

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 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** object opens an action window in which the **Properties** action tab and **Health** subcategory is displayed in the window's data area.

Data Area

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

System Component Status Indicators

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



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. 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.



A red X indicates that a component has a critical (failure) 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.



A blank space indicates that a component's health status is unknown.

Task Buttons

Most windows opened from the Server Administrator home page contain at least four task buttons: **Print**, **Export**, **Email**, and **Refresh**. Other task buttons are included on specific Server Administrator windows. Log windows, for example, also contain **Save As** and **Clear Log** task buttons. For specific information about individual task buttons, click **Help** on any Server Administrator home page window to view detailed information about the specific window you are viewing.

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



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

Using the Online Help

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

Using the Preferences Home Page

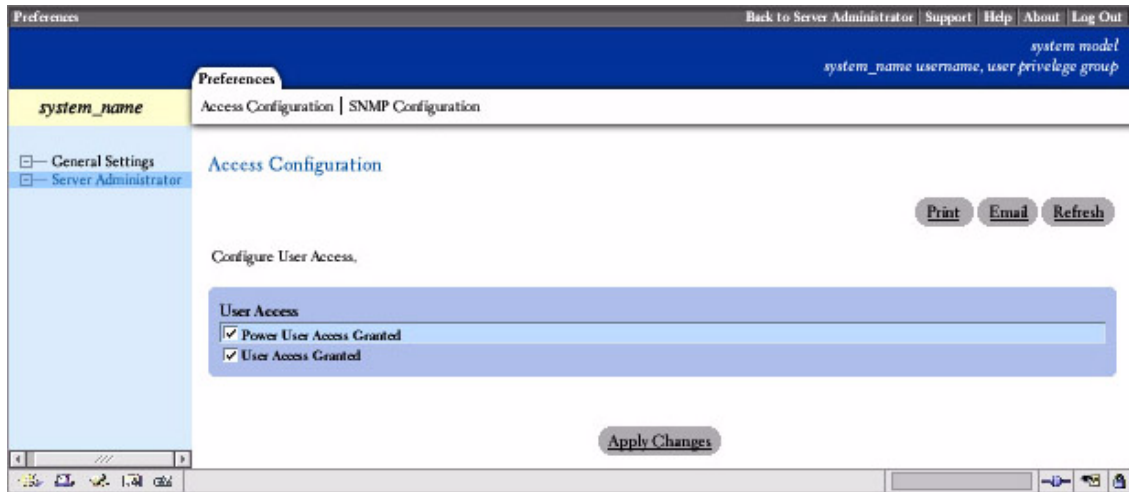
The Preferences home page defaults to the **Access Configuration** window under the **Preferences** tab.

From the Preferences home page you can restrict access to users with User and Power User privileges, set the SNMP password, and configure user settings and secure port server settings.

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

- The global navigation bar provides links to general services.
 - Clicking **Back to Server Administrator** returns you to the Server Administrator home page.
- The left 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.
- The action window displays the available settings and preferences for the managed system.

Figure 4-2 shows a sample Preferences home page layout.

Figure 4-2. Sample Preferences Home Page

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.

In many cases, 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 User's Guide*.

Secure Port Server and Security Setup

This section contains the following topics:

- Setting User and Server Preferences
- X.509 Certificate Management


Setting User and Server Preferences

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

 **NOTE:** You must be logged in with Admin privileges to set or reset user or server preferences.

Perform the following steps to set up your user preferences:


- 1 Click **Preferences** on the global navigation bar.
The **Preferences** home page appears.
- 2 Click **General Settings**.
- 3 To add a preselected e-mail recipient, type the e-mail address of your designated service contact in the **Mail To:** field, and click **Apply Changes**.

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


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

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

- 1 Click **Preferences** on the global navigation bar.
The **Preferences** home page appears.
- 2 Click **General Settings**, and the **Web Server** tab.
- 3 In the **Server Preferences** window, set options as necessary.
 - The **Session Timeout** feature can set a limit on the amount of time that a Server Administrator session can remain active. Select the **Enable** radio button to allow Server Administrator to time out if there is no user interaction for a specified number of minutes. Users whose session times out must log in again to continue. Select the **Disable** radio button to disable the Server Administrator session timeout feature.
 - The **HTTPS Port** field specifies the secure port for Server Administrator. The default secure port for Server Administrator is 1311.

 **NOTE:** Changing the port number to an invalid or in-use port number might prevent other applications or browsers from accessing Server Administrator on the managed system.

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

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

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



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

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

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

X.509 Certificate Management

Web certificates are necessary to ensure the identity of a remote system and ensure that information exchanged with the remote system cannot be viewed or changed by others. To ensure system security, it is strongly recommended that you either generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from a Certification Authority (CA).



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

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

Use the X.509 certificate tool to either generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from a CA. Authorized CAs include Verisign, Entrust, and Thawte.

Controlling Server Administrator

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



NOTE: To control Server Administrator, you must be logged in with administrator privileges (logged in as `root` for Red Hat® Linux 64-bit operating systems).

Starting Server Administrator

This section describes how to start Server Administrator.

Windows Server 2003 64–Bit Operating Systems

To start Server Administrator on systems running the Microsoft® Windows® Server 2003 64-bit operating system, perform the following steps:

- 1 Click the **Start** button and point to **Settings**→ **Control Panel**→ **Administrative Tools**→ **Services**.
The **Services** window appears.
- 2 Right-click the **Secure Port Server** icon.
- 3 Click **Start**.

Red Hat Linux 64–Bit Operating Systems

To start Server Administrator on systems running the Red Hat Linux 64-bit operating system, run the following command from the command line:

```
omawsd start
```

Stopping Server Administrator

This section describes how to stop Server Administrator.

Windows Server 2003 64–Bit Operating Systems

To stop Server Administrator, perform the following steps:

- 1 Click the **Start** button and point to **Settings**→ **Control Panel**→ **Administrative Tools**→ **Services**.
The **Services** window appears.
- 2 Right-click the **Secure Port Server** icon.
- 3 Click **Stop**.

Red Hat Linux 64–Bit Operating Systems

To stop Server Administrator, run the following command from the command line:

```
omawsd stop
```

Restarting Server Administrator

This section describes how to restart Server Administrator.

Windows Server 2003 64–Bit Operating Systems

To restart Server Administrator, perform the following steps:

- 1 Click the **Start** button and point to **Settings**→ **Control Panel**→ **Administrative Tools**→ **Services**.
The **Services** window appears.

- 2 Right-click the **Secure Port Server** icon.
- 3 Click **Restart**.

Red Hat Linux 64-Bit Operating Systems

To restart Server Administrator, run the following command from the command line:

```
omawsd restart
```

Instrumentation Service

Overview

The Server Administrator Instrumentation Service monitors the health of a system and provides rapid access to detailed fault and performance information gathered by industry standard systems management agents. The reporting and viewing features allow retrieval of overall health status for each of the chassis that comprise your system. At the subsystem level, you can view information about the voltages, temperatures, current, 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 summary view. Version information for the BIOS, firmware, operating system, and all installed systems management software is easy to retrieve.

Additionally, systems 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.

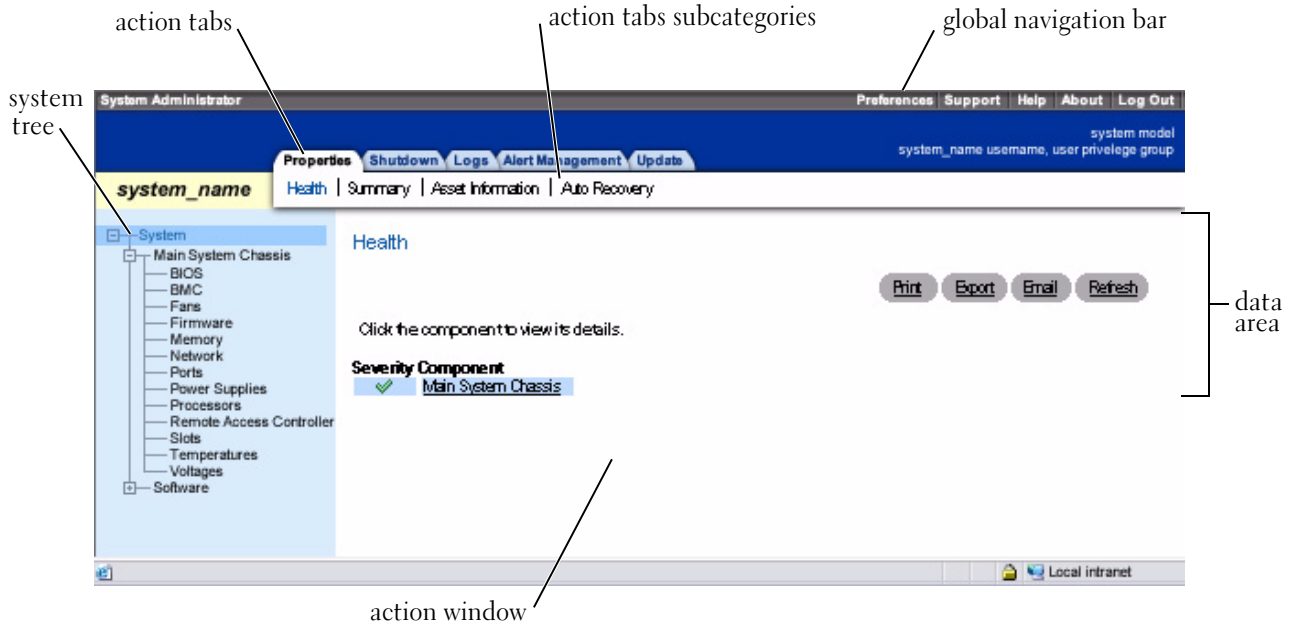


NOTE: For both managed systems and network management stations running Microsoft Windows Server 2003, you must configure the SNMP service to accept SNMP packets. See "Configuring the SNMP Agent for Systems Running Windows Server 2003 64-Bit Operating Systems" for details.

Managing Your System

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

Figure 5-1. Sample Server Administrator Home Page



NOTE: Context-sensitive online help is available for every window of the Server Administrator home page. Clicking **Help** on the global navigation bar 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.

NOTE: Many of the system tree objects, system components, action tabs, action tab subcategories, or data area features are not available to a user logged in with only User privileges. Admin 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 Admin privileges have access to critical system features such as the shutdown functionality included under the **Shutdown** tab.

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

From the Preferences home page you can restrict access to users with User and Power User privileges, set the SNMP password, and configure user settings and secure port server settings.

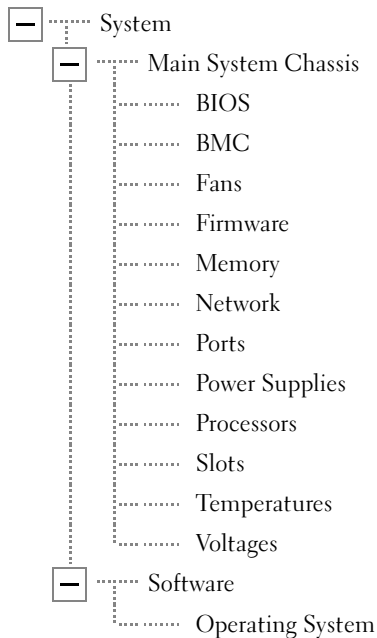
Managing System Tree Objects

The Server Administrator system 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 known as **System**, the major categories of system components that may appear are **Main System Chassis** and **Software**. Under the **Properties** tab, you can view basic information about your operating system.


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.

See Figure 5-2 for available Server Administrator home page system tree objects.

Figure 5-2. Server Administrator Home Page System Tree Objects



Server Administrator Home Page System Tree Objects

-  **NOTE:** Many of the system tree objects, system components, action tabs, action tab subcategories, or data area features are not available to a user logged in with only User privileges. Admin 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 Admin privileges have access to critical system features such as the shutdown functionality included under the **Shutdown** tab

System

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

Properties

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** 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 recovery (watchdog timer) actions for the system being monitored.

Shutdown

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 Server Administrator secure port server (Web server).
 -  **NOTE:** Server Administrator is still available using the CLI when the secure port server is shut down. The CLI functions do not require that the secure port server is running.
 -  **NOTE:** The secure port server starts automatically after a reboot, so you must shut down the secure port server every time a system starts up.


Logs

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 will change from a green check mark (✓) to a yellow triangle containing an exclamation point (⚠) when the log file reaches 80 percent capacity.

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

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

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

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


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

Alert Management

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 component sensor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for instrumented system components. The selected traps will be 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.




Main System Chassis

Clicking the **Main System Chassis** object allows you to manage your system's essential hardware and software components. The system may contain one main system chassis or several chassis. The main system chassis contains the essential components of a system. The **Main System Chassis** object action window can have the **Properties** tab, depending on the user's group privileges.

Properties

Health | Information

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

- View the health or status of hardware components and sensors. Each listed component has a "System Component Status Indicators" icon next to its name. A green check mark () indicates that a component is healthy (normal). A yellow triangle containing an exclamation point () indicates that a component has a warning (noncritical) condition and requires prompt attention. A red X () indicates a component has a critical (failure) condition and requires immediate attention. A blank space () indicates that a component's health status is unknown. The available monitored components include:
 - BIOS
 - BMC
 - Fans
 - Firmware
 - Hardware Log
 - Memory
 - Network
 - Ports
 - Power Supplies
 - Processors
 - Slots
 - Temperatures
 - Voltages
- View information about the main system chassis attributes.

BIOS

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

Properties

Information

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

BMC

Clicking the **BMC** object allows you to manage Baseboard Management Controller (BMC) features such as, general information on BMC. You can also manage the configuration of BMC on a LAN, serial port for BMC, terminal mode settings for the serial port, BMC on a serial over LAN connection, and BMC users.

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

Properties

Information

Under the **Properties** tab, you can view general BMC information.

Configuration

LAN | Serial Port | Serial Over LAN

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

Users

BMC Users

Under the **Users** tab, you can modify the BMC user configuration.



NOTE: If you use another application to configure the BMC while Server Administrator is running, the BMC configuration data displayed by Server Administrator may become out of sync with the BMC. It is recommended that you use Server Administrator to configure the BMC while Server Administrator is running.

Fans

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

Properties

Fan Probes

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

- View the current readings for your system's fan probes.



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

Alert Management

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 will be triggered if the system generates a corresponding event at the selected severity level.

Firmware

Clicking the **Firmware** object allows you 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 **Properties** tab, depending on the user's group privileges.

Properties

Information

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

Alert Management

Alert Actions | SNMP Traps

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

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

Memory

Clicking the **Memory** object allows you 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

Memory

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

Alert Management

Alert Actions | SNMP Traps

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

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

Network

Clicking the **Network** object allows you to manage your system's NICs. Server Administrator monitors the status of each NIC present in your system to ensure continuous remote connection. The **Network** object action window can have the **Properties** tab, depending on the user's group privileges.

Properties

Information

Under the **Properties** tab, you can view information about the NICs installed in your system.

Ports

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

Properties

Information

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

Power Supplies

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

Properties

Elements

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

- View information about your power supply redundancy attributes.
- Check the status of individual power supply elements.

Alert Management

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 power supply returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for power supplies. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Processors

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

Properties

Information

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

Alert Management

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 processor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for processors. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Slots

Clicking the **Slots** object allows you to manage the connectors or sockets on your system board that accept printed circuit boards, such as expansion cards. The **Slots** object action window can have the **Properties** tab, depending on the user's group privileges.

Properties

Information

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

Temperatures

Clicking the **Temperatures** object allows you to manage your system temperature in order to prevent thermal damage to your 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 can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Temperature Probes

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



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

Alert Management

Alert Actions | SNMP Traps

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

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

Voltages

Clicking the **Voltages** object allows you 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

Voltage Probes

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



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

Alert Management

Alert Actions | SNMP Traps

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

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

Software

Clicking the **Software** object allows you 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 can have the **Properties** tab, depending on the user's group privileges.

Properties

Summary

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

Operating System

Clicking the **Operating System** object allows you to view basic information about your operating system. The **Operating System** object action window can have the **Properties** tab, depending on the user's group privileges.

Properties

Information



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

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.

See Figure 5-3 for available Preferences home page configuration options.

Figure 5-3. Preferences Home Page Configuration Options

-  General Settings
-  Server Administrator

Server Administrator

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

Preferences

Access Configuration | SNMP Configuration

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

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

General Settings

Clicking the **General Settings** object allows you to set user and secure port server (Web server) preferences for selected Server Administrator functions. The **General Settings** object action window has the following tabs, depending on the user's group privileges: **User** and **Web Server**.

User

Properties

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

Web Server

Properties | X.509 Certificate

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

- Set secure port server preferences. See "Secure Port Server and Security Setup" for instructions on configuring your server preferences.
- Perform X.509 certificate management by generating a new X.509 certificate, reusing an existing X.509 certificate, or importing a root certificate or certificate chain from a Certification Authority (CA). For more information about certificate management, see "X.509 Certificate Management."

Server Administrator Logs

Overview

Server Administrator allows you 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 Admin or Power User privileges to clear logs or to e-mail logs to their designated service contact.

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

When viewing Server Administrator logs, you can click **Help** on the global navigation bar 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

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

Log Window Task Buttons

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

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

Server Administrator Logs

Server Administrator provides the following logs:

- Hardware Log
- Alert Log
- See the Server Administrator Messages Reference Guide for detailed information about alert messages.
- Command Log

Hardware Log

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

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

Information displayed in the ESM and SEL logs includes:

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

Maintaining the Hardware Log

The status indicator icon next to the log name on the Server Administrator homepage will change from a green check mark (✓) to a yellow triangle containing an exclamation point (⚠) when the log file reaches 80 percent capacity. Be sure to clear the hardware log when it reaches 80 percent capacity. If the log is allowed to reach 100 percent capacity, the latest events are discarded from the log.

Alert Log

Use the Alert log to monitor various system events. The Server Administrator Instrumentation Service 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 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
- A description of the event

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

Command Log

Use the Command log to monitor all of the commands issued by Server Administrator users. The Command log tracks logins, logouts, systems management software initialization, and shutdowns initiated by systems management software, and records the last time the log was cleared.

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 into the Server Administrator home page or the CLI
- A description of the command and its related values

Appendix

Overview

This section provides supplemental information for using Server Administrator.

Setting Alert Actions for Systems Running a Supported Red Hat Linux Operating System

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 writes a message to the console. If the Server Administrator system is running X Windows, you will not see that message by default. To see the alert message when X Windows is running, you must start `xconsole` 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 X Windows, you will not see that message by default. To see the broadcast message when X Windows is running, you must start a terminal such as `gnome-terminal` before the event occurs.

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

- Do not specify X Windows-based applications because Server Administrator cannot execute such applications properly.
- Do not specify applications that require input from the user because Server Administrator cannot execute such applications properly.
- Redirect `stdout` and `stderr` to a file when specifying the application so that you can see any output or error messages.
- If you want to execute multiple applications (or commands) for an alert, create a script to do that and put the full path to the script in the "application to execute" box.

Example 1:

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

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

Example 2:

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

The command in Example 2 executes the mail application to send the message contained in the file `/tmp/alertmsg.txt` to Red Hat® Linux user, Admin, 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.