

Dell OpenManage™
Server Administrator Version 2.0
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*, *PowerEdge*, *Dimension*, *OptiPlex*, *Dell Precision*, *Inspiron*, *Latitude*, and *DellNet* are trademarks of Dell Inc.; *Microsoft*, *Windows*, *MS-DOS*, and *Windows NT* are registered trademarks of Microsoft Corporation; *Novell* and *NetWare* are registered trademarks of Novell Inc.; *Intel* and *Pentium* are registered trademarks and *Intel386* is a trademark of Intel Corporation; *Red Hat* is a registered trademark of Red Hat, Inc.; *VESA* is a registered trademark of Video Electronics Standards Association; *UNIX* is a registered trademark of The Open Group in the United States and other countries; *OS/2* is a registered trademark of International Business Machines Corporation.

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.

December 2004

Contents

1	Introduction	
	Overview	11
	Integrated Features	11
	Installation	11
	Server Administrator Home Page	12
	Instrumentation Service	12
	Remote Access Service	12
	Storage Management Service	12
	Diagnostic Service	13
	Logs	13
	Other Documents You Might Need	13
	Obtaining Technical Assistance	15
2	What's New for Version 2.0	
	Native Install	17
	Installation and Security User's Guide	17
	Update Functionality Moved to Server Update Utility	17
	Enhanced Storage Management Service	17
	Single Sign-On	17
3	Setup and Administration	
	Security Management	19
	Role-Based Access Control	19
	Authentication	20
	Encryption	21
	Assigning User Privileges	21
	Creating Server Administrator Users for Supported Windows Operating Systems	21
	Creating Server Administrator Users for Supported Red Hat Enterprise Linux Operating Systems	23

Creating Server Administrator Users for Supported NetWare Operating Systems	24
Disabling Guest and Anonymous Accounts in Supported Windows Operating Systems	26
Configuring the SNMP Agent	26
Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems	27
Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux Operating Systems	30
Configuring the SNMP Agent on Systems Running Supported NetWare Operating Systems	32
X.509 Certificate Management Prerequisites	35
Prerequisites for Systems Running NetWare Version 5.1.	35
Firewall Configuration on Systems Running Supported Red Hat Enterprise Linux Operating Systems	36
4 Installing Server Administrator	
Overview	39
Dell Installation and Server Management CD	39
Unattended and Silent Installation	40
Before You Begin	40
Installation Requirements	40
Supported Operating Systems	40
System Requirements	41
Installation Procedures	43
Installing Server Administrator with Citrix	43
Considerations Before Installing Storage Management Service	44
5 Using Server Administrator	
Starting Your Server Administrator Session	47
Logging In and Out	47
Systems Running a Supported Microsoft Windows Server 2003 Operating System	48

The Server Administrator Home Page	49
Global Navigation Bar	51
System Tree	51
Action Window	51
Using the Online Help	53
Using the Preferences Home Page	54
Using the Server Administrator Command Line Interface	55
Secure Port Server and Security Setup	55
Setting User and Server Preferences.	55
X.509 Certificate Management	56
Controlling Server Administrator	60
Starting Server Administrator	60
Stopping Server Administrator	60
Restarting Server Administrator	61
6 Instrumentation Service	
Overview	63
Managing Your System	64
Managing System Tree Objects	65
Server Administrator Home Page System Tree Objects	66
System	66
Managing Preferences Home Page Configuration Options	87
General Settings	88
Server Administrator	88
7 Working With the Baseboard Management Controller (BMC)	
Overview	89
Viewing Basic BMC Information	89
Configuring BMC Users	90
Setting BMC Platform Event Filter Alerts	91
Setting Platform Event Alert Destinations.	92

Configuring the BMC to use a Serial Over LAN (SOL) Connection	93
Configuring the BMC to use a Serial Port Connection	94
Configuring the BMC to use a Virtual LAN Connection	95

8 Remote Access Service

Overview	97
Hardware Prerequisites	98
Software Prerequisites	98
Adding and Configuring RAC Users	99
Configuring an Existing RAC User	100
Configuring the RAC Network Properties	102
Configuring the RAC Alert Properties	103
Configuring the SNMP Alert Properties	103
Configuring DRAC III Dial-in (PPP) Users and Modem Settings	104
Adding and Configuring a DRAC III Dial-In (PPP) User	104
Adding and Configuring DRAC III Demand Dial-Out Entries	105
Configuring the DRAC III Modem Settings	106
Configuring the RAC Remote Features Properties	106
Configuring RAC Security	107
Certificate Management	107
Configuring Remote Connect Authentication Options	109
Accessing and Using a Remote Access Controller	110

9 Storage Management Service

Overview	111
Software Prerequisites	112
Hardware Prerequisites	113
Basic Storage Management Service	113
Basic Storage Management and Array Manager	114
Basic Storage Management Tree Objects	114

Enhanced Storage Management Service	114
Enhanced Storage Management Service and Array Manager	115
Enhanced Storage Management Tree Objects	115
Enhanced Storage Management Tasks	116
Comparing the Enhanced Storage Management Service and Array Manager	121
Migrating from Array Manager to the Enhanced Storage Management Service	123
Basic and Enhanced Storage Management Command Line Interface	124
Displaying Online Help	124

10 Diagnostic Service

Overview	125
Devices Supported by the Diagnostic Service	126
Diagnostic Service Features	127
Configuring the Diagnostic Service	128
Configuring the Applications Settings	128
Configuring the Test Execution Settings	129
Re-enumerating Devices	129
Running Diagnostics	130
Scheduling Diagnostics	131
Reviewing Scheduled Tests	132

11 Server Administrator Logs

Overview	133
Integrated Features	133
Log Window Task Buttons	133
Server Administrator Logs	134
Hardware Log	134
Alert Log	134

POST Log	135
Command Log	135

12 Appendix

Overview	137
Setting Alert Actions for Systems Running a Supported Red Hat Enterprise Linux Operating System	137
BMC Platform Events Filter Alert Messages	138
Known Issues	139
Instrumentation Service Issues	139

Glossary	141
--------------------	-----

Figures

Figure 5-1. Sample Server Administrator Home Page	48
Figure 5-2. Gauge Indicator	51
Figure 5-3. Sample Preferences Home Page	52
Figure 6-1. Sample Server Administrator Home Page	62
Figure 6-2. Server Administrator Home Page System Tree Objects	63
Figure 6-3. Preferences Home Page Configuration Options	85

Tables

Table 3-1. User Privileges	17
Table 3-2. Server Administrator User Privilege Levels	18
Table 3-3. Legend for Server Administrator User Privilege Levels	18
Table 4-1. Availability of Systems Management Protocol by Operating Systems	41
Table 4-2. Features Supported by Array Manager and the Enhanced Storage Management Service	42

Table 6-1.	Severity Levels and Component Status	85
Table 8-1.	Certificate Information	107
Table 9-1.	Comparing Enhanced Storage Management Service and Array Manager Features	120
Table 10-1.	Results and Events	124
Table A-1.	BMC PEF Alert Events	136

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.



NOTE: For the purposes of Server Administrator, a system can be a stand-alone system, a server with attached network storage units in separate chassis, or a modular system consisting of one or more server modules in a chassis.

Server Administrator provides information about:

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

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

You can install Server Administrator by using several methods. The *Dell Installation and Server Management* CD provides a setup program to install, upgrade, and uninstall Server Administrator and other managed system software components on your managed system. The *Dell System Management Consoles* CD provides a setup program to install, upgrade, and uninstall management station software components on your management station. Additionally, you can install Server

Administrator on multiple systems through an unattended installation across a network. Lastly, if you have a modular system, or if your Microsoft® Windows® operating system was preinstalled, you already have the Server Administrator installed on your system.

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


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.

Remote Access Service

 **NOTE:** The Remote Access Service is not available on modular systems. You must directly connect to the remote access controller (RAC) on a modular system. See the *Dell Embedded Remote Access/MC User's Guide* for more information.

The Remote Access Service provides a complete, remote system management solution for systems equipped with a RAC solution. The Remote Access Service provides remote access to an inoperable system, allowing you to get the system up and running as quickly as possible. The Remote Access Service also provides alert notification when a system is down and allows you to remotely restart a system. Additionally, the Remote Access Service logs the probable cause of system crashes and saves the most recent crash screen.

Storage Management Service

The Storage Management Service provides storage management information in an integrated graphical view. The current release of Server Administrator provides two staggered versions of the Storage Management Service:

- Basic Storage Management Service

The basic Storage Management Service is similar to the Storage Management Service provided in earlier releases of Server Administrator.

The basic Storage Management Service of Server Administrator:

- Enables you to view the status of local and remote storage attached to a monitored system.
- Supports SCSI, SATA, and ATA. Does not support Fibre Channel.
- Enhanced Storage Management Service

The enhanced Storage Management Service provides additional features for configuring storage. On Windows and Linux, the enhanced Storage Management Service is installed using Express Setup providing that the system does not have an existing Array Manager installation.

In addition to the tasks that you can perform using basic Storage Management Service, enhanced Storage Management Service of Server Administrator:

- Allows you to perform controller and enclosure functions for all supported RAID and non-RAID controllers and enclosures from a single graphical or command line interface without the use of the controller BIOS utilities.
- Protects your data by configuring data redundancy, assigning hot spares, or rebuilding failed drives.

Diagnostic Service



NOTE: The Diagnostic Service is not available on modular systems.

The Diagnostic Service provides a suite of diagnostic programs that run locally on your system or remotely on a system connected to the network. The Diagnostic Service is engineered to diagnose problems on individual systems and to run concurrently with all other applications running on the system under test.

Logs

Server Administrator displays logs of commands issued to or by the system, monitored hardware events, POST 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 documentation CD:

- The *Dell OpenManage™ Installation and Security User's Guide* provides complete information on installation procedures and step-by-step instructions for installing, upgrading, and uninstalling Server Administrator for each supported operating system.
- The *Dell OpenManage Software Quick Installation Guide* provides an overview of applications that you can install on your management station (console) and on your managed systems and procedures for installing your console and managed system applications on systems running supported operating systems.

- The *Dell OpenManage Server Administrator Compatibility Guide* provides compatibility information about Server Administrator installation and operation on various hardware platforms (or systems) running supported Microsoft Windows, Novell® NetWare®, and Red Hat® Enterprise Linux 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 OpenManage Array Manager User's Guide* is a comprehensive reference guide for configuring and managing local and remote storage attached to a system. This document is also available in HTML and PDF formats on the *Dell Installation and Server Management* CD, as well as from the Array Manager console as online help.
- The *Dell Remote Access Controller Installation and Setup Guide* provides complete information about installing and configuring a DRAC III, DRAC III/XT, and an ERA/O controller, configuring an ERA controller, and using a RAC to remotely access an inoperable system.
- The *Dell Remote Access Controller Racadm User's Guide* provides information about using the racadm command-line utility.
- The *Dell Embedded Remote Access/MC Controller User's Guide* provides complete information about configuring and using an ERA/MC controller to remotely manage and monitor your modular system and its shared resources through a network.
- The *Dell™ PowerEdge™ 1655MC Systems — System Configuration Guide* provides an overview of initially setting up a modular system.
- The *Dell OpenManage Remote Install User's Guide* provides information about unattended, simultaneous provisioning and configuration solutions over the network by leveraging image-based technology.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.

- The *Server Update Utility User's Guide* provides information about obtaining and using the Server Update Utility (SUU) to update your Dell PowerEdge server or to view the updates available for any server listed in the Repository.

The *Dell Installation and Server Management* CD contains a readme file for Server Administrator and additional readme files for most applications found on the CD.

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.

What's New for Version 2.0

The following features are new in this release:

Native Install

The Dell OpenManage™ products are now installed using the install process native to the operating system.

Installation and Security User's Guide

The installation information has moved from the User's Guide to the *Dell OpenManage Installation and Security User's Guide*. This guide provides complete information on installation procedures and step-by-step instructions for installing, upgrading, and uninstalling Server Administrator for each supported operating system.

Update Functionality Moved to Server Update Utility

Update functionality is not supported in this release. To update individual components, use component specific Dell Update Packages. Use the Dell Server Update Utility application CD to view the complete version report and to update an entire system. Server Update Utility is a CD-ROM based application for identifying and applying updates to your server. The Server Update Utility can be downloaded from <http://support.dell.com>.

Enhanced Storage Management Service

The enhanced Storage Management Service (Storage Management) is the default install option using Express Setup on Windows systems that do not have an existing Array Manager installation. If Array Manager is already installed on a Windows system, then Express Setup upgrades Array Manager to the latest version and the enhanced Storage Management Service is not installed. On Windows, either the enhanced Storage Management Service or Array Manager can be installed using Custom Setup. Array Manager is not supported on Linux and the enhanced Storage Management Service is installed by default using Express Setup on Linux systems. Likewise, the enhanced Storage Management Service does not support NetWare. On a NetWare system, Array Manager is installed by default using Express Setup.

Single Sign-On


The Single Sign-On option on Windows systems enables all logged in users with sufficient privileges to bypass the login page and access the Server Administrator web application by clicking on the **Dell OpenManage** icon on your desktop. To activate this feature, you must check the

Active Directory Login option on the login page. The desktop icon queries the registry to see if the **Enable Integrated Windows Authentication** option is enabled in Internet Explorer. If this option is enabled, then Single Sign-On is executed, or the normal login page will be displayed. Also ensure that NTLM authentication is not disabled on the Windows network.

 **NOTE:** See the Knowledge Base article at "<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q258063>" for more information.

To check the **Enable Integrated Windows Authentication** option, perform the following steps in Internet Explorer:

- 1 Click **Internet Options** on the **Tools** menu.
- 2 Click the **Advanced** tab, select the **Enable Integrated Windows Authentication (requires restart)** check box under the **Security** section, and then click **OK**.
- 3 Restart Internet Explorer.

 **NOTE:** Server administrators can enable Integrated Windows Authentication by setting the `EnableNegotiate` DWORD value to 1 in the following registry key:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

For local machine access, this does require that you have an account on the machine with the correct privileges (user, power user, or administrator). Other users are authenticated against Microsoft Active Directory.

In order to launch Server Administrator using Single Sign-on authentication against Microsoft Active Directory, the addition of the following parameters must be passed in:

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

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

For example:

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

In order to launch Server Administrator using Single Sign-on authentication against the local machine user accounts, the addition of the following parameters must be passed in:

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

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

For example:

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

Server Administrator has also been extended to allow other products (such as the Dell OpenManage™ IT Assistant) to directly access Server Administrator web pages without going through the logon page (if you are currently logged on and have the requisite privileges).

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, run diagnostic tests, and configure which alert actions are to be taken when a warning or failure event occurs.

Administrators can configure and perform shutdown actions, configure Auto Recovery actions in case a system has a 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 3-1.

Table 3-1. 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 3-2 summarizes which user levels have privileges to access and manage Server Administrator Services.

Table 3-2. Server Administrator User Privilege Levels

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

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

Table 3-3. 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 Authentication

For supported Microsoft® Windows® 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 Authentication

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

Novell NetWare Authentication

For supported Novell[®] NetWare[®] operating systems, Server Administrator authentication is based on the Novell Directory Service (NDS) 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, Red Hat Enterprise Linux, and certain Novell NetWare operating systems to protect the user credentials and other sensitive data that is transmitted over the socket connection when a user accesses the Server Administrator home page. Supported Novell NetWare operating systems use operating system native Java SSL and Secure Authentication Services (SAS)-NetWare International Cryptographic Infrastructure (NICI).

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 Supported Windows Operating Systems
- Creating Server Administrator Users for Supported Red Hat Enterprise Linux Operating Systems
- Creating Server Administrator Users for Supported NetWare 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 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 Supported Windows Operating Systems" for instructions.

Creating Server Administrator Users for Supported Windows Operating Systems



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

Creating Users and Assigning User Privileges for Supported Windows Server 2003 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 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.

Creating Users and Assigning User Privileges for Supported Windows 2000 Operating Systems



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

- 1 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 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 Click the name of the user you want to add, and then click **Add**.
- 10 Click **Check Names** to validate the user name that you are adding.
- 11 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 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 Supported Red Hat Enterprise Linux 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.

Creating Server Administrator Users for Supported NetWare Operating Systems

 **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 Log in with Admin privileges.
- 2 Right-click the container in which a user account is to be created.
- 3 Click **NEW** and select **USER**.
- 4 Complete the required fields and click **OK**.

 **NOTICE:** You must assign a password to every user account that can access Server Administrator to protect access to your critical system components.

An icon labeled with the new user name appears in the current container.

- 5 Right-click the icon labeled with the new user name and click **Trustees of this Object**.
- 6 Select *username.contextName* and click **Assigned Rights**.

By default there are three entries in the **Assigned Rights** category: **Login Script**, **Print Job Configuration**, and **[All Attribute Rights]**.

- 7 Select **Login Script**, and enable the **Read** and **Add Self** fields.
- 8 Select **Print Job Configuration**, and enable the **Read** and **Add Self** fields.
- 9 Select **[All Attribute Rights]**, and enable the **Read** and **Add Self** fields.

New users can now log into Server Administrator with User privileges.

Creating Users With Power User Privileges

- 1 Log in with Admin privileges.
- 2 Right-click the container in which a user account is to be created.
- 3 Click **NEW** and select **USER**.
- 4 Complete the required fields and click **OK**.



NOTICE: You must assign a password to every user account that can access Server Administrator to protect access to your critical system components.

An icon labeled with the new user name appears in the current container.

- 5 Right-click the icon labeled with the new user name and click **Properties**.
- 6 Click **NDS Rights**.
- 7 Select *username.contextName* and click **Assigned Rights**.
- 8 Click **Add Property**.
- 9 Select **ACL** and click **OK**.
- 10 Enable the **Read** and **Write** fields by putting a check mark in the check box.
- 11 Click **OK**.

New users can now log into Server Administrator with Power User privileges.

Creating Users With Admin Privileges

- 1 Log in with Admin privileges.
- 2 Right-click the container in which a user account is to be created.
- 3 Click **NEW** and point to **USER**.
- 4 Complete the required fields and click **OK**.



NOTICE: You must assign a password to every user account that can access Server Administrator to protect access to your critical system components.

An icon labeled with the new user name appears in the current container.


- 5 Right-click the icon labeled with the new user name and click **Trustees of this Object**.
- 6 Select *username.contextName* and click **Assigned Rights**.

By default there are three entries in the **Assigned Rights** category: **Login Script**, **Print Job Configuration**, and **[All Attribute Rights]**.

- 7 Select **Login Script**, and enable the **Read**, **Write**, **Add Self**, and **Supervisor** fields.
- 8 Select **Print Job Configuration**, and enable the **Read**, **Write**, **Add Self**, and **Supervisor** fields.
- 9 Select **[All Attribute Rights]**, and enable the **Read**, **Write**, **Add Self**, and **Supervisor** fields.

New users can now log into Server Administrator with Admin privileges.

Disabling Guest and Anonymous Accounts in Supported Windows Operating Systems

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


- 1 If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer**, and point to **Manage**. If your system is running Windows 2000, 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. In most cases, SNMP is installed as part of your operating system installation. An installed supported systems management protocol standard, such as SNMP, is required before installing Server Administrator. 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 and Array Manager, 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 Supported Windows Operating Systems
- Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux Operating Systems
- Configuring the SNMP Agent on Systems Running Supported NetWare Operating Systems

Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems

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



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

Enabling SNMP Access By Remote Hosts

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

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

- 1 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, click the **Start** button, right-click **My Computer**, and point to **Manage**. If your system is running Windows 2000, 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, click the **Start** button, right-click **My Computer**, and point to **Manage**. If your system is running Windows 2000, 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, click the **Start** button, right-click **My Computer**, and point to **Manage**. If your system is running Windows 2000, 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 box and click **Add** under the **Trap Destinations** box.
 - c The **SNMP Service Configuration** window appears.
Type in the trap destination and click **Add**.
The **SNMP Service Properties** window appears.

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

Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux 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 and Array Manager, 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 Enterprise 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. It 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 above, it modifies the line so that it reads:

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

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

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

Configuring the SNMP Agent on Systems Running Supported NetWare Operating Systems

Server Administrator uses the SNMP services provided by the NetWare 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 station applications such as IT Assistant and Array Manager, perform the following tasks.



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


Changing the SNMP Community Name

The SNMP community name used by management applications must match an SNMP community name configured on the system running Server Administrator so that the management station applications can retrieve management information from Server Administrator.

To change the SNMP community name used for retrieving management information from a Server Administrator system, perform the following steps:

- 1 At the NetWare command line console, type `load inetcfg` and press `<Enter>`.
The **Internetworking Configuration** menu appears.
- 2 Select the **Manage Configuration** menu item.
The **Manage Configuration** menu appears.
- 3 Select the **Configure SNMP Parameters** menu item.
The **SNMP Parameters** menu appears.
- 4 Select the **Monitor State** menu item to configure monitor community handling.

The **Monitor Community Handling** menu choices are **Any Community May Read**, **Leave as Default Setting**, **No Community May Read**, and **Specified Community May Read**.


 **NOTE:** Press <F1> for more information about the **Monitor State** menu item. Press <Esc> to clear the help window.

- 5 Press <Esc> to exit the **SNMP Parameters** menu.
A message box appears, prompting you to save changes.
- 6 Select **Yes**.
The **Manage Configuration** menu appears.
- 7 Press <Esc> to exit the **Manage Configuration** menu.
The **Networking Configuration** menu appears.
- 8 Select the **Reinitialize System** menu item to make the configuration changes active.

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, perform the following steps:


- 1 At the NetWare command line console, type `load inetcfg` and press <Enter>.
The **Networking Configuration** menu appears.
 - 2 Select the **Manage Configuration** menu item.
The **Manage Configuration** menu appears.
 - 3 Select the **Configure SNMP Parameters** menu item.
The **SNMP Parameters** menu appears.
 - 4 Select the **Control State** menu item to configure control community handling.
The **Control Community Handling** menu choices are **Any Community May Write**, **Leave as Default Setting**, **No Community May Write**, and **Specified Community May Write**.
-  **NOTE:** Press <F1> for more information about the **Control State** menu item. Press <Esc> to clear the help window.
- 5 Press <Esc> to exit the **SNMP Parameters** menu.
A message box appears, prompting you to save changes.
 - 6 Select **Yes**.
The **Manage Configuration** menu appears.

- 7 Press < Esc > to exit the **Manage Configuration** menu.
The **Networking Configuration** menu appears.
- 8 Select the **Reinitialize System** menu item to make the configuration changes active.

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. 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 a system running Server Administrator to send SNMP traps to a management station, perform the following steps:

- 1 At the NetWare command line console, type `load inetcfg` and press < Enter > .
The **Networking Configuration** menu appears.
 - 2 Select the **Manage Configuration** menu item.
The **Manage Configuration** menu appears.
 - 3 Select the **Configure SNMP Parameters** menu item.
The **SNMP Parameters** menu appears.
 - 4 Select the **Trap State** menu item to configure trap community handling.
The **Trap Handling** menu choices are **Do Not Send Traps**, **Leave as Default Setting**, and **Send Traps With Specified Community**.
-  **NOTE:** Press < F1 > for more information about the **Trap State** menu item. Press < Esc > to clear the help window.
- 5 Press < Esc > to exit the **SNMP Parameters** menu.
A message box appears, prompting you to save changes.
 - 6 Select **Yes**.
The **Manage Configuration** menu appears.
 - 7 Press < Esc > to exit the **Manage Configuration** menu.
The **Networking Configuration** menu appears.
 - 8 Select the **Protocols** menu item.
The **Protocol Configuration** menu appears.
 - 9 Select the **TCP/IP** menu item.
The **TCP/IP Protocol Configuration** menu appears.
 - 10 Select the **SNMP Manager Table** menu item.
The **SNMP Manager Table** menu appears.

11 Select one of the following **SNMP Manager Table** menu items:

- Press < Ins > to add SNMP trap destinations.
- Press < Enter > to modify SNMP trap destinations.
- Press < Del > to delete SNMP trap destinations.



NOTE: Press <F1> for more information about the **SNMP Manager Table** menu item. Press <Esc> to clear the help window.

12 Press < Esc > to exit the **SNMP Manager Table** menu.

A message box appears, prompting you to update the database.

13 Select **Yes**.

The **TCP/IP Protocol Configuration** menu appears.

14 Press < Esc > twice to exit the **TCP/IP Protocol Configuration** menu.

The **Internetworking Configuration** menu appears.

15 Restart your system to make the configuration changes active.

X.509 Certificate Management Prerequisites

Web certificates are necessary to ensure the identity of a remote system and to ensure that information exchanged with the remote system cannot be viewed or changed by others.


This section explains the administrative prerequisites for ensuring your ability to generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from Certification Authority (CA) on each supported operating system.

The X.509 certificate management is provided through the Server Administrator home page for all supported operating systems except NetWare 5.1. Additionally, NetWare 5.1 is the only supported operating system that has installation prerequisites to allow certificate management. See "Prerequisites for Systems Running NetWare Version 5.1."

Prerequisites for Systems Running NetWare Version 5.1

The X.509 certificate management for systems running NetWare version 5.1 (with Service Pack 5 or later) requires that the following procedures be performed before installing Server Administrator:

- 1 At the NetWare command line console, type `load nwconfig` and press < Enter > .
- 2 Select **Product Options**.
- 3 Select **View/Configure/Remove Installed options**.
- 4 Verify that PKIS (Novell Public Key Infrastructure Services) is installed.
- 5 Verify that SAS (Secure Authentication Services) is installed.
- 6 Verify that NICI (NetWare International Cryptographic Infrastructure) is installed.

 **NOTE:** PKIS, SAS, and NCI are installed by default. If any of these products are not currently installed, you must install the product from your Novell NetWare 5.1 operating system CD. After installation, you must reapply the correct support patch.

After installing Server Administrator, go to "Secure Port Server and Security Setup" to complete the X.509 certificate management procedures.


Firewall Configuration on Systems Running Supported Red Hat Enterprise Linux Operating Systems

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

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

To open the SNMP port using one of the previously described methods, perform the following steps:

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


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

The **Choose a Tool** menu appears.

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

The **Firewall Configuration** screen appears.

- 3 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 using the X Window System GUI, pressing <F1> may not provide information about firewall security levels on newer versions of Red Hat Enterprise Linux.

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

You can install Server Administrator using several methods. The *Dell Installation and Server Management CD* provides a setup program to install, upgrade, and uninstall Server Administrator and other managed system software components on your managed system. The *Dell System Management Consoles CD* provides a setup program to install, upgrade, and uninstall management station software components on your management station. Additionally, you can install Server Administrator on multiple systems through an unattended installation across a network. If you have a factory installed Microsoft® Windows® or Red Hat® Enterprise Linux operating system, Server Administrator will be already installed on your system. Follow the configuration wizard to set up Server Administrator. For details, See the *Dell OpenManage Installation and Security User's Guide*.


 **NOTE:** Upgrading to the most recent version of Server Administrator does not require that you uninstall any previously installed software components. The setup program on the *Installation and Server Management CD* automatically uninstalls, and then upgrades the managed system software components that are appropriate for your particular system's hardware configuration.

See the *Dell OpenManage Installation and Security User's Guide* for information on installation procedures and step-by-step instructions for installing, upgrading, and uninstalling Server Administrator on each supported operating system.

Dell Installation and Server Management CD

The *Dell Installation and Server Management CD* provides a setup program to install, upgrade, and uninstall Server Administrator and other managed system software components on your managed system. Additionally, you can install Server Administrator on multiple systems through an unattended installation across a network.

Using the setup program on the *Dell Installation and Server Management CD*, you can install and upgrade Server Administrator on systems running all supported operating systems. On systems running supported Microsoft Windows and Red Hat Enterprise Linux operating systems, you can uninstall Server Administrator with the *Dell Installation and Server Management CD* or through the operating system. On systems running supported Novell® NetWare® operating systems, you can only uninstall Server Administrator through the operating system.

 **NOTE:** Server Administrator installation is not supported on Dell™ PowerEdge™ 300, 2300, 4300, 4350, 6300, or 6350 systems, or on systems containing a version of systems management software prior to version 3.0.

Unattended and Silent Installation

You can use the *Dell Installation and Server Management* CD to perform an unattended installation and uninstallation of Server Administrator on systems running supported Microsoft Windows, Red Hat Enterprise Linux, and Novell Netware operating systems. Additionally, you can install and uninstall Server Administrator from the command line on systems running supported Microsoft Windows, Red Hat Enterprise Linux, and Novell Netware 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 *Dell OpenManage Installation and Security User's Guide* for step-by-step instructions on installing, upgrading, and uninstalling Server Administrator for each supported operating system.
- Read the *Server Administrator Compatibility Guide*. This document contains compatibility information about Server Administrator installation and operation on various hardware platforms (or systems) running supported Microsoft Windows, Novell NetWare, and Red Hat Enterprise Linux operating systems.
- Read the Dell OpenManage Install readme file on the *Dell Installation and Server Management* CD. The file contains the latest information about new features, in addition to information about known issues.
- Read the Server Administrator readme file on the *Dell Installation and Server Management* 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 2000 Server family (includes Windows 2000 Server SP3 and greater, Windows 2000 Advanced Server SP3 and greater, and Windows 2000 Small Business Server [SBS])

- Microsoft Windows Server 2003 family (includes Web, Standard, and Enterprise editions) and Microsoft Windows Small Business Server [SBS] 2003
- Red Hat Enterprise Linux AS, (Version 2.1)
- Red Hat Enterprise Linux AS, ES, and WS, (Version 3)



NOTE: Support for updated kernels released by Red Hat and for later versions of Red Hat Enterprise Linux may require the use of Dynamic Kernel Support (see *Installation and Security User's Guide* for an explanation of this feature).

- Novell NetWare, version 5.1 (with Service Pack 6 or later, JVM 1.3.1_0)
- Novell NetWare, version 6.5



NOTE: See the Server Administrator readme file on the *Dell Installation and Server Management* CD or the *Compatibility Guide* on the *Product 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.


The Prerequisite Checker (**setup.exe**) on the *Dell Installation and Server Management* CD will automatically analyze your system to determine if the system requirements have been met. (See section on Prerequisite Checker for Windows)

Managed System Requirements

- One of the supported operating systems.
- A minimum of 64 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 screen resolution setting is 1024 x 768.
- The Server Administrator Remote Access Service requires that a remote access controller (RAC) is installed on the system to be managed. See "Remote Access Service" and the *Dell Remote Access Controller Installation and Setup Guide* or the *Dell Embedded Remote Access/MC Controller User's Guide* for complete software and hardware requirements.

 **NOTE:** The RAC software is installed as part of the **Express Setup** and **Custom Setup** installation options when installing managed system software from the *Dell Installation and Server Management* CD, provided that the managed system meets all of the RAC installation prerequisites. See "Remote Access Service" and the *Dell Remote Access Controller Installation and Setup Guide* or the *Dell Embedded Remote Access/MC Controller User's Guide* for complete software and hardware requirements.

- The enhanced Storage Management Service is installed by default using **Express Setup** on systems that do not have an existing installation of Dell OpenManage™ Array Manager. If you wish to install Array Manager instead of the enhanced Storage Management Service, use **Custom Setup**. On the other hand, if the system has an existing installation of Array Manager, then Array Manager is installed by default using **Express Setup**. In this case, if you wish to install the enhanced Storage Management Service, use **Custom Setup**.

 **NOTE:** See the *Dell OpenManage Array Manager User's Guide* for complete software and hardware requirements.


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 6.0
- Mozilla 1.7.1 and 1.7.3

 **NOTE:** For systems running Red Hat Enterprise Linux AS, version 2.1, verify that you have either Mozilla 1.7.1 or 1.7.3 installed.

Supported Systems Management Protocol Standards

A supported systems management protocol standard must be installed on the managed system before installing Server Administrator. On supported Microsoft Windows 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 supported Red Hat Enterprise Linux and Novell NetWare 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 4-1 shows the availability of the systems management standards for each supported operating system.

Table 4-1. Availability of Systems Management Protocol by Operating Systems

Operating System	SNMP	CIM/WMI
Supported Microsoft Windows operating systems.	Available from the operating system installation media.	Always installed.
Supported Red Hat Enterprise Linux operating systems.	You must install the SNMP package provided with the operating system.	Unavailable.
Supported Novell NetWare operating systems.	Always installed.	Unavailable.

Prerequisite Checker for Windows

The **setup.exe** prerequisite checker program, located in the Windows directory on the *Dell Installation and Server Management CD*, provides the capability of examining the pre-requisite status for software components without launching the actual installation. This program displays a status window that provides information about the system hardware that some software components may require for operation.

The Prerequisite Check can be executed silently using **runprereqcheck.exe /s**.

Installation Procedures

See the *Dell OpenManage Installation and Security User's Guide* for information on installation procedures and step-by-step instructions for installing, upgrading, and uninstalling Server Administrator on each supported operating system.

Installing Server Administrator with Citrix

If you want to install Server Administrator with Citrix, you must perform the installation in the following order:

- 1 Install the operating system using the *Dell Installation and Server Management CD*.



NOTE: Do not install Server Administrator or other system management software, until you have installed the Citrix software.

- 2 Install the Citrix software. See your Citrix documentation for complete information about installing and configuring the Citrix software.
- 3 Install Server Administrator using the *Dell Installation and Server Management CD*.

All applications (including Server Administrator) work fine if installed **after** installing Citrix. Citrix remaps all your hard drive letters when installed.

For example, if you install Server Administrator on drive “C:” and then install Citrix, it will change your drive letter “C:” to “M:”. This results in Server Administrator not working properly if you install Citrix after installing Server Administrator. You can repair Server Administrator by typing **msiexec.exe /fa SysMgmt.msi**.

Considerations Before Installing Storage Management Service

The enhanced Storage Management Service and Array Manager are two separate storage management product offerings. These products cannot be installed together; you can use one or the other to manage your storage controllers. After installation, Array Manager is launched separately from the Server Administrator. The enhanced Storage Management Service provides the same features as Array Manager and is integrated with Server Administrator. The enhanced Storage Management Service is a replacement for Array Manager.

The enhanced Storage Management Service is installed by default using Express Setup on systems that do not have an existing installation of Array Manager. If Array Manager is already installed, then Express Setup installs the latest version of Array Management and the enhanced Storage Management Service is not installed. You can use Custom Setup to install either Array Manager or the enhanced Storage Management Service regardless of whether the system has an existing Array Manager installation or not. If you install the enhanced Storage Management Service, any previous installation of Array Manager will be uninstalled.

Choosing between the Enhanced Storage Management Service and Array Manager

Although the enhanced Storage Management Service is a replacement for Array Manager, there may be situations in which Array Manager is the preferred choice.

The following table summarizes significant differences in supported features between Array Manager and the enhanced Storage Management Service.

Table 4-2. Features Supported by Array Manager and the Enhanced Storage Management Service

Feature	Array Manager	Enhanced Storage Management Service
Linux support	No	Yes
NetWare support	Yes	No
Windows Server 2003 32-bit support	Yes	Yes
Windows Server 2003 64-bit support	No	No

Table 4-2. Features Supported by Array Manager and the Enhanced Storage Management Service

Feature	Array Manager	Enhanced Storage Management Service
Fiber Channel hardware management	Yes (Dell PowerVault 660F storage system)	No
Windows 2000 disk and volume management	Yes (See the Array Manager documentation for details.)	No

PERC Console and FAST Compatibility Issues When Installing the Enhanced Storage Management Service

Installing the enhanced Storage Management Service on a system that has FAST or the PERC Console installed is an unsupported configuration. In particular, you may find that the enhanced Storage Management Service or the FAST features are disabled at run time when using the enhanced Storage Management Service on a system that also has FAST installed. Therefore, it is recommended that you uninstall FAST and the PERC Console before installing the enhanced Storage Management Service.

The enhanced Storage Management Service replaces all storage management features provided by FAST and the PERC Console. In addition, the enhanced Storage Management Service has features not provided by FAST and the PERC Console.

Compatibility With Linux Utilities When Installing the Enhanced Storage Management Service

It is recommended to not install the enhanced Storage Management Service on a Linux system that has RAID storage management utilities provided by Dell or other vendors. You should uninstall these utilities before installing the enhanced Storage Management Service. The enhanced Storage Management Service replaces the storage management features provided by these utilities. Examples of the Linux utilities provided by Dell or other vendors include:

- LinFlash
- DellMgr
- DellMON
- LINLib
- MegaMgr
- MegaMON


Prerequisite Drivers and Firmware on Linux and the Enhanced Storage Management Service

On Linux, the enhanced Storage Management Service installation is unable to detect whether the drivers and firmware on the system are at the required level for installing and using Storage Management. When installing on Linux, you will be able to complete the installation regardless of whether the driver and firmware versions meet the required level. If the driver and firmware versions do not meet the required level, however, you may not have access to all functions provided by the enhanced Storage Management Service. At the enhanced Storage Management Service runtime, check your application log files for notifications on outdated firmware versions. See the enhanced Storage Management Service readme for a complete listing of supported controller firmware and driver versions.

Install and Upgrade Scenarios for the Enhanced Storage Management Service and Array Manager

On Windows operating systems, the enhanced Storage Management Service is installed by default (using **Express Setup**) provided that the installation process does not detect the presence of Array Manager on the system. If Array Manager is detected, then the installation upgrades Array Manager to the latest version and the enhanced Storage Management Service is not installed. When using **Custom Setup**, either the enhanced Storage Management Service or Array Manager can be installed. The enhanced Storage Management Service cannot be installed on a system that has Array Manager (managed system component). However, the Array Manager management station component (console) can reside on the same system as the enhanced Storage Management Service.

If you wish to upgrade an Array Manager installation to the enhanced Storage Management Service, use **Custom Setup** and select Storage Management. The installation process will then uninstall Array Manager and install the enhanced Storage Management Service. It is important to upgrade using **Custom Setup** in order to preserve the names of the virtual disks created with Array Manager. If you uninstall Array Manager through any means other than upgrading to the enhanced Storage Management Service using **Custom Setup**, then the enhanced Storage Management Service will rename the virtual disks created with Array Manager.

 **NOTE:** See the *Dell OpenManage Installation and Security User's Guide* for more information on the **Express Setup** and **Custom Setup** options.

On a system with the enhanced Storage Management Service, you cannot replace the enhanced Storage Management Service with Array Manager without first uninstalling the enhanced Storage Management Service manually.

Array Manager is the only installation choice on NetWare. The enhanced Storage Management does not support NetWare in this release. On Linux, the enhanced Storage Management Service is the only installation choice. Array Manager does not support Linux.

Using Server Administrator

Starting Your Server Administrator Session

To start a Server Administrator session on a local system, 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 remote system, 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://` (not `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.




NOTE: Before remotely logging into Server Administrator on a system running a supported Novell® NetWare® operating system, Users and Power Users must first authenticate their user rights by logging into the managed NetWare system.


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. See "Single Sign-On" for information on how you can bypass the login page and access the Server Administrator web application by clicking on the **Dell OpenManage** icon on your desktop.




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 a supported Microsoft® Windows® Server 2003 operating system, you cannot use a blank password due to operating system constraints.

 **NOTE:** When logging into Server Administrator from a remote system running a supported Microsoft Windows Server 2003 operating system, you cannot use a blank password due to operating system constraints.

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.


Click the **Active Directory Login** check box to log in using Microsoft Active Directory.

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 a Supported Microsoft Windows Server 2003 Operating System

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

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.

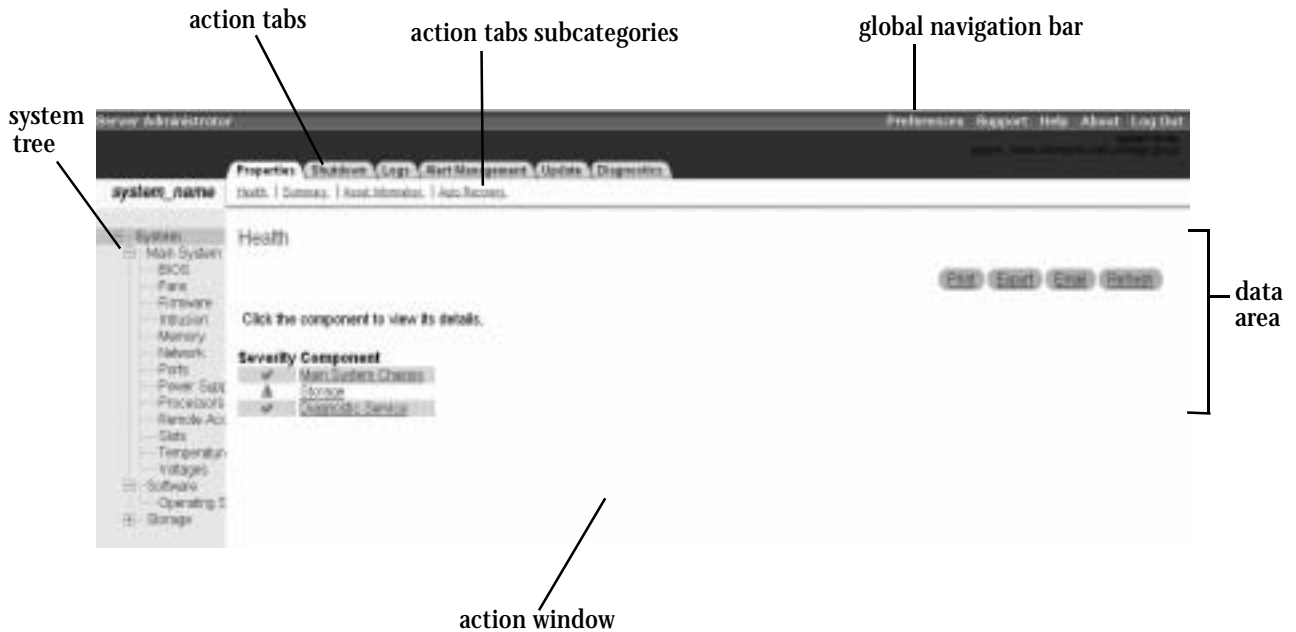
With only a few exceptions, the Server Administrator home page has three main areas:

- 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 5-1 shows a sample Server Administrator home page layout for a user logged in with administrator privileges.

Figure 5-1. 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**, **Software**, and **Storage**.

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

Action Window

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

Clicking an object on the system 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.

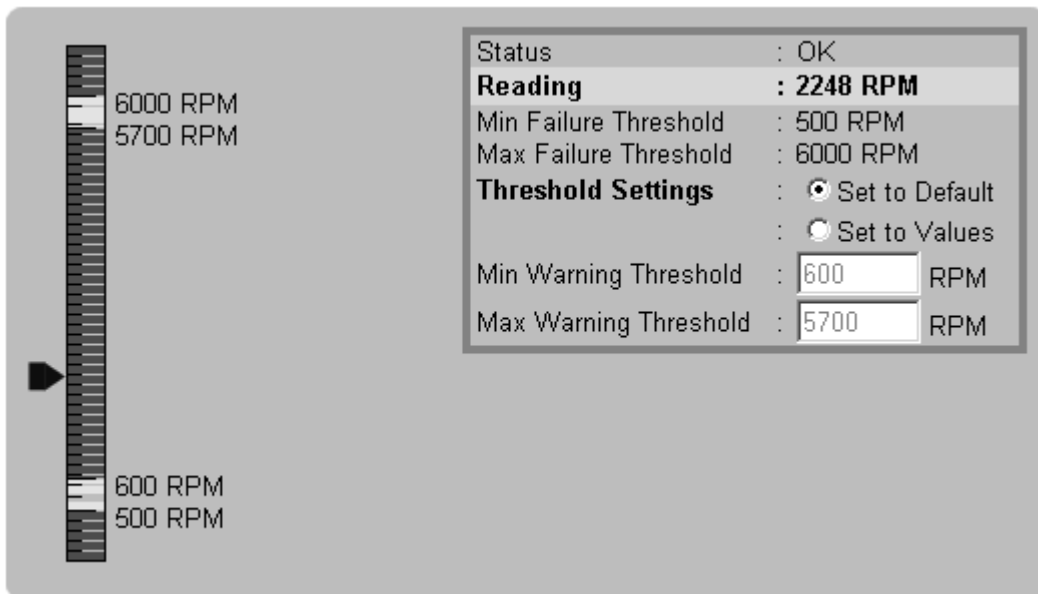
Underlined Items

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. For example, Figure 5-2 shows readings from a system's CPU fan probe.

Figure 5-2. 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 5-3 shows a sample Preferences home page layout.

Figure 5-3. 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.

 **NOTE:** Systems running supported Novell NetWare operating systems must have Novell Java virtual machine (JVM) for NetWare version 1.2 or later to perform certificate management through the Preferences home page. Novell JVM for NetWare version 1.2 or later is installed as part of the NetWare 6.5 or later operating system installation. See the Novell website at www.novell.com for information about upgrading to Novell JVM for NetWare version 1.2 or later.


Exceptions for Systems Running Supported Novell NetWare Operating Systems

The X.509 certificates cannot be managed through the **Preferences** home page for systems running NetWare 5.1 with a version of Novell JVM for NetWare that is earlier than 1.2. You must perform certificate management with the Novell Certificate Server using ConsoleOne running on a NetWare client system if your managed system uses a version of Novell JVM for NetWare that is earlier than 1.2. By default, ConsoleOne is located in the mapped **public** directory of a NetWare client system.

 **NOTE:** Novell Certificate Server cannot be managed using ConsoleOne running on a NetWare server console.

Creating a New Server Certificate

Using ConsoleOne, you can create or recreate a server certificate if yours becomes corrupted.

 **NOTE:** Back up your critical server certificate information before beginning the following procedures.

To create a new server certificate signed by the NDS Organizational CA, perform the following steps:

- 1 Log in with Admin privileges to a NetWare client system and map a drive to the **sys:\public** directory on the managed system.
Double-click **ConsoleOne**.
- 2 Right-click the container object that contains the system to be managed, select **New**, and click **Object**.
The **New Object** window appears.
- 3 Select **NDSPKI: Key Material** and click **OK**.
The **Create Server Certificate (KeyMaterial)** window appears. The **Standard** creation method is selected by default.
- 4 Type the **Certificate name**, and click **Next**.
- 5 Click **Finish**.

- 6 Edit the **sys:\system\dell\omange\IWS\config\server_properties.ini** and **sys:\system\dell\omange\IWS\config\client_properties.ini** files by editing the following line:
`nssl.keystore = certificate name - hostname`
 where *certificate name* is the name of the certificate you just created and *hostname* is the name of the managed system running NetWare
- 7 Log into Server Administrator on the managed system. See "Logging In and Out."
 The **Security Alert** window appears.
- 8 Click **View Certificate**.
 The **Certificate** window appears. A white cross in a red circle appears over the certificate icon at the top of the window. This icon indicates that the certificate cannot be verified to a trusted certificate authority.
- 9 Click the **Certification Path** tab.
- 10 Select **Organizational CA** and click **View Certificate**.
 Information about the organizational CA is displayed.
- 11 Click **Install Certificate**.
 The **Certificate Manager Import Wizard** appears.
- 12 Click **Next**.
Automatically select the certificate store based on the type of certificate is selected by default.
- 13 Click **Next**.
- 14 Click **Finish** to complete the Certificate Manager Import Wizard.
 The **Root Certificate Store** window appears.
- 15 Click **Yes**.
 A window informs you that the import was successful.
- 16 Click **OK**.
 The Java plug-in will now recognize the certificate as valid.
 The Systems Management **Log in** window appears with a yellow lock (in the locked position) at the bottom corner of the window.

To create a new server certificate signed by an external Organizational Authority, perform the following steps:

- 1 Log in with administrator privileges to a client system and map a drive to the **sys:\public** directory on the managed system.
- 2 Double-click **ConsoleOne**.

- 3 Right-click the container object that contains the system to be managed with Server Administrator, select **New**, and click **Object**.
The **New Object** window appears.
- 4 Select **NDSPKI: Key Material** and click **OK**.
The **Create Server Certificate** window appears. The **Standard** creation method is selected by default.
- 5 Select the **Custom** creation method, type the **Certificate name**, and click **Next**.
- 6 Click **External Certificate Authority**, and click **Next**.
- 7 Select the **RSA** key size, and click **Next**.
- 8 Type the **Subject Name**, choose the signature algorithm, and click **Next** (by default, the signature algorithm is set to *RSA Encryption with SHA-1 hash*).
ConsoleOne generates a Certificate Signing Request (CSR).
- 9 Click **Finish**.
The **Save Certificate Signing Request** window appears.
- 10 Save the CSR.
- 11 Send the CSR to a trusted CA such as Verisign, Thawte, or Entrust.
The CA returns two files: one is the root certificate and the other is a response in a Public Key Cryptography Standard #7 (PKCS#7) format.
- 12 Right-click the certificate you named in step 5 and click **Properties**.
- 13 Click **Import**.
- 14 Paste the trusted root certificate in the edit box and click **Next**.
- 15 Paste the response in the edit box and click **Next**.
- 16 Edit the `sys:\system\dell\omanage\IWS\config\server_properties.ini` and the `sys:\system\dell\omanage\IWS\config\client_properties.ini` files by editing the following line:


```
nssl.keystore = certificate name - hostname
```


where *certificate name* is the name of the certificate you just created and *hostname* is the name of the managed system running Novell NetWare.

The next time you log into Server Administrator, the Java plug-in recognizes the certificate as signed by an external trusted certificate authority.

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 supported Red Hat® Enterprise Linux operating systems).

Starting Server Administrator

Supported Microsoft Windows Operating Systems

To start Server Administrator on systems running a supported Microsoft Windows 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**.

Supported Red Hat Enterprise Linux Operating Systems

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

```
omawsd start
```

Supported Novell NetWare Operating Systems

To start Server Administrator on systems running a supported Novell NetWare operating system, run the following command from the command line:

```
Dell/omanage/IWS/bin/netware/omastart
```

Stopping Server Administrator

Supported Microsoft Windows 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**.

Supported Red Hat Enterprise Linux Operating Systems

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

```
omawsd stop
```

Supported Novell NetWare Operating Systems

To stop Server Administrator on systems running a supported Novell NetWare operating system, run the following command from the command line:

```
Dell/omanage/IWS/bin/netware/omastop
```

Restarting Server Administrator

Supported Microsoft Windows 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**.

Supported Red Hat Enterprise Linux Operating Systems

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

```
omawsd restart
```

Supported Novell NetWare Operating Systems

To restart Server Administrator on systems running a supported Novell NetWare operating system, run the following command from the command line:

```
Dell/omanage/IWS/bin/netware/omarestart
```


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 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.

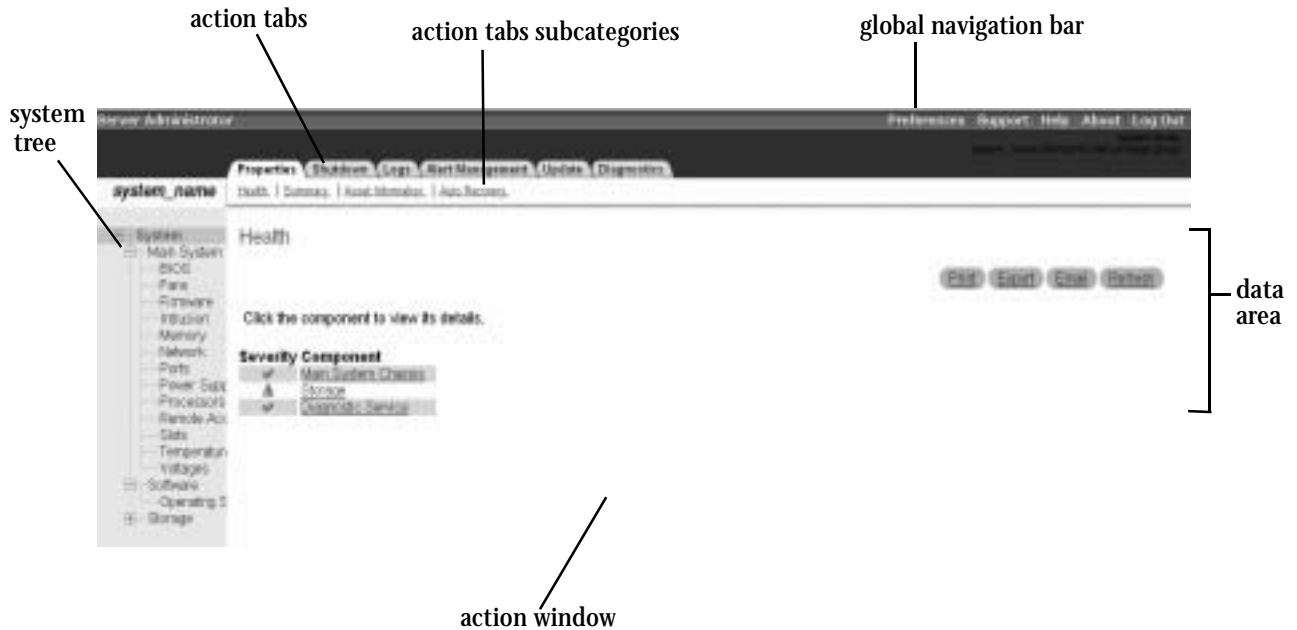


NOTE: For both managed systems and network management stations running Microsoft® Windows® Server 2003, you must configure the SNMP service to accept SNMP packets. See "Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems" for details.

Managing Your System

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

Figure 6-1. 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.

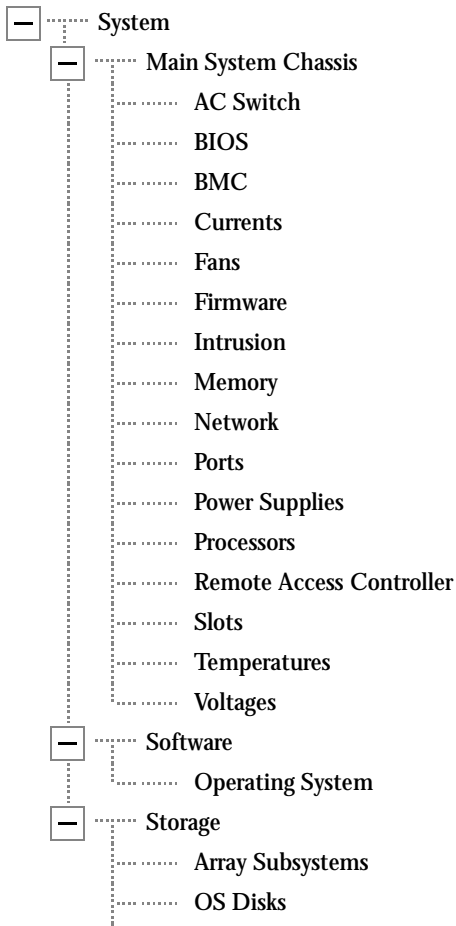
Managing System Tree Objects


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**, **Software**, and **Storage**.

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

See Figure 6-2 available Server Administrator home page system tree objects.


Figure 6-2. Server Administrator Home Page System Tree Objects



 **NOTE:** In the previous figure, the Storage tree object expands to display the Array Systems and OS Disks objects only when Array Manager (basic Storage Management Service) is installed. If enhanced Storage Management Service is installed, depending on the controller and storage attached to the system, the Storage tree object will expand to display the following objects:

1. Controller
2. Battery
3. Channel
4. Enclosure or Backplane
5. Array Disks
6. EMMs
7. Fans
8. Power Supplies
9. Temperatures
10. Virtual Disks

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

Properties

Subtabs: **Health** | **Summary** | **Asset Information** | **Auto Recovery**


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


- View the current health alert status for hardware and software components in the **Main System Chassis** object, the attached storage components, and the Diagnostic Service for the system being monitored.

 **NOTE:** **Diagnostic Service** is not listed on the **Health** page for the **System** object at startup. The Diagnostic Service waits for the Server Administrator service to start completely before enumerating (scanning the system for available devices to diagnose). If you press <F5> to refresh, **Diagnostic Service** shows up when enumeration is complete. This process can take several minutes on some systems.

- View detailed summary information for all components in the system being monitored.

- View and configure asset information for the system being monitored.
- View and set the Automatic System Recovery (watchdog timer) actions for the system being monitored.




 **NOTE:** Automatic System Recovery actions may not execute exactly per the set time out period (n seconds) when the watchdog reflects a hung system. The action execution time ranges from n-h+1 to n+1 seconds, where n is the set time out period and h is the heart beat interval. The value of the heart beat interval is 7 seconds when n <= 30 and 15 seconds when n > 30.

 **NOTE:** On managed systems running a Novell® NetWare® operating system, you must manually disable the watchdog timer feature prior to issuing a "restart server" or "down" command. Otherwise, the watchdog will timeout, resulting in a reboot or power down, depending on the watchdog's selected behavior.

Shutdown


Subtabs: **Remote Shutdown** | **Thermal Shutdown** | **Web Server Shutdown**


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

- Configure the operating system shutdown and remote shutdown options.
- Set the thermal shutdown severity level to shut down your system in the event that a temperature sensor returns a warning or failure value.
 -  **NOTE:** A thermal shutdown occurs only when the temperature reported by the sensor goes above the temperature threshold. A thermal shutdown does not occur when the temperature reported by the sensor goes below the temperature threshold.
- Shut down the 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

Subtabs: **Hardware** | **Alert** | **POST** | **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 POST log for a list of the POST codes and their corresponding descriptions recorded during system start-up.
- View the Command log for a list of each command executed from either the Server Administrator home page or from its command line interface.


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

Alert Management

Subtabs: **Alert Actions** | **Platform Events** | **SNMP Traps**

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


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

Update

Subtab: **Software**

The **Update** tab in Server Administrator allows you to view the system component version report. Use the Dell Server Update Utility application CD to view the complete version report and to update an entire system. To update individual components, use component specific Dell Update Packages.

 **NOTE:** Update functionality is not supported in this release. The Dell Server Update Utility and Dell Update Packages can be downloaded from <http://support.dell.com>. These are supported on Microsoft Windows and Red Hat® Enterprise Linux. Novell NetWare is not supported.

 **NOTE:** The Dell Server Update Utility or Dell Update Packages must be launched from the system you want to update.

Diagnostics

Subtabs: **Select** | **Review** | **Status** | **Results** | **Hardware Changes** | **Settings** | **Scheduled Tasks**

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

- View and select to run all available diagnostics tests for components installed in your system.
- Review the selected tests.
- View the status of the tests being executed.
- View the results for the diagnostics test that have been run.
- View any current hardware configuration changes (hardware configuration differences).
- Configure settings for diagnostics tests and log files.
- View a list of scheduled tests and make changes to them.



NOTE: The **Diagnostics** tab is not available in Server Administrator at startup. The Diagnostic Service waits for the Server Administrator service to start completely before enumerating (scanning the system for available devices to diagnose). If you press <F5> to refresh, the **Diagnostics** tab shows up when enumeration is complete. This process can take several minutes on some systems.



NOTE: See "Diagnostic Service" for complete instructions on using the Server Administrator Diagnostic Service.

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 following tabs, depending on the user's group privileges: **Properties** and **Diagnostics**.


Properties

Subtabs: **Health** | **Information** | **Front Panel**

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:
 - AC Switch
 - BIOS
 - BMC
 - Currents

- Diagnostic Service
- Fans
- Firmware
- Hardware Log
- Intrusion
- Memory
- Network
- Ports
- Power Supplies
- Processors
- Remote Access Controller
- Slots
- Temperatures
- Voltages
- View information about the main system chassis attributes.
- Enable or disable the managed system's front panel buttons, namely Power button and or Non-Masking Interrupt (NMI) button (if present on the system).


 **NOTE: Diagnostic Service** is not listed on the **Health** page for the **Main System Chassis** object at startup. The Diagnostic Service waits for the Server Administrator service to start completely before enumerating (scanning the system for available devices to diagnose). If you press <F5> to refresh, **Diagnostic Service** shows up when enumeration is complete. This process can take several minutes on some systems.

Diagnostics

Subtabs: **Select** | **Review** | **Status** | **Results** | **Hardware Changes** | **Settings** | **Scheduled Tasks**

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

- View and select to run all available diagnostics tests for components installed in your system.
- Review the selected tests.
- View the status of the tests being executed.
- View the results for the diagnostics test that have been run.
- View any current hardware configuration changes (hardware configuration differences).
- Configure settings for diagnostics tests and log files.
- View a list of scheduled tests and make changes to them.

 **NOTE:** See "Diagnostic Service" for complete instructions on using the Server Administrator Diagnostic Service,

AC Switch

Clicking the **AC Switch** object allows you to display key features of your system's AC failover switch. The **AC Switch** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: **Information**

Under the **Properties** tab, you can view AC switch redundancy information and view information about the AC power lines.

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 following tabs, depending on the user's group privileges: **Properties** and **Setup**.

Properties

Subtab: **Information**

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

Setup

Subtab: **BIOS**

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



NOTE: Setting the boot sequence to **Device List** on the **Setup** tab results in the following boot sequence: diskette, IDE CD drive, hard drive, option ROMs (if the devices are available).

BMC

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



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

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

Properties

Subtab: **Information**

Under the **Properties** tab, you can view general BMC information. Click **Reset to Defaults** to reset all the attributes to their system default values.

Configuration

Subtabs: **LAN** | **Serial Port** | **Serial Over LAN**

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

Users


Subtab: **BMC Users**

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

BIOS Setup

Subtabs: **Serial Configuration** | **Console Redirection** | **Console Redirection Failsafe Baud Rate**

Under the **BIOS Setup** tab, you can modify the state of the Serial Port, Console Redirection, and Console Redirection Failsafe Baud Rate.

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

Currents


Clicking the **Currents** object allows you to manage current levels in your system. Server Administrator monitors currents across critical components in various chassis locations in the monitored system. The **Current** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: **Current Probes**

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

- View the current readings and status for your system's current probes.
- Configure current probe warning threshold values.
- Set alert actions in the event that a current probe returns a warning or failure value.

 **NOTE:** When assigning probe threshold values, Server Administrator sometimes rounds the minimum or maximum values you enter to the closest assignable value.

Alert Management

Subtabs: **Alert Actions** | **SNMP Traps**

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

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

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

Subtabs: **Fan Probes** | **Fan Control**

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

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



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

- Select fan control options.

Alert Management

Subtabs: **Alert Actions** | **SNMP Traps**

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

- View current alert actions settings and set the alert actions that you want to be performed in the event that a fan returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for fans. The selected traps 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 following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: **Information**

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

Intrusion

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

Properties

Subtab: **Intrusion**

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

Alert Management

Subtabs: **Alert Actions** | **SNMP Traps**

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

- View current alert actions settings and set the alert actions that you want to be performed in the event that the intrusion sensor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for the intrusion sensor. The selected traps 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**, **Alert Management**, and **Diagnostics**.

Properties

Subtab: **Memory**

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

Alert Management

Subtabs: **Alert Actions** | **SNMP Traps**

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

- View current alert actions settings and set the alert actions that you want to be performed in the event that 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.

Diagnostics

Subtabs: **Select** | **Review** | **Status** | **Results** | **Hardware Changes** | **Settings** | **Scheduled Tasks**

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

- View and select to run all available diagnostics tests for components installed in your system.
- Review the selected tests.
- View the status of the tests being executed.
- View the results for the diagnostics test that have been run.
- View any current hardware configuration changes (hardware configuration differences).
- Configure settings for diagnostics tests and log files.
- View a list of scheduled tests and make changes to them.



NOTE: See "Diagnostic Service" for complete instructions on using the Server Administrator Diagnostic Service.

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 following tabs, depending on the user's group privileges: **Properties** and **Diagnostics**.

Properties

Subtab: **Information**

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

Diagnostics

Subtabs: **Select** | **Review** | **Status** | **Results** | **Hardware Changes** | **Settings** | **Scheduled Tasks**

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

- View and select to run all available diagnostics tests for components installed in your system.
- Review the selected tests.
- View the status of the tests being executed.
- View the results for the diagnostics test that have been run.
- View any current hardware configuration changes (hardware configuration differences).
- Configure settings for diagnostics tests and log files.
- View a list of scheduled tests and make changes to them.



NOTE: See "Diagnostic Service" for complete instructions on using the Server Administrator Diagnostic Service.

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 following tabs, depending on the user's group privileges: **Properties** and **Diagnostics**.

Properties

Subtab: **Information**

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

Diagnostics

Subtabs: **Select** | **Review** | **Status** | **Results** | **Hardware Changes** | **Settings** | **Scheduled Tasks**

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

- View and select to run all available diagnostics tests for components installed in your system.
- Review the selected tests.
- View the status of the tests being executed.
- View the results for the diagnostics test that have been run.
- View any current hardware configuration changes (hardware configuration differences).
- Configure settings for diagnostics tests and log files.
- View a list of scheduled tests and make changes to them.



NOTE: See "Diagnostic Service" for complete instructions on using the Server Administrator Diagnostic Service.

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

Subtab: **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

Subtabs: **Alert Actions** | **SNMP Traps**

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

- View current alert actions settings and set the alert actions that you want to be performed in the event that a 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

Subtab: **Information**

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

Alert Management

Subtabs: **Alert Actions** | **SNMP Traps**

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

- View current alert actions settings and set the alert actions that you want to be performed in the event that a 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.

Remote Access Controller

Clicking the **Remote Access Controller** object allows you to access your system's remote system management capabilities. The Server Administrator Remote Access Service provides remote access to inoperable systems, alert notification when a system is down, and the ability to restart a system. The **Remote Access Controller** object action window can have the following tabs, depending on the user's group privileges: **Properties**, **Configuration**, **Users**, **Remote Connect**, **Security**, **Update**, and **Diagnostics**.

Properties

Subtab: **Information**

Under the **Properties** tab, you can view information about each remote access controller (RAC) attribute.

Configuration

Subtabs: **Network** | **SNMP** | **Demand Dial-Out** | **Dial-In Users** | **Remote Features** | **Modem**

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

- Configure network properties.
- Configure SNMP traps.
- Configure demand dial-out entries.
- Configure dial-in users.
- Configure remote properties such as remote boot parameters.
- Configure modem properties.

Users

Subtab: **Information**

Under the **Users** tab, you can add, configure, and view information about Remote Access Service users.

Remote Connect

Under the **Remote Connect** tab, you can access the RAC.

Security

Subtabs: **CSR Management** | **Authentication Options**

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

- Perform CSR certificate management by generating a new CSR certificate, uploading an existing CSR certificate, viewing an existing server certificate, or viewing an existing CA certificate.
- Set login authentication options to only allow remote access controller login by users created through the Remote Access Service (RAC users), or to allow remote access controller login by users created through the Remote Access Service and through the local operating system.

Update

Subtab: **Firmware Update**

Update is no longer supported. Use the Dell Server Update Utility or the Dell Update Packages to carry out your system software updates. The Dell Server Update Utility and Dell Update Packages can be downloaded from <http://support.dell.com>.


Diagnostics

Subtabs: **Select** | **Review** | **Status** | **Results** | **Hardware Changes** | **Settings** | **Scheduled Tasks**

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

- View and select to run all available diagnostics tests for components installed in your system.
- Review the selected tests.

- View the status of the tests being executed.
- View the results for the diagnostics test that have been run.
- View any current hardware configuration changes (hardware configuration differences).
- Configure settings for diagnostics tests and log files.
- View a list of scheduled tests and make changes to them.

 **NOTE:** See "Diagnostic Service" for complete instructions on using the Server Administrator Diagnostic Service.

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 has the **Properties** tab.

Properties

Subtab: **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

Subtab: **Temperature Probes**

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

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

Alert Management

Subtabs: **Alert Actions** | **SNMP Traps**

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

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



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

Voltages

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

Subtab: **Voltage Probes**

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



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

Alert Management

Subtabs: **Alert Actions** | **SNMP Traps**

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

- View current alert actions settings and set the alert actions that you want to be performed in the event that a system voltage sensor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for voltage sensors. The selected traps 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 following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Summary

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

Operating System

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

Properties

Subtab: Information

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

Storage

The current release of Server Administrator provides two staggered versions of the Storage Management Service:

- Basic Storage Management Service

The basic Storage Management Service is similar to the Storage Management Service provided in earlier releases of Server Administrator. Basic Storage Management Service is available only on Microsoft Windows and Novell NetWare operating systems.

- Advanced Storage Management Service

The enhanced Storage Management Service provides additional features for configuring storage. In most cases, the enhanced Storage Management Service is installed using Express Setup. Advanced Storage Management Service is available only on Microsoft Windows and Linux operating systems.

Depending on which version of the Storage Management Service is installed, clicking the **Storage** object allows you to view the status and settings for various attached array storage devices, volumes, system disks, and so on.

Basic Storage Management Service

In the case of Basic Storage Management Service, depending on the storage attached to the system, the expanded Storage object may display the following lower-level objects:


- Array Subsystems
- OS Disks
- Volumes

In Basic Storage Management Service, the **Storage** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Diagnostics**.

Properties

Subtab: **Health**

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


 **NOTE:** **Diagnostic Service** is not listed on the **Health** page for the **Storage** object at startup. The Diagnostic Service waits for the Server Administrator service to start completely before enumerating (scanning the system for available devices to diagnose). If you press <F5> to refresh, **Diagnostic Service** shows up when enumeration is complete. This process can take several minutes on some systems.

Diagnostics

Subtabs: **Select** | **Review** | **Status** | **Results** | **Hardware Changes** | **Settings** | **Scheduled Tasks**

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

- View and select to run all available diagnostics tests for components installed in your system.
- Review the selected tests.
- View the status of the tests being executed.
- View the results for the diagnostics test that have been run.
- View any current hardware configuration changes (hardware configuration differences).
- Configure settings for diagnostics tests and log files.
- View a list of scheduled tests and make changes to them.

 **NOTE:** See "Diagnostic Service" for complete instructions on using the Server Administrator Diagnostic Service

Array Subsystems

Clicking the **Array Subsystems** object allows you to view information about your array subsystems. Array subsystems include physical and logical objects. The **Array Subsystems** object action window can have the following tab, depending on the user's group privileges: **Properties**

Properties

Subtab: **Array Subsystems**

Under the **Properties** tab, you can view the current status of and detailed information about your array subsystems, including installed RAID controllers, direct attached storage enclosures, and physical and virtual disks.

OS Disks

Clicking the **OS Disks** object allows you to view information about your operating system disks. The **OS Disks** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: **OS Disks**

Under the **Properties** tab, you can view the current status of and detailed information about your operating system disks.

Volumes

Clicking the **Volumes** object allows you to view information about volumes on your system. A volume may be formatted and may have a file system and/or drive letter. The **Volumes** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: **Volumes**

Under the **Properties** tab, you can view the current status of and detailed information about your volumes.

Enhanced Storage Management Service

In the case of Enhanced Storage Management Service, clicking the **Storage** object allows you to view the status and settings for the supported controllers attached to the system. The controller object expands to display the storage attached to the controller.

Depending on the controller and storage attached to the system, the expanded **Storage** object may display the following lower-level objects:

- Controller
- Battery
- Channel
- Enclosure or Backplane
- Array Disks
- EMMs
- Fans
- Power Supplies
- Temperatures
- Virtual Disks

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

Properties

Subtab: **Health**

In the **Health** window of the **Properties** tab, you can view the current health or status of the attached storage components. This window displays the status of all lower-level objects.

A quick way to review the status of all storage components is to select the **Storage** object and view the **Health** window under the **Properties** tab. You can click the required storage components in the **Health** window to view detailed information on the health or status of the component.

Subtab: **Information/Configuration**

In the **Information/Configuration** window of the **Properties** tab, you can view the properties for the controllers attached to the system. You can also execute global tasks that apply to all controllers.

Controller

Clicking the **Controller** object allows you to view information about your controllers and the various components attached to the controller. The components attached to the controller can include battery, virtual disks, and so on. The **Controller** object action window can have the following tabs, depending on the user's group privileges: **Health** and **Information/Configuration**.

Health

Under the **Health** tab, you can view the current status of the battery, virtual disks, and other storage components attached to the controller. The status is visually indicated with the icons described in "Storage Component Severity."

Information/Configuration

Under the **Information/Configuration** tab, you can view the property information of the controller and the components attached to the controller. You can also execute controller tasks in this tab.

Channel

Clicking the **Channel** object allows you to view information about the channel and the enclosure or backplane attached to the channel. The **Channel** object action window can have the following tabs, depending on the user's group privileges: **Health** and **Configuration/Information**.

Health

Under the **Health** tab, you can view the current status of the channel and the enclosure or backplane attached to the channel. The status is visually indicated with the icons described in "Storage Component Severity."

Configuration/Information

Under the **Configuration/Information** tab, you can view the property information of the channel and the enclosure or backplane attached to the channel. You can also execute channel tasks in this tab.

Enclosure or Backplane

Clicking the **Enclosure or Backplane** object allows you to view information about the array disks, temperature probes, and other components attached to the enclosure or backplane. The **Enclosure or Backplane** object action window can have the following tabs, depending on the user's group privileges: **Health** and **Configuration/Information**.

Health

Under the **Health** tab, you can view the current status of array disks and other components attached to the enclosure or backplane. For example, the status of an enclosure's fans, power supplies, temperature probes, and so on is displayed in this tab. The status of array disks attached to the backplane is also displayed here. The status is visually indicated with the icons described in "Storage Component Severity."

Configuration/Information

Under the **Configuration/Information** tab, you can view the property information of the array disks, temperature probes, EMMs (Enclosure Management Modules) and other components attached to the enclosure or backplane. For enclosures, you can also execute enclosure tasks in this tab.

Array Disks

Clicking the **Array Disks** object allows you to view information about the array disks attached to the enclosure or backplane. The **Array Disks** object action window can have the following tabs, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the array disks attached to the enclosure or backplane. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes name, state, capacity, used and available disk space, and other information. You can also execute array disk tasks in this tab.

EMMs

Clicking the **EMMs** object allows you to view information about the Enclosure Management Modules (EMMs). The **EMMs** object action window can have the following tabs, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the EMMs. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes name, state, part number, firmware version, and SCSI rate.

Fans

Clicking the **Fans** object allows you to view information about the enclosure fans. The **Fans** object action window can have the following tabs, depending on the user's group privileges:

Configuration/Information.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the fans. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes fan name, state, part number, and speed.

Power Supplies

Clicking the **Power Supplies** object allows you to view information about the enclosure power supplies. The **Power Supplies** object action window can have the following tabs, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the enclosure power supplies. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes name, state, and part number.

Temperatures

Clicking the **Temperatures** object allows you to view information about the enclosure temperature probes. The **Temperatures** object action window can have the following tabs, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the enclosure temperature probes. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes name, state, and reading (current temperature). The minimum and maximum values set for the temperature probes' **Warning** and **Failure** thresholds are also displayed under this tab.

Virtual Disks

Clicking the **Virtual Disks** object allows you to view information about the virtual disks configured on the controller. The **Virtual Disks** object action window can have the following tabs, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the property information of the virtual disks configured on the controller. Property information includes name, state, and layout (RAID level). The read, write, and cache policy and stripe size are also displayed. You can also execute virtual disk tasks in this tab.

Storage Component Severity

The status of a component is graded for degrees of severity. Each level of severity requires you to take different actions in response. For example, you must take immediate reparative action in response to a **Warning** or **Critical/Failure** status to avoid any data loss.

It may be useful to review the Alert Log for events indicating why a component has a **Warning** or **Critical** status. For additional troubleshooting information, see the Storage Management online help.





 **NOTE:** The status displayed reflects the status at the time the browser first displayed the page. If you believe the status has changed and wish to update the displayed information, click the **Refresh** button in the upper-right corner of the action window. Some storage configuration changes can only be detected if you perform a controller rescan; click the **Information/Configuration** tab in the required controller and click **Rescan**.

Table 6-1 explains the various severity levels and the corresponding component status.

Table 6-1. Severity Levels and Component Status



Severity Level	Component Status
	Normal/OK. The component is working as expected.
	Warning/Non-critical. A probe or other monitoring device has detected a reading for the component that is above or below the acceptable level. The component may still be functioning, but it could fail. The component may also be functioning in an impaired state. Data loss is possible.
	Critical/Failure/Error. The component has either failed or failure is imminent. The component requires immediate attention and may need to be replaced. Data loss may have occurred.

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 6-3 for available Preferences home page configuration options.

Figure 6-3. Preferences Home Page Configuration Options

-  General Settings
-  Server Administrator

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

Subtab: **Properties**

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

Web Server

Subtabs: **Properties** | **X.509 Certificate**

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

- Set 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

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 can have the following tabs, depending on the user's group privileges: **Preferences** and **Diagnostics**.

Preferences

Subtabs: **Access Configuration** | **SNMP Configuration**

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

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

Diagnostics

Subtab: **Settings**

Under the **Diagnostics** tab, you can set preferential options for running diagnostics tests. You can set options for both Applications Settings and Test Execution Settings.

Working With the Baseboard Management Controller (BMC)

Overview

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

Server Administrator allows remote, in-band access to event logs, power control, and sensor status information and provides the ability to configure the BMC. You can manage the BMC through the Server Administrator GUI by clicking the **BMC** object, which is a subcomponent of the **Main System Chassis** group. You can perform the following BMC-related tasks:

- View basic BMC information
- Configure BMC users
- Set BMC platform event filter alerts
- Configure the BMC on a serial over LAN connection
- Configure the BMC on a serial port connection
- Configure the BMC on a virtual LAN connection

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

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

Viewing Basic BMC Information

You can view the basic information about the BMC and also reset the BMC settings to their default values.



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

- 1 Click the **System** object.
- 2 Click the **Main System Chassis** object.

- 3 Click the **BMC** object.

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

- **BMC Name**
- **IPMI Version**
- **System GUID**
- **Number of Possible Active Sessions**
- **Number of Current Active Sessions**
- **LAN Enabled**
- **SQL Enabled**
- **IP Address Source**
- **IP Address**
- **IP Subnet**
- **IP Gateway**
- **MAC Address**

Configuring BMC Users

BMC users can be configured through the **BMC User Configuration** page; this page is accessed by browsing through the following path.

- 1 Click the **System** object.
- 2 Click the **Main System Chassis** object.
- 3 Click the **BMC** object.
- 4 Click the **Users** tab.
- 5 Click the **Users** subtab.

The **BMC Users** window displays information about users that can be configured as **BMC** users.



NOTE: **BMC** Users are created independently of the users assigned or created through Server Administrator or the operating system.

- 6 Click **User ID** to configure a new or existing **BMC** user.

The **BMC User Configuration** window allows you to to configure a specific **BMC** user.

- 7 Specify the following general information:
 - Select **Enable User** to enable the user.
 - Enter the name for the user in the **User Name** field.
 - Select the **Change Password** check box.

- Enter a new password in the **New Password** field.
 - Re-enter the new password in the **Confirm New Password** field.
- 8 Specify the following user privileges:
 - Select the maximum LAN user privilege level limit.
 - Select the maximum serial port user privilege granted.
 - 9 Click **Apply Changes** to save changes.
 - 10 Click **Back to BMC User Window** to go back to the **BMC Users** window.

Setting BMC Platform Event Filter Alerts


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

- 1 Click the **System** object.
- 2 Click the **Alert Management** tab.
- 3 Click **Platform Events**.

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

You can configure the following platform events.

- Fan Probe Failure
- Voltage Probe Failure
- Discrete Voltage Probe Failure
- Temperature Probe Warning
- Temperature Probe Failure
- Chassis Intrusion Detected
- Redundancy Degraded
- Redundancy Lost
- Processor Warning
- Processor Failure
- PS/VRM/DCtoDC Warning
- PS/VRM/DCtoDC Failure
- Hardware Log Failure
- Automatic System Recovery


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

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


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

- 5 Select one of the following actions:

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

 **NOTICE:** If you select a Platform Event shutdown action other than none, your system will shut down forcefully when the specified event occurs. This shutdown is initiated by firmware and is done without first shutting down the operating system or any running applications.

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


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

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

Setting Platform Event Alert Destinations

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

- 1 Click **Configure Destinations** in the **Platform Event Filters** window.
The **Configure Destinations** window displays a number of destinations.
- 2 Click the number of the destination you want to configure.

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

- 3 Click **Destination Number** to enter an individual IP address for that destination. This IP address is the IP address to which the platform event alert will be sent.
- 4 Enter a value in the **Community String** field to act as a password to authenticate messages sent between a management station and a managed system. The community string (also called the community name) is sent in every packet between the management station and a managed system.
- 5 Click **Apply Changes**.
- 6 Click **Go Back to Platform Events Page** to go back to the **Platform Event Filters** window.

Configuring the BMC to use a Serial Over LAN (SOL) Connection

You can configure the BMC on a serial over LAN connection.

- 1 Click the **System** object.
- 2 Click the **Main System Chassis** object.
- 3 Click the **BMC** object.
- 4 Click the **Configuration** tab.
- 5 Click **Serial Over LAN**.

The **Serial Over LAN Configuration** window appears.

- 6 Configure the following details:
 - Enable Serial Over LAN
 - Baud Rate
 - Channel Privilege Limit
- 7 Click **Apply Changes**.
- 8 Click **Advanced Settings** to further configure BMC.
- 9 In the **Serial Over LAN Configuration Advanced Settings** window, specify the following information:
 - Character Accumulate Interval
 - Character Send Threshold
- 10 Click **Apply Changes**.
- 11 Click **Go Back to Serial Over LAN Configuration** to return to the **Serial Over LAN Configuration** window.

Configuring the BMC to use a Serial Port Connection

You can configure the BMC on a serial port connection.

- 1 Click the **System** object.
- 2 Click the **Main System Chassis** object.
- 3 Click the **BMC** object.
- 4 Click the **Configuration** tab.
- 5 Click **Serial Port**.
- 6 In the **Serial Port Configuration** window, specify the following details:
 - Connection Mode Setting
 - Baud Rate
 - Flow Control
 - Channel Privilege Level Limit
- 7 Click **Apply Changes**.
- 8 Click **Terminal Mode Settings**.

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

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

- 9 Specify the following customizations to increase compatibility with existing terminals:
 - Line Editing
 - Delete Control
 - Echo Control
 - Handshaking Control
 - New Line Sequence
 - Input New Line Sequence
- 10 Click **Apply Changes**.
- 11 Click **Back To Serial Port Configuration Window** to go to back to the **Serial Port Configuration** window.

Configuring the BMC to use a Virtual LAN Connection

You can configure the BMC on a virtual LAN (VLAN).

- 1 Click the **System** object.
- 2 Click the **Main System Chassis** object.
- 3 Click the **BMC** object.
- 4 Click the **Configuration** tab.
- 5 Click **LAN**.

The LAN Configuration page appears.



NOTE: BMC management traffic will not function if the LAN on motherboard (LOM) is used in a Port Channel or Link Aggregation team.

- 6 Specify the following NIC configuration details:
 - Enable LAN Interface
 - IP Address Source
 - IP Address
 - Subnet Mask
 - Gateway Address
 - MAC Address
 - Channel Privilege Level Limit
- 7 Specify the following VLAN configuration details:
 - VLAN ID Enable
 - VLAN ID
 - Priority
- 8 Click **Apply Changes**.

Remote Access Service

Overview

The Server Administrator Remote Access Service provides a complete remote system management solution for SNMP- and CIM-instrumented systems equipped with a Dell™ Remote Access Card (DRAC) III, a DRAC III/XT, an Embedded Remote Access (ERA) controller, or an ERA Option (ERA/O) card. These hardware and software solutions are collectively known as remote access controllers (RACs). With regard to the latest RAC solution offering from Dell—DRAC 4, the Remote Access Service also allows a basic management task to be performed from OpenManage Server Administrator: you can connect to DRAC 4 from the Server Administrator GUI.

The DRAC 4 is a systems management hardware and software solution designed to provide remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge™ systems.

By communicating with the system's baseboard management controller (BMC), the DRAC 4 can be configured to send you e-mail alerts for warnings or errors related to voltages, temperatures, and fan speeds. The DRAC 4 also logs event data and the most recent crash screen (for systems running the Microsoft® Windows® operating system only) to help you diagnose the probable cause of a system crash.

Depending on your system, the DRAC 4 hardware is either a system card (DRAC 4/I) or a full-length PCI card (DRAC 4/P). The DRAC 4/I and DRAC 4/P are identical except for the hardware differences.

The DRAC 4 has its own microprocessor and memory, and is powered by the system in which it is installed. The DRAC 4 may be preinstalled on your system, or available separately in a kit.




NOTE: The information contained in this section pertains to the previous generation of RACs. See the *Dell Remote Access Controller 4 User's Guide* for more information on using DRAC 4.


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

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

See the *Server Administrator Command Line Interface User's Guide* and the *Dell Remote Access Controller Racadm User's Guide* for information about running the Remote Access Service from the command line.

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


 **NOTE:** The Remote Access Service is not available on modular systems. You must directly connect to the remote access controller (RAC) on a modular system. See the *Dell Embedded Remote Access/MC Controller User's Guide* for more information.

 **NOTE:** See the *Dell Remote Access Controller Installation and Setup Guide* for complete information about installing and configuring a DRAC III, a DRAC III/XT, or an ERA/O controller, configuring an ERA controller, and using a RAC to remotely access an inoperable system. See the *Dell Embedded Remote Access/MC Controller User's Guide* for complete information about configuring and using an ERA/MC controller to remotely manage and monitor your modular system and its shared resources through a network.

Hardware Prerequisites


The managed system must have a RAC installed to use the Remote Access Service.

For a list of specific hardware requirements for your RAC, see the readme file for your remote access controller on the *Systems Management Consoles* CD and the *Dell Remote Access Controller Installation and Setup Guide* or the *Dell Embedded Remote Access/MC Controller User's Guide* on the documentation CD.

 **NOTE:** The RAC software is installed as part of the **Express Setup** and **Custom Setup** installation options when installing managed system software from the *Dell Installation and Server Management* CD, provided that the managed system meets all of your RAC's installation prerequisites. See the appropriate RAC documentation for complete software and hardware requirements.

Software Prerequisites


The managed system must have the RAC software installed. See the *Dell Remote Access Controller Installation and Setup Guide* or the *Dell Embedded Remote Access/MC Controller User's Guide* for a complete list of software installation prerequisites.

 **NOTE:** The RAC software is installed as part of the **Express Setup** and **Custom Setup** installation options when installing managed system software from the *Dell Installation and Server Management* CD, provided that the managed system meets all of your RAC's installation prerequisites. See the appropriate RAC documentation for complete software and hardware requirements.

Adding and Configuring RAC Users

 **NOTE:** You must have Admin privileges in Server Administrator to use the Remote Access Service.

The RAC can store information for up to 16 users. The Remote Access Service provides security by requiring a user to provide a user name and password prior to establishing a remote connection. The Remote Access Service can also provide paging services to notify users if the system crashes, loses power, or experiences a defined list of other events. Paging services are only available for DRAC III cards.

 **NOTE:** Some configuration capabilities are available only on systems with DRAC III, DRAC III/XT, ERA, and ERA/O, and not on systems with DRAC 4. To configure DRAC 4, use the **Launch Remote Connect Interface** option in the **RAC Properties** window. See the *Dell Remote Access Controller 4 User's Guide* for more information.

To create a RAC user, perform the following steps:

- 1 Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access Controller** object.
- 2 Click the **Users** tab.
The **Remote Access Controller Users** window appears.
- 3 Click **Add**.
The **Add Remote Access Controller User** window appears.
- 4 Type a user name in the **User Name** field.
- 5 Type a new password in the **New Password** field.
- 6 Type the new password again in the **Confirm Password** field.
- 7 Configure numeric paging (for DRAC III users only):
 - a Click the check box next to **Enable Numeric Paging** and enter a pager number in the **Pager Number** field.
 - b Enter the numeric message in the **Numeric Message** field that you want the RAC to send when it receives certain events.
- 8 Configure e-mail paging:
 - a Click the check box next to **Enable Email Paging** and enter an e-mail address in the **Email Address** field.
 - b Enter the message in the **Message** field that you want the RAC to send when it receives certain events.
- 9 Configure alphanumeric paging (for DRAC III users only):
 - a Click the check box next to **Enable Alpha-Numeric Paging** and enter a pager number in the **Pager Number** field.
 - b Select the alphanumeric protocol used by the pager's service provider, **7E0** or **8N1**.


- c Select the pager's baud rate, **300** or **1200**.
 - d Enter the message in the **Custom Message** field that you want the RAC to send when it receives certain events.
 - e Enter the pager's PIN in the **Pager ID** field, and then, if required, enter a pager password in the **Pager Password** field.
 - f Click **Apply Changes** at the bottom of the window.
- 10 Under **Severity Configuration**, specify the trap and the severity that the trap must have to trigger a paging action from the RAC.
- Traps enable you to configure the RAC to respond to alert conditions from the system's ESM hardware or to other conditions such as operating system crashes or power failures.
- The first (left-most) column of check boxes corresponds to the severity level **Informational**, the second column corresponds to the severity level **Warning**, and the third column corresponds to the severity level **Critical**. The last seven events can only report the severity level **Informational**.
- 11 Click **Apply Changes** and then click **OK** to save the alert, paging, and user configuration to the Server Administrator data repository.
- Server Administrator returns to the **Users** tab. The user you just created and configured is displayed in the **User Name** list.

Configuring an Existing RAC User

 **NOTE:** You must have Admin privileges in Server Administrator to use the Remote Access Service.

To configure a RAC user, perform the following steps:

- 1 Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access Controller** object.
- 2 Click the **Users** tab.
The **Remote Access Controller Users** window appears.
- 3 Click the user name for the user you want to configure.
- 4 Change the password:
 - a Click the check box next to **Change Password** and type a new password in the **Password** field.
 - b Type the new password again in the **Confirm Password** field.

 **NOTE:** If you delete all RAC users by using Server Administrator, you must stop and start the Dell OpenManage Server Agent service to display the updated list of users.

- 5 Configure numeric paging (for DRAC III users only):
 - a Click the check box next to **Enable Numeric Paging** and enter a pager number in the **Pager Number** field.
 - b Enter the numeric message in the **Numeric Message** field that you want the RAC to send when it receives certain events.
- 6 Configure e-mail paging:
 - a Click the check box next to **Enable Email Paging** and enter an e-mail address in the **Email Address** field.
 - b Enter the message in the **Message** field that you want the RAC to send when it receives certain events.
- 7 Configure alphanumeric paging (for DRAC III users only):
 - a Click the check box next to **Enable Alpha-Numeric Paging** and enter a pager number in the **Pager Number** field.
 - b Select the alphanumeric protocol used by the pager's service provider, **7E0** or **8N1**.
 - c Select the pager's baud rate, **300** or **1200**.
 - d Enter the message in the **Custom Message** field that you want the RAC to send when it receives certain events.
 - e Enter the pager's PIN in the **Pager ID** field, and then, if required, enter a pager password in the **Pager Password** field.
 - f Click **Apply Changes** at the bottom of the window.
- 8 Under **Severity Configuration**, specify the trap and the severity that the trap must have to trigger a paging action from the RAC.

Traps enable you to configure the RAC to respond to alert conditions from the system's ESM hardware or to other conditions such as operating system crashes or power failures.


The first (left-most) column of check boxes corresponds to the severity level **Informational**, the second column corresponds to the severity level **Warning**, and the third column corresponds to the severity level **Critical**. The last seven events can only report the severity level **Informational**.
- 9 Click **Apply Changes** and then click **OK** to save the alert, paging, and user configuration to the Server Administrator data repository.


Server Administrator returns you to the **Users** tab.

Configuring the RAC Network Properties

 **NOTE:** You must have Admin privileges in Server Administrator to use the Remote Access Service.

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

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

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

To configure the network properties of your RAC, perform the following steps:

- 1 Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access Controller** object.
- 2 Click the **Configuration** tab.
The **Configure Network Properties** window appears.
- 3 Click the check box next to **Enable NIC** (this option is selected by default).
- 4 To have the DHCP system assign the NIC information, click the check box next to **Use DHCP (For NIC IP Address)**. If you do not, clear (deselect) this check box and enter the RAC's NIC information in the **Static IP Address**, **Static Subnet Mask**, and **Static Gateway Address** fields.
- 5 Enable dial-in networking (for DRAC III users only):
 - a Click the check box next to **Enable Dial-In** (this option is selected by default).
 - b To have the DHCP system assign the dial-in information, click the check box next to **Use DHCP (For Dial-In IP Address)**. If you do not, clear (deselect) this check box and enter the DRAC III modem's base IP Address in the **Base IP Address** field.
 - c Specify the **Dial-In Authentication** settings that dial-in connections require:
 - **Any** — Allows the connection to use any type of encryption, including no encryption
 - **Encrypted** — Requires the connection to use some type of encryption
 - **CHAP** — Requires the connection to use the CHAP
- 6 To enable SMTP server address control, click the check box next to **Enable SMTP**, and type the SMTP server address in the **SMTP (Email) Server Address** field.
- 7 Click **Apply Changes** and click **OK** to save your changes.

Configuring the RAC Alert Properties

RACs can be configured to respond to alert conditions from the system's ESM or to other conditions such as operating-system crashes or power failures.

RACs offer the following types of alert actions:

- Alphanumeric paging (DRAC IIIs only) (See "Adding and Configuring RAC Users" for information about configuring this type of alert action.)
- Numeric paging (DRAC IIIs only) (See "Adding and Configuring RAC Users" for information about configuring this type of alert action.)
- E-mail (See "Adding and Configuring RAC Users" for information about configuring this type of alert action.)
- SNMP traps (See the following subsection for information about configuring this type of alert action.)

Configuring the SNMP Alert Properties



NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

To configure the Remote Access Service alert properties, perform the following steps:

- 1 Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access Controller** object.
- 2 Click the **Configuration** tab.
- 3 Click **SNMP**.
- 4 Click **Add** or click the **Destination IP Address** to edit existing SNMP alert properties.
- 5 Click the check box next to **Enable SNMP Trap**, if a check isn't already in the check box.
- 6 Enter the SNMP community name to which the destination management station belongs in the **Community** field.
- 7 Enter a destination IP address of the management station to which you want the RAC to send SNMP traps when an event occurs in the **IP Address** field.
- 8 Use the check boxes under **Severity Configuration** to specify the events and the severity level that those events must have to trigger an alert action from the RAC.

The first (left-most) column of check boxes corresponds to the severity level **Informational**, the second column corresponds to the severity level **Warning**, and the third column corresponds to the severity level **Critical**. The last seven events can only report the severity level **Informational**.

- 9 Click **Apply Changes** and then click **OK** to save your changes.


Configuring DRAC III Dial-in (PPP) Users and Modem Settings

Dial-in (PPP) users and modem features are currently only available for the DRAC III.

Adding and Configuring a DRAC III Dial-In (PPP) User

 **NOTE:** You must have Admin privileges in Server Administrator to use the Remote Access Service.

This subsection describes how to add and configure a dial-in (PPP) user. After dial-in users are authenticated, they must enter the RAC user authentication at the remote access controller login screen to access the DRAC III.

 **NOTE:** The Server Administrator managed-system PPP client uses the 192.168.234.235 network to talk with the installed DRAC III. It is possible that this network IP address could already be in use by other systems or applications. If this situation occurs, the PPP connection fails to operate. If this address is already in use, the user is required to change the managed-system PPP client IP address to a different number. To change the managed-system PPP server IP address to use another network so that conflicts do not occur, you must use the racadm utility. See the *Dell Remote Access Controller Racadm User's Guide* for information about using the racadm utility.


To add and configure dial-in users, perform the following steps:

- 1 On the Server Administrator home page, click the **Main System Chassis** object, and then click the **Remote Access Controller** object.
- 2 Click the **Configuration** tab.
- 3 Click **Dial-In Users**.
- 4 Click **Add**.
- 5 Type a user name in the **User Name** field.
- 6 Type a new password in the **Password** field.
- 7 Type a callback number in the **Callback Number** field.


This number is the one the Remote Access Service calls if **Callback Type** is set to **Preset**.

- 8 Select a setting from the **Callback Type** drop-down menu:
 - **None** — When called, the Remote Access Service does not disconnect and call back; the connection remains active.
 - **Preset** — When called, the Remote Access Service disconnects and calls the number specified in the **Callback Number** field; this setting activates the callback number control.
 - **User Specified** — When called, the Remote Access Service asks the user for the callback number. Then the Remote Access Service disconnects and calls the number the user specified.
- 9 Click **Apply Changes** and then click **OK** to save your changes.

Adding and Configuring DRAC III Demand Dial-Out Entries

 **NOTE:** You must have Admin privileges in Server Administrator to use the Remote Access Service.

If you set the dial-in (PPP) setting to **Preset**, the demand dial-out entry causes the Remote Access Service to disconnect and call the management station back at a preset number. Upon callback, you must provide your RAC user authentication to access the Remote Access Service.

 **NOTE:** The RAC managed system software uses a PPP connection to talk to the installed RAC. The IP address for this PPP connection is 192.168.234.235. It is possible that this network IP address could already be in use by other systems or applications. If this situation occurs, the PPP connection fails to operate. If this address is already in use, the user is required to change the managed-system PPP client IP address to a different number. To change the managed-system PPP server IP address to use another network so that conflicts do not occur, you must use the racadm utility. See the *Dell Remote Access Controller Racadm User's Guide* for information about using the racadm utility.

To add a demand dial-out entry, perform the following steps:

- 1 On the Server Administrator home page, click the **Main System Chassis** object, and then click the **Remote Access Controller** object.
- 2 Click the **Configuration** tab.
- 3 Select **Demand Dial-Out**.
- 4 Click **Add**.
- 5 Enter the management station IP address that the Remote Access Service calls back when called by this user.
- 6 Enter the phone number used by the system's modem in the **Phone Number** field.
- 7 Enter the user name for the demand dial-out user in the **User Name** field.
- 8 Enter the password for the demand dial-out user in the **Password** field.
- 9 Select a setting from the **Authentication** drop-down menu:
 - **Any** — Allows the connection using any type of encryption, including no encryption
 - **Encrypted** — Requires the connection to use some type of encryption
 - **CHAP** — Requires the connection to use the CHAP
- 10 Click **Apply Changes** and click **OK** to save your changes.

Configuring the DRAC III Modem Settings

 **NOTE:** You must have Admin privileges in Server Administrator to use the Remote Access Service.

If your DRAC III kit includes the optional PCMCIA modem, you must configure the modem prior to use.

To configure the DRAC III modem, perform the following steps:

- 1 On the Server Administrator home page, click the **Main System Chassis** object, and then click the **Remote Access Controller** object.
- 2 Click the **Configuration** tab.
- 3 Click **Modem**.
- 4 For **Dial Mode**, choose either **Pulse** or **Tone**.
- 5 From the **Country Code** drop-down menu, select the country where the DRAC III is located.
- 6 For **Initialization String**, enter the required initialization string for the DRAC III modem in the text field.
- 7 Select a **Baud Rate** setting from the drop-down menu (the default is **38400**).
- 8 Click **Apply Changes**, and then click **OK** to save your changes.

Configuring the RAC Remote Features Properties

 **NOTE:** You must have Admin privileges in Server Administrator to use the Remote Access Service.

If the local boot image on the managed system has been corrupted, a RAC has the ability to boot its host server using a diskette boot image that it downloads from a Trivial File Transfer Protocol (TFTP) server. This feature is called remote floppy boot. A RAC can also update its firmware using a firmware image located on a TFTP server. This feature is called remote firmware update, and the process is similar to flashing a system BIOS.

To configure the remote floppy boot feature and the remote firmware update feature of your RAC, perform the following steps:

- 1 Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access Controller** object.
- 2 Click the **Configuration** tab.
The **Configure Network Properties** window appears.
- 3 Click **Remote Features**.
The **Remote Properties** window appears.
- 4 Click the check box next to **Enable Remote Floppy Boot** to configure the remote boot parameters,

- 5 Configure the RAC's remote boot parameters:
 - a Click the check box next to **Enable Remote Floppy Boot**.
 - b Type the TFTP server's IP address in the **Remote Floppy TFTP Address** field.
 - c Type the boot image filename in the **Remote Floppy TFTP Path** field. The path must be relative to the root directory of the TFTP server.
- 6 Configure the RAC's firmware update parameters:
 - a Click the check box next to **Enable Remote Firmware Update**.
 - b Type the TFTP server's IP address in the **Remote Firmware TFTP Address** field.
 - c Type the firmware image filename in the **Remote Firmware Update Path** field. The path must be relative to the root directory of the TFTP server.
- 7 Click **Apply Changes** and click **OK** to save your changes.

Configuring RAC Security



NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.



NOTE: See the *Dell Remote Access Controller Installation and Setup Guide* for more information about RAC security features.

To configure your RAC security from the Server Administrator home page, click **System**→**Main System Chassis**→**Remote Access Controller** and then click the **Security** tab. Under the **Security** tab, you can perform CSR certificate management and set RAC user login authentication options.



NOTE: Some of the RAC certificate management operations use the FTP protocol to communicate with the RAC firmware. If a firewall software is installed on the system, these operations may fail.

Certificate Management

Use the **Certificate Management** window to generate a certificate signing request (CSR), upload a server certificate or certificate authority (CA) certificate to the RAC firmware, or view an existing server certificate or CA certificate. From the **Certificate Management** window, the following options are available:

- Generating a CSR
- Uploading a Certificate
- Viewing a Certificate

A CSR is a digital request to a CA for a secure server certificate. Secure server certificates 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 the security for your RAC, it is strongly recommended that you generate a CSR, submit the CSR to a CA, and upload the certificate returned from the CA.

A certificate authority is a business entity that is recognized in the IT industry for meeting high standards of reliable screening, identification, and other important security criteria. Examples of CAs include Thwate and VeriSign. Once the CA receives your CSR, they review and verify the information the CSR contains. If the applicant meets the CA's security standards, the CA issues a certificate to the applicant that uniquely identifies that applicant for transactions over networks and on the internet.

After the CA approves the CSR and sends you a certificate, you must upload the certificate to the RAC firmware. The CSR information stored on the RAC firmware must match the information contained in the certificate.

Generating a CSR



NOTICE: Each new CSR overwrites any previous CSR on the firmware. It is crucial that the CSR on the firmware matches the certificate returned from a CA.

- 1 From the **Certificate Management** window, select the **Generate a new CSR** option and click **Next**.

The **Certificate Signing Request (CSR) Generation** window appears.

- 2 Type a value or choose a value from a drop-down menu for each listed attribute and click **Generate**.

A message appears stating that the CSR was successfully generated and giving the path where it was saved.

- 3 You are now ready to send your CSR to a CA.

Uploading a Certificate

To upload your server certificate or CA certificate to the RAC firmware, the certificate must reside on the RAC's host server. You must designate the CSR type, the exact filename, and the absolute file path to the certificate on the server. Then, click **Upload**.



NOTE: Failure to enter the correct path for the location of the certificate on the host server does not result in a warning message.

- 1 From the **Certificate Management** window, select the **Upload certificate** option and click **Next**.

The **Upload Certificate** window appears.

- 2 Select the certificate type from the drop-down menu.

The selections are **Server Certificate** and **CA Certificate**.

- 3 Type the exact path and filename of the certificate to be uploaded.



NOTE: When you have a fully qualified path or filename that contains spaces, you must place double quotation marks around the string. For example, if your file is contained in `c:\security files\certificates\sslcert.cer`, you must place the fully qualified path name and filename in double quotations because a space appears between "security" and "files." For example: "`c:\security files\certificates\sslcert.cer`".

- 4 Click **Upload**.

A message appears stating that the certificate was successfully uploaded to the RAC firmware.

- 5 Reset the RAC to enable the new certificate.



NOTE: You must reset the RAC after uploading the certificate to ensure that the new certificate is used.

Viewing a Certificate

The following information is included on both the **View Server Certificate** and **View CA Certificate** windows. See Table 8-1.

Table 8-1. Certificate Information

Attribute	Value
Type	Type of certificate, either a server certificate or a CA certificate
Serial	Certificate serial number
Key Size	Encryption key size
Valid From	Issuance date of the certificate
Valid To	Expiration date of the certificate
Subject	Certificate attributes entered by the subject
Issuer	Certificate attributes returned by the issuer

Configuring Remote Connect Authentication Options

Use the **Remote Connect Authentication Options** window to set RAC user login authentication options. You can configure the RAC to only allow login by users created through the Remote Access Service (RAS users), or to allow RAS login by users created both through the Remote Access Service and through the local operating system.

- 1 Click **System**→**Main System Chassis**→**Remote Access Controller** and then click the **Security** tab.


The **Certificate Management** window appears.

- 2 Click **Authentication Options**.

The **Remote Connect Authentication Options** window appears. There are two configuration options, each preceded by a check box.

The **RAC Authentication** check box is selected by default and cannot be deselected. This setting allows login to the RAC by users created through the RAC (RAC users).

Select the **Local Operating System Authentication** check box to also allow login to the RAC by users created through the local operating system.

 **NOTE:** The **Local Operating System Authentication** check box is grayed out by default and cannot be checked or unchecked for RAC firmware version 3.20 or later. Use Active Directory Authentication for RAC firmware version 3.20 or later. See the *Using Microsoft Active Directory With Your Dell Remote Access Controller (DRAC III, DRAC III/XT, ERA, and ERA/O) User's Guide* for information on configuring Active Directory authentication.

- 3 Click **Apply Changes** and click **OK** to save your changes.

Accessing and Using a Remote Access Controller

To link to the Remote Access Service RAC **Log in** window from the Server Administrator home page, click the **Main System Chassis** object, click the **Remote Access Controller** object, click the **Remote Connect** tab, and then click **Remote Connect**. The RAC **Log in** window appears.

After connecting to the RAC you can monitor and manage your system, including accessing system and session information, managing the RAC configurations, and performing remote access functions on the managed system. See the *Dell Remote Access Controller Installation and Setup Guide* for instructions on using a RAC.

Storage Management Service

Overview

The Storage Management Service provides storage management information in an integrated graphical view. The current release of Server Administrator provides two versions of the Storage Management Service:

- Basic Storage Management Service (Array Manager)

The basic Storage Management Service reports storage status to Server Administrator. Array Manager is also installed with the basic Storage Management Service. Array Manager provides RAID management and is launched as a separate application from Server Administrator. Array Manager is installed using Express Setup on NetWare and on systems that have an existing Array Manager installation.

The basic Storage Management Service of Server Administrator:

- Enables you to view the status of local and remote storage attached to a monitored system.
- Supports SCSI, SATA, and ATA. Does not support Fibre Channel.
- Provides RAID storage management using Array Manager as a separately launched application.
- Enhanced Storage Management Service (Storage Management)


The enhanced Storage Management Service provides RAID storage management that is integrated with Server Administrator. On Windows and Linux, the enhanced Storage Management Service is installed using Express Setup providing that the system does not have an existing Array Manager installation.


In addition to the tasks that you can perform using the basic Storage Management Service, the enhanced Storage Management Service:

- Allows you to perform controller and enclosure functions for all supported RAID and non-RAID controllers and enclosures from a single graphical or command line interface without the use of the controller BIOS utilities.
- Protects your data by configuring data redundancy, assigning hot spares, or rebuilding failed drives.
- Provides a graphical interface that is wizard-driven with features for novice and advanced users and detailed online help.


- Provides a command line interface that is fully featured and scriptable.
- Provides detailed online help.

See the *Server Administrator Command Line Interface User's Guide* for information about running Storage Management Service from the command line.

 **NOTE:** The enhanced Storage Management Service (Storage Management) enables you to perform storage tasks that are data-destructive. Storage Management should be used by experienced storage administrators who are familiar with their storage environment.

 **NOTE:** The enhanced Storage Management Service is available only on systems running Microsoft® Windows® and Red Hat® Enterprise Linux operating systems. On systems running Windows operating systems, you can choose to install either the enhanced Storage Management or the basic Storage Management Service using Custom Setup. On systems running Red Hat Enterprise Linux, you will not see the Array Manager option; enhanced Storage Management will be installed by default.


 **NOTE:** If you are installing on a Red Hat Enterprise Linux system, the enhanced Storage Management Service is the only installation choice and is installed using Express Setup.


 **NOTE:** The enhanced Storage Management Service is not available on systems running Novell® NetWare® operating systems.


When using either the basic or the enhanced Storage Management Service, you can click **Help** on the global navigation bar for more detailed information about the specific window you are viewing. 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.

Software Prerequisites

The Array Manager managed system and the enhanced Storage Management Service (Storage Management) cannot be installed on the same system. Managed systems that do not have either Array Manager or the enhanced Storage Management Service installed will still be able to perform SCSI diagnostics for direct-attached storage devices; however, RAID controller and storage diagnostics cannot be performed. See the *Array Manager User's Guide* for complete software and hardware requirements.

 **NOTE:** Array Manager is an installation choice using **Custom Setup**. If the system already has Array Manager installed, then the most current version of Array Manager is installed using **Express Setup**. See the *Dell OpenManage Array Manager User's Guide* for complete software and hardware requirements. Array Manager has both a managed system and a management station (console) component. The managed system portion of Array Manager replaces the Windows 2000 Disk Management Service. To view the **Disk Management** page, you must install the management station component of Array Manager on the same system as the managed system component.

 **NOTE:** The enhanced Storage Management Service (Storage Management) is also an installation choice using **Custom Setup**. The enhanced Storage Management Service cannot, however, be installed on a system that has the Array Manager managed system. The enhanced Storage Management Service is installed by default using **Express Setup** on systems that do not have an Array Manager installation.

 **NOTE:** Array Manager is not supported on Red Hat® Enterprise Linux operating systems.

 **NOTE:** The enhanced Storage Management Service is not supported on NetWare operating systems.

Hardware Prerequisites

When the basic Storage Management Service is installed, the managed system must have a supported RAID controller installed to view the status of local and remote storage attached to the system.

When the enhanced Storage Management Service is installed, the managed system must have a supported RAID, SCSI, ATA, SATA, or non-RAID SCSI controller attached to the system. These controllers must be attached to storage in order to have all storage status and configuration functions available.


For a list of the supported RAID controllers and for other information about Storage Management Service hardware requirements, see the Storage Management readme file on the *Systems Management CD*.


Basic Storage Management Service

The basic Storage Management Service installed with Express Setup enables you to view the status of a server's direct-attached storage devices. The Storage Management Service obtains logical and physical information about attached storage devices from the Array Manager managed system.

The basic Storage Management Service enables you to perform the following tasks:


- Display all of your storage information in a graphical environment. See the **Storage** object section in "Instrumentation Service" for a description of the available storage information.
- Run the Server Administrator Diagnostic Service to diagnose problems with your storage devices. See "Diagnostic Service" for complete instructions. This feature is only available when the Array Manager managed system is installed.

 **NOTE:** The basic Storage Management Service does not provide storage management functions such as configuring your local and remote attached storage devices, creating and managing software and hardware RAID configurations, formatting disks, assigning drive letters, and creating partitions and volumes. When the basic Storage Management Service is installed, you must use Array Manager Console to perform these storage management functions. See the *Array Manager User's Guide* for instructions. Alternatively, you can install the enhanced Storage Management Service, which replaces Array Manager and provides similar storage management functions. See "Enhanced Storage Management Service Features" for more information.

 **NOTE:** Array Manager does not support volumes management on systems running Microsoft Windows Server 2003.

Basic Storage Management and Array Manager

The basic Storage Management Service and Array Manager are installed by default when using **Express Setup** on systems that have an existing Array Manager installation. The basic Storage Management Service depends on Array Manager to report storage status. Therefore, assuming that the system meets the Array Manager installation requirements, Array Manager is installed when using Express Setup to install the Managed System Software package. Managed systems that do not have Array Manager installed will still be able to perform SCSI diagnostics for direct-attached storage devices; however, RAID controller and storage diagnostics cannot be performed. See the *Array Manager User's Guide* for complete software and hardware requirements.

 **NOTE:** Array Manager is not supported on Red Hat Enterprise Linux operating systems.

Basic Storage Management Tree Objects

The basic Storage Management is accessible by selecting the **Storage** tree object on the Server Administrator graphical user interface (GUI). The **Storage** object expands to display the following objects:

- Array Subsystems
- OS Disks
- Volumes

See the **Storage** object section in “Instrumentation Service” for a description of the available storage information.

Enhanced Storage Management Service

The enhanced Storage Management Service provides advanced features for configuring a system's locally attached RAID and non-RAID disk storage. Storage Management enables you to perform controller and enclosure functions for all supported RAID and non-RAID controllers and SCSI PowerVault™ 2xxS enclosures from the Server Administrator graphical interface without requiring use of the controller BIOS utilities.

Using the enhanced Storage Management Service, you can protect your data by configuring data-redundancy, assigning hot spares, or rebuilding failed drives. You can also perform data-destructive tasks such as deleting virtual disks or resetting the controller configuration. All users of the enhanced Storage Management Service should be familiar with their storage environment and storage management.

In addition to the Server Administrator interface features, the enhanced Storage Management Service provides wizard-driven features for novice and advanced users and detailed online help.

The enhanced Storage Management Service command line interface (CLI) provides extended options for the Server Administrator **omreport** and **omconfig** commands. These options provide a command line interface that is fully featured and scriptable.

The enhanced Storage Management Service supports SCSI, SATA, and ATA; however, Fibre Channel is not supported.

This release of Storage Management does not support Windows volume and disk management or the NetWare operating system.



NOTE: The enhanced Storage Management Service provides 32-bit (not 64-bit) support for Windows Server 2003.

For additional information, see "Enhanced Storage Management Service."

Enhanced Storage Management Service and Array Manager

The enhanced Storage Management Service is a replacement for Array Manager. The enhanced Storage Management Service provides similar storage management and configuration features as Array Manager. There are differences in the operating system support and other features, however. See "Enhanced Storage Management Service" for more information.

Enhanced Storage Management Tree Objects

When installed, the enhanced Storage Management Service is accessible by selecting the **Storage** tree object on the Server Administrator GUI. The **Storage** object expands to display tree objects for the supported controllers attached to the system. The controller object expands to display the storage attached to the controller.

Depending on the controllers and storage attached to the system, the expanded **Storage** object may display the following lower-level objects:

- Controller
- Battery
- Channel
- Enclosure or Backplane
- Array Disks
- EMMs (Enclosure Management Modules)
- Fans
- Power Supplies
- Temperatures
- Virtual Disks

Health Tab

The **Health** tab for each tree object displays status information for the selected object.

Information/Configuration Tab

The **Information/Configuration** tab displays the property information for the selected tree object. When using the enhanced Storage Management Service, the **Information/Configuration** tabs also have drop-down menus and buttons for executing storage tasks and launching wizards.

Enhanced Storage Management Tasks

The enhanced Storage Management Service has drop-down menus and wizards for executing storage management and configuration tasks. This section discusses some of the common storage tasks and wizards provided by the enhanced Storage Management Service.

 **NOTE:** For complete documentation of the enhanced Storage Management Service storage tasks and other features, see the enhanced Storage Management Service online help.

Create Virtual Disk Wizard

The enhanced Storage Management Service provides an Express and an Advanced Create Virtual Disk Wizard. The Express Wizard calculates an appropriate virtual disk configuration based on the available space and controller considerations. When using the Express Wizard, you select the RAID level and size for the virtual disk. The Express Wizard selects a recommended disk configuration for you that matches your RAID level and size selection. The Express Wizard requires minimal user input and is recommended for novice users.

The Create Virtual Disk Advanced Wizard allows you to specify the read, write, and cache policy for the virtual disk. You can also select the array disks and the controller channel to be used. You need a good knowledge of RAID levels and hardware to use the Advanced Wizard. This wizard is recommended for advanced users.

To launch the Express and Advanced Create Virtual Disk Wizards:

- 1 Expand the **Storage** tree object to display the controller objects.
- 2 Expand a controller object.
- 3 Select the **Virtual Disks** object.
- 4 Click **Go To Create Virtual Disk Wizard**.
- 5 See the enhanced Storage Management online help for more information.

Reconfigure Virtual Disk Wizard

The Reconfigure Virtual Disk Wizard enables you to change the virtual disk configuration. Using this task, you can change the RAID level and increase the virtual disk size by adding array disks. On some controllers, you can also remove array disks.

To launch the Reconfigure Virtual Disk Wizard:

- 1 Expand the **Storage** tree object to display the controller objects.
- 2 Expand a controller object.
- 3 Select the **Virtual Disks** object.

- 4 Select **Reconfigure** from the **Available Tasks** drop-down menu.
- 5 Click **Execute**.
- 6 See the enhanced Storage Management online help for more information.

Maintain Integrity of Redundant Virtual Disks

If you have created a redundant virtual disk, the Check Consistency task verifies the accuracy of the redundant (parity) information. This task only applies to redundant virtual disks. When necessary, the Check Consistency task rebuilds the redundant data.

To launch the Check Consistency task:

- 1 Expand the **Storage** tree object to display the controller objects.
- 2 Expand a controller object.
- 3 Select the **Virtual Disks** object.
- 4 Select **Check Consistency** from the **Available Tasks** drop-down menu.
- 5 Click **Execute**.
- 6 See the enhanced Storage Management online help for more information.

Assign a Hot Spare

A hot spare is an unused backup array disk that can be used to rebuild data from a redundant virtual disk. Hot spares remain in standby mode. When an array disk that is used in a redundant virtual disk fails, the assigned hot spare is activated to replace the failed array disk without interrupting the system or requiring your intervention. If a virtual disk using the failed array disk is not redundant, then the data is permanently lost without any method (unless you have a backup) to restore the data.

You can assign either a dedicated or a global hot spare.

To assign a dedicated hot spare:

- 1 Expand the **Storage** tree object to display the controller objects.
- 2 Expand a controller object.
- 3 Select the **Virtual Disks** object.
- 4 Select **Assign Dedicated Hot Spare** from the **Available Tasks** drop-down menu.
- 5 Click **Execute**.
- 6 See the enhanced Storage Management online help for more information.

To assign a global hot spare:

- 1 Expand the **Storage** tree object to display the controller objects.
- 2 Expand a controller object.
- 3 Expand a channel object.

- 4 Expand the enclosure or backplane object.
- 5 Select the **Array Disks** object.
- 6 Select the **Information/Configuration** subtab.
- 7 Select a **Assign Global Hot Spare** from the **Available Tasks** drop-down menu.
- 8 Click **Execute**.
- 9 See the enhanced Storage Management online help for more information.

Rebuild a Failed Array Disk

If the failed array disk is part of a redundant virtual disk, then the array disk failure should not result in data loss if replaced immediately. The rebuild task is available when the Array Disks object is selected. See the enhanced Storage Management online help for more information.

Additional Enhanced Storage Management Features

There are many tasks associated with controllers, enclosures, virtual disks, and array disks that you can perform with the enhanced Storage Management Service. See the enhanced Storage Management online help for more information.

Global Tasks

The following global tasks are available when the Storage object is selected. See the enhanced Storage Management online help for more information.

- **Global Rescan.** A global rescan updates configuration changes (such as new or removed devices) for all controllers and their attached components.
- **Enable and Disable Smart Thermal Shutdown.** By default, the operating system and server shut down when the PV220S and PV221S enclosures reach a critical temperature of 0 or 50 degrees celsius. Using the Enable Smart Thermal Shutdown task, however, you can specify that only the enclosure and not the operating system and server be shut down when the enclosure reaches a critical temperature. To restore the system to its default setting use the Disable Smart Thermal Shutdown task.

Controller Tasks

The following controller tasks are available when the **Controller** object is selected. See the enhanced Storage Management online help for more information.

- **Rescan Controller.** A controller rescan updates configuration changes (such as new or removed devices) for all components attached to the controller.
- **Create Virtual Disk.** See "Create Virtual Disk Wizard."
- **Enable, Disable, Quiet, and Test Alarm.** These tasks enable you to manage the controller alarm. For example, you can set the alarm to sound in the event of a device failure or quiet the alarm once it is sounding.

- **Set Rebuild Rate.** The rebuild rate refers to how much of the system's resources are dedicated to rebuilding a failed array disk. This task enables you to adjust this setting.
- **Reset Configuration.** This task erases all information on the controller, so that you can perform a fresh configuration. This operation destroys all virtual disks on the controller.
- **Export Log File.** This task exports the controller log to a text file.

Battery Tasks

The following battery tasks are available when the **Battery** object is selected. This task is only available for controllers that have batteries that require reconditioning. See the enhanced Storage Management online help for more information.

- **Recondition Battery.** This task fully discharges and recharges the controller battery.

Channel Tasks

The following channel tasks are available when the **Channel** object is selected. See the enhanced Storage Management online help for more information.

- **Rescan Channel.** This task rescans the controller channels to verify the currently connected devices or to recognize new devices that have been added to the channels. Performing a rescan on a channel is similar to performing a rescan on the controller.

Enclosure Tasks

The following enclosure tasks are available when the **Enclosure** object is selected. See the enhanced Storage Management online help for more information.

- **Enable and Disable Alarm.** Use these tasks to manage the enclosure alarm. When enabled, the alarm sounds when the enclosure encounters an error condition.
- **Set Asset Data.** Use this task to change the enclosure's asset tag and asset name.
- **Set Temperature Probe Values.** The temperature probes monitor the enclosure's temperature. Each temperature probe has a Warning and a Failure threshold. The Warning threshold indicates that the enclosure is approaching an unacceptably warm or cool temperature. Use this task to modify the Warning threshold.

Temperatures Tasks

The following temperature probe tasks are available when the **Temperatures** object is selected. See the enhanced Storage Management online help for more information.

- **Set Temperature Probe.** The temperature probes monitor the enclosure's temperature. Each temperature probe has a Warning and a Failure threshold. The Warning threshold indicates that the enclosure is approaching an unacceptably warm or cool temperature. Use this task to modify the Warning threshold.

Array Disk Tasks

The following array disk tasks are available when the **Array Disks** object is selected. See the enhanced Storage Management online help for more information.

- **Blink and Unblink.** The Blink task allows you to find a disk within an enclosure by blinking one of the light-emitting diodes (LEDs) on the disk. The Unblink task cancels the Blink task.
- **Remove Dead Segments.** In certain circumstances, this task enables you to recover disk space that is currently unusable.
- **Assign and Unassign Global Hot Spare.** See "Assign a Hot Spare."
- **Prepare to Remove.** Use this task before removing a disk from an enclosure. It is recommended that you perform this task before removing a disk to prevent data loss.
- **Online and Offline.** Use the Offline task to deactivate a disk before removing it. Use the Online task to reactivate an offline disk.
- **Initialize.** On some controllers, the Initialize task prepares an array disk for use as a member of a virtual disk.
- **Rebuild.** See "Rebuild a Failed Array Disk."

Virtual Disk Tasks

The following virtual disk tasks are available when the **Virtual Disks** object is selected. See the enhanced Storage Management online help for more information.

- **Reconfigure.** See "Reconfigure Virtual Disk Wizard."
- **Format or Initialize.** Use the Format or Initialize task to erase the files and remove the file systems on a virtual disk.
- **Cancel Background Initialization.** On some controllers, background initialization of redundant virtual disks begins automatically after the virtual disk is created. Use this task if you need to cancel the background initialization.
- **Restore Dead Segments.** Use the Restore Dead Segments task to recover data from a RAID-5 virtual disk that has been corrupted.
- **Delete.** Use this task to destroy all data on the virtual disk.
- **Assign and Unassign Dedicated Hot Spare.** See "Assign a Hot Spare."
- **Check Consistency, Cancel Check Consistency, Pause Check Consistency, and Resume Check Consistency.** See "Maintain Integrity of Redundant Virtual Disks."
- **Blink and Unblink.** The Blink and Unblink tasks blink or unblink the lights on the array disks included in the virtual disk.
- **Rename.** Use this task to rename a virtual disk.
- **Change Policy.** Use this task to change a virtual disk's read, write, or cache policy.

- **Split Mirror:** Use this task to separate mirrored data originally configured as a RAID 1, RAID 1-concatenated, or RAID 10 virtual disk.
- **Unmirror:** Use this task to separate mirrored data and restore one half of the mirror to free space.

Additional Enhanced Storage Management Features and Documentation

The enhanced Storage Management online help provides additional information for using the storage management features and tasks. For information on how to launch the online help, see "Displaying Online Help."

Comparing the Enhanced Storage Management Service and Array Manager

Although the enhanced Storage Management Service features are similar to Array Manager, there are differences in operating system support. Array Manager also supports fibre channel whereas the enhanced Storage Management Service does not. Because of these differences, the decision whether or not to install the enhanced Storage Management Service should be made based on the needs of your storage environment.

The following summarizes notable differences in operating system and feature support between Array Manager and the enhanced Storage Management Service:

- Disk and volume management are provided by Array Manager on Windows 2000. Disk and volume management are not provided by the enhanced Storage Management Service. If you need disk and volume management, you can use the native disk and volume management utilities provided by your operating system. On a Windows 2000 system, you have the option of installing Array Manager which replaces the Windows 2000 disk and volume management.
- Fibre channel support for the Dell PowerVault 660F storage system is provided by Array Manager, but not by the enhanced Storage Management Service.
- NetWare support is provided by Array Manager, but not by the enhanced Storage Management Service.
- Linux support is provided by the enhanced Storage Management Service, but not by Array Manager.

The following table provides a comprehensive comparison of enhanced Storage Management Service and Array Manager features.

Table 9-1. Comparing Enhanced Storage Management Service and Array Manager Features

Feature	Array Manager	Enhanced Storage Management Service
Storage Status	Displayed	Displayed
Storage Management and Configuration	Available when launched as a separate application	Available from the Server Administrator graphical or command line interface.
Graphical interface	All features available from graphical interface launched separately from Server Administrator.	All features available from Server Administrator graphical interface.
Command Line Interface	Has limited command line interface that does not support storage configuration tasks. Does not support the Server Administrator omreport and omconfig commands.	Fully-featured, scriptable command line interface. Supports omreport storage commands and has expanded omconfig storage command options.
Wizards for common storage tasks	Yes	Yes
Detailed Online Help	Yes	Yes
Windows 2000 Disk and Volume Management	Yes	No
Fibre Channel Support	Yes	No
Linux Support	No	Yes

Table 9-1. Comparing Enhanced Storage Management Service and Array Manager Features

Feature	Array Manager	Enhanced Storage Management Service
NetWare Support	Yes	No (NetWare support to be added in future release.)
Windows Server 2003 32-bit Support	Yes	Yes
Windows Server 2003 64-bit Support	No	No

Migrating from Array Manager to the Enhanced Storage Management Service

If you already have Array Manager installed and wish to upgrade to the enhanced Storage Management Service using **Custom Setup**, there are migration considerations that apply when installing the enhanced Storage Management Service. In particular, these considerations apply to the preservation of virtual disk names created with Array Manager and to any applications that have been modified to receive SNMP traps from Array Manager. The following describes these migration considerations:

- **Virtual Disk Preservation.** When migrating from Array Manager to the enhanced Storage Management Service, you can preserve the virtual disk names that were created with Array Manager. Virtual disk name preservation is made possible when you install the enhanced Storage Management Service using the OpenManage install process (Custom Setup). The Custom Setup process will uninstall Array Manager and install the enhanced Storage Management Service.

If you uninstall Array Manager outside of the OpenManage install process, the Array Manager virtual disks will be renamed after installing the enhanced Storage Management service.

Whether or not Array Manager is manually uninstalled before installing the enhanced Storage Management Service, the enhanced Storage Management Service will be able to identify and manage the virtual disks created with Array Manager.

- **SNMP Traps.** In the enhanced Storage Management Service, the architecture for handling the SNMP traps and the Management Information Base (MIB) is different from that of Array Manager. You must modify applications that have been customized to receive SNMP traps from Array Manager.
- **Event Numbering.** The numbering scheme for the enhanced Storage Management Service alerts or events is different from the numbers used for the corresponding Array Manager events. See the enhanced Storage Management Service online help for more information.

Basic and Enhanced Storage Management Command Line Interface

See the *Server Administrator Command Line Interface User's Guide* for information about running the basic and enhanced Storage Management Service from the command line. If you have the enhanced Storage Management Service installed, you can also refer to the online help for information about the expanded **omreport** and **omconfig** command line options.

Displaying Online Help

Both the basic and the enhanced Storage Management Services provide context-sensitive online help. To access the online help, click **Help** on the global navigation bar. This navigation 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.

The enhanced Storage Management Service provides additional online help. This help is available when the **Storage** or a lower-level tree object is selected.

The online help of the enhanced Storage Management Service:

- Provides conceptual information on storage concepts such as virtual disks, RAID, and so on
- Describes the GUI components in the various windows of the application
- Gives detailed, step-by-step instructions on the tasks that you can perform in the GUI
- Describes the available CLI commands and their subcommands

The enhanced Storage Management online help is available in two formats:

- **Context-sensitive Help.** To access the context-sensitive online help, click **Help** on the global navigation bar.
- **Table of Contents.** The help screens for the context-sensitive help contain links to the online help Table of Contents. To access the Table of Contents, first click **Help** on the global navigation bar. Next, click the **Go to Table of Contents for Storage Management Online Help** link to display the Table of Contents. This link is displayed at the top and bottom of each help screen. Use the Table of Contents to access all topics covered in the online help.


Diagnostic Service

Overview

The Server Administrator Diagnostic Service is a suite of diagnostic programs, or *test modules*, that run locally on your system and can be accessed either locally or remotely over the network. You select diagnostics tests to run from a hierarchical menu representing the hardware that Server Administrator discovers on your system. You can select tests for various parts of a system and run them simultaneously or sequentially in a single session. In addition, you can view results for each individually selected test or hardware component.

 **NOTE:** You must have Admin or Power User privileges in Server Administrator to run diagnostics tests through the Diagnostic Service.


The Diagnostic Service is engineered to diagnose problems on individual systems. It does not address problems that arise on the network level, unless the problem resides with a NIC on a single system.

 **NOTE:** The Diagnostic Service runs concurrently with all other applications running on the system under test. Running these diagnostics causes significant additional system load that will impact the performance of your system and all running applications. If you are running critical applications that require rapid response or consume significant system resources, take the appropriate precautions before running these diagnostics. Close all nonessential applications and only run diagnostics during nonpeak hours of system use.

 **NOTE:** The Diagnostic Service is not supported on Novell® NetWare® operating systems.

See the *Server Administrator Command Line Interface User's Guide* for information about running the Diagnostic Service from the command line.

When using the Diagnostic Service, you can click **Help** on the global navigation bar for more detailed information about the specific window you are viewing. Diagnostic Service help is available for all diagnostics tests that can be run for the device groups that Server Administrator discovers on your system.

 **NOTE:** At startup, the **Diagnostics** tab is not available in Server Administrator and the **Diagnostic Service** is not listed on any of the **Health** pages. The Diagnostic Service waits for the Server Administrator service to start completely before enumerating (scanning the system for available devices to diagnose). If you press <F5> to refresh, the **Diagnostic** tab shows up when enumeration is complete. This process can take several minutes on some systems.

Devices Supported by the Diagnostic Service

The Diagnostic Service provides diagnostics for the following Dell-supplied hardware devices:

- Remote Access Controller (RAC)
- RAID controller
- SCSI controller
- USB controller
- Complementary Metal-Oxide Semiconductor (CMOS)
- DVD/CD/CD-RW drive
- Diskette drive
- Hard drive
- Memory
- Modem
- NIC
- Parallel port
- PCI bus
- Serial port
- Tape drive
- Tape Autoloaders



NOTE: For a complete list of hardware devices that Server Administrator diagnostics specifically supports, see the *Server Administrator Compatibility Guide*.

Table 10-1 lists the different results and events reported by the diagnostic tests.

Table 10-1. Results and Events

Result	Explanation
Passed	The test completed successfully. This results in an Information event.
Failed	The test failed due to a critical error. This results in an Error event and an error message is displayed.
Unusual Status	The test result cannot be determined because of an internal error or the unavailability of resources. This results in a Warning event and a warning message is displayed.
Aborted	The test was aborted by the user.

Diagnostic Service Features

In addition to diagnostic tests for devices listed in the section "Devices Supported by the Diagnostic Service," the Diagnostic Service offers the following features:

- **Device Enumeration**

This feature enables you to reenumerate all testable devices on your system.

To access this feature, click the **Diagnostics** tab and then click **Re-enumerate**.

- **Device and Test Selection**

This feature enables you to select the devices on which you want to run diagnostic tests and the tests you want to run.

To access this feature, click the **Diagnostics** tab.

- **Diagnostic Scheduler**

This feature enables you to select diagnostic tests to run at specific times and at specific frequencies.

For more information on configuring this feature, see "Scheduling Diagnostics."

- **Diagnostic Test Review**

This feature enables you to review the selected diagnostic tests.

To access this feature, click the **Diagnostics** tab and then click **Review**.

- **Diagnostic Test Status**

This feature enables you to view the status of the diagnostic tests that are running.

To access this feature, click the **Diagnostics** tab and then click **Status**.

- **Diagnostic Result History**

This feature enables you to view the result history log file. This log file contains a record of the results of previously run diagnostics tests. You can specify the maximum size of this log file in the **Diagnostic Application Settings** window.

To access this feature, click the **Diagnostics** tab and then click **Results**.

- **Hardware Configuration Changes**

This feature enables you to view changes that have occurred to the testable devices on your system since the system was rebooted, the secure port server was restarted, or reenumeration was performed. It reports the changes in the system configuration, such as the addition or removal of the hard drive.

To access this feature, click the **Diagnostics** tab and then click **Hardware Changes**.

- **Hardware Configuration Change History**

This feature enables you to view a log file that contains a history of hardware configuration changes.

To access this feature, click the **Diagnostics** tab, click **Hardware Changes**, and then click **Hardware Change History**.

Configuring the Diagnostic Service

The Diagnostic Service enables you to set options for running diagnostic tests. You can set options for both Applications Settings and Test Execution Settings.

Configuring the Applications Settings

To configure the Application Settings, perform the following steps:

- 1 In the Server Administrator home page, click **Preferences** on the global navigation bar and then click the **Diagnostics** tab.
- 2 In the **Diagnostic Application Settings** window, set the options as desired.

The following controls are available on the **Diagnostic Applications Settings** window:

- Select the **Show Test Warning Messages** check box to enable the display of warning messages before running certain resource-intensive tests, such as memory tests.
 - Select the **Show Diagnostic Warning Screen** check box to enable the display of the **Diagnostic Warning Screen**.
 - The **RMI Registry Port** specifies the server socket port where the RMI registry is listening for a connection.
 - The **Maximum Diagnostic Result History File Size** specifies the largest file size in MB for the result history file. If the file grows beyond this limit, the Diagnostic Service purges old file entries, starting with the earliest entry, until the file conforms to the specified limit.
 - The **Maximum Hardware Configuration Change History File Size** specifies the largest file size in MB for the hardware configuration change history file. If the file grows beyond this limit, the Diagnostic Service purges old file entries, starting with the earliest entry, until the file conforms to the specified limit.
 - The **Maximum Completed Tests Displayed** specifies the maximum number of completed tests to be displayed on the **Status** window.
 - The **Timeout for Completed Results in Memory** specifies the maximum time period in minutes for keeping the test results in the application cache.
- 3 When you finish setting options in the **Diagnostic Application Settings** window, click **Apply Changes**.

Configuring the Test Execution Settings

To configure the Test Execution Settings, perform the following steps:

- 1 In the Server Administrator home page, click the **Diagnostics** tab and then click **Settings**.
- 2 In the **Diagnostic Test Execution Settings** window, set the options as desired.

The following controls are available on the **Diagnostic Test Execution Settings** window:

- Select the **Halt Execution of Test on First Error** check box to stop the test immediately when an error is encountered.
- Select the **Quick Test** check box to use a faster algorithm to conduct the test, if one is available for the specified test. If errors are not reported after running in Quick Test mode and you believe that the hardware tested still has problems, it is recommended that you deselect **Quick Test** and run the same test.
- Select the **Halt Multiple Pass Test Execution on Error** check box to stop subsequent passes of a test if an error is encountered.
- Select one of the following options to specify either the number of passes or the run time for selected tests:
 - **Enable Number of Passes** to specify the number of times that you want tests to run. Then type the number in the **Number of Passes** field.
 - **Enable Run Time** to specify the amount of time in minutes that you want the tests to run. Then type the time in the **Run Time** field.



NOTE: The test will not stop within the specified Run Time until it completes the current pass. The test will start the next pass only if there is an optimum amount of Run Time remaining for the test to run.

- 3 When finished setting options in the **Diagnostic Test Execution Settings** window, click **Apply Changes**.

Re-enumerating Devices

The system enumerates the testable devices on your system whenever the system is rebooted or the secure port server is restarted. In addition, you can perform an enumeration by using the reenumeration feature.

To reenumerate devices, perform the following steps:

- 1 In the Server Administrator main window, click the **Diagnostics** tab.
- 2 In the **Diagnostic Selection** window, click **Re-enumerate**.



NOTE: This process can take several minutes on some systems.

- 3 Click **Enumeration Status** to view the progress of the enumeration process.


The **Diagnostic Re-Enumeration Progress** window opens. A progress bar indicates the percentage complete of the enumeration process.

Running Diagnostics

To run diagnostic tests, perform the following steps:


- 1 In the Server Administrator main window, click the **Diagnostics** tab.
- 2 In the **Diagnostic Selection** window, select the tests you want to run.

The following controls are available on the **Diagnostic Selection** window:

- In the **Available Devices** list, select a device to view the applicable tests for that device.
To get information about a device and the tests that can be run on it, click the Information () icon.
- Select **Show All Applicable Tests** to view all the tests that are applicable to the system.
Select **Show Tests for Selected Device Only** to view only those tests that are applicable to the device selected in the **Available Devices** list.
- Select the desired tests in the **Available Tests** list.

- 3 Click **Review Selection**.

- 4 The **Diagnostic Selection Review** window lists the currently selected diagnostics tests.

- Click the  icon to remove a test from the list.
- Click **Change** to change the test settings.

The **Diagnostic Test Execution Settings** window lists the current settings. Make the required changes and click **Apply Changes**.

If you do not make any changes, click **Go Back to Review Selection Page**.


- Click **View** to view the test details.

In the **Diagnostic Review Selection Details** window, click **Back to Review Screen**.

- Click **Select More Tests** to navigate to the **Diagnostic Selection** window and select more tests.




- 5 After you have selected the tests you want to run, click **Execute Tests**.

The tests are queued for execution in the order in which they were selected.


 **NOTE:** If you want to schedule the tests to run at a later time, see "Scheduling Diagnostics."


- 6 Click **Status** to monitor the status of the test execution.


The **Diagnostic Status** window opens. The icons in the **Status** column indicate the status of each test.


The In Progress icon () indicates that the test is being executed. If you have executed this test from the command line, you will see the CLI icon () next to the In Progress icon. If it is a scheduled test, you will see the Scheduler icon () next to the In Progress icon.

The Aborted icon () indicates that the test has been aborted.

The Suspended icon () indicates that test has been suspended. Click **Resume** to resume the execution of this test.

The OK icon () indicates that test has been executed successfully.

The Noncritical icon () indicates that noncritical errors were encountered during the execution of the test.

The Critical icon () indicates that the test has failed.

- Click **Abort** to stop the current test. Click **Abort All** to stop all the queued tests.
- Click **Suspend** to suspend the execution of the test. Click **Resume** when you want the test execution to be resumed.
- Click **Clear Completed** to remove the completed tests from the window. However, clicking this button will not clear the following tests:
 - Tests that are currently running
 - Tests that have been submitted from the CLI, irrespective of whether they are completed or not
- Click **View** to view the test execution progress.


The **Diagnostic Progress** window opens. A progress bar indicates the percentage complete for each pass of every test.


Click **Back to Status Page** to return to the **Diagnostic Selection** window.

- Click **View Results** to view the details of the test results. The **Diagnostic Result History - Result Details** window opens.

Scheduling Diagnostics


Instead of executing the diagnostic tests immediately, you can also schedule tests to run automatically at a specified time and date.

 **NOTE:** The date and time you enter when scheduling diagnostics are validated against the date and time on the system running Server Administrator.

 **NOTE:** Any previously scheduled tasks, hardware changes history, or result history from Server Administrator 1.8 or earlier will not be preserved when Diagnostic Service is upgraded from an earlier release to the current release.

To schedule diagnostics to run at a specific date and time or to remove previously scheduled tests, perform the following steps:

- 1 Select the tests you want to schedule. See "Running Diagnostics" for information on selecting tests.
- 2 In the **Diagnostic Selection Review** window, click **Schedule**.
 - a Type the name of the task in the **Task Name** field.

- b Type the description of the task in the **Task Description** field.
 - c Select a time in the **Select Time** field to specify the time of day you want to run the selected diagnostics.
 - d Click the  (calendar) button to select the **Start Date** from a calendar graphic.
 - e Select the **Frequency** of the test.
 - Click **Once** to run the selected diagnostics tests once on the **Start Date** at the **Start Time**.
 - Click **Daily** to run the selected diagnostics tests every day on and after the **Start Date** at the **Start Time**.
 - Click **Weekly** to run the selected diagnostics tests on the **Start Date** at the **Start Time**, and then at weekly intervals from the **Start Date** at the **Start Time**.
 - Click **Monthly** to run the selected diagnostics tests on the **Start Date** at the **Start Time**, and then at monthly intervals from the **Start Date** at the **Start Time**.
 - f Click **View Scheduled Tasks** to display the list of scheduled diagnostic tasks.
- 3 Click **Schedule** to schedule the tests.
 - 4 Repeat step 2 and step 3 until you have scheduled all applicable tests.




NOTE: Do not schedule diagnostics to run in parallel on multiple tape devices. Also, do not run diagnostic tests in parallel with SCSI communication tests.

Reviewing Scheduled Tests

You can review the diagnostic tests you have scheduled and make changes to them. You can also add, delete, or reschedule tests. To review the scheduled tests, perform the following steps:

- 1 In the Server Administrator main window, click the **Diagnostics** tab, then click **Scheduled Tasks**.

The **Diagnostic Scheduled Tasks** window opens. This displays the test schedule details such as, the Last Run Time and the Next Run Time.

- 2 Click **Cancel All** to cancel the execution of all the scheduled tasks.
- 3 Click **Refresh** to refresh the window to get the latest information on the scheduled tests.
- 4 Click the  icon next to each test to delete that particular record from the list.
- 5 Click **View** to display detailed information about the device, test, and test settings or to reschedule the test.
- 6 In the **Diagnostic Scheduling** window, make the required changes and click **Reschedule**.

Server Administrator Logs

Overview

Server Administrator allows you view and manage hardware, alert, POST, 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 privileges to clear logs or must be logged in with Admin or Power User privileges 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
- POST Log
- 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

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


Use the Alert log to monitor various system events. The Server Administrator generates events in response to changes in the status of sensors and other monitored parameters. Each status change event recorded in the Alert log consists of a unique identifier called the event ID for a specific

event source category and an event message that describes the event. The event ID and message uniquely describe the severity and cause of the event and provide other relevant information such as the location of the event and the monitored component's previous state.

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

Information displayed in the Alert log includes:


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

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

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

POST Log

Use the POST log to view and analyze events from the POST that your system performs during boot. Before the operating system loads when you turn on your system, the POST tests various system components, such as RAM, the hard drives, and the keyboard.


 **NOTE:** The POST log is not supported on all systems.

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

Information displayed in the POST log includes:

- The POST code
- A description of the code

Command Log

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

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

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



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

Appendix

Overview

This section provides supplemental information and discusses known issues with using Server Administrator.

Setting Alert Actions for Systems Running a Supported Red Hat Enterprise 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 Window System, you will not see that message by default. To see the alert message when X Window System 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 Window System, you will not see that message by default. To see the broadcast message when X Window System 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 Window System based applications because Server Administrator cannot execute such applications properly.
- Do not specify applications that require input from the user because Server Administrator cannot execute such applications properly.
- Redirect **stdout** and **stderr** to a file when specifying the application so that you can see any output or error messages.
- If you want to execute multiple applications (or commands) for an alert, create a script to do that and put the full path to the script in the "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® Enterprise 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.

BMC Platform Events Filter Alert Messages

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

Table A-1. BMC PEF Alert Events

Event	Description
Fan Probe Failure	The fan is running too slow or not at all.
Voltage Probe Failure	The voltage is too low for proper operation.
Discrete Voltage Probe Failure	The voltage is too low for proper operation.
Temperature Probe Warning	The temperature is approaching excessively high or low limits.
Temperature Probe Failure	The temperature is either too high or too low for proper operation.
Chassis Intrusion Detected	The system chassis has been opened.
Redundancy (PS or Fan) Degraded	Redundancy for the fans and/or power supplies has been reduced.
Redundancy (PS or Fan) Lost	No redundancy remains for the system's fans and/or power supplies.
Processor Warning	A processor is running at less than peak performance or speed.
Processor Failure	A processor has failed.
PPS/VRM/DCtoDC Warning	The power supply, voltage regulator module, or DC to DC converter is pending a failure condition.
Power Supply/VRM/D2D Failure	The power supply, voltage regulator module, or DC to DC converter has failed.
Hardware log is full or emptied	Either an empty or a full hardware log requires administrator attention.
Automatic System Recovery	The system is hung or is not responding and is taking an action configured by Automatic System Recovery.

Known Issues

Instrumentation Service Issues

- The functionality of the watchdog timer feature cannot be guaranteed in a case where a multibit error occurs in system DRAM Bank_1. If a multibit error occurs in this location, it is possible for the BIOS code resident in this space to become corrupted. Because the watchdog feature utilizes a call to BIOS to effect the shutdown or reboot behavior, it is conceivable that the feature will not work properly in this instance. If this occurs, you must manually reboot the system.
- If a system with spare bank memory enabled enters a "redundancy lost" state, it may not be apparent which memory module is the cause. If you cannot determine which DIMM to replace, see the "switch to spare memory bank detected" log entry in the ESM system log to find which memory module failed.
- On managed systems running a Novell® NetWare® operating system, the Instrumentation Service loads multiple Netware Loadable Modules (NLMs) at system startup. Some NLMs are automatically uninstalled because they are not required on a particular system. The process for uninstalling the NLMs occurs approximately 2 minutes after you boot the system. During this uninstallation process, a module unloading message appears on the NetWare system console.
- Novell NetWare version 5.1 might sometimes be incorrectly reported as Novell NetWare version 5.0.

Glossary

The following list defines or identifies technical terms, abbreviations, and acronyms used in your system documents.

A

Abbreviation for ampere(s).

AC

Abbreviation for alternating current.

AC power switch

A switch with two AC power inputs that provides AC power redundancy by failing over to a standby AC input in the event of a failure to the primary AC input.

access

Refers to the actions a user can take on a variable value. Examples include read-only and read-write.

ACL

Abbreviation for access control list. ACL files are text files that contain lists that define who can access resources stored on a Novell[®] Web server.

adapter card

An expansion card that plugs into an expansion-card connector on the system's system board. An adapter card adds some specialized function to the system by providing an interface between the expansion bus and a peripheral device. Examples of adapter cards include network cards, sound cards, and SCSI adapters.

ADB

Abbreviation for assign database.

AGP

Abbreviation for advanced graphics port.

ASCII

Acronym for American Standard Code for Information Interchange. A text file containing only characters from the ASCII character set (usually created with a text editor, such as Notepad in Microsoft[®] Windows[®]), is called an ASCII file.

ASIC

Acronym for application-specific integrated circuit.

ASPI

Acronym for advanced SCSI programming interface.

asset tag code

An individual code assigned to a system, usually by a system administrator, for security or tracking purposes.

attribute

As it relates to an attribute is a piece of information related to a component. Attributes can be combined to form groups. If an attribute is defined as read-write, it may be defined by a management application.

autoexec.bat file

The **autoexec.bat** file is executed when you boot your system (after executing any commands in the **config.sys** file). This start-up file contains commands that define the characteristics of each device connected to your system, and it finds and executes programs stored in locations other than the active directory.

backup

A copy of a program or data file. As a precaution, you should back up your system's hard drive on a regular basis. Before making a change to the configuration of

your system, you should back up important start-up files from your operating system.

baud rate

A measurement of data transmission speed. For example, modems are designed to transmit data at one or more specified baud rate(s) through the COM (serial) port of a system.

beep code

A diagnostic message in the form of a pattern of beeps from your system's speaker. For example, one beep, followed by a second beep, and then a burst of three beeps is beep code 1-1-3.

BGA

Abbreviation for ball grid array, an integrated circuit (IC) package that uses an array of solder balls, instead of pins, to connect to a system board.

binary

A base-2 numbering system that uses 0 and 1 to represent information. The system performs operations based on the ordering and calculation of these numbers.

BIOS

Acronym for basic input/output system. Your system's BIOS contains programs stored on a flash memory chip. The BIOS controls the following:

- Communications between the microprocessor and peripheral devices, such as the keyboard and the video adapter
- Miscellaneous functions, such as system messages

bit

The smallest unit of information interpreted by your system.

BMC

Abbreviation for baseboard management controller, which is a controller that provides the intelligence in the IPMI structure.

boot routine

When you start your system, it clears all memory, initializes devices, and loads the operating system. Unless the operating system fails to respond, you can reboot (also called warm boot) your system by pressing < Ctrl> < Alt> < Del> ; otherwise, you must perform a cold boot by pressing the reset button or by turning the system off and then back on.

bootable diskette

You can start your system from a diskette. To make a bootable diskette, insert a diskette in the diskette drive, type `sys a:` at the command line prompt, and press < Enter> . Use this bootable diskette if your system will not boot from the hard drive.

bpi

Abbreviation for bits per inch.

bps

Abbreviation for bits per second.

BTU

Abbreviation for British thermal unit.

bus

An information pathway between the components of a system. Your system contains an expansion bus that allows the microprocessor to communicate with controllers for all the various peripheral devices connected to the system. Your system also contains an address bus and a data bus for communications between the microprocessor and RAM.

byte

Eight contiguous bits of information, the basic data unit used by your system.

C

Abbreviation for Celsius.

CA

Abbreviation for certification authority.

cache

A fast storage area that keeps a copy of data or instructions for quicker data retrieval. For example, your system's BIOS may cache ROM code in faster RAM. Or, a disk-cache utility may reserve RAM in which to store frequently accessed information from your system's disk drives; when a program makes a request to a disk drive for data that is in the cache, the disk-cache utility can retrieve the data from RAM faster than from the disk drive.

capability

Refers to the actions that an object can perform, or actions that can be taken on a managed object. For example, if a card is hot-pluggable, it is capable of being replaced while the system power is on.

CDRAM

Abbreviation for cached DRAM, which is a high-speed DRAM memory chip developed by Mitsubishi that includes a small SRAM cache.

CD-ROM

Abbreviation for compact disc read-only memory. CD drives use optical technology to read data from CDs. CDs are read-only storage devices; you cannot write new data to a CD with standard CD drives.

CHAP

Acronym for Challenge-Handshake Authentication Protocol, an authentication scheme used by PPP servers to validate the identity of the originator of the connection upon connection or any time later.

chip

A set of microminiaturized, electronic circuits that are designed for use as processors and memory in systems. Small chips can hold from a handful to tens of thousands of transistors. They look like tiny chips of aluminum, no more than 1/16 inch square by 1/30 inch thick, which is where the term "chip" came from. Large chips, which can be more than a half inch square, hold millions of transistors. It is actually only the top one thousandth of an inch of a chip's surface that holds the circuits. The rest of it is just a base.

CIM

Acronym for Common Information Model, which is a model for describing management information from the DMTF. CIM is implementation independent, allowing different management applications to collect the required data from a variety of sources. CIM includes schemas for systems, networks, applications and devices, and new schemas will be added. It provides mapping techniques for interchange of CIM data with MIB data from SNMP agents.

CIMOM

Acronym for common information model object manager.

CI/O

Abbreviation for comprehensive input/output.

CLI

Abbreviation for command line interface.

cm

Abbreviation for centimeter(s).

CMOS

Acronym for complementary metal-oxide semiconductor. In systems, CMOS memory chips are often used for NVRAM storage.

COM n

The device names for the first through fourth serial ports on your system are COM1, COM2, COM3, and COM4. The default interrupt for COM1 and COM3 is IRQ4, and the default interrupt for COM2 and COM4 is IRQ3. Therefore, you must be careful when configuring software that runs a serial device so that you don't create an interrupt conflict.

config.sys file

The **config.sys** file is executed when you boot your system (before running any commands in the **autoexec.bat** file). This start-up file contains commands that specify which devices to install and which drivers to use. This file also contains commands

that determine how the operating system uses memory and controls files.

ConsoleOne

Novell ConsoleOne is a Java-based foundation for graphical utilities that manage and administer network resources from different locations and platforms. ConsoleOne provides a single point of control for all Novell and external products.

controller

A chip that controls the transfer of data between the microprocessor and memory or between the microprocessor and a peripheral device such as a disk drive or the keyboard.

control panel

The part of the system that contains indicators and controls, such as the power switch, hard drive access indicator, and power indicator.

conventional memory

The first 640 KB of RAM. Conventional memory is found in all systems. Unless they are specially designed, MS-DOS[®] programs are limited to running in conventional memory.

COO

Abbreviation for cost of ownership.

cooling unit

Sets of fans or other cooling devices in a system chassis.

coprocessor

A chip that relieves the system's microprocessor of specific processing tasks. A math coprocessor, for example, handles numeric processing. A graphics coprocessor handles video rendering. The Intel[®] Pentium[®] microprocessor, for example, includes a built-in math coprocessor.

cpi

Abbreviation for characters per inch.

CPU

Abbreviation for central processing unit. See also microprocessor.

CRC

Abbreviation for cyclic redundancy code, which is a number derived from, and stored or transmitted with, a block of data in order to detect corruption. By recalculating the CRC and comparing it to the value originally transmitted, the receiver can detect some types of transmission errors.

CSR

Abbreviation for certificate signing request.

cursor

A marker, such as a block, underscore, or pointer that represents the position at which the next keyboard or mouse action will occur.

DAT

Acronym for digital audio tape.

dB

Abbreviation for decibel(s).

dBa

Abbreviation for adjusted decibel(s).

DC

Abbreviation for direct current.

Also, abbreviation for Dual Channel.

device driver

A program that allows the operating system or some other program to interface correctly with a peripheral device, such as a printer. Some device drivers—such as network drivers—must be loaded from the config.sys file (with a device= statement) or as memory-resident programs (usually, from the autoexec.bat file). Others—such as video drivers—must load when you start the program for which they were designed.

DHCP

Abbreviation for Dynamic Host Configuration Protocol, a protocol that provides a means to dynamically allocate IP addresses to computers on a LAN.

DIMM

Acronym for dual in-line memory module. A small circuit board containing DRAM chips that connects to the system board.

DIN

Acronym for Deutsche Industrie Norm which is the standards-setting organization for Germany. A DIN connector is a connector that conforms to one of the many standards defined by DIN. DIN connectors are used widely in personal computers. For example, the keyboard connector for personal computers is a DIN connector.

DIP

Acronym for dual in-line package. A circuit board, such as a system board or expansion card, may contain DIP switches for configuring the circuit board. DIP switches are always toggle switches, with an on position and an off position.

directory

Directories help keep related files organized on a disk in a hierarchical, "inverted tree" structure. Each disk has a "root" directory; for example, a `C:\>` prompt normally indicates that you are at the root directory of hard drive C. Additional directories that branch off of the root directory are called subdirectories. Subdirectories may contain additional directories branching off of them.

display adapter

See video adapter.

DKS

Abbreviation for dynamic kernel support.

DMA

Abbreviation for direct memory access. A DMA channel allows certain types of data transfer between RAM and a device to bypass the microprocessor.

DMTF

Abbreviation for Distributed Management Task Force, a consortium of companies representing hardware and software providers.

dpi

Abbreviation for dots per inch.

DPMS

Abbreviation for Display Power Management Signaling. A standard developed by the Video Electronics Standards Association (VESA[®]) that defines the hardware signals sent by a video controller to activate power management states in a monitor. A monitor is said to be DPMS-compliant when it is designed to enter a power management state after receiving the appropriate signal from a system's video controller.

DRAC 4

Acronym for Dell™ Remote Access Card 4.

DRAC II

Acronym for Dell OpenManage™ Remote Assistant Card II.

DRAC III

Acronym for Dell Remote Access Card III.

DRAC III/XT

Acronym for Dell Remote Access Card III/XT.

DRAM

Acronym for dynamic random-access memory. A system's RAM is usually made up entirely of DRAM chips. Because DRAM chips cannot store an electrical charge indefinitely, your system continually refreshes each DRAM chip in the system.

drive-type number

Your system can recognize a number of specific hard drives. Each is assigned a drive-type number that is stored in NVRAM. The hard drive(s) specified in your system's System Setup program must match the actual drive(s) installed in the system. The System Setup program also allows you to specify physical parameters (logical cylinders, logical heads, cylinder number, and logical sectors per pack) for drives not included in the table of drive types stored in NVRAM.

DTE

Abbreviation for data terminal equipment. Any device, such as a computer system, that can send data in digital form by means of a cable or communications line. The DTE is connected to the cable or communications line through a data communications equipment (DCE) device, such as a modem.

ECC

Abbreviation for error checking and correction.

ECP

Abbreviation for Extended Capabilities Port.

EDO

Acronym for extended data output dynamic random access memory which is a type of DRAM that is faster than conventional DRAM. EDO RAM can start fetching the next block of memory at the same time that it sends the previous block to the microprocessor.

EEPROM

Acronym for electrically erasable programmable read-only memory.

EIDE

Abbreviation for enhanced integrated drive electronics. EIDE devices add one or more of the following enhancements to the traditional IDE standard:

- Data transfer rates of up to 16 MB/sec
- Support for drives other than just hard drives, such as CD and tape drives

- Support for hard drives with capacities greater than 528 MB
- Support for up to two controllers, each with up to two devices attached

EISA

Acronym for Extended Industry-Standard Architecture, a 32-bit expansion-bus design. The expansion-card connectors in an EISA system are also compatible with 8- or 16-bit ISA expansion cards.

To avoid a configuration conflict when installing an EISA expansion card, you must use the EISA Configuration Utility. This utility allows you to specify which expansion slot contains the card and obtains information about the card's required system resources from a corresponding EISA configuration file.

EMC

Abbreviation for electromagnetic compatibility.

EMI

Abbreviation for electromagnetic interference.

EMM

Abbreviation for expanded memory manager. A utility that uses extended memory to emulate expanded memory on systems with an Intel386™ or higher microprocessor.

EMS

Abbreviation for Expanded Memory Specification.

EPP

Abbreviation for Enhanced Parallel Port which provides improved bidirectional data transmission. Many devices are designed to take advantage of the EPP standard, especially devices, such as network or SCSI adapters that connect to the parallel port of a portable computer.

EPROM

Acronym for erasable programmable read-only memory.

ERA

Abbreviation for embedded remote access.

ERA/MC

Abbreviation for embedded remote access modular computer. See modular system.

ERA/O

Abbreviation for embedded remote access option.

ESD

Abbreviation for electrostatic discharge.

ESM

Abbreviation for embedded systems management.

expanded memory

A technique for accessing RAM above 1 MB. To enable expanded memory on your system, you must use an EMM. You should configure your system to support expanded memory only if you run application programs that can use (or require) expanded memory.

expansion bus

Your system contains an expansion bus that allows the microprocessor to communicate with controllers for peripheral devices, such as a network card or an internal modem.

expansion-card connector

A connector on the system's system board or riser board for plugging in an expansion card.

extended memory

RAM above 1 MB. Most software that can use it, such as the Windows operating system, requires that extended memory be under the control of an XMM.

external cache memory

A RAM cache using SRAM chips. Because SRAM chips operate at several times the speed of DRAM chips, the microprocessor can retrieve data and instructions faster from external cache memory than from RAM.

F

Abbreviation for Fahrenheit.

FAT

Acronym for file allocation table. FAT and FAT32 are file systems that are defined as follows:

- **FAT** — A file system used by MS-DOS, Windows 3.x, Windows 95, and Windows 98. Windows NT® and Windows 2000 also can use the FAT file system. The operating system maintains a table to keep track of the status of various segments of disk space used for file storage.
- **FAT32** — A derivative of the FAT file system. FAT32 supports smaller cluster sizes than FAT, thus providing more efficient space allocation on FAT32 drives.

FCC

Abbreviation for Federal Communications Commission.

FEEPROM

Acronym for flash erasable programmable read-only memory. Flash memory is a kind of nonvolatile storage device similar to EEPROM, but the erasing is done only in blocks or the entire chip.

Fibre Channel

A data transfer interface technology that allows for high-speed I/O and networking functionality in a single connectivity technology. The Fibre Channel Standard supports several topologies, including Fibre Channel Point-to-Point, Fibre Channel Fabric (generic switching topology), and Fibre Channel Arbitrated Loop (FC_AL).

firmware

Software (programs or data) that has been written onto read-only memory (ROM). Firmware can boot and operate a device. Each controller contains firmware which helps provide the controller's functionality.

flash bios

A BIOS that is stored in flash memory rather than in ROM. A flash BIOS chip can be updated in place, whereas a ROM BIOS must be replaced with a newer chip.

flash memory

A type of EEPROM chip that can be reprogrammed from a utility on diskette while still installed in a system; most EEPROM chips can only be rewritten with special programming equipment.

format

To prepare a hard drive or diskette for storing files. An unconditional format deletes all data stored on the disk.

FPBGA

Abbreviation for field programmable gate array, a programmable logic chip (PLD) with a high density of gates.

FRU

Abbreviation for field replaceable unit.

ft

Abbreviation for feet.

FTP

Abbreviation for file transfer protocol.

g

Abbreviation for gram(s).

G

Abbreviation for gravities.

GB

Abbreviation for gigabyte(s). A gigabyte equals 1024 megabytes or 1,073,741,824 bytes.

gcc

Abbreviation for gnu C compiler.

graphics coprocessor

See coprocessor.

graphics mode

A video mode that can be defined as x horizontal by y vertical pixels by z colors.

GUI

Acronym for graphical user interface.

h

Abbreviation for hexadecimal. A base-16 numbering system, often used in programming to identify addresses in the system's RAM and I/O memory addresses for devices. The sequence of decimal numbers from 0 through 16, for example, is expressed in hexadecimal notation as: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 10. In text, hexadecimal numbers are often followed by h.

HBA

Abbreviation for host bus adapter. A PCI adapter card that resides in the system whose only function is to convert data commands from PCI-bus format to storage interconnect format (examples: SCSI, Fibre Channel) and communicate directly with hard drives, tape drives, CD drives, or other storage devices.

heat sink

A metal plate with metal pegs or ribs that help dissipate heat. Most microprocessors include a heat sink.

HMA

Abbreviation for high memory area. The first 64 KB of extended memory above 1 MB. A memory manager that conforms to the XMS can make the HMA a direct extension of conventional memory. Also see XMM.

host adapter

A host adapter implements communication between the system's bus and the controller for a peripheral device. (hard drive controller subsystems include integrated host adapter circuitry.) To add a SCSI

expansion bus to your system, you must install or connect the appropriate host adapter.

hot plug

The ability to remove and replace a redundant part while the system is still running. Also called a "hot spare."

HPFS

Abbreviation for the High Performance File System option in the Windows NT operating systems.

HTTP

Abbreviation for Hypertext Transfer Protocol. HTTP is the client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents.

HTTPS

Abbreviation for HyperText Transmission Protocol, Secure. HTTPS is a variant of HTTP used by Web browsers for handling secure transactions. HTTPS is a unique protocol that is simply SSL underneath HTTP. You need to use "https://" for HTTP URLs with SSL, whereas you continue to use "http://" for HTTP URLs without SSL.

Hz

Abbreviation for hertz.

ICES

Abbreviation for Interface-Causing Equipment Standard (in Canada).

ICMP

Abbreviation for Internet Control Message Protocol. ICMP is a TCP/IP protocol used to send error and control messages.

ICU

Abbreviation for ISA Configuration Utility.

ID

Abbreviation for identification.

IDE

Abbreviation for Integrated Drive Electronics. IDE is a computer system interface, used primarily for hard drives and CDs.

I/O

Abbreviation for input/output. The keyboard is an input device, and a printer is an output device. In general, I/O activity can be differentiated from computational activity. For example, when a program sends a document to the printer, it is engaging in output activity; when the program sorts a list of terms, it is engaging in computational activity.

IHV

Abbreviation for independent hardware vendor. IHVs often develop their own MIBs for components that they manufacture.

interlacing

A technique for increasing video resolution by only updating alternate horizontal lines on the screen. Because interlacing can result in noticeable screen flicker, most users prefer noninterlaced video adapter resolutions.

internal microprocessor cache

An instruction and data cache built in to the microprocessor. The Intel Pentium microprocessor includes a 16-KB internal cache, which is set up as an 8-KB read-only instruction cache and an 8-KB read/write data cache.

IP address

Abbreviation for Internet Protocol address. See TCP/IP.

IPMI

Abbreviation for Intelligent Platform Management Interface, which is an industry standard for management of peripherals used in enterprise computers based on Intel architecture. The key characteristic of IPMI is that inventory, monitoring, logging, and recovery control functions are available

independent of the main processors, BIOS, and operating system.

IPX

Abbreviation for internetwork packet exchange.

IRQ

Abbreviation for interrupt request. A signal that data is about to be sent to or received by a peripheral device travels by an IRQ line to the microprocessor. Each peripheral connection must be assigned an IRQ number. For example, the first serial port in your system (COM1) is assigned to IRQ4 by default. Two devices can share the same IRQ assignment, but you cannot operate both devices simultaneously.

ISA

Acronym for Industry-Standard Architecture. A 16-bit expansion bus design. The expansion-card connectors in an ISA system are also compatible with 8-bit ISA expansion cards.

ISV

Abbreviation for independent software vendor.

ITE

Abbreviation for information technology equipment.

Java

A cross-platform programming language developed by Sun Microsystems.

JSSE

Abbreviation for Java Secure Socket Extension.

jumper

Jumpers are small blocks on a circuit board with two or more pins emerging from them. Plastic plugs containing a wire fit down over the pins. The wire connects the pins and creates a circuit. Jumpers provide a simple and reversible method of changing the circuitry in a printed circuit board.

K

Abbreviation for kilo-, indicating 1000.

KB

Abbreviation for kilobyte(s), 1024 bytes.

KB/sec

Abbreviation for kilobyte(s) per second.

Kbit(s)

Abbreviation for kilobit(s), 1024 bits.

Kbit(s)/sec

Abbreviation for kilobit(s) per second.

key combination

A command requiring you to press multiple keys at the same time. For example, you can reboot your system by pressing the <Ctrl> <Alt> key combination.

kg

Abbreviation for kilogram(s), 1000 grams.

kHz

Abbreviation for kilohertz, 1000 hertz.

LAN

Acronym for local area network. A LAN system is usually confined to the same building or a few nearby buildings, with all equipment linked by wiring dedicated specifically to the LAN.

lb

Abbreviation for pound(s).

LCC

Abbreviation for leaded or leadless chip carrier.

LIF

Acronym for low insertion force. Some systems use LIF sockets and connectors to allow devices, such as the microprocessor chip, to be installed or removed with minimal stress to the device.

LED

Abbreviation for light-emitting diode. An electronic device that lights up when a current is passed through it.

local bus

On a system with local-bus expansion capability, certain peripheral devices (such as the video adapter circuitry) can be designed to run much faster than they would with a traditional expansion bus. Some local-bus designs allow peripherals to run at the same speed and with the same width data path as the system's microprocessor.

LPT*n*

The device names for the first through third parallel printer ports on your system are LPT1, LPT2, and LPT3.

LRA

Abbreviation for local response agent.

m

Abbreviation for meter(s).

mA

Abbreviation for milliamperes(s).

mAh

Abbreviation for milliamperes-hour(s).

managed system

A managed system is any system that is monitored and managed using Server Administrator. Systems running Server Administrator can be managed locally or remotely through a supported Web browser. See remote management system.

math coprocessor

See coprocessor.

Mb

Abbreviation for megabit.

MB

Abbreviation for megabyte(s). The term megabyte means 1,048,576 bytes; however, when referring to hard drive storage, the term is often rounded to mean 1,000,000 bytes.

MB/sec

Abbreviation for megabytes per second.

Mbps

Abbreviation for megabits per second.

MBR

Abbreviation for master boot record.

MCA

Abbreviation for Micro Channel Architecture, which is designed for multiprocessing. MCA eliminates potential conflicts that arise when installing new peripheral devices. MCA is not compatible with either EISA or XT bus architecture, so older cards cannot be used with it.

memory

A system can contain several different forms of memory, such as RAM, ROM, and video memory. Frequently, the word memory is used as a synonym for RAM; for example, an unqualified statement such as "a system with 16 MB of memory" refers to a system with 16 MB of RAM.

memory address

A specific location, usually expressed as a hexadecimal number, in the system's RAM.

memory manager

A utility that controls the implementation of memory in addition to conventional memory, such as extended or expanded memory.

memory module

A small circuit board containing DRAM chips that connects to the system board.

MHz

Abbreviation for megahertz.

MIB

Acronym for management information base. The MIB is used to send detailed status/commands from or to an SNMP managed device.

microprocessor

The primary computational chip inside the system that controls the interpretation and execution of arithmetic and logic functions. Software written for one microprocessor must usually be revised to run on another microprocessor. CPU is a synonym for microprocessor.

MIDI

Acronym for musical instrument digital interface.

mm

Abbreviation for millimeter(s).

modem

A device that allows your system to communicate with other systems over telephone lines.

modular system

A system that can include multiple server modules. Each server module functions as an individual system. To function as a system, a server module is inserted into a chassis which includes power supplies, fans, a system management module, and at least one network switch module. The power supplies, fans, system management module, and network switch module are shared resources of the server modules in the chassis. See server module.

MOF

Acronym for managed object format, which is an ASCII file that contains the formal definition of a CIM schema.

mouse

A pointing device that controls the movement of the cursor on a screen. Mouse-aware software allows you to activate commands by clicking a mouse button while pointing at objects displayed on the screen.

MPEG

Acronym for Motion Picture Experts Group. MPEG is a digital video file format.

ms

Abbreviation for millisecond(s).

MS-DOS

Acronym for Microsoft Disk Operating System.

MTBF

Abbreviation for mean time between failures.

multifrequency monitor

A monitor that supports several video standards. A multifrequency monitor can adjust to the frequency range of the signal from a variety of video adapters.

mV

Abbreviation for millivolt(s).

name

The name of an object or variable is the exact string that identifies it in an SNMP Management Information Base (MIB) file or in a CIM Management Object File (MOF).

NDIS

Abbreviation for Network Driver Interface Specification.

NDS

Abbreviation for NetWare® Directory Structure.

NIC

Acronym for network interface controller.

NICI

Abbreviation for NetWare International Cryptographic Infrastructure.

NIF

Acronym for network interface function. This term is equivalent to NIC.

NLM

Abbreviation for NetWare Loadable Module.

NMI

Abbreviation for nonmaskable interrupt. A device sends an NMI to signal the microprocessor about hardware errors, such as a parity error.

noninterlaced

A technique for decreasing screen flicker by sequentially refreshing each horizontal line on the screen.

ns

Abbreviation for nanosecond(s), one billionth of a second.

NTFS

Abbreviation for the Windows NT File System option in the Windows NT operating system. NTFS is an advanced file system designed for use specifically within the Windows NT operating system. It supports file system recovery, extremely large storage media, and long file names. It also supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes. See also FAT and FAT32.

NTLM

Abbreviation for Windows NT LAN Manager. NTLM is the security protocol for the Windows NT operating system.

NuBus

Proprietary expansion bus used on Apple Macintosh personal computers.

NVRAM

Acronym for nonvolatile random-access memory. Memory that does not lose its contents when you turn off your system. NVRAM is used for maintaining the date, time, and system configuration information.

OID

Abbreviation for object identifier. An implementation-specific integer or pointer that uniquely identifies an object.

online access service

A service that typically provides access to the Internet, e-mail, bulletin boards, chat rooms, and file libraries.

OTP

Abbreviation for one-time programmable.

PAM

Acronym for Pluggable Authentication Modules. PAM allows system administrators to set an authentication policy without having to recompile authentication programs.

parallel port

An I/O port used most often to connect a parallel printer to your system. You can usually identify a parallel port on your system by its 25-hole connector.

parameter

A value or option that you specify to a program. A parameter is sometimes called a switch or an argument.

partition

You can divide a hard drive into multiple physical sections called partitions with the fdisk command. Each partition can contain multiple logical drives. After partitioning the hard drive, you must format each logical drive with the format command.

PC card

A credit-card sized, removable module for portable computers standardized by PCMCIA. PC Cards are also known as "PCMCIA cards." PC Cards are 16-bit

devices that are used to attach modems, network adapters, sound cards, radio transceivers, solid state disks and hard disks to a portable computer. The PC Card is a "plug and play" device, which is configured automatically by the Card Services software.

PCI

Abbreviation for Peripheral Component Interconnect. The predominant 32-bit or 64-bit local-bus standard developed by Intel Corporation.

PCMCIA

Personal Computer Memory Card International Association. An international trade association that has developed standards for devices, such as modems and external hard drives, that can be plugged into portable computers.

PERC

Acronym for Expandable RAID controller.

peripheral device

An internal or external device—such as a printer, a disk drive, or a keyboard—connected to a system.

PGA

Abbreviation for pin grid array, a type of microprocessor socket that allows you to remove the microprocessor chip.

physical memory array

The physical memory array is the entire physical memory of a system. Variables for physical memory array include maximum size, total number of memory slots on the motherboard, and total number of slots in use.

physical memory array mapped

The physical memory array mapped refers to the way physical memory is divided.

For example, one mapped area may have 640 KB and the other mapped area may have between 1 MB and 127 MB.

PIC

Acronym for programmable interrupt controller.

PIP

Acronym for peripheral interchange program.

pixel

A single point on a video display. Pixels are arranged in rows and columns to create an image. A video resolution, such as 640 x 480, is expressed as the number of pixels across by the number of pixels up and down.

PKCS #7

Abbreviation for Public Key Cryptography Standard #7. PKCS #7 is an RSA Data Security, Inc., standard for encapsulating signed data such as a certificate chain.

PKIS

Abbreviation for Novell Public Key Infrastructure Services.

PLCC

Abbreviation for plastic leaded chip carrier.

Plug and Play

An industry-standard specification that makes it easier to add hardware devices to personal computers. Plug and Play provides automatic installation and configuration, compatibility with existing hardware, and dynamic support of mobile computing environments.

PME

Abbreviation for Power Management Event. A PME is a pin on a peripheral component interconnect that allows a PCI device to assert a wake event.

POST

Acronym for power-on self-test. Before the operating system loads when you turn on your system, the POST tests various system components such as RAM, the disk drives, and the keyboard.

power supply

An electrical system that converts AC current from the wall outlet into the DC currents required by the system circuitry. The power supply in a personal computer typically generates multiple voltages.

power unit

A set of power supplies in a system chassis.

ppm

Abbreviation for pages per minute.

PPP

Abbreviation for Point-to-Point Protocol.

PQFP

Abbreviation for plastic quad flat pack, a type of microprocessor socket in which the microprocessor chip is permanently mounted.

program diskette set

The set of diskettes from which you can perform a complete installation of an operating system or application program. When you reconfigure a program, you often need its program diskette set.

protected mode

An operating mode supported by 80286 or higher microprocessors, protected mode allows operating systems to implement:

- A memory address space of 16 MB (80286 microprocessor) to 4 GB (Intel386 or higher microprocessor)
- Multitasking
- Virtual memory, a method for increasing addressable memory by using the hard drive

The Windows NT, OS/2[®], and UNIX[®] 32-bit operating systems run in protected mode. MS-DOS cannot run in protected mode; however, some programs that you can start from MS-DOS, such as the Windows operating system, are able to put the system into protected mode.

provider

A provider is an extension of a CIM schema that communicates with managed objects and accesses data and event notifications from a variety of sources. Providers forward this information to the CIM Object Manager for integration and interpretation.

PS

Abbreviation for power supply.

PS/2

Abbreviation for Personal System/2.

PXE

Abbreviation for Pre-boot eXecution Environment.

QFP

Abbreviation for quad flat pack.

RAC

Acronym for remote access controller.

RAID

Acronym for redundant array of independent drives.

RAM

Acronym for random-access memory. A system's primary temporary storage area for program instructions and data. Each location in RAM is identified by a number called a memory address. Any information stored in RAM is lost when you turn off your system.

RAMDAC

Acronym for random-access memory digital-to-analog converter.

RAW

Unprocessed. The term refers to data that is passed along to an I/O device without being interpreted. In contrast, cooked refers to data that is processed before being passed to the I/O device. It often refers to uncompressed text that is not stored in any proprietary

format. The term comes from UNIX, which supports cooked and raw modes for data output to a terminal.

RBAC

Abbreviation for role-based access control.

RDRAM

Acronym for Rambus DRAM. A dynamic RAM chip technology from Rambus, Inc. Direct RDRAMs are used in systems. Direct RDRAM chips are housed in RIMM modules, which are similar to DIMMs but have different pin settings. The chips can be built with dual channels, doubling the transfer rate to 3.2 GB/sec.

read-only file

A read-only file is one that you are prohibited from editing or deleting. A file can have read-only status if:

- Its read-only attribute is enabled.
- It resides on a physically write-protected diskette or on a diskette in a write-protected drive.
- It is located on a network in a directory to which the system administrator has assigned read-only rights to you.

readme file

A text file included with a software package or hardware product that contains information supplementing or updating the documentation for the software or hardware. Typically, readme files provide installation information, describe new product enhancements or corrections that have not yet been documented, and list known problems or other things you need to be aware of as you use the software or hardware.

real mode

An operating mode supported by 80286 or higher microprocessors, real mode imitates the architecture of an 8086 microprocessor.

refresh rate

The rate at which the monitor redraws the video image on the monitor screen. More precisely, the refresh rate is the frequency, measured in Hz, at which the screen's horizontal lines are recharged (sometimes also referred

to as its vertical frequency). The higher the refresh rate, the less video flicker can be seen by the human eye. The higher refresh rates are also noninterlaced.

remote management system

A remote management system is any system that accesses the Server Administrator home page on a managed system from a remote location using a supported Web browser. See managed system.

RFI

Abbreviation for radio frequency interference.

RGB

Abbreviation for red/green/blue.

RIMM

Acronym for Rambus In-line Memory Module, which is the Rambus equivalent of a DIMM module.

RMI

Acronym for Remote Method Invocation. RMI is a part of the Java programming language library that enables a Java program running on one system to access the objects and methods of another Java program running on a different system.

ROM

Acronym for read-only memory. Your system contains some programs essential to its operation in ROM code. Unlike RAM, a ROM chip retains its contents even after you turn off your system. Examples of code in ROM include the program that initiates your system's boot routine and the POST.

rpm

Abbreviation for revolutions per minute.

RPM

Abbreviation for Red Hat® Package Manager.

RTC

Abbreviation for real-time clock. Battery-powered clock circuitry inside the system that keeps the date and time after you turn off the system.

SAN

Acronym for storage area network.

SAS

Acronym for Secure Authentication Services.

SCA

Abbreviation for single connector attachment.

schema

A collection of class definitions that describes managed objects in a particular environment. A schema is a collection of class definitions used to represent managed objects that are common to every management environment, which is why CIM is called the Common Information Model.

SCSI

Acronym for small computer system interface. An I/O bus interface with faster data transmission rates than standard ports. You can connect up to seven devices (15 for some newer SCSI types) to one SCSI interface.

SEL

Acronym for system event log.

SDMS

Abbreviation for SCSI device management system.

sec

Abbreviation for second(s).

SEC

Abbreviation for single-edge contact.

secure port server

An application that makes Web pages available for viewing by Web browsers using the HTTPS protocol. See Web server.

serial port

An I/O port used most often to connect a modem to your system. You can usually identify a serial port on your system by its 9-pin connector.

settings

Settings are conditions of a manageable object help to determine what happens when a certain value is detected in a component. For example, a user can set the upper critical threshold of a temperature probe to 75 degrees Celsius. If the probe reaches that temperature, the setting results in an alert being sent to the management system so that user intervention can be taken. Some settings, when reached, can trigger a system shutdown or other response that can prevent damage to the system.

server module

A modular system component that functions as an individual system. To function as a system, a server module is inserted into a chassis which includes power supplies, fans, a system management module, and at least one network switch module. The power supplies, fans, system management module, and network switch module are shared resources of the server modules in the chassis. See modular system.

service tag number

A bar code label that identifies each system in the event that you need to call for customer or technical support.

SGRAM

Acronym for synchronous graphics RAM.

shadowing

A computer's system and video BIOS code is usually stored on ROM chips. Shadowing refers to the performance-enhancement technique that copies BIOS code to faster RAM chips in the upper memory area (above 640 KB) during the boot routine.

SIMD

Abbreviation for Single Instruction Multiple Data.

SIMM

Acronym for single in-line memory module. A small circuit board containing DRAM chips that connects to the system board.

SIP

Acronym for single in-line package, which is a type of housing for electronic components in which the connecting pins protrude from one side. A SIP is also called a Single In-line Pin Package (SIPP).

SKU

Acronym for stock keeping unit.

SMART

Acronym for Self-Monitoring Analysis and Reporting Technology. A technology that allows hard drives to report errors and failures to the system BIOS, which then displays an error message on the screen. To take advantage of this technology, you must have a SMART-compliant hard drive and the proper support in the system BIOS.

SMBIOS

Acronym for system management BIOS.

SMD

Abbreviation for surface mount device.

SMTP

Abbreviation for Simple Mail Transfer Protocol.

SNMP

Abbreviation for Simple Network Management Protocol. SNMP, a popular network control and monitoring protocol, is part of the original TCP/IP protocol suite. SNMP provides the format in which vital information about different network devices, such as network servers or routers, can be sent to a management application.

SODIMM

Acronym for small outline-DIMM. A DIMM module with a thinner profile due to the use of TSOP chip

packages. SODIMMs are commonly used in portable computers.

SOIC

Abbreviation for Small Outline IC, a small-dimension, plastic, rectangular, surface mount chip package that uses gull-wing pins extending outward.

SOJ

Abbreviation for small outline package J-lead, a small-dimension, plastic, rectangular surface mount chip package with j-shaped pins on its two long sides.

SRAM

Abbreviation for static random-access memory. Because SRAM chips do not require continual refreshing, they are substantially faster than DRAM chips.

SSL

Abbreviation for secure socket layer.

state

Refers to the condition of an object that can have more than one condition. For example, an object may be in the "not ready" state.

status

Refers to the health or functioning of an object. For example, a temperature probe can have the status normal if the probe is measuring acceptable temperatures. When the probe begins reading temperatures that exceed limits set by the user, it reports a critical status.

SVGA

Abbreviation for super video graphics array. VGA and SVGA are video standards for video adapters with greater resolution and color display capabilities than previous standards.

To display a program at a specific resolution, you must install the appropriate video drivers and your monitor must support the resolution. Similarly, the number of colors that a program can display depends on the

capabilities of the monitor, the video driver, and the amount of video memory installed in the system.

switch

On a system board, switches control various circuits or functions in your computer system. These switches are known as DIP switches; they are normally packaged in groups of two or more switches in a plastic case. Two common DIP switches are used on system boards: slide switches and rocker switches. The names of the switches are based on how the settings (on and off) of the switches are changed.

syntax

The rules that dictate how you must type a command or instruction so that the system understands it. A variable's syntax indicates its data type.

system board

As the main circuit board, the system board usually contains most of your system's integral components, such as the following:

- Microprocessor
- RAM
- Controllers for standard peripheral devices, such as the keyboard
- Various ROM chips

Frequently used synonyms for system board are motherboard and logic board.

system configuration information

Data stored in memory that tells a system what hardware is installed and how the system should be configured for operation.

system diskette

System diskette is a synonym for bootable diskette.

system memory

System memory is a synonym for RAM.

System Setup program

A BIOS-based program that allows you to configure your system's hardware and customize the system's operation by setting such features as password protection and energy management. Some options in the System Setup program require that you reboot the system (or the system may reboot automatically) in order to make a hardware configuration change. Because the System Setup program is stored in NVRAM, any settings remain in effect until you change them again.

system.ini file

A start-up file for the Windows operating system. When you start Windows, it consults the **system.ini** file to determine a variety of options for the Windows operating environment. Among other things, the **system.ini** file records which video, mouse, and keyboard drivers are installed for Windows.

Running the Control Panel or Windows Setup program may change options in the **system.ini** file. On other occasions, you may need to change or add options to the **system.ini** file manually with a text editor, such as Notepad.

table

In SNMP MIBs, a table is a two dimensional array that describes the variables that make up a managed object.

TCP/IP

Abbreviation for Transmission Control Protocol/Internet Protocol. A system for transferring information over a computer network containing dissimilar systems, such as systems running Windows and UNIX.

termination

Some devices (such as the last device at each end of a SCSI cable) must be terminated to prevent reflections and spurious signals in the cable. When such devices are connected in a series, you may need to enable or disable the termination on these devices by changing jumper or switch settings on the devices or by changing settings in the configuration software for the devices.

text editor

An application program for editing text files consisting exclusively of ASCII characters. Windows Notepad is a text editor, for example. Most word processors use proprietary file formats containing binary characters, although some can read and write text files.

TFTP

Abbreviation for Trivial File Transfer Protocol. TFTP is a version of the TCP/IP FTP protocol that has no directory or password capability.

text mode

A video mode that can be defined as x columns by y rows of characters.

threshold values

Systems are normally equipped with various sensors that monitor temperature, voltage, current, and fan speed. The sensor's threshold values specify the ranges (min and max values) for determining whether the sensor is operating under normal, noncritical, critical or fatal conditions. Server Administrator-supported threshold values are

- UpperThresholdFatal
- UpperThresholdCritical
- UpperThresholdNon-critical
- Normal
- LowerThresholdNon-critical
- LowerThresholdCritical
- LowerThresholdFatal

time-out

A specified period of system inactivity that must occur before an energy conservation feature is activated.

tpi

Abbreviation for tracks per inch.

TQFP

Abbreviation for thin quad flat pack.

TSR

Abbreviation for terminate-and-stay-resident. A TSR program runs "in the background." Most TSR programs implement a predefined key combination (sometimes referred to as a hot key) that allows you to activate the TSR program's interface while running another program. When you finish using the TSR program, you can return to the other application program and leave the TSR program resident in memory for later use. TSR programs can sometimes cause memory conflicts. When troubleshooting, rule out the possibility of such a conflict by rebooting your system without starting any TSR programs.

TSOP

Abbreviation for thin small outline package. A very thin, plastic, rectangular surface mount chip package with gull-wing pins on its two short sides.

UART

Acronym for universal asynchronous receiver transmitter, the electronic circuit that makes up the serial port.

UDP

Abbreviation for user datagram protocol.

UL

Abbreviation for Underwriters Laboratories.

UMB

Abbreviation for upper memory blocks.

unicode

A fixed width, 16-bit world wide character encoding, developed and maintained by the Unicode Consortium.

upper memory area

The 384 KB of RAM located between 640 KB and 1 MB. If the system has an Intel386 or higher microprocessor, a utility called a memory manager can create UMBs in the upper memory area, in which you can load device drivers and memory-resident programs.

UPS

Abbreviation for uninterruptible power supply. A battery-powered unit that automatically supplies power to your system in the event of an electrical failure.

URL

Abbreviation for Uniform Resource Locator (formerly Universal Resource Locator).

USB

Abbreviation for Universal Serial Bus. A USB connector provides a single connection point for multiple USB-compliant devices, such as mice, keyboards, printers, and computer speakers. USB devices can also be connected and disconnected while the system is running.

utility

A program used to manage system resources—memory, disk drives, or printers, for example.

utility partition

A bootable partition on the hard drive that provides utilities and diagnostics for your hardware and software. When activated, the partition boots and provides an executable environment for the partition's utilities.

UTP

Abbreviation for unshielded twisted pair.

UUID

Abbreviation for Universal Unique Identification.

V

Abbreviation for volt(s).

VAC

Abbreviation for volt(s) alternating current.

varbind

An algorithm used to assign an object identifier (OID). The varbind gives rules for arriving at the decimal prefix

that uniquely identifies an enterprise, as well as the formula for specifying a unique identifier for the objects defined in that enterprise's MIB.

variable

A component of a managed object. A temperature probe, for example, has a variable to describe its capabilities, its health or status, and certain indexes that you can use to help you in locating the right temperature probe.

VCCI

Abbreviation for Voluntary Control Council for Interference.

VDC

Abbreviation for volt(s) direct current.

VESA

Acronym for Video Electronics Standards Association.

VGA

Abbreviation for video graphics array. VGA and SVGA are video standards for video adapters with greater resolution and color display capabilities than previous standards. To display a program at a specific resolution, you must install the appropriate video drivers and your monitor must support the resolution. Similarly, the number of colors that a program can display depends on the capabilities of the monitor, the video driver, and the amount of video memory installed for the video adapter.

VGA feature connector

On some systems with a built-in VGA video adapter, a VGA feature connector allows you to add an enhancement adapter, such as a video accelerator, to your system. A VGA feature connector can also be called a VGA pass-through connector.

video adapter

The logical circuitry that provides—in combination with the monitor—your system's video capabilities. A video adapter may support more or fewer features than

a specific monitor offers. Typically, a video adapter comes with video drivers for displaying popular application programs and operating systems in a variety of video modes.

On some systems, a video adapter is integrated into the system board. Also available are many video adapter cards that plug into an expansion-card connector.

Video adapters often include memory separate from RAM on the system board. The amount of video memory, along with the adapter's video drivers, may affect the number of colors that can be simultaneously displayed. Video adapters can also include their own coprocessor for faster graphics rendering.

video driver

A program that allows graphics-mode application programs and operating systems to display at a chosen resolution with the desired number of colors. A software package may include some "generic" video drivers. Any additional video drivers may need to match the video adapter installed in the system.

video memory

Most VGA and SVGA video adapters include memory chips in addition to your system's RAM. The amount of video memory installed primarily influences the number of colors that a program can display (with the appropriate video drivers and monitor capabilities).

video mode

Video adapters normally support multiple text and graphics display modes. Character-based software displays in text modes that can be defined as x columns by y rows of characters. Graphics-based software displays in graphics modes that can be defined as x horizontal by y vertical pixels by z colors.

video resolution

Video resolution—800 x 600, for example—is expressed as the number of pixels across by the number of pixels up and down. To display a program at a specific graphics resolution, you must install the appropriate video drivers and your monitor must support the resolution.

virtual memory

A method for increasing addressable RAM by using the hard drive. For example, in a system with 16 MB of RAM and 16 MB of virtual memory set up on the hard drive, the operating system would manage the system as though it had 32 MB of physical RAM.

virus

A self-starting program designed to inconvenience you. Virus programs have been known to corrupt the files stored on a hard drive or to replicate themselves until a computer system or network runs out of memory. The most common way that virus programs move from one system to another is via "infected" diskettes, from which they copy themselves to the hard drive. To guard against virus programs, you should do the following:

- Periodically run a virus-checking utility on your system's hard drive
- Always run a virus-checking utility on any diskettes (including commercially sold software) before using them

VLSI

Abbreviation for very-large-scale integration.

VLVESA

Acronym for very low voltage enterprise system architecture.

vpp

Abbreviation for peak-point voltage.

VRAM

Acronym for video random-access memory. Some video adapters use VRAM chips (or a combination of VRAM and DRAM) to improve video performance. VRAM is dual-ported, allowing the video adapter to update the screen and receive new image data at the same time.

VRM

Abbreviation for voltage regulator module.

W

Abbreviation for watt(s).

Wakeup on LAN

The ability for the power in a client station to be turned on by the network. Remote wake-up enables software upgrading and other management tasks to be performed on users' machines after the work day is over. It also enables remote users to gain access to machines that have been turned off. Intel calls remote wake-up "Wake-on-LAN."

Web server

An application that makes Web pages available for viewing by Web browsers using the HTTP protocol.

WH

Abbreviation for watt-hour(s).

win.ini file

A start-up file for the Windows operating system. When you start Windows, it consults the **win.ini** file to determine a variety of options for the Windows operating environment. Among other things, the **win.ini** file records what printer(s) and fonts are installed for Windows. The **win.ini** file also usually includes sections that contain optional settings for Windows application programs that are installed on the hard drive. Running the Control Panel or Windows Setup program may change options in the **win.ini** file. On other occasions, you may need to change or add options to the **win.ini** file manually with a text editor such as Notepad.

Windows 95

An integrated and complete Microsoft Windows operating system that does not require MS-DOS and that provides advanced operating system performance, improved ease of use, enhanced workgroup functionality, and simplified file management and browsing.

Windows NT

High-performance server and workstation operating system software developed by Microsoft that is

intended for technical, engineering, and financial applications.

write-protected

Read-only files are said to be write-protected. You can write-protect a 3.5-inch diskette by sliding its write-protect tab to the open position or by setting the write-protect feature in the System Setup program.

WMI

Acronym for Windows Management Instrumentation. WMI provides CIM Object Manager services.

X.509 Certificate

An X.509 certificate binds a public encryption key to the identity or other attribute of its principal. Principals can be people, application code (such as a signed applet) or any other uniquely identified entity (such as a secure port server or Web server).

XMM

Abbreviation for extended memory manager, a utility that allows application programs and operating systems to use extended memory in accordance with the XMS.

XMS

Abbreviation for eXtended Memory Specification.

X Window System

The graphical user interface used in the Red Hat Enterprise Linux environment.

ZIF

Acronym for zero insertion force. Some systems use ZIF sockets and connectors to allow devices such as the microprocessor chip to be installed or removed with no stress applied to the device.

ZIP

A 3.5-inch removable disk drive from Iomega. Originally, it provided 100-MB removable cartridges. The drive is bundled with software that can catalog the disks and lock the files for security. A 250-MB version of the Zip drive also reads and writes the 100-MB Zip cartridges.

