Dell OpenManage™ Version 5.1 Installation and Security 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.

Frequently Asked Questions

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- General
- Microsoft® Windows®
- Red Hat® Enterprise Linux or SUSE® Linux Enterprise Server

General

Is the *Dell™ PowerEdge™ Installation and Server Management* CD a bootable CD?

Yes, the CD is bootable. It boots into the Dell OpenManage™ Server Assistant operating system setup mode by default. After installing managed system software, if an operating system was previously installed, you will be given the option to boot from the operating system. It is recommended that you eject the CD to avoid booting into Server Assistant setup mode.

Where can I find the quick installation instructions?

The *Quick Installation Guide* comes as a small brochure with the CD kit. Also, you can find the guide on the Dell Support website at **support.dell.com** and at the following location on the *Dell PowerEdge Installation and Server Management* CD:

\srvadmin\docs*language*\OpenManage_QIG\QUICK_INSTALL_GUIDE.htm

where **language** is the appropriate language directory for you.

How do I install Dell OpenManage Server Administrator with only the CLI features?

By choosing not to install the Server Administrator Web server, you will get CLI features only.

What ports do Dell OpenManage applications use?

The default port used by Server Administrator is 1311. The default ports used by Dell OpenManage IT Assistant are 2606 (for the connection service) and 2607 (for the network monitoring service). These ports are configurable. See Table 2-1 in this guide for additional details.

Microsoft® Windows®

How do I fix a faulty installation of Server Administrator?

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

- ⎯ Find out the version of Server Administrator that was previously installed.

- ⎯ Download the installation package for that version from the Dell Support website at **support.dell.com**.

- ⎯ Locate **SysMgmt.msi** from the **srvadmin\windows\SystemsManagement** directory and enter the following command at the command prompt to force a reinstall.

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

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

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

Once the application is installed, you can uninstall it from **Add/Remove Programs**.

How do I perform a silent (unattended) upgrade from Dell OpenManage 4.*x* (where *x* is >=3) to Dell OpenManage 5.1?

Use the following commands for a Management Station:

  ```
  msiexec /i MgmtSt.msi/qn (for fresh installs or major upgrades. For example, upgrading from Dell OpenManage version 4.3 to version 5.1.)
  ```

Use the following commands for a managed system:

  ```
  msiexec /i SysMgmt.msi/qn (for fresh installs or major upgrades. For example, upgrading from Dell OpenManage version 4.3 to version 5.1.)
  ```

  ```
  msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus /qn (for minor upgrades. For example, upgrading from Dell OpenManage version 5.0 to version 5.1.)
  ```

How do I prevent the system from rebooting after a silent (unattended) install/uninstall?

Use the optional command line switch:

  ```
  Reboot=ReallySuppress
  ```

Here is an example for the Management Station:

```
msiexec /i SysMgmt.msi /qb Reboot=ReallySuppress
```

What is an MSP service pack file? Should I upgrade my Dell OpenManage 4.3 version with the MSP file?

A Microsoft Service Pack (MSP) file stores only the differences between an old version and a new version. It is much smaller in size than the upgrade file. You can either use the MSP file or the new MSI file to upgrade your Dell OpenManage 4.3. Using the MSP file is a good idea as it is more efficient.

> **NOTE:** You can upgrade from Dell OpenManage software version 4.3 to 5.1 through a full MSI Installation only. You cannot upgrade using a MSP service pack file.

Where can I find the MSI log files?

By default, the MSI log files are stored in the path defined by the **%TEMP%** environment variable.

I downloaded the Server Administrator files for Windows from the Dell Support website and copied it to my own CD. When I tried to launch the SysMgmt.msi file, it failed. What is wrong?

MSI requires all installers to specify the **MEDIAPACKAGEPATH** property if the MSI file does not reside on the root of the CD.

This property is set to **\srvadmin\windows\SystemsManagement** for the managed system software MSI package. If you decide to make your own CD you must ensure that the CD layout stays the same. The **SysMgmt.msi** file must be located in the **\srvadmin\windows\SystemsManagement** directory on the CD. For more detailed information, go to **http://msdn.microsoft.com** and search for: MEDIAPACKAGEPATH Property.

I cannot upgrade from Dell OpenManage 4.2 to the latest version of Dell OpenManage without uninstalling and losing my managed system software settings. Is there a way to upgrade to the latest version while preserving my managed system software settings?

Yes, but you must upgrade from Dell OpenManage version 4.2 to 4.3 first, before upgrading to a later version of Dell OpenManage. If you are working with Windows Server™ 2003, do not apply Service Pack 1 until you have completed the Dell OpenManage upgrade.

How do I perform an unattended operating system installation with the *Installation and Server Management* CD?

You can install a Windows operating system on many systems using identical settings, which allows consistent configurations across all systems. To use this feature, it is necessary that the target Dell PowerEdge systems be configured identically, with the same hardware and operating system components. Any difference in configuration makes the replication feature unusable.

To perform unattended installations, do the following:

1. On the first system that is set up, ensure that the system's BIOS is set to boot from the CD. Insert the *Dell PowerEdge Installation and Server Management* CD and reboot your system. Follow the installation interview, which includes setting the date and time, configuring the RAID controllers, selecting the operating system and specifying its settings, configuring the hard drive, entering the network settings, and configuring Windows. If any information is omitted, an unattended installation can still be accomplished, but the system will prompt you for the missing information.

2. In the **Installation Summary** window, select **Save Unattended Installation Script at C:\unattended.txt, C:\txtsetup.oem** and select **Save Profile for Replication at C:\replication.** Click the **Continue** button.

3. Insert the appropriate operating system CD and follow the instructions to complete the installation. Reboot the system to complete the installation.

4. When the installation is completed on the first server, copy the files from the **C:\replication** directory to a diskette.

5. For each subsequent unattended installation, insert the disk containing the replication files into the diskette drive and boot the system. The installation interview will be done automatically. Then, insert the operating system CD to install the operating system, and reboot the system to complete the installation.

What is the best way to use the Prerequisite Checker information?

The Prerequisite Checker is available for Windows. See the readme file **\srvadmin\windows\PreReqChecker\readme.txt** on the *Dell PowerEdge Installation and Server Management* CD for detailed information about how to use the Prerequisite Checker.

In the Prerequisite Checker screen, I get the message "An error occurred while attempting to execute a Visual Basic Script. Please confirm that Visual Basic files are installed correctly." What can I do to resolve this problem?

This error occurs when the prerequisite checker calls the Dell OpenManage script, **vbstest.vbs** (a visual basic script), to verify the installation environment, and the script fails.

The possible causes are:

- Incorrect Internet Explorer Security Settings.

   Ensure that **Tools→ Internet Options→ Security→ Custom Level→ Scripting→ Active Scripting** is set to **Enable**

   Ensure that **Tools→ Internet Options→ Security→ Custom Level→ Scripting→ Scripting of Java Applets** is set to **Enable**.

- Windows Scripting Host (WSH) has disabled the running of VBS scripts. WSH is installed during operating system installation, by default. WSH can be configured to prevent the running of scripts with a **.VBS** extension.

   e. Right click **My Computer** on your desktop and click **Open→ Tools→ Folder Options→ File Types**.

   f. Look for the **VBS** file extension and ensure that **File Types** is set to **VBScript Script File**.

   g. If not, click **Change** and choose **Microsoft Windows Based Script Host** as the application that gets invoked to run the script.

- WSH is the wrong version, corrupted, or not installed. WSH is installed during operating system installation, by default. Go to the following location for the current WSH to download: **http://msdn.microsoft.com/downloads/list/webdev.asp**

Can I launch my installation without running the Prerequisite Checker? How do I do that?

Yes, you can. You can run the MSI directly from the **\Windows\SystemsManagement** folder. In general, it is not a good idea to bypass the prerequisite information as there could be important information that you would not know otherwise.

How do I know what version of systems management software is installed on the system?

Go to **Start→ Settings→ Control Panel→ Add/Remove programs** and select **Dell OpenManage Server Administrator**. Select the link for **support information**.

What are the names of all the Dell OpenManage features under Windows?

The following table lists the names of all Dell OpenManage features and their corresponding names in Windows.

Table 10-1. Dell OpenManage Features Under Windows

Feature	Name in Windows
Managed System Services	
Server Administrator Instrumentation Service	DSM SA Data Manager
	DSM SA Event Manager
Server Administrator	DSM SA Connection Service
	DSM SA Shared Services
Server Administrator Storage Management Service	Mr2kserv
Remote Access Controller Console (DRAC III)	Remote Access Controller (RAC) Service
	RAC Win VNC
Remote Access Controller Console (DRAC 4)	Remote Access Controller 4 (DRAC 4)
Management Station Services	
IT Assistant	DSM IT Assistant Network Monitor
	DSM IT Assistant Connection Service
	DSM IT Assistant Common Services
Baseboard Management Controller (BMC)	DSM BMU SOL Proxy

Red Hat® Enterprise Linux or SUSE® Linux Enterprise Server

How do I perform an unattended operating system installation with the *Installation and Server Management* CD?

You can install a Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system on many systems using identical settings, which is called a kickstart, and allow consistent configurations across all systems. To use this feature, the PowerEdge systems must be configured identically with the same hardware and operating system installed. Any difference in configuration makes the replication feature unusable.

To perform unattended installations, do the following:

1. On the first server being set up, ensure that the server's BIOS is set to boot from the CD. Insert the *Installation and Server Management* CD and reboot your server. Follow the installation interview, which includes setting the date and time, configuring the RAID controllers, selecting the operating system and specifying its settings, configuring the hard drive, entering the network settings, and configuring Red Hat Enterprise Linux or SUSE Linux Enterprise Server. If any information is omitted, an unattended installation can still be accomplished, but the system will prompt you for the missing information.

2. In the **Installation Summary** window, select **Save Unattended Installation Script at /root/install-ks.cfg** and select **Save Profile for Replication at /root/replication.** Click the **Continue** button.

3. Insert the Red Hat Enterprise Linux or SUSE Linux Enterprise Server installation CD and follow the instructions to complete the installation. Reboot the system to complete the installation.

4. When the installation is completed on the first system, copy the files from the **/root/replication** directory to a diskette.

5. For each subsequent unattended installation, insert the disk containing the replication files into the diskette drive and boot the system. The installation interview will be done automatically. Then, insert the Red Hat Enterprise Linux or SUSE Linux Enterprise Server installation CD to install the operating system, and reboot the system to complete the installation.

I manually installed my Red Hat Enterprise Linux 4 - x86_64 or SUSE Linux Enterprise Server 9 x86_64 operating system and am seeing RPM dependencies when trying to install Server Administrator. Where could I find these dependent RPM files?

For Red Hat Enterprise Linux, the dependent RPM files are on the Red Hat Enterprise Linux installation CD. For convenience, they are captured in one of the following directories corresponding to a supported Red Hat Enterprise Linux operating system:

/srvadmin/linux/RPMS/supportRPMS/RH3_i386

/srvadmin/linux/RPMS/supportRPMS/RH3_x86_64

/srvadmin/linux/RPMS/supportRPMS/RH4_i386

/srvadmin/linux/RPMS/supportRPMS/RH4_x86_64

For SUSE Linux Enterprise Server, the dependent RPM files are captured in the following directory:

/srvadmin/linux/RPMS/supportRPMS/SUSE9_x86_64

For instance, in the **RH4_x86_64** subdirectory, execute the following command to install or update all the dependent RPM files:

```
rpm -Uvh /srvadmin/linux/RPMS/supportRPMS/RH4_x86_64
```

You will then be able to continue with the Server Administrator installation.

Why am I getting a warning concerning the RPM package key during installation?

The RPM files are signed with a digital signature. To avoid this warning, you should mount the CD or package, and import the key using a command such as the following:

```
rpm --import /mnt/cdrom/srvadmin/linux/RPM-GPG-KEY
```

Why is the Prerequisite Checker not available under Red Hat Enterprise Linux and SUSE Linux Enterprise Server?

The Prerequisite Checker is built into the **omilcore** RPM package. The checker uses a combination of RPM dependency checks and Dell hardware checks.

What are the names of all the Dell OpenManage features under Red Hat Enterprise Linux or SUSE Linux Enterprise Server?

The following table lists the names of all Dell OpenManage features and their corresponding init script names under Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems:

Table 10-2. Dell OpenManage Features Under Red Hat Enterprise Linux and SUSE Linux Enterprise Server

Feature	Name in Red Hat Enterprise Linux and SUSE Linux Enterprise Server
Managed System Services Feature	Feature init Script Name
DSM SA Device Drivers	instsvcdrv
DSM SA Data Engine Service	dataeng
DSM SA Shared Service	dsm_om_shrsvc
DSM SA Connection Service	dsm_om_connsvc
DSM SM LSI Manager	mptctl
Remote Access Controller (DRAC III)	
RAC3 Event Service	racsrvc
RAC3 ppp Daemon	racser
RAC3 VNC X Server	racvnc
Remote Access Controller (DRAC 4)	racsvc
Remote Access Controller (DRAC 5)	None
Management Station Services	Feature init Script Name
Baseboard Management Controller (BMC)	dsm_bmu_sol_proxy
Non-Dell OpenManage Features	Feature init Script Name
OpenIPMI	ipmi (if not present, dsm_sa_ipmi)

What do the directories under srvadmin/linux/custom contain?

The following table lists the names of the directories in the **srvadmin/linux/custom** directory.

Table 10-3. Names of the Directories Under the srvadmin/linux/custom Directory

Name of RPM	Description	Other Server Administrator RPMs required
srvadmin-base — This is the core code for Server Administrator. It provides motherboard alerts and contains the CLI that allows for monitoring and control of Server Administrator, for example, omconfig, omdiag, and omreport. All peripheral packages, except the standalone DRAC support, require all or most of the RPM's in this directory to be installed. NOTE: You may need to install IPMI drivers for proper functionality.		
instsvc-drivers	Server Administrator Device Drivers — The systems management package, **srvadmin-hapi**, now provides the device drivers and libraries. This RPM is needed for legacy Server Administrator applications.	NA
srvadmin-cm	Server Administrator Inventory Collector — Systems management change management inventory collector.	srvadmin-omilcore, srvadmin-deng, and srvadmin-omacore.
srvadmin-deng	Server Administrator Data Engine — Systems management provides a data management framework for systems management software.	srvadmin-omilcore
srvadmin-hapi	Server Administrator Hardware Application Programming Interface — This systems management package	srvadmin-omilcore and

	provides the device drivers and libraries needed by systems management software to access information about the hardware on supported systems.	srvadmin-ipmi
srvadmin-isvc	Server Administrator Instrumentation Service — Server Administrator provides a suite of systems management information for keeping supported systems on your network healthy. Server Administrator Instrumentation Service provides fault management information, prefailure information, and asset and inventory information to management applications. The Instrumentation Service monitors the health of the system and provides rapid access to detailed fault and performance information about the hardware on supported systems. The Instrumentation Service requires installation of systems management device drivers.	srvadmin-omilcore, srvadmin-deng, and srvadmin-hapi
srvadmin-jre	Server Administrator Sun Java Runtime Environment — Systems management managed node Java runtime.	srvadmin-omilcore, srvadmin-deng, and srvadmin-omacore
srvadmin-odf	Server Administrator Online Diagnostic Common Components — Systems management online diagnostics framework. NOTE: The **srvadmin-odf** RPM, though installed, will not be functional as Diagnostics is no longer available through Server Administrator. To run diagnostics on your system, install Dell PowerEdge Diagnostics from your *Dell PowerEdge Service and Diagnostic Utilities* CD or download and install Dell PowerEdge Diagnostics from the Dell Support website at **support.dell.com**. Dell PowerEdge Diagnostics is a stand-alone application that can be run without installing Server Administrator.	srvadmin-omilcore, srvadmin-deng, and srvadmin-omacore
srvadmin-omacore	Server Administrator — Systems management managed mode core and CLI.	srvadmin-omilcore and srvadmin-deng
srvadmin-omhip	Server Administrator Instrumentation Service Integration Layer — Provides Instrumentation CLI.	srvadmin-omilcore, srvadmin-deng, srvadmin-hapi, srvadmin-isvc, and srvadmin-omacore
srvadmin-omilcore	Server Administrator Install Core — This is the core install package that provides the tools necessary for the rest of the Systems management install packages. All Server Administrator RPM's require this RPM.	
add-RAC3 — Software for remote management of third generation Remote Access Controllers. **For example: DRAC III.**		
srvadmin-rac3-components	Remote Access Card Data Populator Remote Access Controller components.	srvadmin-omilcore, srvadmin-deng, srvadmin-hapi, and srvadmin-racser
srvadmin-racdrsc3	DRAC III Integration Layer — **Remote Access CLI and Web Plugin to Server Administrator.**	srvadmin-omilcore, srvadmin-deng, srvadmin-omacore, and srvadmin-rac3 components
srvadmin-racser	Remote Access Card Managed Node — Remote Access Controller (RAC) services for the central administration of server clusters and remote administration of distributed resources.	srvadmin-omilcore
srvadmin-racser-devel	Remote Access Card Tools — The tools and libraries necessary to interface with the RAC board. This includes a managed node server daemon, a CLI tool named racadm, and the shared library these components require.	srvadmin-omilcore and srvadmin-racser
srvadmin-racvnc	RAC VNC Remote Service and Remote Services Server Agent.	srvadmin-omilcore and srvadmin-racser
add-RAC4 — Software for remote management of fourth generation Remote Access Controllers. **For example: DRAC 4.**		
srvadmin-rac4-components	Remote Access Card Data Populator — Remote Access Controller components.	srvadmin-omilcore, srvadmin-deng, srvadmin-hapi, and srvadmin-racsvc
srvadmin-racadm4	RAC Command Interface — The command line user interface to the Remote Access Controller (RAC).	srvadmin-omilcore
srvadmin-racdrsc4	DRAC 4 Integration Layer — **Remote Access CLI and Web Plugin to Server Administrator**	srvadmin-omilcore, srvadmin-deng, srvadmin-rac4 components, and srvadmin-omacore
srvadmin-racsvc	Remote Access Card Managed Node — Remote Access Controller (RAC) services supporting the central administration of server clusters and the remote administration of distributed resources.	srvadmin-omilcore
add-RAC5 — Software for remote management of fifth generation Remote Access Controllers. **For example: DRAC 5.**		
srvadmin-rac5-components	Remote Access Card Data Populator, DRAC 5 and Remote Access Controller components, DRAC 5.	srvadmin-omilcore, srvadmin-deng, and srvadmin-hapi
srvadmin-racadm5	RAC Command Interface — The command line user interface to the Remote Access Controller (RAC).	srvadmin-omilcore and srvadmin-hapi
srvadmin-racdrsc5	DRAC 5 Integration Layer — Remote Access CLI and Web Plug-in to Server Administrator	srvadmin-omilcore, srvadmin-deng, srvadmin-omacore, and srvadmin-rac5 components
add-storageservices — Storage Management RAID configuration utility and storage alert software		
srvadmin-storage	Storage Management — Provides Systems Management Storage Services.	srvadmin-omilcore, srvadmin-deng, srvadmin-omacore, and srvadmin-odf
add-webserver — Provides Web access to management of the server		
srvadmin-iws	Secure Port Server — Systems Management Managed Node Web Server package.	srvadmin-omilcore, srvadmin-deng, srvadmin-omacore, and srvadmin-jre

add-openipmi-RHEL3 — Provides OpenIPMI support for Red Hat Enterprise Linux (version 3)

dkms	Dynamic Kernel Module Support Framework — This package contains the framework for the Dynamic Kernel Module Support (DKMS) method for installing module RPMS as originally developed by Dell Computer Corporation.	
openipmi	Openipmi XX.Y.RHEL3 dkms package — Kernel modules for openipmi XX.Y.RHEL3 in a DKMS wrapper.	dkms
srvadmin-ipmi	This RPM forces the proper install sequence for the DKMS, openipmi XX.Y.RHEL3, and **srvadmin-hapi** RPMS.	openipmi XX.Y.RHEL3

add-openipmi-RHEL4 — Provides OpenIPMI support for Red Hat Enterprise Linux (version 4)

dkms	Dynamic Kernel Module Support Framework — This package contains the framework for the Dynamic Kernel Module Support (DKMS) method for installing module RPMS as originally developed by Dell Computer Corporation.	
openipmi	Openipmi XX.Y.RHEL4 dkms package — Kernel modules for openipmi XX.Y.RHEL4 in a DKMS wrapper.	dkms
srvadmin-ipmi	This RPM forces the proper install sequence for the DKMS, openipmi XX.Y.RHEL4, and **srvadmin-hapi** RPMS.	openipmi XX.Y.RHEL4

add-openipmi-SLES9 — Provides OpenIPMI support for SUSE Linux Enterprise Server (version 9)

dkms	Dynamic Kernel Module Support Framework — This package contains the framework for the Dynamic Kernel Module Support (DKMS) method for installing module RPMS as originally developed by Dell Computer Corporation.	
openipmi	Openipmi XX.Y.SLES9 dkms package — Kernel modules for openipmi XX.Y.SLES9 in a DKMS wrapper.	dkms
srvadmin-ipmi	This RPM forces the proper install sequence for the DKMS, openipmi XX.Y.SLES9, and **srvadmin-hapi** RPMS.	openipmi XX.Y.SLES9

add-openipmi-SLES10 — Provides OpenIPMI support for SUSE Linux Enterprise Server (version 10)

srvadmin-ipmi	This RPM is used to address the RPM dependency of srvadmin-hapi package.	openipmi XX.Y.SLES10

What daemons run on Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems after Server Administrator is started?

The daemons that run on Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems depend on what has been installed and what is enabled to run. The following table displays the daemons that typically run for a full install:

Table 10-**4. Daemons that run on Red Hat Enterprise Linux and SUSE Linux Enterprise Server once Server Administrator is started**

Daemon Name	Name in Red Hat Enterprise Linux and SUSE Linux Enterprise Server
For RPMs in the srvadmin-base directory	
dsm_sa_datamgr32d	DSM SA Data Manager — Server Administrator data manager daemon started by DSM SA Data Engine service.
dsm_sa_eventmgr32d	DSM SA Event Manager — Server Administrator event and logging daemon started by DSM SA Data Engine service.
dsm_sa_snmp32d	DSM SA SNMP daemon — Server Administrator SNMP daemon started by DSM SA Data Engine service.
dsm_om_shrsvc32d	DSM SA Shared Services — Server Administrator core daemon.
For RPMs in the add-webserver directory	
dsm_om_connsvc32d	DSM SA Connection Services — Server Administrator Web server daemon.
For systems that support DRAC 4: add-RAC4	
racsvc	DRAC 4 Administrator daemon
For systems that support DRAC III: add-RAC3	
racser	DRAC III Administrator daemon
racvnc	DRAC III virtual network daemon
racsrvc	DRAC III VNC X server

What kernel modules are loaded when Server Administrator is started?

This is dependent on the type of systems instrumentation. The following table displays the kernel modules loaded when Server Administrator is started.

Table 10-**5. Kernel Modules Loaded when Server Administrator Services are Started**

Driver Name	Description
For a system with IPMI	
dell_rbu	Dell BIOS Update Driver
ipmi_devintf	IPMI device driver
ipmi_msghandler	IPMI device driver
ipmi_si	IPMI device driver — For systems running Red Hat Enterprise Linux (version 4) or SUSE Linux Enterprise Server (version 9 and 10)
ipmi_si_drv	IPMI device driver — For systems running Red Hat Enterprise Linux (version 3)
For a TVM system	
dcdbas	Dell Systems Management Base Driver
dell_rbu	Dell BIOS Update Driver
For an ESM system	
dcdbas	Dell Systems Management Base Driver
dell_rbu	Dell BIOS Update Driver

For support of Server Administrator Storage Systems	
mptctl	Device driver for LSI RAID

Glossary

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

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

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.

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.

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

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.

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.

CA

Abbreviation for certification authority.

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.

CI/O

Abbreviation for comprehensive input/output.

CLI

Abbreviation for command line interface.

cm

Abbreviation for centimeter(s).

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.

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.

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.

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.

DNS

Abbreviation for Domain Name Service.

DRAC 4

Acronym for Dell™ Remote Access Controller 4.

DRAC III

Acronym for Dell Remote Access Controller III.

DRAC III/XT

Acronym for Dell Remote Access Controller 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.

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.

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 Microsoft® 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:

l   **FAT** — The operating system maintains a table to keep track of the status of various segments of disk space used for file storage.

l   **FAT32** — A derivative of the FAT file system. FAT32 supports smaller cluster sizes than FAT, thus providing more efficient space allocation on FAT32 drives.

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.

format

To prepare a hard drive or diskette for storing files. An unconditional format deletes all data stored on the disk.

FSMO

Abbreviation for Flexible Single Master Operation.

FTP

Abbreviation for file transfer protocol.

GB

Abbreviation for gigabyte(s). A gigabyte equals 1024 megabytes or 1,073,741,824 bytes.

gcc

Abbreviation for GNU C complier.

GNU

Acronym for GNU's Not UNIX®. GNU software is published under the GPL open-source license.

GPG

Abbreviation for GNU Privacy Guard.

GUI

Acronym for graphical user interface.

GUID

Acronym for Globally Unique Identifier.

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.

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.

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.

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.

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.

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.

K

Abbreviation for kilo-, indicating 1000.

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><Del> key combination.

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.

LDAP

Abbreviation for Lightweight Directory Access Protocol.

LDIF

Abbreviation for Lightweight Directory Interchange Format.

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.

LRA

Abbreviation for local response agent.

managed system

A managed system is any system that is monitored and managed using Dell OpenManage™ Server Administrator. Systems running Server Administrator can be managed locally or remotely through a supported Web browser. See remote management system.

management station

A system used to remotely manage one or more managed systems from a central location.

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.

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.

MIB

Acronym for management information base. The MIB is used to send detailed status or 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.

mm

Abbreviation for millimeter(s).

MMC

Abbreviation for Microsoft Management Console.

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).

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).

NDS

Abbreviation for Novell Directory Service.

NIC

Acronym for network interface card.

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 Microsoft 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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

RBAC

Abbreviation for role-based access control.

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.

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 Red Hat® Package Manager.

SAN

Acronym for storage area network.

SAS

Acronym for serial attached SCSI.

SCA

Abbreviation for single connector attachment.

schema

A collection of class definitions that describes managed objects in a particular environment. A CIM 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.

sec

Abbreviation for second(s).

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.

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.

SIMM

Acronym for single in-line memory module. A small circuit board containing DRAM chips that connects to the system board.

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.

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

- l   UpperThresholdFatal
- l   UpperThresholdCritical
- l   UpperThresholdNon-critical
- l   Normal
- l   LowerThresholdNon-critical
- l   LowerThresholdCritical
- l   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.

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.

UDP

Abbreviation for user datagram protocol.

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 1MB. 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.

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.

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.

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

VMS

Acronym for Virtual Media Server.

VNC

Acronym for Virtual Network Computing. In a VNC system, servers provide applications, data, and the desktop environment, all of which may be accessed through the Internet.

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.

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.

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 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 and SUSE Linux Enterprise Server environments.

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.

Installing Managed System Software on
Red Hat® Enterprise Linux and SUSE® Linux Operating Systems
Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- Overview
- Before You Begin
- Installation Requirements
- Installation Procedures
- Using Dell OpenManage with VMware® ESX Server™ Software
- Managed System Software Installation Using Third-Party Deployment Software

Overview

You can install managed systems software by one of two methods. The *Dell™ PowerEdge™ Installation and Server Management* CD provides installation scripts and RPM packages to install**,** upgrade**,** and uninstall Dell OpenManage™ 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.

The first install method uses the provided custom install script **srvadmin-install.sh**. This script allows unattended express installation and custom, unattended, or interactive installation. By including the **srvadmin-install.sh** script in your Linux scripts you may install Server Administrator on single or multiple systems, in attended or unattended mode, and locally or across a network.

The second install method uses the Server Administrator RPM packages provided in the custom directories and the Linux **rpm** command. This allows custom interactive installation. You may write Linux scripts that install Server Administrator on a single or multiple systems through an unattended installation locally or across a network.

Using a combination of the two install methods is not recommended and may require that you manually install required Server Administrator RPM packages provided in the custom directories, using the Linux **rpm** command.

> **NOTE:** See the *Dell PowerEdge Installation and Server Management* CD's **readme_ins.txt** file for a list of the systems that are currently supported.

Unattended and Scripted Silent Installation

You can use the *Dell PowerEdge Installation and Server Management* CD to perform an unattended and scripted silent installation of managed systems software through the command line (using RPM packages) on systems running supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems.

Before You Begin

- Read the installation requirements to ensure that your system meets or exceeds the minimum requirements.

- Read the *Dell OpenManage Server Administrator Compatibility Guide*. This guide contains compatibility information about Server Administrator installation and operation on various hardware platforms running supported Microsoft® Windows®, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems.

- Read the Dell OpenManage installation **readme_ins.txt** file on the *Dell PowerEdge Installation and Server Management* CD. The file contains the latest information about new features, fixes, and hardware requirements, in addition to information about known issues.

- Read the Server Administrator readme file on the *Dell PowerEdge 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 general requirements for managed systems software.

Supported Operating System Versions

The managed systems software runs, at a minimum, on each of the following operating systems:

- Red Hat Enterprise Linux AS, ES, and WS, (version 3) x86, Update 6

- Red Hat Enterprise Linux AS, ES, and WS, (version 3) for Intel® Extended Memory 64 Technology (Intel EM64T) Update 6

- Red Hat Enterprise Linux AS, ES, and WS, (version 4) for Intel x86

- Red Hat Enterprise Linux AS, ES, and WS, (version 4) for Intel EM64T

- SUSE Linux Enterprise Server (version 9), SP3 for Intel EM64T

l   SUSE Linux Enterprise Server (version 10) Gold, for Intel EM64T

NOTE: See the Server Administrator readme file on the *Dell PowerEdge Installation and Server Management* CD or the *Dell OpenManage Server Administrator Compatibility Guide* on the *Documentation* CD for the latest detailed list of the Server Administrator services that are supported on each supported operating system.

System Requirements

Managed systems software must be installed on each system to be managed. You can then manage each system running the managed systems software locally or remotely through a supported Web browser.

Managed System Requirements

l   One of the supported operating system versions.

l   A minimum of 64 MB of RAM.

l   A minimum of 256 MB of free hard drive space.

l   Administrator rights.

l   A TCP/IP connection on the monitored system and the remote system to facilitate remote system management.

l   The Simple Network Management Protocol (SNMP).

l   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.

l   The Server Administrator Remote Access Service requires that a remote access controller (RAC) be installed on the system to be managed.

   NOTE: See the *Dell Remote Access Controller 4 User's Guide,* the *Dell Remote Access Controller 5 User's Guide,* or the *Dell Embedded Remote Access Controller/MC User's Guide* for complete software and hardware requirements.

l   The Server Administrator Storage Management Service requires that Dell OpenManage Storage Management be installed on the system in order to be properly managed. See the *Dell OpenManage Server Administrator User's Guide* for complete software and hardware requirements.

Supported Systems Management Protocol Standards

A supported systems management protocol standard must be installed on the managed system before installing Server Administrator. On supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, Server Administrator only supports the SNMP systems management standard. You must install the SNMP package provided with the operating system. CIM and WMI are unavailable.

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

Installation Procedures

This section explains how to install, upgrade, and uninstall Server Administrator on a system that is running a supported Red Hat Enterprise Linux or a supported SUSE Linux Enterprise Server operating system. Server Administrator can be installed and upgraded from the *Dell PowerEdge Installation and Server Management* CD using scripts or RPM commands.

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

l   Dynamic Kernel Support (DKS)

l   OpenIPMI Device Driver

l   Installing and Upgrading managed system software

l   Performing an Unattended Installation of the managed system software

l   Upgrading from Previous Versions

l   Uninstalling Server Administrator

Software License Agreement

The software license for the Red Hat Enterprise Linux and SUSE Linux Enterprise Server version of the Dell OpenManage software is located on the CD in the root directory. Read the **license.txt** file. By installing or copying any of the files on this CD, you are agreeing to the terms found in this file. This file is also copied to the root of the software tree where you choose to install the Dell OpenManage software.

Dynamic Kernel Support (DKS)

Server Administrator provides precompiled device drivers for the precompiled kernels listed in the Server Administrator readme file on the *Dell PowerEdge Installation and Server Management* CD. If the running kernel is not one of the precompiled kernels listed in the readme file, or if the running kernel is

reconfigured and recompiled in such a way that none of the precompiled Server Administrator device drivers support the recompiled kernel, then Server Administrator may need to use its DKS feature to support the running kernel.

If you see the following message during Server Administrator Device Drivers startup, then Server Administrator attempted to use its DKS feature, but was unable to use the feature because certain prerequisites were not met:

     Building <*driver*> using DKS... [FAILED]

     where <*driver*> is dcdbas or dell_rbu

> **NOTE:** Server Administrator logs messages to the **/var/log/messages** log file.

To use DKS, you should identify which kernel you have running, then check the DKS prerequisites.

Determining the Running Kernel

1. Log in as root.

2. Type the following command at a console and press <Enter>:

    uname –r

The system displays a message identifying the running kernel. If it is not one of those listed in the managed system software readme file, then the managed system software may need to use DKS to support it.

Dynamic Kernel Support Prerequisites

For managed system software to use DKS, the following dependencies must be met before starting Server Administrator.

   l   The running kernel must have loadable module support enabled.

   l   The source for building kernel modules for the running kernel must be available from **/lib/modules/`uname –r`/build**. On systems running Red Hat Enterprise Linux (version 3) and SUSE Linux Enterprise Server (version 9 and 10), the **kernel-source** RPM provides the necessary kernel source. **On systems running Red Hat Enterprise Linux (version 4), the kernel*-devel** RPMs provide the necessary kernel source for building kernel modules.

   l   The GNU make utility must be installed. The **make** RPM provides this utility.

   l   The GNU C compiler (gcc) must be installed. The **gcc** RPM provides this compiler.

   l   The GNU linker (ld) must be installed. The **binutils** RPM provides this linker.

When these prerequisites have been met, DKS will automatically build a device driver when needed during Server Administrator startup.

> **NOTE:** *Unsupported kernels* are kernels that are not supported by a precompiled device driver. If you are running a supported kernel, see "[Installing and Upgrading Managed System Software](#)."

Using Dynamic Kernel Support After Server Administrator Installation

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

1. Ensure that the DKS prerequisites are met on the system to be managed.

2. Boot the new kernel on the system.

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

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

When Server Administrator dynamically builds a device driver for the running kernel, it installs the device driver into the **/lib/modules/<*kernel*>/kernel/drivers/firmware** directory, where <*kernel*> is the kernel name (returned by typing uname –r). If you have a system running the same kernel for which a device driver was built, you can copy the newly built device driver to the **/var/omsa/dks/<*kernel*>** directory on the other system for use by Server Administrator. This action allows Server Administrator to use DKS on multiple systems without having to install the kernel source on every system.

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

1. Ensure that the DKS prerequisites are met on system A.

2. Start Server Administrator on system A.

Server Administrator builds a device driver for the kernel running on system A during startup.

3. Type `uname -r` on system A to determine the name of the running kernel.

4. Copy any **dcdbas.*** or **dell_rbu.*** files in the **/lib/modules/_<kernel>_/kernel/drivers/firmware** directory on system A to the **/var/omsa/dks/_<kernel>_** directory on system B, where **_<kernel>_** is the kernel name returned by typing `uname -r` in step 3.

   📝 **NOTE:** The **/lib/modules/_<kernel>_/kernel/drivers/firmware** directory may contain one or more of the following files: **dcdbas.*** or **dell_rbu.***

   📝 **NOTE:** You might have to create the **/var/omsa/dks/_<kernel>_** directory on system B. For example, if the kernel name is 1.2.3-4smp, you can create the directory by typing: `mkdir -p /var/omsa/dks/1.2.3-4smp`

5. Start Server Administrator on system B.

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

   📝 **NOTE:** You can also use this procedure when upgrading Server Administrator if the new version of Server Administrator does not support the running kernel with a precompiled device driver.

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

Forcing Dynamic Kernel Support on Red Hat Enterprise Linux Update Releases When Kernel is Tainted

Server Administrator provides precompiled device drivers for the "Gold" releases of supported Red Hat Enterprise Linux operating systems. Red Hat Enterprise Linux supports loading device drivers built for the "Gold" release, on the Update releases. This means Server Administrator does not have to ship precompiled device drivers for every Red Hat Enterprise Linux Update release and users are not forced to use DKS in order to run Server Administrator on every system that is running a Red Hat Enterprise Linux Update release. However, loading a device driver built for the "Gold" release of Red Hat Enterprise Linux (version 3) on an Update release may taint the kernel. If the kernel on a system running a Red Hat Enterprise Linux (version 3) Update release has been tainted by this device driver load process, Server Administrator's init script command **restart-forcekernelmatch** can be used to force DKS to be used in this situation. DKS will build device drivers that do not taint the running kernel.

Determining if the Running Kernel is Tainted

After Server Administrator services have been started, perform the following steps on Red Hat Enterprise Linux Update releases to determine if the kernel has been tainted:

1. Log in as `root`.

2. Execute the following command:

   `lsmod`

If you see **Tainted: GF** in the first line of the output as in the following message, the running kernel is tainted:

   `Module Size Used by Tainted: GF`

The "tainted" status may be caused by the Server Administrator device driver load process.

Forcing Dynamic Kernel Support on Red Hat Enterprise Linux Update Releases

After the installation of Server Administrator, perform the following steps to force DKS to be used on Red Hat Enterprise Linux Update releases to build device drivers for the running kernel, if needed, so that they do not taint the kernel:

1. Ensure that the prerequisites of DKS are met.

2. Execute the following command:

   `/etc/init.d/instsvcdrv restart-forcekernelmatch`

This command will first stop the Server Administrator device drivers. It will then search for precompiled device drivers to load, by checking for precompiled device drivers built for a kernel whose name is an exact match as the name of the running kernel. If it fails to find an exact match, it will use DKS to build device drivers for the running kernel. Finally, the command will restart the Server Administrator device drivers.

📝 **NOTE:** The system must be rebooted to clear the kernel "tainted" status.

OpenIPMI Device Driver

The Server Administrator Instrumentation Service of Server Administrator requires the OpenIPMI device driver in order to provide IPMI-based information and functionality. It also requires a minimum version of the OpenIPMI device driver. The minimum version required is defined based on the Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system.

This requirement is checked and enforced by Server Administrator at three instances. Two of the instances are during installation, while the third is a run-time

step. The instances are:

- l During custom installation of Server Administrator using the **srvadmin-install.sh** shell script.

- l During installation of Server Administrator using RPM.

- l At run-time when the Server Administrator Instrumentation Service is started.

NOTE: SUSE Linux Enterprise Server (version 10) contains the required version of IPMI module in the default kernel itself. You do not need to install the IPMI RPM.

Blocking During Custom Installation of Server Administrator Using the srvadmin-install.sh Shell Script

During custom installation of Server Administrator using the **srvadmin-install.sh** shell script, the script automatically calls another shell script called **srvadmin-openipmi.sh**, to ensure that a sufficient version of the OpenIPMI device driver (for example, a version that is equal to or greater than the minimum version of the OpenIPMI device driver that is required by the Server Administrator Instrumentation Service) is currently installed on the system. If a sufficient version is not found, the **srvadmin-install.sh** shell script calls the **srvadmin-openipmi.sh** shell script again to attempt to install a sufficient version. If the attempt fails for any reason, an appropriate error message is displayed with instructions describing how to resolve the error. You must resolve errors, if any, before re-running the **srvadmin-install.sh** shell script to install Server Administrator.

Blocking During Installation of Server Administrator Using RPM

To assist in the correct order of RPM installation, the **srvadmin-hapi** RPM is dependent on one of the **srvadmin-ipmi** RPMs. Each **srvadmin-ipmi** RPM is distribution-specific and depends on a distribution-specific OpenIPMI RPM. The **srvadmin-hapi** RPM will not install unless the RPM dependencies are met.

During installation of Server Administrator using RPM, the **srvadmin-hapi** RPM will check if a sufficient version of the OpenIPMI device driver is currently installed on the system. If a sufficient version is not found, the **srvadmin-hapi** RPM will fail to install and will display an error message stating that you must install/upgrade the OpenIPMI device driver. In such a case, RPMs that depend on the **srvadmin-hapi** RPM will also fail to install. In such cases, you must install/upgrade the OpenIPMI driver by performing the following additional steps:

1. Navigate to the **srvadmin/linux/supportscripts** directory.

2. Run the following **srvadmin-openipmi.sh** shell script:

   `sh srvadmin-openipmi.sh install`

Re-attempt to install the **srvadmin-hapi** RPM and any other RPMs that failed to install as they depend on the **srvadmin-hapi** RPM. Perform the following steps:

1. Navigate to the **srvadmin/linux/custom/*** directory that you previously were at.

2. Run the following command to see which Server Administrator packages were previously successfully installed.

   `rpm -qa | grep srvadmin`

   The query displays a list of all installed Server Administrator packages.

3. Install every RPM in the directory that was previously not installed, as they depended on the **srvadmin-hapi** RPM that previously failed to install, by running the following command:

   `rpm -ihv srvadmin-hapi*.rpm srvadmin-isvc*.rpm srvadmin-omhip*.rpm srvadmin-<any-other-packages>*.rpm`

Alternately, during installation of the **srvadmin-hapi** RPM using RPM, if the OpenIPMI RPM for a version of the OpenIPMI driver that meets the minimum version of the OpenIPMI driver that is required by Server Administrator is currently installed on the system, but OpenIPMI driver modules have not yet been built and installed for the given version of the OpenIPMI driver because the **kernel-source** RPM is required but is not currently installed, the **srvadmin-hapi** RPM will fail to install and will display an error message. The error message will state that you need to install the **kernel-source** RPM and build the OpenIPMI driver. In such a case, any RPMs that depend on the **srvadmin-hapi** RPM will also fail to install. You must then install the **kernel-source** RPM, and build and install the OpenIPMI driver modules, by performing the following additional steps:

1. For systems running Red Hat Enterprise Linux (version 3), get a copy of the appropriate **kernel-source** RPM for running the kernel off your operating system installation CDs (or from some other source).

   On systems running Red Hat Enterprise Linux (version 4) and SUSE Linux Enterprise Server, the **kernel*-devel** RPMs provide the necessary source for building kernel modules.

2. Install the **kernel-source** RPM or **kernel*-devel** RPMs by running the following command from where you have found or copied the RPM(s):

   `rpm -ihv kernel*.rpm`

3. Navigate to the **srvadmin/linux/supportscripts** directory.

4. Run the **srvadmin-openipmi.sh** shell script as shown below. This will build and install the OpenIPMI driver modules.

   `sh srvadmin-openipmi.sh install`

Re-attempt to install the **srvadmin-hapi** RPM and any RPMs that failed to install as they depend on the **srvadmin-hapi** RPM.

Degradation of Functionality When Server Administrator Instrumentation Service is Started

After Server Administrator is installed, the Server Administrator Instrumentation Service will do a run-time check of the OpenIPMI device driver whenever it is started. The Server Administrator Instrumentation Service is started whenever you run either the **srvadmin-services.sh start** or **srvadmin-services.sh restart** commands, or you restart the system (during which the Server Administrator Instrumentation Service is started).

While Server Administrator installation will block the installation of Server Administrator if a sufficient version of the OpenIPMI device driver is not currently installed on the system, it is still possible, though not typical, that a user can uninstall or replace a sufficient version of the OpenIPMI device driver after Server Administrator has been installed. Server Administrator cannot prevent this.

To account for a user uninstalling or replacing a sufficient version of the OpenIPMI device driver after Server Administrator has been installed, the Server Administrator Instrumentation Service checks the OpenIPMI device driver version whenever it is started. If a sufficient version of the OpenIPMI device driver is not found, the Server Administrator Instrumentation Service will degrade itself so that it does not provide any of its IPMI-based information or functionality. Primarily, this means that it will not provide any probe data (for example, fans, temperatures, and voltage probe data).

If you know or suspect that the OpenIPMI device driver on the system is not sufficient, you can run the **srvadmin-openipmi.sh** shell script on the *Dell PowerEdge Installation and Server Management* CD to install a sufficient version by, again, performing the following steps:

1. Navigate to the **srvadmin/linux/supportscripts** directory.

2. Run the **srvadmin-openipmi.sh** shell script as shown below.

   sh srvadmin-openipmi.sh install

If you are unsure as to whether or not the OpenIPMI device driver on the system is sufficient, run the **srvadmin-openipmi.sh status** command instead. Rather than attempting to install or upgrade the OpenIPMI device driver, if necessary, which is what the **srvadmin-openipmi.sh install** command does, the **srvadmin-openipmi.sh status** command displays information that informs you whether or not the OpenIPMI device driver on the system is sufficient or not. After running the **srvadmin-openipmi.sh** status command, you can then decide whether or not you need and want to run the **srvadmin-openipmi.sh install** command.

Installing and Upgrading Managed System Software

This section explains how to install and upgrade managed system software using the following installation options:

l Use the **srvadmin-install.sh** shell script for Express installs or Custom installs, in either interactive or unattended mode

l Use RPM commands for Custom installs, in either interactive or unattended mode

Prerequisites for Installing Managed System Software

l You must be logged in as root.

l The running kernel must have loadable module support enabled.

l Your **/opt** directory must have at least 250 MB of free space, and your **/tmp** and **/var** directories must each have at least 20 MB of free space. If you choose to use a non-default directory for the installation, then that directory must also have at least 250 MB of free space.

l The **ucd-snmp** or **net-snmp** package that is provided with the operating system must be installed if you use SNMP to manage your server. If you want to use supporting agents for the **ucd-snmp** or **net-snmp** agent, you must install the operating system support for the SNMP standard before you install Server Administrator. For more information about installing SNMP, see the installation instructions for the operating system you are running on your system.

   NOTE: When installing an RPM package in Red Hat Enterprise Linux or SUSE Linux Enterprise Server, to avoid warnings concerning the RPM–GPG key, import the key with a command similar to the following:

   rpm --import /mnt/cdrom/srvadmin/linux/RPM-GPG-KEY

l You must install all the prerequisite RPMs required for successful installation.

   If your system came with a factory installed Red Hat Enterprise Linux (versions 3 and 4) or SUSE Linux Enterprise Server (versions 9 and 10) operating system, see the Server Administrator installation readme file (**readme_ins.txt**) on the *Dell PowerEdge Installation and Server Management* CD for information on any RPMs that you need to manually install prior to installing managed system software. In most cases you will not need to manually install any RPMs. See the readme file to be sure.

   If your system did not come with a factory installed Linux operating system, and you did not install a Red Hat Enterprise Linux (versions 3 and 4) or SUSE Linux Enterprise Server (version 9 and 10) operating system using Server Assistant, then you need to manually install the prerequisite RPMs prior to installing managed system software. For convenience, these RPM files are provided on the *Dell PowerEdge Installation and Server Management* CD or package. Navigate to the appropriate **/srvadmin/linux/RPMS/supportRPMS/***operating-system* subfolder for your specific Red Hat Enterprise Linux (versions 3 and 4) or SUSE Linux Enterprise Server (versions 9 and 10) operating system and run
   rpm -Uvh * to install these RPM files before installing managed system software.

Installing Managed System Software Using the Dell PowerEdge Installation and Server Management CD

The *Dell PowerEdge Installation and Server Management* CD uses RPMs to install each component. The CD is divided into subdirectories to enable easy Custom Installs.

If you would like to review the software before you install it, follow this procedure:

1. Load the *Dell PowerEdge Installation and Server Management* CD into your system's CD drive.

2. If necessary, use the command line to mount the CD using a command such as:
    `mount /dev/cdrom /mnt/cdrom`

3. When you have mounted the CD, you can navigate to it with
    `cd /mnt/cdrom/srvadmin/linux/`

4. Get a listing of the directories with `ls`.

    The directories on the CD that pertain to Red Hat Enterprise Linux and SUSE Linux Enterprise Server are the following:

    `srvadmin/linux`

    `srvadmin/linux/custom`

    `srvadmin/linux/RPMS`

    `srvadmin/linux/supportscripts`

Express Install

Use the provided shell script to perform the express installation in silent and unattended mode.

1. Log on as `root` to the system running the supported Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system where you want to install the managed system components.

2. Insert the *Dell PowerEdge Installation and Server Management* CD into the CD drive.

3. If necessary, use the command line to mount the CD using a command such as:
    `mount /dev/cdrom /mnt/cdrom`

4. Navigate to the `srvadmin/linux/supportscripts` directory.

5. Run the **srvadmin-install.sh** shell script as shown below, which performs a silent and unattended express installation. All of the components, including any applicable remote access controller (DRAC III, DRAC 4, or DRAC 5) software components, will be installed.

    `sh srvadmin-install.sh --express`

    or

    `sh srvadmin-install.sh -x`

    🖉 **NOTE:** Just before the Server Administrator RPMs are installed, the **srvadmin-install.sh** shell script automatically calls the **srvadmin-openipmi.sh** shell script to ensure that a sufficient version of the OpenIPMI driver is currently installed on the system. If a sufficient version is not found, the **srvadmin-install.sh** shell script calls the **srvadmin-openipmi.sh** shell script to attempt to install a sufficient version. If the attempt fails for any reason, an appropriate error message will be displayed with instructions describing how to resolve the error. After resolving any error, you should then re-run the **srvadmin-install.sh** shell script to install the managed system components.

    Server Administrator services do not start automatically.

6. Start the Server Administrator services after the installation using the **srvadmin-services.sh** script by using the **sh srvadmin-services start** command.

Custom Install

Managed system software provides two custom installation paths. One is RPM-based, with pre-configured custom directories, and the other is shell script-based.

Using **Pre-configured Custom Directories** to Perform the Custom Installation

See <u>Table 7-1</u> for details about using the RPMs to perform a custom installation using pre-configured custom directories.

Table 7-1. Custom Installation Using Pre-Configured Directories

Directory	Details
To facilitate an RPM-based custom installation, add the RPMs from the following directory:	
/srvadmin/linux/custom/srvadmin-base	Contains base Server Administrator with command line interface
Then customize the installation by adding the RPMs from the following directories:	
/srvadmin/linux/custom/add-storageservices	Storage Management component packages
/srvadmin/linux/custom/add-webserver	Web Server component packages
/srvadmin/linux/custom/add-openipmi-RHEL3	IPMI RPM packages for Red Hat Enterprise Linux (version 3)
/srvadmin/linux/custom/add-openipmi-RHEL4	IPMI RPM packages for Red Hat Enterprise Linux (version 4)

/srvadmin/linux/custom/add-openipmi-SLES9	IPMI RPM packages for SUSE Linux Enterprise Server (version 9)
/srvadmin/linux/custom/add-openipmi-SLES10	IPMI RPM packages for SUSE Linux Enterprise Server (version 10)

The following is an example of custom RPMs-based installation of Server Administrator, including the installation of the Storage Management Service components.

1. Log on as `root` to the system running the supported Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system where you want to install the managed system components.

2. Insert the *Dell PowerEdge Installation and Server Management* CD into the CD drive.

3. If necessary, mount the CD using a command such as: `mount /dev/cdrom /mnt/cdrom`.

4. Navigate to the `srvadmin/linux/custom` directory.

5. Type the following command.

   `rpm -ihv srvadmin-base/*.rpm add-openipmi-RHEL4/srvadmin-ipmi*.rpm add-storageservices/*.rpm`

   > **NOTE:** This command is for the RedHat Enterprise Linux (Version 4) operating system. Apply the operating system specific **srvadmin-ipmi** RPM corresponding to your system.

   Server Administrator services do not start automatically.

6. Start the Server Administrator services after the installation by using the command:

   `sh srvadmin-services start`

Using the Shell Script to Perform the Custom Installation

You can run the Server Administrator Custom Install script in interactive mode or in silent and unattended mode.

The basic usage of the script is:

   `srvadmin-install.sh [OPTION]...`

Server Administrator Custom Installation Utility

This utility will run in interactive mode if you do not specify any options, and it will run silently if you provide one or more options.

The options are:

[-x|--express] installs all components including RAC. Any other options passed will be ignored.

[-b|--base] installs Base components.

[-s|--storage] installs Storage components, including Base.

[-r|--rac] installs applicable RAC components, including Base.

[-w|--web] installs Web Server components, including Base.

[-u|--update] updates applicable components in upgrade of prior versions (same as -x for upgrade).

[-a|--autostart] starts the installed services after components have been installed.

[--prefix PATH] installs the selected components to the specified "PATH". This option does not apply to OpenIPMI RPMs as they are not relocatable.

Using the Custom Install Script To Run in the Silent and Unattended Mode

The following is an example of a silent and unattended custom installation using the **srvadmin-install.sh** shell script.

1. Log on as `root` to the system running the supported Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system where you want to install the managed system components.

2. Insert the *Dell PowerEdge Installation and Server Management CD* into the CD drive.

3. If necessary, mount the CD using a command such as: `mount /dev/cdrom /mnt/cdrom`.

4. Navigate to the `srvadmin/linux/supportscripts` directory.

5. **To install the Storage Management Service components, type the following command.**

   `sh srvadmin-install.sh --storage` (these are long options)

or

`sh srvadmin-install.sh -s` (these are short options)

> ![NOTE icon] **NOTE:** Long options can be combined with short options, and vice-versa.

> ![NOTE icon] **NOTE:** Just before the Server Administrator RPMs are installed, the **srvadmin-install.sh** shell script automatically calls the **srvadmin-openipmi.sh** shell script to ensure that a sufficient version of the OpenIPMI driver is currently installed on the system. If a sufficient version is not found, the **srvadmin-install.sh** shell script calls the **srvadmin-openipmi.sh** shell script to attempt to install a sufficient version. If the attempt fails for any reason, an appropriate error message will be displayed with instructions describing how to resolve the error. After resolving any error, you should then re-run the **srvadmin-install.sh** shell script to install the managed system components.

Server Administrator services do not start automatically.

6. Start Server Administrator services after the installation by using the command:

   `sh srvadmin-services start`

Using the Shell Script to Perform the Custom Installation in Interactive Mode

This procedure uses the installation shell script to prompt you for the installation of specific components through the installation.

1. Log on as `root` to the system running the supported Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system where you want to install the managed system components.

2. Insert the *Dell PowerEdge Installation and Server Management* CD into the CD drive.

3. If necessary, mount the CD using the `mount /dev/cdrom /mnt/cdrom` command.

4. Navigate to the `srvadmin/linux/supportscripts` directory.

5. Execute the script with the **sh srvadmin-install.sh** command, which displays a list of component options. If any of the components are already installed, then those components are listed separately with a check mark next to them. The Server Administrator custom installation options are displayed.

6. Choose **c** to copy, **i** to install, **r** to reset and start over, or **q** to quit.

   l If you choose **c**, you are prompted to enter the absolute destination path.

   l If you choose **i**, a message states that the RPMs will be installed in the **/opt/dell/srvadmin** directory. You can then choose **y** to change, or <Enter> to use the default installation path.

   When the installation is completed, the script will have an option for starting the services.

   > ![NOTE icon] **NOTE:** Just before the Server Administrator RPMs are installed, the **srvadmin-install.sh** shell script automatically calls the **srvadmin-openipmi.sh** shell script to ensure that a sufficient version of the OpenIPMI driver is currently installed on the system. If a sufficient version is not found, the **srvadmin-install.sh** shell script calls the **srvadmin-openipmi.sh** shell script to attempt to install a sufficient version. If the attempt fails for any reason, an appropriate error message will be displayed with instructions describing how to resolve the error. After resolving any error, you should then re-run the **srvadmin-install.sh** shell script to install the managed system components.

7. Choose **n** to start the services manually.

Performing an Unattended Installation of the Managed System Software

You can use The *Dell PowerEdge Installation and Server Management* CD's **Express Install** and **Custom Install** options for the unattended installation procedure.

Unattended installation allows you simultaneously to install Server Administrator on multiple systems. You can perform an unattended installation by creating an unattended installation package that contains all of the necessary managed system software files.

The unattended installation package is distributed to the remote systems using a software distribution tool from an ISV. After the package is distributed, RPM installs the software.

The custom unattended installation package is located in the directory you created as detailed in the section "Using the Shell Script to Perform the Custom Installation in Interactive Mode." This directory contains all the RPMs for the managed system software components for distribution.

1. Configure your ISV software distribution software to execute `rpm -i *.rpm` after the unattended installation package has been distributed.

2. Use your ISV distribution software to distribute the unattended installation package to the remote systems. The RPM command installs Server Administrator on each remote system.

Dependency Check

RPM has a test feature that verifies software dependencies without actually installing any software. To execute this dependency check, type `rpm -ihv *.rpm --test`. This command is valid for all the the types of installation.

> ![NOTE icon] **NOTE:** The rpm command's `--test` feature does not perform any hardware verification. It will only check for RPM software dependencies.

Creating and Distributing the Express Unattended Installation Package

The **Express Install** unattended installation option uses the **/srvadmin/linux/supportscripts** and the **/srvadmin/linux/RPMS** subdirectories of the *Dell PowerEdge Installation and Server Management* CD as the unattended installation package. RPM accesses the *Dell PowerEdge Installation and Server Management* CD to install all required Server Administrator components on selected remote systems.

Distributing the Express-Install subdirectory as the Express Unattended Installation Package

1. Distribute the **/srvadmin/linux/supportscripts** and the **/srvadmin/linux/RPMS** subdirectory of the *Dell PowerEdge Installation and Server Management* CD to your target systems.

2. Configure your ISV software distribution software to execute `sh srvadmin-install.sh -x` from the **supportscripts** subdirectory.

   When the ISV software runs, it executes the RPMs to install Server Administrator on each remote system.

   > **NOTE:** If a sufficient version of the OpenIPMI driver is currently not installed on your remote systems, the **srvadmin-hapi** RPM will fail to install and will display an error message stating that you must install/upgrade the OpenIPMI driver. In such a case, any RPMs that depend on the s**rvadmin-hapi** RPM will also fail to install. In such cases, you should also distribute the OpenIPMI-related RPM files in the **srvadmin/linux/custom/add-openipmi**-*operating-system* subdirectory that is applicable to your operating system. Copy the RPMs from the applicable OpenIPMI subdirectory to the same directory on your target systems from where you distribute the custom unattended installation package.

Creating and Distributing the Custom Unattended Installation Package

The **Custom Install** unattended installation option creates an unattended installation package in a directory on your system's hard drive. To create an unattended installation package, use the copy capability described in the section "Using the Shell Script to Perform the Custom Installation in Interactive Mode" to create a custom directory with the RPM's you want to install. This directory will be your unattended installation directory. Copy the RPMs in the applicable OpenIPMI subdirectory to the same directory on your target systems where you distribute the custom unattended installation package.

Distributing Unattended Installation Packages

The custom unattended installation package is located in the directory you created in the preceding step 6 of the custom installation (see "Custom Install"). This directory contains all of the RPMs for the managed system software components to distribute.

1. Configure your ISV software distribution software to execute `rpm -i *.rpm` after the unattended installation package has been distributed.

2. Use your ISV distribution software to distribute the unattended installation package to the remote systems. The RPM command installs Server Administrator on each remote system.

Upgrading From Previous Versions

If your system is running Dell OpenManage software prior to version 4.2, uninstall the current version before attempting to install the new version.

Upgrading From Version 4.3 or Later

For Dell OpenManage software versions 4.3 and later, you can upgrade your system using RPM commands or the `srvadmin-install.sh` shell script. Ensure that all installed components are upgraded when you perform either procedure.

> **NOTE:** Use of the install script, **srvadmin-install.sh** is recommended.

Using the RPM

1. Log on as `root` to the system running Red Hat Enterprise Linux or SUSE Linux Enterprise Server that requires the upgraded managed system components.

2. Insert the *Dell PowerEdge Installation and Server Management* CD into the CD drive on your system.

   If the CD does not mount automatically, use a command similar to the following:

   `mount /dev/cdrom/ mnt/cdrom`

   `mount /dev/cdrom /media/cdrom`

3. After the CD mounts, navigate to the **RPMS** directory by using a command similar to the following:

   `cd /media/cdrom/srvadmin/linux/RPMS/<os>`

Where <os> is RHEL3 or RHEL4 or SLES9 or SLES10. Enter the appropriate directory name that applies to your system.

4. Upgrade the Red Hat Enterprise Linux or SUSE Linux Enterprise Server system using a single long command or individual RPMs. The single long command is a combination of RPMs and can be executed by typing just one command.

    Upgrade with the following command if you are upgrading from version 5.0:

    ```
    rpm -Uhv `rpm -q --queryformat "%{NAME}* " \`rpm -qa | grep srvadmin\``
    ```

    If upgrading from 4.x, use a command like the following:

    ```
    rpm -Uhv openipmi/openipmi*.rpm srvadmin-ipmi*.rpm `rpm -q --queryformat "%{NAME}* " \`rpm -qa | grep srvadmin\``
    ```

    NOTE: The commands upgrade the existing Server Administrator RPM packages on your system. Starting with version 5.0, the **openipmi** and **srvadmin-ipmi** packages are new requirements for Server Administrator. The **dkms** RPM package under the **openipmi** sub-directory depends on the **openipmi** package. You may have to adjust the commands depending on the status of these packages on your system.

    To upgrade all the previously installed packages using individual RPMs, perform the following steps:

    a. Query the rpm database for all installed srvadmin packages by typing:

    ```
    rpm -qa | grep srvadmin
    ```

    The query displays a list of all installed packages, including any existing or older versions.

    For example:

    ```
    srvadmin-omilcore-4.3.0-1.386.rpm
    srvadmin-hapi-4.3.0-1.386.rpm
    srvadmin-deng-4.3.0-1.386.rpm
    srvadmin-isvc-4.3.0-1.386.rpm
    ...
    ```

    b. Type the RPM upgrade command, incorporating the packages returned in step a. This command updates the installed Dell OpenManage software components.

    For example:

    ```
    rpm -Uhv srvadmin-omilcore-4.3.0-1.386.rpm srvadmin-hapi-4.3.0-1.386.rpm srvadmin-deng-4.3.0-1.386.rpm srvadmin-isvc-4.3.0-1.386.rpm
    ```

If the OpenIPMI driver is currently not installed on the system, or the version of the OpenIPMI driver installed on the system is less than the minimum version that is required by Server Administrator, the **srvadmin-hapi** RPM will fail to upgrade and will display an error message stating that you must install/upgrade the OpenIPMI driver. In such a case, any RPMs that depend on the **srvadmin-hapi** RPM will also fail to upgrade. In such cases, you must install/upgrade the OpenIPMI driver by performing the following additional steps:

1. Navigate to the **srvadmin/linux/supportscripts** directory.

2. Run the **srvadmin-openipmi.sh** shell script as shown below.

    ```
    sh srvadmin-openipmi.sh install
    ```

Reattempt to upgrade the **srvadmin-hapi** RPM and any other RPMs that failed to upgrade as they depend on the **srvadmin-hapi** RPM. Perform the following steps:

1. Navigate back to the previous directory that you were at.

2. Run the following commands to see which Server Administrator packages were previously successfully upgraded.

    ```
    rpm -qa | grep srvadmin
    ```

    The query displays a list of all installed Server Administrator packages. Those that have already been upgraded will display the new version number. Those that have not yet been upgraded will display the old version number.

3. Upgrade every RPM in the directory that was not previously upgraded, because the **srvadmin-hapi** RPM previously failed to upgrade, by running the following command:

    ```
    rpm -Uhv srvadmin-hapi*.rpm srvadmin-isvc*.rpm srvadmin-omhip*.rpm srvadmin-<any-other-packages>*.rpm
    ```

If the OpenIPMI RPM for a version of the OpenIPMI driver that meets the minimum version of the OpenIPMI driver that is required by Server Administrator is currently installed on the system, but the OpenIPMI driver modules have not yet been built and installed for the given version of the OpenIPMI driver because the **kernel-source** RPM is required but is not currently installed, the **srvadmin-hapi** RPM will fail to upgrade and will display an error message. The error message will state that you need to install the **kernel-source** RPM and build the OpenIPMI driver. In such a case, any RPMs that depend on the **srvadmin-hapi** RPM will also fail to upgrade. You must install the **kernel-source** RPM, and build and install the OpenIPMI driver modules, by performing the following additional steps:

1. For systems running Red Hat Enterprise Linux (version 3), install a copy of the **kernel-source** RPM appropriate for the kernel currently running, from your operating system installation CDs (or from some other source). On systems running Red Hat Enterprise Linux (version 4) and SUSE Linux Enterprise Server, the **kernel*-devel** RPMs provide the necessary source for building kernel modules.

2. Install the **kernel-source** RPM or **kernel*-devel** RPMs by running the following command from where you have found or copied the RPM(s):

```
rpm -ihv kernel*.rpm
```

3. Navigate to the **srvadmin/linux/supportscripts** directory.

4. Run the **srvadmin-openipmi.sh** shell script as shown below. This will build and install the OpenIPMI driver modules.

```
sh srvadmin-openipmi.sh install
```

Reattempt to upgrade the **srvadmin-hapi** RPM and any RPMs that failed to upgrade as they depend on the **srvadmin-hapi** RPM. Perform the steps described in .

Using the srvadmin-install Shell Script

1. Log on as `root` to the system running Red Hat Enterprise Linux that requires the upgrade.

2. Insert the *Dell PowerEdge Installation and Server Management* CD into the CD drive on your system. If the CD does not mount automatically, type `mount /dev/cdrom /mnt/cdrom`.

3. After the CD mounts, navigate to the subdirectory containing the shell script on the CD by typing one of the following commands:

```
cd /mnt/cdrom/srvadmin/linux/supportscripts
cd /media/cdrom/srvadmin/linux/supportscripts.
```

4. Run the following script:

```
sh srvadmin-install.sh
```

The script detects any previous version of Server Administrator. If a previous version is installed, a message appears stating the current version and installed components.

For example:

```
Server Administrator version 4.4.0 is currently installed.
Installed components are:
- srvadmin-omilcore
- srvadmin-hapi
- srvadmin-deng
- srvadmin-isvc
```

Next, the script prompts you with the following message:

```
Do you want to upgrade Server Administrator to 5.1?
Press ('y' for yes | 'Enter' to exit):
```

5. Select **y** to upgrade the system.

Server Administrator is upgraded to version 5.1.

NOTE: Just before the Server Administrator RPMs are upgraded, the **srvadmin-install.sh** shell script automatically calls the **srvadmin-openipmi.sh** shell script to ensure that a sufficient version of the OpenIPMI driver is currently installed on the system. If a sufficient version is not found, the **srvadmin-install.sh** shell script calls the **srvadmin-openipmi.sh** shell script to attempt to install a sufficient version. If the attempt fails for any reason, an appropriate error message will be displayed with instructions describing how to resolve the error. After resolving any error, you should then re-run the **srvadmin-install.sh** shell script to upgrade the managed system components.

Uninstalling Managed System Software

You can uninstall managed system software from the Red Hat Enterprise Linux or SUSE Linux Enterprise Server command line. Additionally, you can perform an unattended uninstallation on multiple systems simultaneously.

Prerequisites for Uninstalling Managed System Software

You must be logged in as `root`.

Uninstalling Managed System Software From the Red Hat Enterprise Linux or SUSE Linux Enterprise Server Command Line

An uninstallation script is installed when Server Administrator is installed. You can execute the script by typing `srvadmin-uninstall.sh` and then pressing <Enter>.

NOTE: When executed, the **srvadmin-uninstall.sh** will not attempt to uninstall the OpenIPMI driver even if the OpenIPMI driver was installed or upgraded during previous execution of the **srvadmin-install.sh** script or the **srvadmin-openipmi.sh** script.

Custom Uninstallation of Specific Components

Some individual components of Dell OpenManage can be uninstalled without uninstalling all of Dell OpenManage. Following are examples:

To uninstall only the Web server, use the command:

```
rpm -e `rpm -qa | grep srvadmin-iws`
```

To uninstall storage, use the command:

```
rpm -e `rpm -qa | grep srvadmin-storage`
```

Using Dell OpenManage with VMware® ESX Server™ Software

NOTE: Dell OpenManage installation with VMware ESX Server software requires special steps. These steps vary depending on the Dell OpenManage version and ESX Server version; only a limited number of combinations are supported.

See the *VMware Systems Compatibility Guide* located in the Resource Center at **www.dell.com/vmware** to determine the versions of ESX Server software compatible with this release of Dell OpenManage. Each ESX Server release from Dell has an associated Dell VMware ESX Server *Deployment Guide*, also posted at this Web location. Instructions for installing supported versions of Dell OpenManage available at the time of that ESX Server release are found in that ESX Server release's *Deployment Guide.* Instructions for installing any supported subsequently released versions of Dell OpenManage are posted to the same location in a separate, clearly labeled document.

Managed System Software Installation Using Third-Party Deployment Software

You can use third-party deployment software, such as Altiris Deployment Solution, to install managed system software onto supported Dell servers. To distribute and install managed system software using Altiris, start your Altiris application and import **OpenManage_Jobs.bin** located on the *Dell PowerEdge Installation and Server Management* CD at **\srvadmin\support\Altiris**. Specify a job folder into which you want to import it. You might need to modify the **Run Script** and **Copy File** tasks to match your deployment environment. Once complete, you can then schedule your job to run on the supported Dell systems that are managed from within your Altiris Deployment Solution.

Back to Contents Page

Installing Management Station Software

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- Overview
- Installation Requirements
- Installing, Upgrading, and Uninstalling Management Station Software on Systems Running Supported Windows Operating Systems
- Installing, Upgrading, and Uninstalling Management Station Software on Systems Running Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

Overview

The *Dell™ Systems Management Consoles* CD provides a setup program to install, upgrade, and uninstall Dell OpenManage™ Management Station software on your system.

Using the setup program on the *Dell Systems Management Consoles* CD, you can install and upgrade Management Station software on systems running Microsoft® Windows® operating systems. You can uninstall Dell OpenManage Management Station software with the *Dell Systems Management Consoles* CD or through the operating system on systems running supported Windows operating systems.

The Management Station applications include Dell OpenManage IT Assistant, DRAC Tools, the BMC Utilities, and the Microsoft Active Directory® Snap-in Utility.

Some Management Station applications also run on Red Hat® Enterprise Linux and SUSE® Linux Enterprise Server operating systems. See "Installing, Upgrading, and Uninstalling Management Station Software on Systems Running Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems" for more specific information.

NOTE: See the *Dell OpenManage IT Assistant User's Guide* for additional setup and configuration information.

Installation Requirements

These are general requirements for management stations. Operating system-specific installation prerequisites are listed below as part of the installation procedures for the respective applications.

Supported Operating Systems

The Management Station software runs, at a minimum, on each of the following operating systems:

- Red Hat Enterprise Linux AS, ES, and WS, (version 3) x86 and Intel® Extended Memory 64 Technology (EM64T), Update 6 (BMC management utility and DRAC Tools)

- Red Hat Enterprise Linux AS, ES, and WS, (version 4) for Intel x86 and Intel EM64T, (BMC management utility and DRAC Tools)

- Windows 2000 Server SP4 (includes Server and Advanced Server)

- Windows 2000 Professional SP4

- Windows Server™ 2003 R2 (includes Standard and Enterprise editions)

- Windows Server 2003 SP1 (Web Edition)

- Windows SBS 2003 SP1 (except IT Assistant)

- Windows Server 2003 Standard and Enterprise x64 R2 (except IT Assistant)

- Windows Storage Server 2003 R2 (includes Express, Standard, Workgroup, and Enterprise editions)

- Windows XP SP2

- SUSE Linux Enterprise Server (version 9), SP3, (BMC management utility and RAC Management Station)

- SUSE Linux Enterprise Server (version 10) Gold for Intel EM64T

NOTE: The Dell OpenManage 5.1 installer offers Multilingual User Interface support on Windows Storage Server 2003 R2, Microsoft Windows Storage Server 2003 R2, Express x64 Edition with Unified Storage, and Microsoft Windows Storage Server 2003 R2, Workgroup x64 Edition with Unified Storage. The Multilingual User Interface Pack is a set of language specific resource files that can be added to the English version of a supported Windows operating system. However, the Dell OpenManage 5.1 installer supports only five languages: German, Spanish, French, Simplified Chinese, and Japanese

For more application-specific operating systems requirements, see the documentation for that application.

System Requirements

On Windows systems, the setup program (**setup.exe**) will start the **Prerequisite Checker** on the CD to automatically analyze your system to determine if the system requirements have been met. (See "Prerequisite Checker.")

Management Station Requirements

Microsoft Software Installer (MSI) version 3.1 or later is required on your system. Dell OpenManage software detects the MSI version on your system. If the version is lower than 3.1, the Prerequisite Checker prompts you to upgrade to MSI version 3.1.

IT Assistant Database Requirements

A fresh installation of IT Assistant 8.0 prompts you to install Microsoft SQL Server™ 2005 Express Edition in the absence of a supported database on your system. SQL Server 2005 Express Edition can be installed using your *Systems Management Consoles* CD before installing the management station software. However, IT Assistant works with Microsoft SQL Server 2000 Desktop Engine (MSDE 2000), if it is already installed on your system. If you are upgrading from IT Assistant 7.*x* to 8.0, you can use the existing MSDE 2000.

Enabling CIM Discovery and Security in IT Assistant

Some applications, such as IT Assistant, can use the Common Information Model (CIM) protocol. If you use the CIM protocol, ensure that it is installed and enabled. For detailed information on configuring CIM for IT Assistant, see the *Dell OpenManage IT Assistant User's Guide*.

Installing SNMP

The SNMP service must be installed and running on the IT Assistant system. SNMP (or CIM) must also be installed on the systems that you want to discover and manage. If you attempt to install the IT Assistant on a system without SNMP, the installation program stops and prompts you to install SNMP. In addition, if you stop the SNMP service, the IT Assistant services also stop.

For information about installing SNMP on the IT Assistant management station, see the *Dell OpenManage IT Assistant User's Guide.*

Installing, Upgrading, and Uninstalling Management Station Software on Systems Running Supported Windows Operating Systems

This section explains how to install, upgrade, and uninstall Management Station software on a system that is running a supported Windows operating system. If the prerequisites are met on a system, the default features that get installed are IT Assistant, BMC Utilities, and Remote Access Controller Console.

NOTE: Dell OpenManage Array Manager Console is not available under Windows if no previous Management Station software (with Array Manager Console installed) is detected. It is only available for upgrade. Support for Array Manager Console will be discontinued in a future release.

Prerequisite Checker

The setup program (**setup.exe**) will start the Prerequisite Checker program. The setup program is located in the **windows** directory on the *Dell Systems Management Consoles* CD. The Prerequisite Checker program examines the prerequisite requirement for software features without launching the actual installation. The Prerequisite Checker program displays a status window that provides information about your system's hardware and software that might affect the installation and operation of software features.

The Prerequisite Checker displays three types of messages: informational, warning, and error messages.

- l   An informational message describes a condition of which you should be aware. It does not prevent a feature from being installed.

- l   A warning message describes a condition that prevents a software feature from being installed during **Typical** installation. It is recommended that you resolve the condition causing the warning before proceeding with the installation of the software. If you decide to continue, you can select and install the software using the **Custom** installation.

- l   An error message describes a condition of which you should be aware that prevents the software feature from being installed. You must resolve the condition causing the error before proceeding with the installation of that software feature. If you do not resolve the issue, the software feature will not be installed.

You can run the prerequisite check silently from the **\windows\PreReqChecker** directory, by executing `RunPreReqChecks.exe /s`. For further details on running the Prerequisite Checker silently, see the section titled "Prerequisite Checker."

Installing and Upgrading Management Station Software

This section explains how to install and upgrade Management Station software. The installation options are as follows:

- l   Use the setup program on the *Dell Systems Management Consoles* CD to install or upgrade IT Assistant and other Management Station software.

- l   Use the unattended installation method through the **msiexec.exe** Windows Installer Engine (see Table 5-1) to install IT Assistant and other Management Station software on multiple systems.

Typical and Custom Installations

The *Dell Systems Management Consoles* CD features a **Typical Setup** option and a **Custom Setup** option for installing IT Assistant and other Management Station software.

When you insert the *Dell Systems Management Consoles* CD in your system's CD drive, the setup program runs the Prerequisite Checker to provide information about your system's hardware and software that might affect installation and operation of the features.

You can install all of the Management Station software products that are currently installed on your system by doing the following:

1. Launch the Management Station installation.

2. Click **Install, Modify, Repair or Remove Management Station** and click **Next**.

3. Select the **Typical Setup** option.

If the prerequisites are met, IT Assistant and the DRAC Tools and BMC Utilities are installed by default, while the Active Directory Snap-in Utility is not selected by default and can be installed using the **Custom Setup** option. (For more information about how to perform a **Typical Setup**, see the *Software Quick Installation Guide*, which you can access by clicking **Info** on the task bar within the setup program.)

> **NOTE:** During a **Typical** installation, individual Management Station services will not be installed on managed systems that do not meet the specific hardware and software requirements for that service. For example, the Dell OpenManage Server Administrator Remote Access Service software module will not be installed during a **Typical** installation unless the managed system has an installed remote access controller. A user, however, can go to **Custom Setup** and select the Remote Access Service software module for installation.

When you select the **Custom Setup** option, you can deselect one or more software features that the setup program has identified as appropriate for the installed options on the system. During a **Typical Setup**, you cannot add to the list of features to install because all of the features that are appropriate for the hardware configuration are pre-selected.

The sections that follow illustrate the **Custom Setup** option using an install and upgrade of IT Assistant as an example. You can install other Management Station software using the **Custom Setup** option.

Custom Installation

The custom installation path enables you to choose specific software features to install.

> **NOTE:** Management Station and managed system services can be installed in the same or in different directories. You can select the directory for installation.

Installing Management Station

1. Log on with Administrator privileges to the system where you want to install the Management Station software features.

2. Close any open application programs.

3. Insert the *Dell Systems Management Consoles* CD into your system's CD drive.

   If the installer does not automatically start, navigate to the **windows** folder on the CD and double-click the **setup.exe** file.

   The **Dell OpenManage Management Station Prerequisite Status** screen opens and runs the prerequisite checks for the Management Station. **Prerequisite Status** displays any relevant informational, warning, or error messages. Review the messages and, if necessary, resolve any warning and error messages before proceeding with the installation.

4. Click the **Install, Modify, Repair or Remove Management Station** option.

   The **Welcome to the Install Wizard for Dell OpenManage Management Station** screen opens.

5. Click **Next**.

   The Dell Software License Agreement appears.

6. Click **Accept** if you agree.

   The **Setup Type** dialog box opens.

7. Select **Custom** and click **Next**.

   The **Custom Setup** dialog box opens.

   To select a specific Management Station software application, click the drop-down arrow beside the listed feature and select to either install or not to install the application.

   A selected feature has a hard drive icon next to it. A deselected feature has a red **X** next to it. By default, if the Prerequisite Checker finds software features with no supporting hardware, the Checker deselects them.

   To accept the default directory path to install Management Station software, click **Next**. Otherwise, click **Change** and navigate to the directory where you want to install your Management Station software, and then click **Next**.

   Make sure that **Dell OpenManage IT Assistant** is selected.

8. Click **Next** to accept the selected software features for installation.

    The **IT Assistant Custom Settings** dialog box opens.

    > **NOTE:** IT Assistant requires a default instance of a database to be installed on the system. IT Assistant cannot use a named instance of database.

    > **NOTE:** Microsoft SQL Server 2005 Express requires Microsoft Data Access components 2.8 (MDAC 2.8) and .NET 2.0 Runtime to be installed. The prerequisite checker utility will prompt you to install MDAC 2.8, If MDAC 2.8 is not installed on your system.

9. Modify the **Custom Settings for IT Assistant** fields as necessary.

10. Click **Next** to accept the custom settings for IT Assistant.

    The **Ready to Install the Program** dialog box opens.

> **NOTE:** You can cancel the installation process by clicking **Cancel.** The installation rolls back the changes that you made. If you click **Cancel** at a later point in the installation process, the installation may not roll back properly, leaving the system with an incomplete installation. See "System Recovery on Failed Installation" for more information.

11. Click **Install** to install the selected software features.

    The **Installing Dell OpenManage Management Station** screen opens.

    When the selected features are installed, the **Install Wizard Completed** dialog box opens.

12. Click **Finish** to leave the Management Station installation.

Upgrade

The *Dell Systems Management Consoles* CD features an **Upgrade** option for upgrading IT Assistant and other Management Station software.

When you insert the *Dell Systems Management Consoles* CD into your system's CD drive, the prerequisite checker program checks your system.

To upgrade all of the Management Station software products that are currently installed on your system, click **Install, Modify, Repair or Remove Management Station** and select **Next**.

All features appropriate for your system are pre-selected during an upgrade.

The following procedures describe how to upgrade IT Assistant and other management station software.

> **NOTE:** There is no Windows Installer Patch (.MSP) support for the latest version of the Management Station software as it is a major upgrade. You can use MSP files to upgrade only in minor upgrades.

Custom Upgrade

1. Insert the *Dell Systems Management Consoles* CD into your system's CD drive.

    If the installer does not automatically start, navigate to the **windows** folder on the CD and double-click the **setup.exe** file.

    The **Dell OpenManage Management Station Prerequisite Status** screen opens and runs the prerequisite checks for the Management Station. **Prerequisite Status** displays any relevant informational, warning, or error messages. Review the messages and, if necessary, resolve any problems before proceeding with the installation.

2. Click the **Install, Modify, Repair or Remove Management Station** option.

    The **Welcome to the Install Wizard for Dell OpenManage Management Station** screen opens.

3. Click **Next**.

    The **Installing Dell OpenManage Management Station** screen opens. Messages provide the status and progress of the software features being installed or upgraded.

    When the selected features are installed or upgraded, the **Install Wizard Completed** dialog box opens.

4. Click **Finish** to leave the Management Station installation.

Custom Modify

1. Click the **Start** button, point to **Settings→ Control Panel**.

2. Double-click **Add/Remove Programs**.

3. Click **Dell OpenManage Management Station** and click **Change**.

   The **Welcome to the Install Wizard for Dell OpenManage Management Station** dialog box opens.

4. Click **Next**.

   The **Program Maintenance** dialog box opens.

5. Select the **Modify** option and click **Next**.

   The **Custom Setup** dialog box opens.

6. To select a specific Management Station software application, click the drop-down arrow beside the listed feature and select either to install the application or not to install it.

   A selected feature has a hard drive icon next to it. A deselected feature has a red X next to it. By default, if the Prerequisite Checker finds software features with no supporting hardware, the checker deselects them.

7. Click **Next** to accept the selected software features for installation.

   The **Ready to Modify the Program** dialog box opens.

8. Click **Install** to install the selected software features.

   The **Installing Dell OpenManage Management Station** screen opens. Messages provide the status and progress of the software features being installed.

   When the selected features are installed, the **Install Wizard Completed** dialog box opens.

9. Click **Finish** to leave the Management Station installation.

Custom Repair

1. Click the **Start** button, point to **Settings→ Control Panel**.

2. Double-click **Add/Remove Programs**.

3. Click **Dell OpenManage Management Station** and click **Change**.

   The **Welcome to the Install Wizard for Dell OpenManage Management Station** dialog box opens.

4. Click **Next**.

   The **Program Maintenance** dialog box opens.

5. Select the **Repair** option and click **Next**.

   The **Ready to Repair the Program** dialog box opens.

6. Click **Install** to install the selected software features.

   The **Installing Dell OpenManage Management Station** screen opens. Messages provide the status and progress of the software features being installed.

   When the selected features are installed, the **Install Wizard Completed** dialog box opens.

7. Click **Finish** to leave the Management Station installation.

System Recovery on Failed Installation

If a software installation utility encounters a fatal error during setup, your system may become unstable. To address this problem, Dell OpenManage installers provide the ability to roll back, or return, the system to its fully-working condition prior to the failed installation.

The Windows Installer service provides Dell OpenManage installers the ability to roll back by maintaining an *undo* operation for every operation that it performs during an installation, uninstallation, or any other configuration change. If some aspect of the installation fails during an installation session, the Windows Installer service can precisely return the system to its previous state. This feature includes restoration of deleted or overwritten files, registry keys, and other resources. Files that are deleted or overwritten during the course of an installation or removal are temporarily saved to a backup location, so they can be restored if necessary. After an installation finishes successfully, all temporary backup files are deleted.

An installation cannot be rolled back once it has successfully completed. A transacted installation is intended as a safety net that protects the system during a given installation session. If you want to remove an installed application, for example, you should uninstall that application.

When upgrading from Dell OpenManage software version 4.3 to version 5.x, an error will roll back the system to its previous state.

NOTE: Installations, uninstallations, and upgrades canceled by the administrator during installer cleanup or after the installation transaction is completed will not be rolled back.

Performing an Unattended Installation of Management Station Software

The *Dell Systems Management Consoles* CD features a **Typical Setup** option and a **Custom Setup** option for the unattended installation procedure.

Unattended installation allows you to install Management Station Software simultaneously on multiple systems. You can perform an unattended installation by creating an unattended installation package that contains all of the necessary Management Station files. The unattended installation option also provides several features that enable you to configure, verify, and view information about unattended installations.

The unattended installation package is distributed to the remote systems using a software distribution tool from an independent software vendor (ISV). When the package is distributed, the installation script installs the software.

Unattended Installation Features

Unattended installation provides the following features:

- l   A set of optional command line settings to customize an unattended installation

- l   Customization parameters to designate specific software features for installation

- l   A prerequisite checker program that examines the dependency status of selected software features without having to perform an actual installation

Creating and Distributing the Typical Unattended Installation Package

The **Typical Setup** unattended installation option uses the *Dell Systems Management Consoles* CD as the unattended installation package. The **msiexec.exe /i MgmtSt.msi /qb** command accesses the *Dell Systems Management Consoles* CD to accept the software license agreement and install all required Management Station software products on selected remote systems. The **msiexec.exe /i MgmtSt.msi /qb** command installs Management Station software on each remote system, based on the system's hardware and software configuration.

You can make the *Dell Systems Management Consoles* CD image available to the remote system either by distributing the entire contents of the CD, or by mapping a drive from the target system to the location of the CD image.

Mapping a Drive to Act as the Typical Unattended Installation Package

To map a drive to act as the Typical unattended installation package, do the following:

1. Share an image of the *Dell Systems Management Consoles* CD with each remote system on which you want to install Management Station.

    You can accomplish this task by directly sharing the CD or by copying the entire CD to a drive and sharing the copy.

2. Create a script that maps a drive from the remote systems to the shared drive described in step 1. This script should execute the following command after you have mapped the drive:

    msiexec.exe /i *Mapped Drive*\windows\ManagementStation\MgmtSt.msi /qb

3. Configure your ISV distribution software to distribute and execute the script created in step 2.

4. Distribute this script to the target systems by using your ISV software distribution tools.

    The **msiexec.exe /i *Mapped Drive*\windows\ManagementStation\MgmtSt.msi /qb** command then installs Management Station on each remote system.

    NOTE: IT Assistant requires a supported database to be installed before IT Assistant can be installed. See **CD drive:\Windows\ManagementStation\support database** to find the sample batch file and the necessary utilities.

Distributing the Entire CD as the Typical Unattended Installation Package

To distribute the entire CD as the Typical unattended installation package, do the following:

1. Distribute the entire image of the *Dell Systems Management Consoles* CD to your target systems.

2. Configure your ISV distribution software to execute the **msiexec.exe /i *CD Drive*\windows\ManagementStation\MgmtSt.msi /qb** command from the *Dell Systems Management Consoles* CD image.

The **msiexec.exe /i *CD Drive*\windows\ManagementStation\MgmtSt.msi /qb** command executes from the CD to install Management Station on each

remote system.

Creating and Distributing Custom Unattended Installation Packages

To create a custom unattended installation package for distribution, simply copy the **windows** directory from the CD onto the system's hard drive.

Create a batch script that will execute the installation using the Windows Installer Engine (**msiexec.exe**). For example:

```
msiexec.exe /i MgmtSt.msi ADDLOCAL=ITA,RACMS,ADS /qb
```

NOTE: For a customized unattended installation, each required feature must be included as a command line interface (CLI) parameter for it to be installed.

Also, put the batch script in the **windows** directory on the system hard drive.

See "Customization Parameters" for additional details and available feature identification.

Distributing Custom Unattended Installation Packages

NOTE: The **MgmtSt.msi** installation package for Management Station used in the **Custom Setup** unattended installation as described in the previous section is located in the **\windows\ManagementStation** directory.

1. Configure your ISV distribution software to execute the batch script once your installation package has been distributed.

2. Use your ISV distribution software to distribute the custom unattended installation package to the remote systems.

The following command executes from the script to install Management Station, along with specified features, on each remote system:

```
msiexec.exe /i System Drive\windows\ManagementStation\MgmtSt.msi ADDLOCAL=ITA,RACMS,ADS /qb
```

Specifying Log File Locations

Run the following command to perform an unattended installation while specifying the log file location:

```
msiexec.exe /i MgmtSt.msi /l*v "C:\openmanage\logs\MgmtSt.log"
```

Optional Command Line Settings

Table 5-1 shows the optional command line settings available for the **msiexec.exe**. Type the optional settings on the command line after **msiexec.exe** with a space between each setting.

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

Table 5-1. Command Line Settings for MSI Installer

Setting	Result
/i <Package|Product Code>	Installs or configures a product. /i MgmtSt.msi – This command installs the Server Administrator software.
/x <Package|Product Code>	Uninstalls a product. /x MgmtSt.msi – This command uninstalls the Server Administrator software.
/q[n|b|r|f]	Sets the User Interface (UI) level. **/q** or **/qn** – no UI. This option is used for silent and unattended installation. **/qb** – basic UI. This option is used for unattended but not silent installation. **/qr** – reduced UI. This option is used for unattended installation while displaying a modal dialog box showing install progress. **/qf** – full UI. This option is used for standard attended installation.
/f[p|o|e|d|c|a|u|m|s|v] <Package|ProductCode>	Repairs a product. **/fp** – This option reinstalls a product only if a file is missing. **/fo** – This option reinstalls a product if a file is missing or if an older version of a file is installed. **/fe** – This option reinstalls a product if a file is missing or an equal or older version of a file is installed. **/fd** – This option reinstalls a product if a file is missing or a different version of a file is installed.

	/fc – This option reinstalls a product if a file is missing or the stored checksum value does not match the calculated value.
	/fa – This option forces all files to be reinstalled.
	/fu – This option rewrites all required user-specific registry entries.
	/fm – This option rewrites all required system-specific registry entries.
	/fs – This option overwrites all existing shortcuts.
	/fv – This option runs from the source and re-caches the local package. Do not use the **/fv** reinstall option for the first installation of an application or feature.
INSTALLDIR=<path>	This command installs a product to a specific location. If you specify an installation directory with this switch, it must be created manually prior to executing the CLI install commands or they will fail with no error or message as to why they failed. `/i MgmtSt.msi INSTALLDIR=c:\OpenManage /qn` – This command installs a product to a specific location using **c:\OpenManage** as the install location.

An example command with MSI is `msiexec.exe /i MgmtSt.msi /qn`. This command installs Management Station features on each remote system, based on the systems' hardware and software configuration, silently and without asking for prompts.

Uninstalling Management Station Software

You can uninstall Management Station software features by using the *Dell Systems Management Consoles* CD or your operating system. Additionally, you can simultaneously perform an unattended uninstallation on multiple systems.

Uninstall Management Station Software Using the Dell Systems Management Consoles CD

To uninstall the Management Station software using the *Dell Systems Management Consoles* CD, do the following:

1. Insert the *Dell Systems Management Consoles* CD into your system's CD drive.

   If the CD does not automatically start the setup program, go to your system's desktop, double-click **My Computer**, double-click the **CD drive** icon, double-click the **windows** folder and double-click the **setup.exe** file.

   The **Dell OpenManage Management Station Prerequisite Status** screen opens and runs the prerequisite checks for the Management Station. **Prerequisite Status** displays any relevant informational, warning, or error messages.

2. Click the **Install, Modify, Repair or Remove Management Station** option.

   The **Welcome to the Install Wizard for Dell OpenManage Management Station** screen opens.

3. Click **Next**.

   The **Program Maintenance** dialog box opens. This dialog allows you to modify, repair, or remove the program.

4. Select the **Remove** option and click **Next**.

   The **Remove the Program** dialog box opens.

5. Click **Remove**.

   The **Uninstalling Dell OpenManage Management Station** screen opens. Messages provide the status and progress of the software features being uninstalled.

   When the selected features are uninstalled, the **Install Wizard Completed** dialog box opens.

6. Click **Finish** to exit the Management Station uninstallation.

   All Management Station features will be uninstalled.

Uninstalling Management Station Software Features Using the Microsoft Windows Operating System

To uninstall the Management Station software features using Windows, do the following:

1. Click the **Start** button and point to **Settings→ Control Panel**.

2. Double-click **Add/Remove Programs**.

3. Click **Dell OpenManage Management Station** and click **Remove**.
   The **Add or Remove Programs** question box opens.

4. Click **Yes** to confirm uninstallation of Management Station.

    The **Uninstall Summary** screen opens. Messages provide the status and progress of the software features being uninstalled.

    All Management Station features will be uninstalled.

Performing an Unattended Uninstallation of Management Station Software

The *Dell Systems Management Consoles* CD features a procedure for the unattended uninstallation of the Management Station software.

Unattended uninstallation enables you to uninstall Management Station software simultaneously from multiple systems. The unattended uninstallation package is distributed to the remote systems using a software distribution tool from an ISV. When the package is distributed, the uninstallation script executes to uninstall the software.

Distributing the Unattended Uninstallation Package

The *Dell Systems Management Consoles* CD is preconfigured to act as the unattended uninstallation package. To distribute the package to one or more systems, perform the following steps:

1. Configure your ISV distribution software to execute the **msiexec.exe /x** *CD Drive***\windows\ManagementStation\MgmtSt.msi /qb** command after the unattended uninstallation package has been distributed.

2. Use your ISV distribution software to distribute the Typical unattended uninstallation package to the remote systems.

3. The **msiexec.exe /x** *CD Drive***\windows\ManagementStation\MgmtSt.msi /qb** command executes to uninstall IT Assistant and other management station software on each remote system.

Unattended Uninstall Command Line Settings

Table 5-1 shows the unattended uninstallation command line settings available for unattended uninstallation. Type the optional settings on the command line after
`msiexec.exe /x MgmtSt.msi` with a space between each setting.

For example, running `msiexec.exe /x MgmtSt.msi /qb` runs the unattended uninstallation and displays the unattended installation status while it is running.

Running `msiexec.exe /x MgmtSt.msi /qn` runs the unattended uninstallation, but silently (without status displays).

Customization Parameters

The ADDLOCAL, REINSTALL, and REMOVE CLI parameters provide a way to specify the exact software features to install, reinstall, or uninstall when running silently or unattended. With the customization parameters, you can selectively install, reinstall, or uninstall software features for different systems using the same unattended installation package. For example, you can choose to install IT Assistant, but not Remote Access Controller Management Station on a specific group of systems. You can also choose to uninstall one or multiple features on a specific group of systems.

Table 5-2. Feature IDs for the Management Station

Feature ID	Description
ADS	Active Directory Snap-in Utility
BMU	Baseboard Management Controller Management Utility
ITA	IT Assistant
RACMS	DRAC Tools

NOTE: You have to type the ADDLOCAL, REINSTALL, and REMOVE CLI parameters in upper case as they are case-sensitive.

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

    msiexec.exe /i MgmtSt.msi ADDLOCAL=ITA /qb

This command runs the installation for Management Station and installs only IT Assistant, in an unattended and verbose (with messages) mode.

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

    msiexec.exe /i MgmtSt.msi REINSTALL=RACMS /qb

This command runs the installation for only the Management Station and reinstalls Remote Access Controller Management Station, in an unattended and verbose mode.

The REMOVE customization parameter can be included on the command line and assigned the feature ID (or IDs) of the software feature that you would like to uninstall. An example is

    msiexec.exe /i MgmtSt.msi REMOVE=RACMS /qb

This command runs only the installation for Management Station and uninstalls Remote Access Controller Management Station, in an unattended and verbose mode.

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

    msiexec.exe /i MgmtSt.msi ADDLOCAL=ADS REINSTALL=ITA REMOVE=BMC /qb

This command runs the installation for Management Station and simultaneously installs Active Directory Snap-in Utility, reinstalls IT Assistant, and uninstalls the Baseboard Management Controller. This execution will be in an unattended and verbose mode.

> **NOTE:** A Dell OpenManage Globally Unique Identifier (GUID) is 128 bits long. The product GUID uniquely identifies the application. In this case the product GUID for Dell OpenManage Management Station is {DA60872C-9147-4A6E-9AEF-95BAB5EF3A3B}.

Supported Management and Alerting Agents

With Dell OpenManage software, *agent* is a general term applied to the software features of systems management instrumentation. Degrees of support vary among agents. For example, IT Assistant automatically discovers, displays, receives alerts from, and can perform actions on the systems managed by Server Administrator, but IT Assistant can only receive alerts from certain storage device agents. See the *Dell OpenManage IT Assistant User's Guide* for a list of Agents supported by IT Assistant.

Upgrading IT Assistant After Migrating to Windows Server 2003

If a system with IT Assistant installed is migrated to Windows Server 2003, then upgraded to a more recent version of IT Assistant, a problem may occur due to encryption differences between Windows Server 2003 and earlier versions of Windows.

After an upgrade on a system that has been migrated to Windows Server 2003, systems configured with the CIM protocol might no longer be discovered. If this issue occurs, reset the password for the CIM user. In the IT Assistant user interface, go to **Discovery and Monitoring,** select **Ranges** and right-click **Include Ranges**. Click **New Include Range** to run the New Discovery Wizard, where you can specify the new CIM user name in the **CIM Configuration** window. See the IT Assistant online help for additional information.

Other Known Issues for Microsoft Installations

- l Directories might be left behind during an uninstall for reasons such as sharing violations or open user interface connections. It is recommended that you close all open interface sessions before you perform an uninstallation. Manually remove directories left behind in the default installation directory or the user-specified installation directory. You might also have to manually remove the registry entries under **HKEY_LOCAL_MACHINE\SOFTWARE\Dell Computer Corporation\Dell OpenManage IT Assistant**.

Installing, Upgrading, and Uninstalling Management Station Software on Systems Running Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

Installing Management Station Software

Only the BMC and the RAC features of the Management Station suite of software can be used on a management station running Red Hat Enterprise Linux and SUSE Linux Enterprise Server.

To install the BMC Management Utility onto a management station, perform the following steps:

1. Log on as `root` to the system where you want to install the Management Station features.

2. If necessary, mount the *Dell Systems Management Consoles* CD to a desired location using the `mount` command or a similar command.

3. Navigate to the **/linux/bmc** directory and install the BMC software using the rpm commands specific to the operating system:

    - l For systems running Red Hat Enterprise Linux, use `osabmcutil*-RHEL-*.rpm`, for example, `rpm -Uvh osabmcutil*-RHEL-*.rpm`.

    - l For systems running SUSE Linux Enterprise Server, use `osabmcutil*-SUSE-*.rpm`, for example, `rpm -Uvh osabmcutil*-SUSE-*.rpm`.

To install the DRAC Tools feature, perform the following steps:

1. Log on as `root` to the system where you want to install the Management Station features.

2. If necessary, mount the CD to a desired location using the `mount` command or a similar command.

3. Navigate to the **/linux/rac** directory and install the RAC software using the `rpm -ivh *.rpm` command.

Upgrading Management Station Software

To upgrade the BMC Management Utility onto a management station, perform the following steps:

1. Log on as `root` to the system where you want to upgrade the Management Station features.

2. If necessary, mount the *Dell Systems Management Consoles* CD to a desired location using the `mount` command or a similar command.

3. Navigate to the **/linux/bmc** directory and upgrade the BMC software using the rpm commands specific to the operating system:
   - For systems running Red Hat Enterprise Linux, use `osabmcutil*-RHEL-*.rpm`, for example, `rpm -Uvh osabmcutil*-RHEL-*.rpm`.
   - For systems running SUSE Linux Enterprise Server, use `osabmcutil*-SUSE-*.rpm`, for example, `rpm -Uvh osabmcutil*-SUSE-*.rpm`.

To upgrade the DRAC Tools feature, perform the following steps:

1. Log on as `root` to the system where you want to upgrade the Management Station features.

2. If necessary, mount the CD to a desired location using the `mount` command or a similar command.

3. Navigate to the **/linux/rac** directory and upgrade the RAC software using the `rpm -Uvh *.rpm` command.

Uninstalling Management Station Software

To uninstall the BMC Management Utility onto a management station, perform the following steps:

1. Log on as `root` to the system where you want to install the Management Station features.

2. Use the rpm query command to determine which version of the BMC Management Utility is installed. Use the `rpm -qa | grep osabmcutil` command.

3. Verify that is the version to be uninstalled, and if so, uninstall the feature by using the `rpm -e `rpm -qa | grep osabmcutil`` command.

To uninstall the DRAC Tools feature, perform the following steps:

1. Log on as `root` to the system where you want to install the Management Station features.

2. Use the rpm query command to determine which version of the DRAC Tools is installed. Use the `rpm -qa | grep mgmtst-racadm` command.

3. Verify that is the version to be uninstalled, and if so, uninstall the feature by using the `rpm -e `rpm -qa | grep mgmtst-racadm`` command.

Using Server Assistant to Install an Operating System

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- ● Overview
- ● Before You Begin

Overview

Dell OpenManage™ Server Assistant provides a streamlined and time-saving installation procedure by guiding you through an easy-to-follow, step-by-step process for installing the Microsoft® Windows®, Red Hat® Enterprise Linux, and SUSE® Linux Enterprise Server operating systems. Server Assistant is used to install operating systems for systems being installed as managed systems.

When you use Server Assistant to install Windows, Red Hat Enterprise Linux, or SUSE Linux Enterprise Server operating systems, Server Assistant automatically copies the relevant Dell OpenManage Server Administrator installation files onto the hard drive and places **Install Server Administrator** and **Delete Server Administrator Installation Files** icons on the desktop.

> **NOTE:** On a system running a Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system, you will be prompted to install Server Administrator on first boot after the operating system is installed.

Before You Begin

Installation Requirements

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

Supported Operating Systems (Minimum Levels)

- Red Hat Enterprise Linux AS, ES, and WS, (version 3) x86, Update 6
- Red Hat Enterprise Linux AS, ES, and WS, (version 3) for Intel® Extended Memory 64 Technology (Intel EM64T) Update 6
- Red Hat Enterprise Linux AS, ES, and WS, (version 4) for Intel x86
- Red Hat Enterprise Linux AS, ES, and WS, (version 4) for Intel EM64T
- Windows 2000 Server SP4 (includes Server and Advanced Server)
- Windows Server™ 2003 R2 (includes Standard and Enterprise editions)
- Windows Server 2003 SP1(Web Edition)
- Windows SBS 2003 SP1 (except IT Assistant)
- Windows Server 2003 x64 R2 (includes Standard and Enterprise Editions)
- Windows Storage Server 2003 R2 (includes Express, Standard, Workgroup, and Enterprise Editions)
- SUSE Linux Enterprise Server (version 9) SP3 for Intel EM64T
- SUSE Linux Enterprise Server (version 10) Gold, for Intel EM64T

Installing Your Operating System

Perform the following steps to determine if an operating system has been installed on your system:

1. Ensure that the keyboard, mouse, and monitor are connected to your system, and turn on your system.

2. Read and accept the software license agreement to continue.

   If a message appears and states that bootable drives do not exist or that an operating system was not found, then an operating system has not been installed on your system. Have your operating system CD available and continue with the next steps.

   If an operating system has been preinstalled on your system, it is not necessary to continue with this process. Locate the operating system's *Installation Instructions* document that was provided with your system and follow those instructions to complete the installation process.

Perform the following steps to install an operating system on your system:

1. Insert the *Dell™ PowerEdge™ Installation and Server Management* CD into the CD drive and restart your system.

2. Select **Server Setup** on the **Server Assistant** main page.

3. Follow the step-by-**step instructions to configure your hardware and to install your operating system.**

   📝 **NOTE:** Remove the CD when you restart the system, or Server Assistant will start again.

For additional information about installing RAID, see *Getting Started With RAID* on the *Documentation* CD.

You can use the **Install Server Administrator** icon to install Server Administrator without the installation CD. On a system running Windows, clicking this icon brings up the standard installation interface. On a system running a Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system, clicking this icon runs the Server Administrator custom installation script.

If you do not want to install Server Administrator, or you want to remove the installation files, you can click the **Delete Server Administrator Installation Files** icon. After you confirm that you want to continue, all Server Administrator files, including the icons, are removed.

Installing Managed System Software on Microsoft® Windows® Operating Systems

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- Overview
- Before You Begin
- Installation Requirements
- Installation Procedures
- Managed System Software Installation Using Third-Party Deployment Software

Overview

You can install managed system software using several methods. The *Dell™ PowerEdge™ Installation and Server Management* CD provides a setup program to install, upgrade, and uninstall managed system software features on your managed systems. You can install the software on multiple systems through an unattended installation across a network.

The managed system features that you can install include Dell OpenManage™ Server Administrator, the Intel® SNMP agent, and the Broadcom SNMP agent.

From within Server Administrator, you can choose the Server Administrator Web server (not choosing it restricts you to use Server Administrator only from its command line interface), Remote Access Service, and Storage Management Service subfeatures.

> **NOTE:** DRAC III, DRAC 4, and DRAC 5 cannot be used together.

Dell PowerEdge Installation and Server Management CD

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

Using the setup program in the Windows directory on the *Dell PowerEdge 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 operating systems, you can uninstall the features through the operating system.

> **NOTE:** See the **readme_ins.txt** file on the *Dell PowerEdge Installation and Server Management* CD for a list of the systems that are currently supported.

Unattended and Scripted Silent Installation

You can use the *Dell PowerEdge Installation and Server Management* CD to perform an unattended and scripted silent installation of the managed system features on systems running supported Windows operating systems. Additionally, you can install and uninstall the features from the command line on systems running supported Windows operating systems.

Before You Begin

- Read the installation requirements section below to ensure that your system meets or exceeds the minimum requirements.

- Read the *Dell OpenManage Server Administrator Compatibility Guide*. This guide contains compatibility information about Server Administrator installation and operation on various hardware platforms running supported Windows, Red Hat® Enterprise Linux, and SUSE® Linux Enterprise Server operating systems.

- Read the installation **readme_ins.txt** file on the *Dell PowerEdge Installation and Server Management* CD. This readme file contains the latest information about new features, in addition to information about known issues.

- Read the Server Administrator readme file on the *Dell PowerEdge Installation and Server Management* CD. This readme 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 general requirements for Server Administrator.

Supported Operating System Versions

Server Administrator supports each of the following operating systems:

- Windows 2000 Server SP4 (includes Server and Advanced Server)

l   Windows Server™ 2003 R2 (includes Standard and Enterprise editions)

l   Windows Server 2003 SP1 (Web Edition)

l   Windows Server 2003 Standard and Enterprise x64 R2 (except Remote Access Controller III and IT Assistant)

l   Windows Storage Server 2003 R2 (includes Express, Standard, Workgroup, and Enterprise editions)

NOTE: The Dell OpenManage 5.1 installer offers Multilingual User Interface support on Windows Storage Server 2003 R2, Microsoft Windows Storage Server 2003 R2, Express x64 Edition with Unified Storage, and Microsoft Windows Storage Server 2003 R2, Workgroup x64 Edition with Unified Storage. The Multilingual User Interface Pack is a set of language specific resource files that can be added to the English version of a supported Windows operating system. However, the Dell OpenManage 5.1 installer supports only five languages: German, Spanish, French, Simplified Chinese, and Japanese

NOTE: See the Server Administrator **readme_ins.txt** file on the *Dell PowerEdge Installation and Server Management* CD or the *Dell OpenManage Server Administrator Compatibility Guide* on the *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 managed system. You can then manage each system running Server Administrator locally or remotely through a supported Web browser.

The **setup.exe** utility calls the Prerequisite Checker on the CD to determine if the system requirements have been met. (For more information see the section titled "Prerequisite Checker.")

Managed System Requirements

l   One of the supported operating systems

l   A minimum of 64 MB of RAM

l   A minimum of 256 MB of free hard drive space

l   Administrator rights

l   A TCP/IP connection on the managed system and the Management Station to facilitate remote system management

l   One of the supported Systems Management Protocol Standards

l   A mouse, keyboard, and monitor to manage a system locally. The monitor must have a minimum screen resolution of 800 x 600. The recommended screen resolution setting is 1024 x 768.

l   The Server Administrator Remote Access Service requires that a remote access controller (RAC) be installed on the system to be managed. See the *Dell Remote Access Controller 4 User's Guide* or the *Dell Embedded Remote Access Controller/MC User's Guide* for complete software and hardware requirements.

NOTE: The RAC software is installed as part of the **Typical Setup** and **Custom Setup** installation options when installing managed system software from the *Dell PowerEdge 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.

l   The Server Administrator Storage Management Service requires that Dell OpenManage Storage Management be installed on the system in order to be properly managed. See the *Dell OpenManage Server Administrator User's Guide* for complete software and hardware requirements.

l   Microsoft Software Installer (MSI) version 3.1 or later

   NOTE: Dell OpenManage software detects the MSI version on your system. If the version is lower than 3.1, the Prerequisite Checker prompts you to upgrade to MSI version 3.1.

Supported Systems Management Protocol Standards

A supported systems management protocol standard must be installed on the managed system before installing Server Administrator. On supported Windows operating systems, Server Administrator supports the Common Information Model/Windows Management Instrumentation (CIM/WMI) and Simple Network Management Protocol (SNMP). CIM and WMI are always installed, and SNMP is available from the operating system installation media.

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

Windows Server 2003 R2 and the R2 IPMI Device Driver

The information in this section is applicable only to PowerEdge *x8xx* systems and PowerEdge *x9xx* systems.

Windows Server 2003 R2 and Windows Storage Server R2 contain an optional component called Hardware Management. This component contains an IPMI driver. During installation, the component installs and enables its IPMI driver.

NOTE: On PowerEdge *x8xx* systems, after you install the Hardware Management component, you must perform an additional step to get the R2 IPMI driver installed.

When Server Administrator starts, it first determines if the Windows Server 2003 R2 IPMI driver is enabled. If enabled, then Server Administrator uses the Windows Server 2003 R2 IPMI driver to provide its IPMI-based functionality. If the Windows Server 2003 R2 IPMI driver is not enabled, Server Administrator uses its own internal IPMI support to provide its IPMI-based functionality. For Server Administrator, it is recommended that you use the Windows Server 2003

R2 IPMI driver instead of the internal IPMI support. If your system is running Windows Server 2003 R2 or Windows Storage Server R2, it is recommended that after you install or upgrade Server Administrator, you also install the optional Hardware Management component of R2.

To install the Windows Server 2003 R2 IPMI driver on PowerEdge *x8xx* systems, perform the following additional step:

      l   From a command shell, execute the following command:

         `Rundll32 ipmisetp.dll, AddTheDevice`

         NOTE: This step is not required on PowerEdge *x9xx* systems.

After you install the Hardware Management component of Windows Server 2003 R2 operating system and have performed the additional step to install the Windows Server 2003 R2 IPMI driver (on PowerEdge *x8xx* systems), you must also restart the **DSM SA Data Manager** service so that Server Administrator can switch over from using its own internal IPMI support to using the Windows Server 2003 R2 IPMI driver. To restart the service, you can either manually restart the service or reboot the system.

At a later date, if you uninstall the Windows Server 2003 R2 IPMI driver either directly by manually uninstalling it or by uninstalling the Hardware Management component (which will uninstall the driver), you must restart the **DSM SA Data Manager** service so that Server Administrator can switch over from using the Windows Server 2003 R2 IPMI driver to using its own internal IPMI support. To restart the service, you can either manually restart the service or reboot the system.

Digital Certificates

All Server Administrator packages for Microsoft are digitally signed with a Dell certificate that helps guarantee the integrity of the installation packages. If these packages are repackaged, edited, or manipulated in other ways, the digital signature will be invalidated. This manipulation results in an unsupported installation package and the Prerequisite Checker will not allow you to install the software.

Installation Procedures

This section explains how to install, upgrade, and uninstall Server Administrator on a system that is running a supported Windows operating system.

Prerequisites for Installing or Upgrading Server Administrator

You must have Administrator privileges.

If you want to use supporting agents for the Simple Network Management Protocol (SNMP), you must install the operating system support for the SNMP standard before or after you install Server Administrator. For more information about installing SNMP, see the installation instructions for the operating system you are running on your system.

      NOTE: During a Typical installation, individual Server Administrator services will not be installed on managed systems that do not meet the specific hardware and software Installation Requirements for that service. For example, the Server Administrator Remote Access Service software module will not be installed during a Typical installation unless the managed system has an installed remote access controller. You can, however, go to **Custom Setup** and select the Remote Access Service software module for installation.

Prerequisite Checker

The setup program (**setup.exe**) will start the Prerequisite Checker program. The setup program is located in the **\srvadmin\Windows** directory on the *Dell PowerEdge Installation and Server Management* CD. The Prerequisite Checker program examines the prerequisite requirements for software features without launching the actual installation. This program displays a status window that provides information about your system's hardware and software that might affect the installation and operation of software features.

The Prerequisite Checker displays three types of messages: informational, warning, and error messages.

An informational message describes a condition of which you should be aware. It does not prevent a feature from being installed.

A warning message describes a condition that prevents a software product from being installed during Typical installation. It is recommended that you resolve the condition causing the warning before proceeding with the installation of that software. If you decide to continue, you can select and install the software using the Custom installation. For example, if an Intel network interface card (NIC) is not detected on the system, you will see the following message:

      `An Intel(R) NIC was not detected on this system. This will disable the "Typical" installation of the Intel(R) SNMP Agent.`

      `Use the "Custom" installation setup type later during installation to select this feature if you have an Intel(R) NIC installed.`

An error message describes a condition of which you should be aware that prevents the software feature from being installed. You must resolve the condition causing the error before proceeding with the installation of the software feature. If you do not resolve the issue, the software feature will not be installed.

You can run the prerequisite check silently by running `RunPreReqChecks.exe /s` from the **srvadmin\windows\PreReqChecker** directory. For further details see "Prerequisite Checker."

Installing and Upgrading Server Administrator

This section explains how to install and upgrade the Server Administrator using two installation options:

      l   Use the setup program in the **windows** directory on the *Dell PowerEdge Installation and Server Management* CD to install or upgrade Server Administrator and other managed system software.

l   Use the unattended installation method through the Windows Installer Engine **msiexec.exe** (see Table 6-1) to install Server Administrator and other managed system software on multiple systems.

NOTE: For modular systems, you must install Server Administrator on each server module installed in the chassis.

NOTE: You can go to **Add/Remove Programs** to find out what features are currently installed.

NOTE: You can upgrade from Dell OpenManage software version 4.3 to 5.1 through a full MSI Installation only.

NOTE: After you install Server Administrator on PowerEdge 1650, 2650, and 4600 systems, you may be prompted to reboot your system if you have chosen to install Storage Management Service.

Typical and Custom Installations

The *Dell PowerEdge Installation and Server Management* CD features a **Typical Setup** option and a **Custom Setup** option for installing Server Administrator and other managed system software.

When you insert the *Dell PowerEdge Installation and Server Management* CD in your system's CD drive, the setup program calls the Prerequisite Checker, which uses your system's PCI bus to search for installed hardware such as controller cards.

When you launch the Server Administrator installation from the Prerequisite Checker and select the **Typical Setup** option, the setup program installs or upgrades all of the managed system software features that are appropriate for your particular system's hardware configuration. For more information about how to perform a **Typical Setup**, see the *Quick Installation Guide*. You can access the *Quick Installation Guide* by clicking **Quick Install Guide** on the menu bar within the Prerequisite Checker user interface.

When you select the **Custom Setup** option, you can deselect one or more software features that the install program has identified as appropriate for the installed options on the system. During a **Typical Setup**, you cannot add to the list of features to install because all the features that are appropriate for the hardware configuration are preselected. The Server Administrator Storage Management Service is installed by default during **Typical Setup**.

Custom Installation

The sections that follow show how to install and upgrade Server Administrator and other managed system software using the **Custom Setup** option.

NOTE: Management station and managed system services can be installed in the same or in different directories. You can select the directory for installation.

1. Log on with Administrator privileges to the system where you want to install the system management software features.

2. Close any open application programs and disable any virus-scanning software.

3. Insert the *Dell PowerEdge Installation and Server Management* CD into your system's CD drive.

   If the CD does not automatically start the setup program, go to your system's desktop, double-click **My Computer** (or open Windows Explorer), double-click the CD drive icon, double-click the **srvadmin** folder, double-click the **windows** folder, and double-click the **setup.exe** file.

   The **Dell OpenManage Server Administrator** prerequisite status screen opens and runs the prerequisite checks for the managed station. Any relevant informational, warning, or error messages are displayed.

4. Click the **Install, Modify, Repair, or Remove Server Administrator** option.

   The **Welcome to the Install Wizard for Dell OpenManage Server Administrator** screen opens.

5. Click **Next**.

   The **Dell Software License Agreement** is displayed.

6. Click **Accept** and **Next** if you agree.

   The **Setup Type** dialog box opens.

7. Select **Custom** and click **Next**.

   The **Custom Setup** dialog box opens.

   To select a specific managed system software application, click the drop-down arrow beside the listed feature and select either to install or not to install the software.

   A selected feature has a hard drive icon depicted next to it. A deselected feature has a red **X** depicted next to it. By default, if the Prerequisite Checker finds a software feature with no supporting hardware, the checker deselects them.

   To accept the default directory path to install managed system software, click **Next**.

   Otherwise, click **Change** and navigate to the directory where you want to install your managed system software, and click **OK**. You will return to the **Custom Setup** dialog box.

8. Click **Next** to accept the selected software features for installation.

The **Ready to Install the Program** dialog box appears.

> **NOTE:** You can cancel the installation process by clicking **Cancel**. The installation rolls back the changes that you made. If you click **Cancel** after a certain point in the installation process, the installation may not roll back properly, leaving the system with an incomplete installation. See "System Recovery on Failed Installation."

9. Click **Install** to install the selected software features.

   The **Installing Dell OpenManage Server Administrator** screen opens. Messages provide the status and progress of the software features being installed. After the selected features are installed, the **Install Wizard Completed** dialog box opens.

10. Click **Finish** to exit the Server Administrator installation.

   If you are prompted to reboot your system, you must reboot it to make the installed managed system software services available for use. If you are prompted to reboot your system, select a reboot option:

   - **Yes, reboot my system now.**

   - **No, I will reboot my system later.**

Server Administrator Installation With 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:**. The remapping results in Server Administrator not working properly.

In order to avoid this problem, select one of these options:

Option 1:

1. Uninstall Server Administrator.

2. Install Citrix.

3. Reinstall Server Administrator.

Option 2:

After installing Citrix, type the following command:

```
msiexec.exe /fa SysMgmt.msi
```

Upgrading Managed System Software

The *Dell PowerEdge Installation and Server Management* CD features an **Upgrade** option for upgrading Server Administrator and other managed system software.

When you insert the *Dell PowerEdge Installation and Server Management* CD in your system's CD drive, the Prerequisite Checker program uses your system's PCI bus to search for installed hardware, such as controller cards.

The setup program installs or upgrades all of the managed system software features that are appropriate for your particular system's hardware configuration.

During the upgrade, you cannot add to the list of managed system software features to install because all features appropriate for your system are pre-selected.

> **NOTICE:** Dell OpenManage Array Manager is no longer supported. If you are upgrading a system (installed with Dell OpenManage version 4.3 or later) with Array Manager installed, Array Manager will be removed during the upgrade process. You can use Storage Management Service instead.

> **NOTE:** All user settings are preserved during upgrades.

> **NOTE:** During an upgrade, you cannot add to the list of Management Station software features to install.

The following procedures show how to upgrade Server Administrator and other managed system software.

Custom Upgrade

1. Insert the *Dell PowerEdge Installation and Server Management* CD into your system's CD drive.

   If the CD does not automatically start the setup program, go to your system's desktop, double-click **My Computer** (or open Windows Explorer), double-click the CD drive icon, double-click the **srvadmin** folder, double-click the **windows** folder, and double-click the **setup.exe** file.

   The **Dell OpenManage Server Administrator prerequisite** status screen opens and runs the prerequisite checks for the managed station. Any relevant informational, warning, or error messages are displayed.

2. Click the **Install, Modify, Repair, or Remove Server Administrator** option.

The **Welcome to the Install Wizard for Dell OpenManage Server Administrator** screen opens.

This screen then switches to the **Resuming the Install Wizard for Dell OpenManage Server Administrator** screen.

3. Click **Next**.

   The **Installing Dell OpenManage Server Administrator** screen opens. Messages are displayed, stating the status and progress of the software features being installed or upgraded.

   After the selected features are installed or upgraded, the **Install Wizard Completed** dialog box opens.

4. Click **Finish** to exit the Server Administrator installation.

   If you are prompted to reboot your system, you must reboot your system to make the installed managed system software services available for use.

   You must also reboot your system before changing your operating system disk; an example is when upgrading from a basic disk to a dynamic disk. If you are prompted to reboot your system, select a reboot option:

   - l **Yes, reboot my system now.**

   - l **No, I will reboot my system later.**

Upgrade Using the Windows Installer Patch File

You can upgrade your Managed System software using the Windows Installer Patch (.MSP) file. The MSP file is available on the Dell Support website at **support.dell.com**. To apply the MSP file either double-click on the MSP file or enter the following command in your command-prompt window:

   Msiexec.exe /p filename.msp

NOTE: You can use other msiexec parameters like "/q" for silent upgrades.

Custom Modify

1. Click the **Start** button, point to **Settings→ Control Panel**.

2. Double-click **Add/Remove Programs**.

3. Click **Dell OpenManage Server Administrator** and click **Change**.

   The **Welcome to the Install Wizard for Dell OpenManage Server Administrator** dialog box opens.

4. Click **Next**.

   The **Program Maintenance** dialog box opens.

5. Select the **Modify** option and click **Next**.

   The **Custom Setup** dialog box opens.

6. To select a specific managed system software application, click on the drop-down arrow beside the listed feature and select either **This feature will be installed...** to install the feature, or **This feature will not be available** to not install the feature.

   A selected feature has a hard drive icon depicted next to it. A deselected feature has a red **X** next to it. By default, if the Prerequisite Checker finds a software feature with no supporting hardware, the checker deselects the feature.

7. Click **Next** to accept the selected software features for installation.

   The **Ready to Modify the Program** dialog box opens.

8. Click **Install** to install the selected software features.

   The **Installing Dell OpenManage Server Administrator** screen opens. Messages give the status and progress of the software features being installed.

   When the selected features are installed, the **Install Wizard Completed** dialog box opens.

9. Click **Finish** to exit the Server Administrator installation.

   If you are prompted to reboot your system, you must do so to make the installed managed system software services available for use. If you are prompted to reboot your system, select a reboot option:

   - l **Yes, reboot my system now.**

   - l **No, I will reboot my system later.**

1. Click the **Start** button, point to **Settings**→ **Control Panel**.

2. Double-click **Add/Remove Programs**.

3. Click **Dell Server Administrator** and click **Change**.

   The **Welcome to the Install Wizard for Dell OpenManage Server Administrator** dialog box opens**.**

4. Click **Next**.

   The **Program Maintenance** dialog box opens.

5. Select the **Repair** option and click **Next**.

   The **Ready to Repair the Program** dialog box opens.

6. Click **Install** to install the selected software features.

   The **Installing Dell OpenManage Server Administrator** screen opens. Messages provide the status and progress of the software features being installed.

   When the selected features are installed, the **Install Wizard Completed** dialog box opens.

7. Click **Finish** to exit the Server Administrator installation.

   If you are prompted to reboot your system, select a reboot option:

   - **Yes, reboot my system now.**
   - **No, I will reboot my system later.**

System Recovery on Failed Installation

The Microsoft Software Installer (MSI) provides the ability to return a system to its fully working condition after a failed installation. MSI does this by maintaining an undo operation for every Standard Action it performs during an install, upgrade, or uninstall. This operation includes restoration of deleted or overwritten files, registry keys, and other resources. Windows temporarily saves any files that it deletes or overwrites during the course of an installation or removal, so they can be restored if necessary, which is a type of rollback. After a successful installation finishes, Windows deletes all of the temporary backup files.

In addition to the rollback of MSI Standard Actions, the Dell OpenManage library also has the ability to undo commands listed in the INI file for each application if a rollback occurs. All files that are modified by the Dell OpenManage installation actions will be restored to their original state if a rollback occurs.

When the MSI engine is going through the installation sequence, it ignores all actions that are scheduled as rollback actions. If a Custom Action, MSI Standard Action, or a Dell OpenManage installation action fails, then a rollback starts.

An installation cannot be rolled back once it has finished; transacted installation is only intended as a safety net that protects the system during an installation session. If you want to remove an installed application, for instance, you should simply uninstall that application.

NOTE: Driver installation and removal is not executed as part of the installation transaction and therefore cannot be rolled back if a fatal error occurs during execution.

NOTE: Installations, uninstallations, and upgrades that you cancel during installer cleanup, or after the installation transaction is completed, will not be rolled back.

Failed Updates

MSI patches and updates provided by vendors must be applied to the original vendor MSI packages provided. If you intentionally or accidentally repackage an MSI package, or make changes to it directly, patches and updates might fail. MSI packages must not be repackaged; doing so changes the feature structure and GUIDs, which break any provided patches or updates. When it is necessary to make any changes to a vendor-provided MSI package, a **.mst** transform file should always be used to do so.

Windows Installer Logging

Windows includes a registry-activated logging service to help diagnose Windows Installer issues. To enable this logging service during a silent install, open the registry with **Regedt32.exe** and create the following path and keys:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
Reg_SZ: Logging
Value: voicewarmup
```

The letters in the value field can be in any order. Each letter turns on a different logging mode. Each letter's actual function is as follows for MSI version 3.1:

```
v - Verbose output
o - Out-of-disk-space messages
i - Status messages
c - Initial UI parameters
e - All error messages
w - Non-fatal warnings
a - Startup of actions
r - Action-specific records
m - Out-of-memory or fatal exit information
u - User requests
p - Terminal properties
+ - Append to existing file
! - Flush each line to the log
"*" - Wildcard, log all information except for the v option. To include the v option, specify "/l*v".
```

Once activated, you can find the log files that are generated in your %TEMP% directory. Some log files generated in this directory are:

- **Managed System Installation**

  - **SysMgmt.log**

- **Management Station Installation**

  - **MgmtSt.log**

These particular log files are created by default if the Prerequisite Checker user interface (UI) is running.

Upgrading the MSI Engine

Dell OpenManage software allows you to upgrade the MSI engine while doing interactive installs. For silent installs, you have to add appropriate command to the install scripts.

Use the following command in your deployment script to upgrade the MSI engine (if required) and to install/upgrade the systems management software.

NOTE: Dell OpenManage systems management and Management Station installers require MSI version 3.1 or later. Update the MSI engine if you are using a system running Windows Server 2003 (without a Service Pack), Windows 2000 Server, or Windows XP operating system. If you are using a system running Windows Server 2003 SP1 or Windows Server 2003 x64 operating system, you do not have to update the MSI engine.

```
:retry
start /wait msiexec /i SysMgmt.msi /qn
if %errorlevel% == 1613 (
REM UPGRADE THE WINDOWS INSTALLER ENGINE
start /wait WindowsInstaller-KB893803-v2-x86.exe /quiet /norestart
goto retry
)
if %errorlevel% == 1638 (
REM THIS IS A MINOR UPGRADE
start /wait msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus/qn
)
```

Performing an Unattended Installation of Managed System Software

The *Dell PowerEdge Installation and Server Management* CD features a **Typical Setup** option and a **Custom Setup** option for the unattended installation procedure.

Unattended installation enables you simultaneously to install Server Administrator on multiple systems. You can perform an unattended installation by creating an unattended installation package that contains all of the necessary managed system software files. The unattended installation option also provides several features that enable you to configure, verify, and view information about unattended installations.

The unattended installation package is distributed to the remote systems using a software distribution tool from an ISV, an independent software vendor. When the package is distributed, the installation script executes to install the software.

Creating and Distributing the Typical Unattended Installation Package

The **Typical Setup** unattended installation option uses the *Dell PowerEdge Installation and Server Management* CD as the unattended installation package. The **msiexec.exe /i SysMgmt.msi /qb** program accesses the *Dell PowerEdge Installation and Server Management* CD to accept the software license agreement and install all required Server Administrator features on selected remote systems. The **msiexec.exe /i SysMgmt.msi /qb** command installs Server Administrator features on each remote system based on the system's hardware configuration.

NOTE: After an unattended installation has finished, in order to use the command line interface (CLI) feature of Server Administrator, you must open a new console window and execute CLI commands from there. Executing CLI commands from the same console window in which Server Administrator was installed will not work.

You can make the *Dell PowerEdge Installation and Server Management* CD image available to the remote system by either distributing the entire contents of the CD, or by mapping a drive from the target system to the location of the CD image.

Mapping a Drive to Act as the Typical Unattended Installation Package

1. Share an image of the *Dell PowerEdge Installation and Server Management* CD with each remote system on which you want to install Server Administrator.

   You can accomplish this task by directly sharing the CD or by copying the entire CD to a drive and sharing the copy.

2. Create a script that maps a drive from the remote systems to the shared drive described in step 1. This script should execute **msiexec.exe /i** *Mapped Drive***\srvadmin\windows\SystemsManagement\SysMgmt.msi /qb** after the drive has been mapped.

3. Configure your ISV distribution software to distribute and execute the script created in step 2.

4. Distribute this script to the target systems by using your ISV software distribution tools.

   The **msiexec.exe /i** *Mapped Drive***\srvadmin\windows\SystemsManagement\SysMgmt.msi /qb** program executes to install Server Administrator on each remote system.

5. Reboot each remote system to enable Server Administrator.

Distributing the Entire CD as the Typical Unattended Installation Package

1. Distribute the entire image of the *Dell PowerEdge Installation and Server Management* CD to your target systems.

2. Configure your ISV distribution software to execute the **msiexec.exe /i** *CD Drive***\srvadmin\windows\SystemsManagement\SysMgmt.msi /qb** program from the *Dell PowerEdge Installation and Server Management* CD image.

   The **msiexec.exe /i** *CD Drive***\srvadmin\windows\SystemsManagement\SysMgmt.msi /qb** program executes to install Server Administrator on each remote system.

3. Reboot each remote system to enable Server Administrator.

Creating and Distributing Custom Unattended Installation Packages

To create a custom unattended installation package, perform the following steps:

1. Copy the **windows** directory from the CD onto the system hard drive.

2. Create a batch script that will execute the installation using the Windows Installer Engine (**msiexec.exe**).

   ✍ **NOTE:** For Customized Unattended Installation, each required feature must be included as a Command Line Interface (CLI) parameter for it to be installed.

   An example is msiexec.exe /i SysMgmt.msi ADDLOCAL=SA,IWS,BRCM /qb. (See the "Customization Parameters" section below for additional details and available feature identifications.)

3. Place the batch script in the **windows** directory on the system hard drive.

Distributing Custom Unattended Installation Packages

✍ **NOTE:** The **SysMgmt.msi** installation package for Server Administrator used in **Custom Setup** unattended installation (see "Creating and Distributing Custom Unattended Installation Packages") is located in the **srvadmin\windows\SystemsManagement** directory.

1. Configure your ISV distribution software to execute the batch script once your installation package has been distributed.

2. Use your ISV distribution software to distribute the custom unattended installation package to the remote systems.
   The **msiexec.exe /i** *System Drive***\srvadmin\windows\SystemsManagement\SysMgmt.msi ADDLOCAL=SA,IWS,BRCM /qb** program installs Server Administrator along with specified features on each remote system.

3. Reboot each remote system to enable Server Administrator.

Specifying Log File Locations

For managed system MSI installation, run the following command to perform an unattended installation while specifying the log file location:

    msiexec.exe /i SysMgmt.msi /l*v "C:\openmanage\logs\SysMgmt.log"

Unattended Installation Features

Unattended installation provides the following features:

- A set of optional command line settings to customize an unattended installation
- Customization parameters to designate specific software features for installation
- A Prerequisite Checker program that examines the dependency status of selected software features without having to perform an actual installation

Optional Command Line Settings

Table 6-1 shows the optional settings available for the **msiexec.exe** MSI installer. Type the optional settings on the command line after **msiexec.exe** with a space between each setting.

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

Table 6-1. Command Line Settings for MSI Installer

Setting	Result
/i<Package|Product Code>	This command installs or configures a product. **/i SysMgmt.msi** – Installs the Server Administrator software.
/i SysMgmt.msi /qn	This command carries out a fresh installation of version 5.1. This command also carries out major upgrades from version 4.3 to 5.1. You have to update your MSI engine before running this command if you are using a system running Windows Server 2003 (without a Service Pack), Windows 2000 Server, or Windows XP operating system. See "Upgrading the MSI Engine" for information on upgrading the MSI engine and installing/upgrading systems management software.
/i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus /qn	This commands carries out a minor upgrade, say from version 4.3 to version 4.4. You have to update your MSI engine before running this command if you are using a system running Windows Server 2003 (without a Service Pack), Windows 2000 Server, or Windows XP operating system. See "Upgrading the MSI Engine" for information on upgrading the MSI engine and installing/upgrading systems management software.
/x<Package|Product Code>	This command uninstalls a product. **/x SysMgmt.msi** – Uninstalls the Server Administrator software.
/q[n|b|r|f]	This command sets the user interface (UI) level. **/q** or **/qn** – no UI. This option is used for silent and unattended installation. **/qb** – basic UI. This option is used for unattended but not silent installation. **/qr** – reduced UI. This option is used for unattended installation while displaying a modal dialog box showing install progress. **/qf** – full UI. This option is used for standard attended installation.
/f[p|o|e|d|c|a|u|m|s|v] <Package|ProductCode>	This command repairs a product. **/fp** – This option reinstalls a product only if a file is missing. **/fo** – This option reinstalls a product if a file is missing or if an older version of a file is installed. **/fe** – This option reinstalls a product if a file is missing or an equal or older version of a file is installed. **/fd** – This option reinstalls a product if a file is missing or a different version of a file is installed. **/fc** – This option reinstalls a product if a file is missing or the stored checksum value does not match the calculated value. **/fa** – This option forces all files to be reinstalled. **/fu** – This option rewrites all required user-specific registry entries. **/fm** – This option rewrites all required system-specific registry entries. **/fs** – This option overwrites all existing shortcuts. **/fv** – This option runs from the source and re-caches the local package. Do not use the **/fv** reinstall option for the first installation of an application or feature.
INSTALLDIR=<path>	This command installs a product to a specific location. If you specify an install directory with this switch, it must be created manually prior to executing the CLI install commands or they will fail with no error or message as to why they failed. **/i SysMgmt.msi INSTALLDIR=c:\OpenManage /qn** – installs a product to a specific location using **c:\OpenManage** as the install location.

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

Customization Parameters

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

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

Table 6-2. Software Feature IDs

Feature ID	Description
BRCM	Broadcom NIC Agent
INTEL	Intel NIC Agent
IWS	Server Administrator Web Server
OMSM	Storage Management
RAC3	Remote Access Controller (DRAC III)
RAC4	Remote Access Controller (DRAC 4)
RAC5	Remote Access Controller (DRAC 5)
SA	Server Administrator

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

    msiexec.exe /i SysMgmt.msi ADDLOCAL=BRCM /qb.

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

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

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

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

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

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

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

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

    msiexec.exe /i SysMgmt.msi ADDLOCAL=INTEL REMOVE=BRCM /qb

This command runs the installation for managed system software, and simultaneously installs the Intel agent, and uninstalls the Broadcom agent. This execution will be in an unattended but not silent mode.

> **NOTE:** A Globally Unique Identifier (GUID) is 128 bits long, and the algorithm used to generate a GUID guarantees each GUID to be unique. The product GUID uniquely identifies the application. In this case, the product GUID for Server Administrator is {89C7A9F7-2C31-4739-842D-F037B6C9B674}.

MSI Return Code

An application event log entry is recorded in the **SysMgmt.log** file. Table 6-3 shows some of the error codes returned by the **msiexec.exe** Windows Installer Engine.

Table 6-3. Windows Installer Return Codes

Error Code	Value	Description
ERROR_SUCCESS	0	The action completed successfully.
ERROR_INVALID_PARAMETER	87	One of the parameters was invalid.
ERROR_INSTALL_USEREXIT	1602	The user canceled the installation.
ERROR_SUCCESS_REBOOT_REQUIRED	3010	A restart is required to complete the installation. This message is indicative of a successful installation.

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

Uninstalling Managed System Software

You can uninstall managed system software features by using the *Dell PowerEdge Installation and Server Management* CD or your operating system. Additionally, you can simultaneously perform an unattended uninstallation on multiple systems.

NOTE: After you uninstall Server Administrator on PowerEdge 1650, 2650, and 4600 systems, you may be prompted to reboot your system if you have chosen to uninstall Storage Management Service. You may also be prompted for a reboot if any of the files being upgraded are under use.

Uninstalling Managed System Software Using the Installation and Server Management CD

1. Insert the *Dell PowerEdge Installation and Server Management* CD into your system's CD drive.

   If the CD does not automatically start the setup program, go to your system's desktop, double-click **My Computer** (or open Windows Explorer), double-click the CD drive icon, double-click the **srvadmin** folder, double-click the **windows** folder, and double-click the **setup.exe** file.

   The **Dell OpenManage Server Administrator prerequisite** status screen opens and runs the prerequisite checks for the managed system. Any relevant informational, warning, or error messages detected during checking are displayed.

2. Click the **Install, Modify, Repair, or Remove Server Administrator** option.

   The **Welcome to the Install Wizard for Dell OpenManage Server Administrator** screen opens**.**

3. Click **Next**.

   The **Program Maintenance** dialog box opens.

   This dialog enables you to modify, repair, or remove the program.

4. Select the **Remove** option and click **Next**.

   The **Remove the Program** dialog box opens.

5. Click **Remove**.

   The **Uninstalling Dell OpenManage Server Administrator** screen opens. Messages provide the status and progress of the software features being uninstalled.

   When the selected features are uninstalled, the **Install Wizard Completed** dialog box opens.

6. Click **Finish** to exit the Server Administrator uninstallation.

   If you are prompted to reboot your system, you must reboot your system in order for the uninstallation to be successful. If you are prompted to reboot your system, select a reboot option:

   - **Yes, reboot my system now.**

   - **No, I will reboot my system later.**

   All Server Administrator features are uninstalled.

Uninstalling Managed System Software Features Using the Operating System

1. Click the **Start** button, point to **Settings**→ **Control Panel**.

2. Double-click **Add/Remove Programs**.

3. Click **Dell OpenManage Server Administrator** and click **Remove**.

   The **Add or Remove Programs** dialog box opens.

4. Click **Yes** to confirm uninstallation of Server Administrator.

   The **Dell OpenManage Server Administrator** screen opens. Messages provide the status and progress of the software features being uninstalled.

   If you are prompted to reboot your system, you must do so in order for the uninstallation to be successful. If you are prompted to reboot your system, select a reboot option:

   - **Yes, reboot my system now.**

   - **No, I will reboot my system later.**

   All Server Administrator features are uninstalled.

Unattended Uninstall Using the Product GUID

If you do not have the installation CD or the MSI package available during an uninstallation, you can use the following command line to uninstall Dell OpenManage systems management software on managed systems or management stations running Windows. For these cases, you can use the package GUIDs to uninstall the product.

For managed systems, use this command:

```
msiexec.exe /x {89C7A9F7-2C31-4739-842D-F037B6C9B674}
```

For management stations, use this command:

```
msiexec.exe /x {DA60872C-9147-4A6E-9AEF-95BAB5EF3A3B}
```

Performing an Unattended Uninstallation of Managed System Software

The *Dell PowerEdge Installation and Server Management* CD features an unattended uninstallation procedure. Unattended uninstallation enables you simultaneously to uninstall managed systems software from multiple systems. The unattended uninstallation package is distributed to the remote systems using a software distribution tool from an ISV. When the package is distributed, the uninstallation script executes to uninstall the software.

Distributing the Unattended Uninstallation Package

The *Dell PowerEdge Installation and Server Management* CD is preconfigured to act as the unattended uninstallation package. To distribute the package to one or more systems, perform the following steps:

1. Configure your ISV distribution software to execute the **msiexec.exe /x** *CD Drive***\srvadmin\windows\SystemsManagement\SysMgmt.msi /qb** program after the unattended uninstallation package has been distributed.

2. Use your ISV distribution software to distribute the Typical unattended uninstallation package to the remote systems.

   The **msiexec.exe /x** *CD Drive***\srvadmin\windows\SystemsManagement\SysMgmt.msi /qb** program executes to uninstall managed systems software on each remote system.

3. Reboot each remote system to complete the uninstallation process.

Unattended Uninstall Command Line Settings

Table 6-1 shows the unattended uninstall command line settings available for unattended uninstallation. Type the optional settings on the command line after `msiexec.exe /x SysMgmt.msi` with a space between each setting.

For example, running `msiexec.exe /x SysMgmt.msi /qb` runs the unattended uninstallation, and displays the unattended installation status while it is running.

Running `msiexec.exe /x SysMgmt.msi /qn` runs the unattended uninstallation, but silently (without display windows).

Managed System Software Installation Using Third-Party Deployment Software

You can use third-party deployment software, such as Altiris Deployment Solution, to install managed systems software onto supported Dell systems. To distribute and install Server Administrator using Altiris, start your Altiris application and import **OpenManage_Jobs.bin** located on the *Dell PowerEdge Installation and Server Management* CD at **\srvadmin\support\Altiris**. Specify a job folder into which to import it. You might need to modify the **Run Script** and **Copy File** tasks to match your deployment environment. When complete, you can then schedule your job to run on the supported Dell systems that are managed from within your Altiris Deployment Solution.

Introduction

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- Overview
- Dell OpenManage Systems Management Software Components
- Other Documents You Might Need
- Obtaining Technical Assistance

Overview

This guide contains information to help you install Dell OpenManage™ software on management stations and their managed systems. A *managed system* is a system that has supported instrumentation or agents installed that allow the system to be discovered and polled for status. A *management station* is used to remotely manage one or more managed systems from a central location. See Figure 1-1 for a view of a management station and its managed systems. In addition, this guide provides information and instructions for configuring your systems before and during a deployment or upgrade. The following topics are covered:

l   Dell OpenManage™ Security

l   Setup and Administration

l   Using Server Assistant to Install an Operating System

l   Installing Management Station Software

l   Installing Managed System Software on Microsoft® Windows® Operating Systems

l   Installing Managed System Software on Red Hat® Enterprise Linux and SUSE® Linux Operating Systems

l   Using Microsoft® Active Directory®

l   Prerequisite Checker

l   Frequently Asked Questions

Systems Management Software Overview

Dell OpenManage systems management software is a suite of application programs for Dell™ PowerEdge™ systems and some Dell PowerVault™ systems. This software enables you to manage your systems with proactive monitoring, diagnosis, notification, and remote access.

Each system managed by Dell OpenManage systems management software is called a managed system. You can manage a managed system either locally or remotely. Software applications that you may install onto the managed systems include Dell OpenManage Server Administrator (which includes the Storage Management Service, and the Server Administrator Web server), SNMP agents for Intel® or Broadcom network interface cards (NICs), and remote access controller (RAC) software.
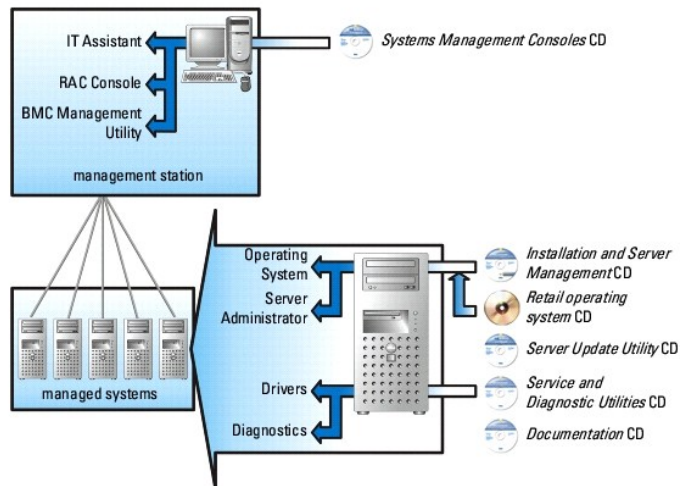
A management station can be used to remotely configure and maintain one or more managed systems from a central location. Dell OpenManage IT Assistant and the other management station applications enable you to manage from one to thousands of managed systems. For instance, a management station can be used to deploy images of physical media to virtual media at many managed systems.

NOTE: If you install management station and managed system software on the same system, install identical software versions to avoid system conflicts.

Figure 1-1 illustrates the relationship between a management station and its managed systems. Also, Figure 1-1 shows the operating systems and the Dell OpenManage software products that you can install on the managed systems. The documentation CD can be accessed from any system with a monitor, keyboard, and mouse.

NOTE: The *Dell PowerEdge Server Update Utility* CD is included in the Dell OpenManage Subscription Service Kit only; it is not included in the Dell OpenManage Systems Management Software Kit.

Figure 1-1. Example of a Management Station and Managed Systems

IT Assistant

RAC Console

BMC Management Utility

management station

Systems Management Consoles CD

managed systems

Operating System

Server Administrator

Drivers

Diagnostics

Installation and Server Management CD

Retail operating system CD

Server Update Utility CD

Service and Diagnostic Utilities CD

Documentation CD

Dell OpenManage Systems Management Software Kit Contents

The Dell OpenManage Systems Management Software Kit includes, but is not limited to, the following components:

l *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. This guide—located on the *Documentation* CD—also contains procedures for installing your console and managed system applications on systems running supported operating systems.

l *Dell Systems Management Consoles* CD — Contains the Dell systems management console products for your management stations. The CD includes IT Assistant and other systems management applications.

l *Dell PowerEdge Installation and Server Management* CD — Provides the tools that you need to install an operating system and configure your managed systems, including Server Administrator Instrumentation, Diagnostics, Storage Management, and Remote Access services.

l *Dell PowerEdge Service and Diagnostic Utilities* CD — Provides tools to configure your managed systems and delivers the latest diagnostics and Dell-optimized drivers for your managed systems.

l *Dell PowerEdge Documentation* CD — Helps you stay current with documentation for systems, systems management software products, peripherals, and RAID controllers.

l *Dell PowerEdge Server Update Utility CD* - Contains the Server Update Utility (SUU), which is a CD-based application for identifying and applying updates to your system. SUU is delivered on separate CDs for Microsoft Windows and Linux.

Most of these CDs also contain readme files, which provide the latest product information.

NOTE: The *Dell PowerEdge Server Update Utility* CD is only available as part of the Subscription Service Kit or from the Dell Support website at **support.dell.com**.

Compare the contents of your system accessories box with the packing slip or invoice enclosed with your system. If any components are missing or damaged, call Dell within 30 days of the invoice date for a free replacement. For more information, see "Obtaining Technical Assistance."

What's New

l Support for SUSE Linux Enterprise Server (version 10) Gold, for Intel Extended Memory 64 Technology (Intel EM64T).

l Support for Dell OpenManage IT Assistant 8.0.

l Diagnostics is no longer available through Server Administrator. To run diagnostics on your system, install Dell PowerEdge Diagnostics from your Dell PowerEdge Service and Diagnostic Utilities CD or download and install Dell PowerEdge Diagnostics from the Dell Support website at **support.dell.com**. Dell PowerEdge Diagnostics is a stand-alone application that can be run without installing Server Administrator.

For more information, see the Dell OpenManage website at **www.dell.com/openmanage**.

Dell OpenManage Systems Management Software Components

Deployment Software (Dell PowerEdge Installation and Server Management CD)

For managed systems, Dell OpenManage Server Assistant provides streamlined operating system installation, reducing the time required for the installation of

Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems by guiding you through an easy-to-follow, step-by-step process.

In addition, Server Assistant provides the necessary tools for setting up and configuring PowerEdge systems and software. The tools permit discovery and configuration of Dell-provided RAID controllers and network adapters.

Management Station Software (Dell Systems Management Consoles CD)

IT Assistant

IT Assistant is a Web-based graphical user interface (GUI) that provides a central point of access to monitor and manage systems on a local area network (LAN) or a wide area network (WAN). By providing a comprehensive view across the enterprise, IT Assistant can increase system uptime, reduce repetitive tasks, and prevent interruption during critical business operations.

Using IT Assistant, you can:

- Identify the groups of systems that you want to manage remotely

- Consolidate your view of all systems, providing a central launch point for systems management

- Create alert filters and actions that will automatically notify you when system uptime is affected

- Create custom enterprise-wide reports that show the status of each system, including switches, storage devices, BIOS, firmware, and driver versions

- Create customized tasks that allow you to coordinate configuration management across the entire enterprise, including performing software updates, shutdown and wakeup, and command line execution

- View a graphical presentation of the devices in your network, from which you can launch applications, refresh inventory and status, and perform troubleshooting

- Launch the following Dell systems management applications: Server Administrator, Remote Access Console, Dell PowerConnect™, and Digital KVM (keyboard/video/mouse)

- Load Dell Update Packages and System Update Sets into the IT Assistant repository, then run a compliance check of all the systems in your enterprise against the Update Packages. A System Update Set is a logical set of Dell-certified packages that work together without problems. Dell Update Packages are available from the Dell Support website at **support.dell.com** or from the *Dell PowerEdge Server Update Utility* CD. This CD is available through the Dell OpenManage Subscription Service or as an ISO image downloadable from the support.dell.com. You can download the Dell OpenManage Subscription Service from **www.dell.com**.

Dell Remote Access Controller Management Station

The Dell Remote Access Controller (DRAC) console is management station software designed to provide remote management capabilities for PowerEdge systems. You can remotely connect to RAC hardware using the DRAC Tools software. The following RAC features are implemented in the hardware and are available either by using a browser or by way of the racadm CLI:

- Hardware sensor monitors, such as temperature, voltage, and fans

- Access to hardware and alert logs

- Ability to generate alerts, even when the system is down

- Remote system power up and power down

- Remote floppy boot operations

See the *Dell Remote Access Controller 4 User's Guide* or *Dell Remote Access Controller 5 User's Guide* for more information about how to use the racadm CLI to connect to a managed system to execute racadm commands from a remote console, or to connect to a management station using the IP address of the managed station.

Baseboard Management Controller (BMC) Management Utility

The BMC Management Utility provides a command line based remote management station to manage all supported BMC functions. Use the BMC Management Utility to manage a BMC from a remote management station, and as a managed system's emergency management console. The utility gives you the option of using either a command line interface (Intelligent Platform Management Interface [IPMI shell] or a Serial-Over-LAN proxy [SOL Proxy]) to access and manage the BMC.

The BMC monitors the system for critical events by communicating with various sensors on the system board and sending alerts and logs events when certain parameters exceed their preset thresholds. The BMC supports the industry-standard IPMI specification, enabling you to configure, monitor, and recover systems remotely.

The BMC provides the following features:

- Management access through the system's serial port and integrated NIC

- Fault logging and SNMP alerting

- Access to the system event log (SEL) and sensor status

- System function controls, including power on and off

- Support that is independent of the system's power or operating state

- Text console redirection for system setup, text-based utilities, and operating system consoles

- Access to Red Hat Enterprise Linux and SUSE Linux Enterprise Server serial console interfaces using SOL

Active Directory Snap-in Utility

The Microsoft Active Directory Snap-in utility provides an extension snap-in to the Microsoft Active Directory, which allows you to manage Dell-specific Active Directory objects.

You can use this option when the Dell-specific schema classes have been added to the Active Directory schema.

Managed System Software (Dell PowerEdge Installation and Server Management CD)

Server Administrator

Server Administrator provides a comprehensive, one-to-one systems management solution using an integrated Web browser-based GUI (the Server Administrator home page) or a command line interface (CLI) feature. Server Administrator includes the following integrated services and features:

Instrumentation Service

The Instrumentation Service provides rapid access to detailed fault and performance information gathered by 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 RAC on a modular system. See the *Dell Embedded Remote Access/MC User's Guide,* the *Dell Remote Access Controller 4 User's Guide,* or the *Dell Remote Access Controller 5 User's Guide* for more information.

The Remote Access Service provides the following features:

- Remote access to an inoperable system, allowing you to shut down, restart, and get the system up and running as quickly as possible

- Alert notification when a system is down

- System crash logs that record the probable cause of system crashes and saves the most recent crash screen

You must have Server Administrator on your system to install the Remote Access Service.

NOTE: The Server Administrator Remote Access Service and Remote Access Controller Management Station cannot be installed on a system at the same time. If both Server Administrator and Management Station are installed at the same time and RAC support is required, install Server Administrator Remote Access Service. It provides all the functionality of the Remote Access Controller Management Station.

Storage Management Service

The Storage Management Service provides enhanced features for managing a system's locally-attached RAID and non-RAID disk storage.

The Storage Management Service provides the following features:

- Enables you to view the status of local and remote storage attached to a monitored system

- Supports SAS, SCSI, SATA, and ATA, but does not support Fibre Channel

- Allows you to perform controller and enclosure functions for all supported RAID and non-RAID controllers and enclosures from a single graphical interface or a CLI, without the use of the controller BIOS utilities

- Protects your data by configuring data redundancy, assigning hot spares, or rebuilding failed drives

Diagnostics (Dell PowerEdge Service and Diagnostic Utilities CD)

The Dell PowerEdge Diagnostics is a suite of diagnostic programs, or test modules, that run locally on your system. You can select the appropriate diagnostics tests to run from the **Diagnostic Selection** tree containing the hardware that PowerEdge Diagnostics discovers on your system.

Drivers (Dell PowerEdge Service and Diagnostic Utilities CD)

The Extraction Utility enables you to view and create Dell software driver and diagnostic floppy disks.

Change Management (Dell PowerEdge Server Update Utility CD)

The *Dell PowerEdge Server Update Utility* CD includes the Server Update Utility (SUU). SUU is a CD-based application for identifying and applying updates to your system. SUU is a dual-purpose application and is easy to use. You can use SUU to update your PowerEdge server or to view the updates available for any system listed in the Repository.

SUU facilitates change management by allowing you to update system components using an application that compares the version of currently installed components with updated components packaged on a CD and stored in a Repository. A full session of SUU would typically run an inventory of installed components and their versions, provide a comparison report between what is installed currently on the system and what the latest component versions are in the Repository, and leave to you the decision whether to apply the Dell component System Update Set to update the system or not. You can customize the packages you want to upgrade. You can roll back newer versions of components on your system to the corresponding component version contained on the *Dell PowerEdge Server Update Utility* CD. SUU is delivered on separate CDs for Microsoft Windows and Linux.

Other Documents You Might Need

Besides this *guide*, you can find the following guides either on the Dell Support website at **support.dell.com** or on the *Documentation* CD:

l   The *Dell OpenManage Software Quick Installation Guide* provides an overview of applications that you can install on your management station, or console, and on your managed systems. It also has procedures for installing your console and managed system applications.

l   The *Dell OpenManage Server Administrator User's Guide* describes the installation and use of Server Administrator. Server Administrator provides easy-to-use management and administration of local and remote systems through a comprehensive set of integrated management services.

l   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, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems.

l   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.

l   The *Dell OpenManage Server Administrator CIM Reference Guide* documents the Common Information Model (CIM) provider, which is an extension of the standard management object format (MOF) file. This guide explains the supported classes of management objects.

l   The *Dell OpenManage Server Administrator Messages Reference Guide* lists the messages that are displayed in the Server Administrator home page Alert log, or on your operating system's event viewer. This guide explains the text, severity, and cause of each alert message that Server Administrator issues.

l   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.

l   The *Dell OpenManage IT Assistant User's Guide* has information about installing, configuring, and using IT Assistant. IT Assistant provides a central point of access to monitor and manage systems on a local area network (LAN) or wide area network (WAN). By allowing an administrator a comprehensive view across the enterprise, IT Assistant can increase system uptime, automate repetitive tasks, and prevent interruption in critical business operations.

l   The *Dell Remote Access Controller 4 User's Guide* provides complete information about installing and configuring a DRAC 4 controller and using DRAC 4 to remotely access an inoperable system.

l   The *Dell Remote Access Controller 5 User's Guide* provides complete information about installing and configuring a DRAC 5 controller and using DRAC 5 to remotely access an inoperable system.

l   The *Dell Remote Access Controller/MC User's Guide* provides complete information about installing and configuring a DRAC/MC controller and using DRAC/MC to remotely access an inoperable system.

l   The *Dell Remote Access Controller Installation and Setup Guide* provides complete information about installing and configuring a DRAC III, DRAC III/XT, or ERA/O controller, configuring an ERA controller, and using a RAC to remotely access an inoperable system.

l   The *Dell Remote Access Controller Racadm User's Guide* provides information about using the racadm command line utility to manage DRAC III, DRAC III/XT, ERA, and ERA/O controllers.

l   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.

l   The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.

l   The *Dell PowerEdge Installation and Server Management* and *Systems Management Consoles* CDs contain readme files for most applications found on the CDs.

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, different types of help are available. For more information, see "Getting Help" in your system's *Hardware Owner's Manual*.

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

Using Microsoft® Active Directory®

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- Controlling Access to Your Network
- Extending the Active Directory Schema

Controlling Access to Your Network

If you use Active Directory service software, you can configure it to control access to your network. Dell has modified the Active Directory database to support remote management authentication and authorization. Dell OpenManage™ IT Assistant and Dell OpenManage Server Administrator, as well as Dell™ remote access controllers, can now interface with Active Directory. With this tool, you can add and control users and privileges from one central database.

NOTE: Using Active Directory to recognize Dell Remote Access Controller (DRAC), IT Assistant, or Server Administrator users is supported on the Microsoft Windows® 2000 and Windows Server™ 2003 operating systems.

Active Directory Schema Extensions

The Active Directory data exists in a distributed database of **Attributes** and **Classes**. An example of a Active Directory **Class** is the **User** class. Some example **Attributes** of the user class might be the user's first name, last name, phone number, and so on. Every **Attribute** or **Class** that is added to an existing Active Directory schema must be defined with a unique ID. To maintain unique IDs throughout the industry, Microsoft maintains a database of Active Directory Object Identifiers (OIDs).

The Active Directory schema defines the rules for what data can be included in the database. To extend the schema in Active Directory, Dell received unique OIDs, unique name extensions, and unique linked attribute IDs for the new attributes and classes in the directory service.

Dell extension is: dell

Dell base OID is: 1.2.840.113556.1.8000.1280

Dell LinkID range is: 12070 to 12079

The Active Directory OID database maintained by Microsoft can be viewed at **msdn.microsoft.com/certification/ADAcctInfo.asp** by entering our extension, *dell*.

Overview of the Active Directory Schema Extensions

Dell created Classes, or groups of objects, that can be configured by the user to meet their unique needs. New Classes in the schema include an Association, a Product, and a Privilege class. An Association object links the users or groups to a given set of privileges and to systems (Product Objects) in your network. This model gives an administrator control over the different combinations of users, privileges, and systems or RAC devices on the network, without adding complexity.
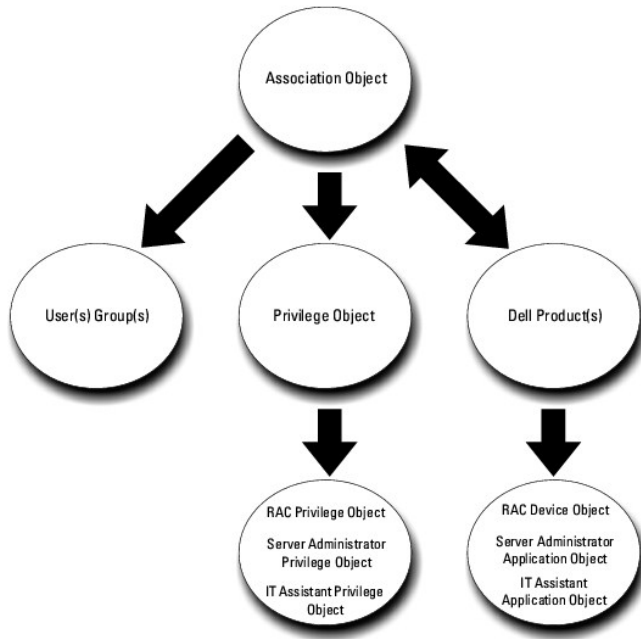
Active Directory Object Overview

For each of the systems that you want to integrate with Active Directory for authentication and authorization, there must be at least one Association Object and one Product Object. The Product Object represents the system. The Association Object links it with users and privileges. You can create as many Association Objects as you need.

Each Association Object can be linked to as many users, groups of users, and Product Objects as desired. The users and Product Objects can be from any domain. However, each Association Object may only link to one Privilege Object. This behavior allows an Administrator to control which users have which rights on specific systems.

The Product Object links the system to Active Directory for authentication and authorization queries. When a system is added to the network, the Administrator must configure the system and its product object with its Active Directory name so that users can perform authentication and authorization with Active Directory. The Administrator must also add the system to at least one Association Object in order for users to authenticate.

Figure 8-1 illustrates that the Association Object provides the connection that is needed for all of the authentication and authorization.

Figure 8-1. Typical Setup for Active Directory Objects

In addition, you can set up Active Directory objects in a single domain or in multiple domains. Setting up objects in a single domain does not vary, whether you are setting up RAC, Server Administrator, or IT Assistant objects. When multiple domains are involved, however, there are some differences.

For example, you have two DRAC 4 cards (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). You want to give user1 and user2 an Administrator privilege on both DRAC 4 cards and give user3 a Login privilege on the RAC2 card. Figure 8-2 shows how you set up the Active Directory objects in this scenario.

Figure 8-2. Setting Up Active Directory Objects in a Single Domain
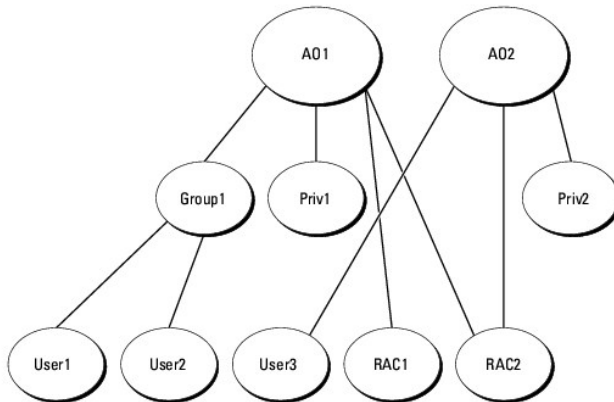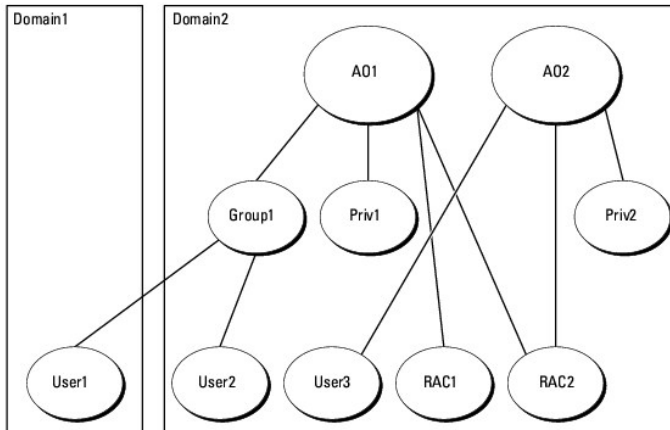

To set up the objects for the single domain scenario, perform the following tasks:

1. Create two Association Objects.

2. Create two RAC Product Objects, RAC1 and RAC2, to represent the two DRAC 4 cards.

3. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (Administrator) and Priv2 has Login privileges.

4. Group User1 and User2 into Group1.

5. Add Group1 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and both RAC1 and RAC2 as RAC Products in AO1.

6. Add User3 as Members in Association Object 2 (AO2), Priv2 as Privilege Objects in AO2, and RAC2 as RAC Products in AO2.

See "Adding Users and Privileges to Active Directory" for detailed instructions.

shows how to setup the Active Directory objects in multiple domains for RAC. In this scenario, you have two DRAC 4 cards (RAC1 and RAC2) and three existing Active Directory users (User1, User2, and User3). User1 is in Domain1, but User2 and User3 are in Domain2. You want to give User1 and User2 Administrator privileges on both the RAC1 and the RAC2 card and give User3 a Login privilege on the RAC2 card.

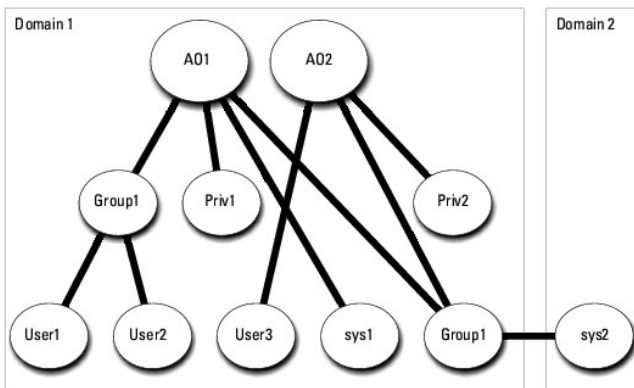**Figure 8-3. Setting Up RAC Active Directory Objects in Multiple Domains**

To set up the objects for this multiple domain scenario, perform the following tasks:

1. Ensure that the domain forest function is in Native or Windows 2003 mode.

2. Create two Association Objects, AO1 (of Universal scope) and AO2, in any domain. The figure shows the objects in Domain2.

3. Create two RAC Device Objects, RAC1 and RAC2, to represent the two remote systems.

4. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (Administrator) and Priv2 has Login privileges.

5. Group User1 and User2 into Group1. The group scope of Group1 must be Universal.

6. Add Group1 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and both RAC1 and RAC2 as Products in AO1.

7. Add User3 as Members in Association Object 2 (AO2), Priv2 as Privilege Objects in AO2, and RAC2 as a Product in AO2.

For Server Administrator or IT Assistant, on the other hand, the users in a single Association can be in separate domains without needing to be added to a universal group. The following is a very similar example to show how Server Administrator or IT Assistant *systems* in separate domains affect the setup of directory objects. Instead of RAC devices, you'll have two systems running Server Administrator (Server Administrator Products sys1 and sys2). Sys1 and sys2 are in different domains. You can use any existing Users or Groups that you have in Active Directory. shows how to set up the Server Administrator Active Directory objects for this example.

Figure 8-4. Setting Up Server Administrator Active Directory Objects in Multiple Domains

To set up the objects for this multiple domain scenario, perform the following tasks:

1. Ensure that the domain forest function is in Native or Windows 2003 mode.

2. Create two Association Objects, AO1 and AO2, in any domain. The figure shows the objects in Domain1.

3. Create two Server Administrator Products, sys1 and sys2, to represent the two systems. Sys1 is in Domain1 and sys2 is in Domain2.

4. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (Administrator) and Priv2 has Login privileges.

5. Group sys2 into Group1. The group scope of Group1 must be universal.

6. Add User1 and User2 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and both sys1 and Group1 as Products in AO1.

7. Add User3 as a Member in Association Object 2 (AO2), Priv2 as a Privilege object in AO2, and Group1 as a Product in AO2.

Note that neither of the Association objects needs to be of Universal scope in this case.

Configuring Active Directory to Access Your Systems

Before you can use Active Directory to access your systems, you must configure both the Active Directory software and the systems.

1. Extend the Active Directory schema (see "Extending the Active Directory Schema").

2. Extend the Active Directory Users and Computers Snap-in (see "Installing the Dell Extension to the Active Directory Users and Computers Snap-In").

3. Add system users and their privileges to Active Directory (see "Adding Users and Privileges to Active Directory").

4. For RAC systems only, enable SSL on each of your domain controllers (see "Enabling SSL on a Domain Controller (RAC Only)").

5. Configure the system's Active Directory properties using either the Web-based interface or the CLI (see "Configuring Your Systems or Devices").

Extending the Active Directory Schema

RAC, Server Administrator, and IT Assistant schema extensions are available. You only need to extend the schema for software or hardware that you are using. Each extension must be applied individually to receive the benefit of its software-specific settings. Extending your Active Directory schema will add schema classes and attributes, example privileges and association objects, and a Dell organizational unit to the schema.

NOTE: Before you extend the schema, you must have **Schema Admin** privileges on the Schema Master Flexible Single Master Operation (FSMO) Role Owner of the domain forest.

You can extend your schema using two different methods. You can use the Dell Schema Extender utility, or you can use the Lightweight Directory Interchange Format (LDIF) script file.

NOTE: The Dell organizational unit will not be added if you use the LDIF script file.

The LDIF script files and Dell Schema Extender are located on your *Dell PowerEdge™ Installation and Server Management* CD in the following respective directories:

  l *CD drive***:\support\OMActiveDirectory Tools***installation type***\LDIF Files**

  l *CD drive***:\support\OMActiveDirectory Tools***installation type***\Schema Extender**

Installation type will be either RAC4, RAC3, Server Administrator, or IT Assistant version 7.0 or later, depending on your choice of schema extension.

To use the LDIF files, see the instructions in the readme that is in the LDIF files directory. To use the Dell Schema Extender to extend the Active Directory Schema, perform the steps in "Using the Dell Schema Extender."

You can copy and run the Schema Extender or LDIF files from any location.

Using the Dell Schema Extender

NOTICE: The Dell Schema Extender uses the **SchemaExtenderOem.ini** file. To ensure that the Dell Schema Extender utility functions properly, do not modify the name or the contents of this file.

1. Click **Next on the Welcome screen.**

2. Read the warning and click **Next** again.

3. Either select **Use Current Log In Credentials** or enter a user name and password with schema administrator rights.

4. Click **Next** to run the Dell Schema Extender.

5. Click **Finish**.

To verify the schema extension, use the Active Directory Schema Snap-in in the Microsoft Management Console (MMC) to verify the existence of the following classes (listed in Table 8-1, Table 8-6, Table 8-7, Table 8-9, Table 8-10, Table 8-11, and Table 8-12) and attributes (listed in Table 8-13, Table 8-14, and Table 8-15). See your Microsoft documentation for more information on how to enable and use the Active Directory Schema Snap-in in the MMC.

Table 8-1. Class Definitions for Classes Added to the Active Directory Schema

Class Name	Assigned Object Identification Number (OID)	Class Type
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1	Structural Class
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2	Structural Class
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3	Auxiliary Class
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4	Structural Class
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5	Structural Class
dellRAC3Privileges	1.2.840.113556.1.8000.1280.1.1.1.6	Auxiliary Class
dellOmsa2AuxClass	1.2.840.113556.1.8000.1280.1.2.1.1	Auxiliary Class
dellOmsaApplication	1.2.840.113556.1.8000.1280.1.2.1.2	Structural Class
dellIta7AuxClass	1.2.840.113556.1.8000.1280.1.3.1.1	Auxiliary Class
dellItaApplication	1.2.840.113556.1.8000.1280.1.3.1.2	Structural Class

Table 8-2. dellRacDevice Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.1**
Description	This class represents the Dell RAC device. The RAC Device must be configured as dellRacDevice in Active Directory. This configuration enables the DRAC 4 to send LDAP queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	**dellSchemaVersion** **dellRacType**

Table 8-3. dellAssociationObject Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.2**
Description	This class represents the Dell Association Object. The Association Object provides the connection between the users and the devices or products.
Class Type	Structural Class
SuperClasses	Group
Attributes	dellProductMembers dellPrivilegeMember

Table 8-4. dellRAC4Privileges Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Description	This class is used to define the privileges (Authorization Rights) for the DRAC 4 device.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Table 8-5. dellPrivileges Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**

Description	This class is used as a container Class for the Dell Privileges (Authorization Rights).
Class Type	Structural Class
SuperClasses	User
Attributes	dellRAC4Privileges
	dellRAC3Privileges
	dellOmsaAuxClass
	dellItaAuxClass

Table 8-6. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Description	This is the main class from which all Dell products are derived.
Class Type	Structural Class
SuperClasses	Computer
Attributes	dellAssociationMembers

Table 8-7. dellRAC3Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.6
Description	This class is used to define the privileges (Authorization Rights) for the DRAC III, DRAC III/XT, ERA, ERA/O, and ERA/MC devices.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellIsLoginUser

Table 8-8. dellOmsa2AuxClass Class

OID	1.2.840.113556.1.8000.1280.1.2.1.1
Description	This class is used to define the privileges (Authorization Rights) for Server Administrator.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellOmsaIsReadOnlyUser
	dellOmsaIsReadWriteUser
	dellOmsaIsAdminUser

Table 8-9. dellOmsaApplication Class

OID	1.2.840.113556.1.8000.1280.1.2.1.2
Description	This class represents the Server Administrator application. Server Administrator must be configured as dellOmsaApplication in Active Directory. This configuration enables the Server Administrator application to send LDAP queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	dellAssociationMembers

Table 8-10. dellIta7AuxClass Class

OID	1.2.840.113556.1.8000.1280.1.3.1.1
Description	This class is used to define the privileges (Authorization Rights) for IT Assistant.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellItaIsReadOnlyUser
	dellItaIsReadWriteUser
	dellItaIsAdminUser

Table 8-11. dellItaApplication Class

OID	1.2.840.113556.1.8000.1280.1.3.1.2
Description	This class represents the IT Assistant application. IT Assistant must be configured as dellItaApplication in Active Directory. This configuration enables IT Assistant to send LDAP queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	dellAssociationMembers

Table 8-**12. General Attributes Added to the Active Directory Schema**

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellPrivilegeMember List of dellPrivilege Objects that belong to this Attribute.	1.2.840.113556.1.8000.1280.1.1.2.1 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers List of dellRacDevices Objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link. Link ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellAssociationMembers List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers Linked attribute. Link ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Table 8-13. RAC-**specific Attributes Added to the Active Directory Schema**

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellIsLoginUser TRUE if the User has Login rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.3 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE if the User has Card Configuration rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE if the User has User Configuration rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE if the User has Log Clearing rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE if the User has Server Reset rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE if the User has Console Redirection rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE if the User has Virtual Media rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE if the User has Test Alert User rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE if the User has Debug Command Administrator rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion The Current Schema Version is used to update the schema.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType This attribute is the Current Rac Type for the dellRacDevice object and the backward link to the dellAssociationObjectMembers forward link.	1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE

Table 8-14. Server Administrator-**Specific Attributes Added to the Active Directory Schema**

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellOMSAIsReadOnlyUser TRUE if the User has Read-Only rights in Server Administrator	1.2.840.113556.1.8000.1280.1.2.2.1 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellOMSAIsReadWriteUser TRUE if the User has Read-Write rights in Server Administrator	1.2.840.113556.1.8000.1280.1.2.2.2 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellOMSAIsAdminUser TRUE if the User has Administrator rights in Server Administrator	1.2.840.113556.1.8000.1280.1.2.2.3 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Table 8-15. IT Assistant-Specific Attributes Added to the Active Directory Schema

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellItalsReadWriteUser TRUE if the User has Read-Write rights in IT Assistant	1.2.840.113556.1.8000.1280.1.3.2.1 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellItalsAdminUser TRUE if the User has Administrator rights in IT Assistant	1.2.840.113556.1.8000.1280.1.3.2.2 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellItalsReadOnlyUser TRUE if the User has Read-Only rights in IT Assistant	1.2.840.113556.1.8000.1280.1.3.2.3 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Active Directory Users and Computers Snap-In

Installing the Dell Extension to the Active Directory Users and Computers Snap-In

When you extend the schema in Active Directory, you must also extend the Active Directory Users and Computers snap-in so that the administrator can manage Products, Users and User Groups, Associations, and Privileges. You only need to extend the snap-in once, even if you have added more than one schema extension. You must install the snap-in on each system that you intend to use for managing these objects. The Dell Extension to the Active Directory Users and Computers Snap-In is an option that can be installed when you install your systems management software using the *Dell PowerEdge Installation and Server Management* CD.

NOTE: You must install the Administrator Pack on each management station that is managing the new Active Directory objects. The installation is described in the following section, "Opening the Active Directory Users and Computers Snap-In." If you do not install the Administrator Pack, then you cannot view the new object in the container.

NOTE: For more information about the Active Directory Users and Computers snap-in, see your Microsoft documentation.

Opening the Active Directory Users and Computers Snap-In

To open the Active Directory Users and Computers snap-in, perform the following steps:

1. If you are on the domain controller, click **Start Admin Tools→ Active Directory Users and Computers**. If you are not on the domain controller, you must have the appropriate Microsoft administrator pack installed on your local system. To install this administrator pack, click **Start→ Run**, type MMC and press **Enter**.

   The Microsoft Management Console (MMC) window opens.

2. Click **File** (or **Console** on systems running Windows 2000) in the **Console 1** window.

3. Click **Add/Remove Snap-in**.

4. Select the **Active Directory Users and Computers** snap-in and click **Add**.

5. Click **Close** and click **OK**.

Adding Users and Privileges to Active Directory

The Dell-extended Active Directory Users and Computers snap-in allows you to add DRAC, Server Administrator, and IT Assistant users and privileges by creating RAC, Association, and Privilege objects. To add an object, perform the steps in the applicable subsection.

Creating a Product Object

NOTE: Server Administrator and IT Assistant users must use Universal-type Product Groups to span domains with their product objects.

NOTE: When adding Universal-type Product Groups from separate domains, you have to create an Association object with Universal scope. The default Association objects created by the Dell Schema Extender utility are domain Local Groups and will not work with Universal-type Product Groups from other domains.

In the **Console Root** (MMC) window, right-click a container.

1. Select **New**.

2. Select a RAC, Server Administrator, or IT Assistant object, depending on which you have installed.

   The **New Object** window opens.

3. Type in a name for the new object. This name must match the **Active Directory product name** as discussed in "Configuring Active Directory Using CLI on Systems Running Server Administrator", or for a RAC device, the name that you will type in step 4 of "Configuring Your Systems or Devices", or for IT Assistant, the name discussed in "Configuring Active Directory on Systems Running IT Assistant."

4. Select the appropriate **Product Object**.

5. Click **OK**.

Creating a Privilege Object

Privilege Objects must be created in the same domain as the Association Object to which they are associated.

1. In the **Console Root** (MMC) window, right-click a container.

2. Select **New**.

3. Select a RAC, Server Administrator, or IT Assistant object, depending on which you have installed.

   The **New Object** window opens.

4. Type in a name for the new object.

5. Select the appropriate **Privilege Object**.

6. Click **OK**.

7. Right-click the privilege object that you created and select **Properties**.

8. Click the appropriate **Privileges** tab and select the privileges that you want the user to have (for more information, see Table 8-1 and Table 8-10).

Creating an Association Object

The Association Object is derived from a Group and must contain a group Type. The Association Scope specifies the Security Group Type for the Association Object. When you create an Association Object, you must choose the Association Scope that applies to the type of objects you intend to add. Selecting **Universal**, for example, means that Association Objects are only available when the Active Directory Domain is functioning in Native Mode or above.

1. In the **Console Root** (MMC) window, right-click a container.

2. Select **New**.

3. Select a RAC, Server Administrator, or IT Assistant object, depending on which you have installed.

   The **New Object** window opens.

4. Type in a name for the new object.

5. Select **Association Object**.

6. Select the scope for the **Association Object**.

7. Click **OK**.

Adding Objects to an Association Object

By using the **Association Object Properties** window, you can associate users or user groups, privilege objects, systems, RAC devices, and system or device groups.

> **NOTE:** RAC users must use Universal Groups to span domains with their users or RAC objects.

You can add groups of Users and Products. You can create Dell-related groups in the same way that you created other groups.

To add Users or User Groups:

1. Right-click the **Association Object** and select **Properties**.

2. Select the **Users** tab and click **Add**.

3. Type the User or User Group name or browse to select one and click **OK**.

Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to a system.

> **NOTE:** You can add only one Privilege Object to an association object.

To add a privilege:

1. Select the **Privileges Object** tab and click **Add**.

2. Type the Privilege Object name or browse for one and click **OK**.

Click the **Products** tab to add one or more systems or devices to the association. The associated objects specify the products connected to the network that are available for the defined users or user groups.

> **NOTE:** You can add multiple systems or RAC devices to an Association Object.

To add Products:

1. Select the **Products** tab and click **Add.**

2. Type the system, device, or group name and click **OK**.

3. In the **Properties** window, click **Apply** and then **OK**.

Enabling SSL on a Domain Controller (RAC Only)

If you plan to use Microsoft Enterprise Root CA to automatically assign all your domain controllers SSL certificates, you must perform the following steps to enable SSL on each domain controller.

1. Install a Microsoft Enterprise Root CA on a Domain Controller.

   a. Select **Start→ Control Panel→ Add or Remove Programs**.

   b. Select **Add/Remove Windows Components**.

   c. In the **Windows Components Wizard**, select the **Certificate Services** check box.

   d. Select **Enterprise root CA** as **CA Type** and click **Next**.

   e. Enter **Common name for this CA**, click **Next**, and click **Finish**.

2. Enable SSL on each of your domain controllers by installing the SSL certificate for each controller.

   a. Click **Start→ Administrative Tools→ Domain Security Policy**.

   b. Expand the **Public Key Policies** folder, right-click **Automatic Certificate Request Settings** and click **Automatic Certificate Request**.

   c. In the **Automatic Certificate Request Setup Wizard**, click **Next** and select **Domain Controller**.

   d. Click **Next** and click **Finish**.

Exporting the Domain Controller Root CA Certificate (RAC Only)

> **NOTE:** The following steps may vary slightly if you are using Windows 2000.

1. Go to the domain controller on which you installed the Microsoft Enterprise CA service.

2. Click **Start→ Run**.

3. Type mmc and click **OK**.

4. In the **Console 1** (MMC) window, click **File (or Console on Windows 2000 systems)** and select **Add/Remove Snap-in**.

5. In the **Add/Remove Snap-in** window, click **Add**.

6. In the **Standalone Snap-in** window, select **Certificates** and click **Add**.

7. Select **Computer** account and click **Next**.

8. Select **Local Computer** and click **Finish**.

9. Click **OK**.

10. In the **Console 1** window, expand the **Certificates** folder, expand the **Personal** folder, and click the **Certificates** folder.

11. Locate and right-click the root CA certificate, select **All Tasks**, and click **Export**.

12. In the **Certificate Export Wizard**, click **Next** and select **No do not export the private key**.

13. Click **Next** and select **Base-64 encoded X.509 (.cer)** as the format.

14. Click **Next** and save the certificate to a location of your choice. You will need to upload this certificate to the DRAC 4. To do this, go to the **DRAC 4 Web-based interface→ Configuration tab→ Active Directory page**. Or, you can use the **racadm** CLI commands (see "Configuring the DRAC 4 Active Directory Settings Using the racadm CLI").

15. Click **Finish** and click **OK**.

Importing the DRAC 4 Firmware SSL Certificate to All Domain Controllers' Trusted Certificate Lists

NOTE: If the DRAC 4 firmware SSL certificate is signed by a well-known CA, you do not need to perform the steps described in this section.

NOTE: The following steps may vary slightly if you are using Windows 2000.

1. The DRAC 4 SSL certificate is the same certificate that is used for the DRAC 4 Web server. All DRAC 4 controllers are shipped with a default self-signed certificate. You can get this certificate from the DRAC 4 by selecting **Download DRAC 4 Server Certificate** (see the DRAC 4 Web-based interface **Configuration** tab and the **Active Directory** subtab).

2. On the domain controller, open an **MMC Console** window and select **Certificates → Trusted Root Certification Authorities**.

3. Right-click **Certificates**, select **All Tasks** and click **Import**.

4. Click **Next** and browse to the SSL certificate file.

5. Install the RAC SSL Certificate in each domain controller's **Trusted Root Certification Authority**.

   If you have installed your own certificate, ensure that the CA signing your certificate is in the **Trusted Root Certification Authority** list. If the CA is not in the list, you must install it on all your Domain Controllers.

6. Click **Next** and select whether you would like Windows to automatically select the certificate store based on the type of certificate, or browse to a store of your choice.

7. Click **Finish** and click **OK**.

Configuring Your Systems or Devices

For instructions on how to configure your Server Administrator or IT Assistant systems using CLI commands, see "Configuring Active Directory Using CLI on Systems Running Server Administrator" and "Configuring Active Directory on Systems Running IT Assistant." For DRAC users, there are two ways to configure DRAC 4. See either "Configuring the DRAC 4 Using the Web-Based Interface" or "Configuring the DRAC 4 Active Directory Settings Using the racadm CLI."

NOTE: The systems on which Server Administrator and/or IT Assistant are installed must be a part of the Active Directory domain and should also have computer accounts on the domain.

Configuring Active Directory Using CLI on Systems Running Server Administrator

You can use the **omconfig preferences dirservice** command to configure the Active Directory service. The **productoem.ini** file is modified to reflect these

changes. If the **adproductname** is not present in the **product**oem.ini file, a default name will be assigned. The default value will be **system name-software-product name**, where **system name** is the name of the system running Server Administrator, and **software-product name** refers to the name of the software product defined in **omprv32.ini (that is, *computerName*-omsa)**.

NOTE: This command is applicable only on systems running the Windows operating system.

NOTE: Restart the Server Administrator service after you have configured Active Directory.

Table 8-16 shows the valid parameters for the command.

Table 8-16. Active Directory Service Configuration Parameters

name=value pair	Description
prodname=<text>	Specifies the software product to which you want to apply the Active Directory configuration changes. *Prodname* refers to the name of the product defined in **omprv32.ini**. For Server Administrator, it is *omsa*.
enable=<true | false>	**true:** Enables Active Directory service authentication support. **false:** Disables Active Directory service authentication support
adprodname=<text>	Specifies the name of the product as defined in the Active Directory service. This name links the product with the Active Directory privilege data for user authentication.

Configuring Active Directory on Systems Running IT Assistant

By default, the Active Directory product name corresponds to the *machinename*-ita, where *machinename* is the name of the system on which IT Assistant is installed. To configure a different name, locate the **itaoem.ini** file in your installation directory. Edit the file to add the line "adproductname=*text*" where *text* is the name of the product object that you created in Active Directory. For example, the **itaoem.ini** file will contain the following syntax if the Active Directory product name is configured to **mgmtStationITA**.

```
productname=IT Assistant
startmenu=Dell OpenManage Applications
autdbid=ita
accessmask=3
startlink=ITAUIServlet
adsupport=true
adproductname=mgmtStationITA
```

NOTE: Restart the IT Assistant services after saving the **itaoem.ini** file to the disk.

Configuring the DRAC 4 Using the Web-Based Interface

1. Log in to the Web-based interface using the default user, root, and its password.

2. Click the **Configuration** tab and select the **Active Directory**.

3. Select the **Enable Active Directory** check box.

4. Type the **DRAC 4 Name.** This name must be the same as the common name of the RAC object you created in your Domain Controller (see "Installing the Dell Extension to the Active Directory Users and Computers Snap-In").

5. Type the **Root Domain Name**. The **Root Domain Name** is the fully qualified root domain name for the forest.

6. Type the **DRAC 4 Domain Name** (for example, drac4.com**). Do not use the NetBIOS name. The **DRAC 4 Domain Name** is the fully qualified domain name of the subdomain where the RAC Device Object is located.

7. Click **Apply** to save the Active Directory settings.

8. Click **Upload Active Directory CA Certificat**e to upload your domain forest Root CA certificate into the DRAC 4. Your domain forest domain controllers' SSL certificates need to have signed this root CA certificate. Have the root CA certificate available on your local system (see "Exporting the Domain Controller Root CA Certificate (RAC Only)"). Specify the full path and filename of the root CA certificate and click **Upload** to upload the root CA certificate to the DRAC 4 firmware. The DRAC 4 Web server automatically restarts after you click **Upload**. You must log in again to complete the DRAC 4 Active Directory feature configuration.

9. Click the **Configuration** tab and select **Network**.

10. If **DRAC 4 NIC DHCP** is enabled, place a check next to **Use DHCP to obtain DNS server address.** If you want to input a DNS server IP address manually, remove the check next to **Use DHCP to obtain DNS server address** and input your primary and alternate DNS Server IP addresses.

11. Click **Apply** to complete the DRAC 4 Active Directory feature configuration.

Configuring the DRAC 4 Active Directory Settings Using the racadm CLI

Using the following commands to configure the DRAC 4 Active Directory feature using the racadm CLI instead of the Web-based interface.

1. Open a command prompt and type the following racadm commands:

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1
   racadm config -g cfgActiveDirectory -o cfgADRacDomain <fully qualified rac domain name>
   racadm config -g cfgActiveDirectory -o cfgADRootDomain <fully qualified root domain name>
   racadm config -g cfgActiveDirectory -o cfgADRacName <RAC common name>
   racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
   racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
   ```

2. If DHCP is enabled on the DRAC 4 and you want to use the DNS provided by the DHCP server, type the following:

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
   ```

3. If DHCP is disabled on the DRAC 4, or you want manually to input your DNS IP address, type the following commands:

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
   racadm config -g cfgLanNetworking -o cfgDNSServer1 <primary DNS IP address>
   racadm config -g cfgLanNetworking -o cfgDNSServer2 <secondary DNS IP address>
   ```

4. Press **Enter** to complete the DRAC 4 Active Directory feature configuration.

See the *Dell Remote Access Controller 4 User's Guide* for more information.

Prerequisite Checker

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

---

Command Line Operation of the Prerequisite Checker

You can run the prerequisite check silently by executing runprereqchecks.exe /s from the **\windows\PreReqChecker** directory. After running the prerequisite check, an HTML file will be created in the **%Temp%** directory. The file is named **omprereq.htm**, and it contains the results of the prerequisite check. The **Temp** directory is not usually **X:\Temp**, but **X:\Documents and Settings\username\Local Settings\Temp**. To find **%TEMP%**, go to a command line prompt and type echo %TEMP%.

The results of the Prerequisite Checker are written to the registry for the Management Station under the registry key:

HKEY_LOCAL_MACHINE\Software\Dell Computer Corporation\OpenManage \PreReqChecks\MS

The are written under the following key for a Managed System:

HKEY_LOCAL_MACHINE\Software\Dell Computer Corporation\OpenManage \PreReqChecks\MN

When running the Prerequisite Check silently, the return code from **runprereqchecks.exe** will be the number associated with the highest severity condition for all of the software products. The return code numbers are the same as those used in the registry. Table 9-1 details the codes that are returned.

Table 9-1. Return Codes While Running the Prerequisite Check Silently

Return Code	Description
0	No condition, or conditions, is associated with the software.
1	An informational condition, or conditions, is associated with the software. It does not prevent a software product from being installed.
2	A warning condition, or conditions, is associated with the software. It is recommended that you resolve the conditions causing the warning before you proceed with the installation of the software.
3	An error condition, or conditions, is associated with the software. It is required that you resolve the conditions causing the error before proceeding with the installation of that software. If you do not resolve the issues, the software will not be installed.
-1	A Microsoft® Windows® Script Host (WSH) error. The Prerequisite Checker will not run.
-2	The operating system is not supported. The Prerequisite Checker will not run.
-3	The user does not have Administrator privileges. The Prerequisite Checker will not run.
-4	Not an implemented return code.
-5	The user failed to change the working directory to **%TEMP%.** The Prerequisite Checker will not run.
-6	The destination directory does not exist. The Prerequisite Checker will not run.
-7	An internal error has occurred. The Prerequisite Checker will not run.
-8	The software is already running. The Prerequisite Checker will not run.
-9	The Windows Script Host is corrupted, is a wrong version, or is not installed. The Prerequisite Checker will not run.
-10	An error has occurred with the scripting environment. The Prerequisite Checker will not run.

Each software product has an associated value set after running the prerequisite check. Table 9-2 and Table 9-3 provide the list of feature IDs for each software feature. The feature ID is a 2- to 5-character designation.

Table 9-2. Feature IDs for the Management Station

Feature ID	Description
ADS	Microsoft Active Directory® Snap-in Utility
BMC	Baseboard Management Controller Management Utility
ITA	Dell OpenManage™ IT Assistant
RACMS	Remote Access Controller

Table 9-3. Software Feature IDs

Feature ID	Description
ALL	All features
BRCM	Broadcom NIC Agent
INTEL	Intel® NIC Agent
IWS	Dell OpenManage Server Administrator Web Server
OMSM	Server Administrator Storage Management Service

RAC3	Remote Access Controller (DRAC III)
RAC4	Remote Access Controller (DRAC 4)
RAC5	Remote Access Controller (DRAC 5)
SA	Server Administrator

Dell OpenManage™ Security

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- Security Features
- Built-in Security Features
- Security Management

Security Features

The Dell OpenManage systems management software components provide the following security features:

- Authentication for users through hardware-stored user IDs and passwords, or by using the optional Microsoft® Active Directory®.

- Role-based authority that allows specific privileges to be configured for each user.

- User ID and password configuration through the Web-based interface or the command line interface (CLI), in most cases.

- SSL encryption of 128 bit and 40 bit (for countries where 128 bit is not acceptable).

   NOTE: Telnet does not support SSL encryption.

- Session time-out configuration (in minutes) through the Web-based interface or CLI.

- Configuration of many of the commonly known ports.

Built-in Security Features

Ports

Table 2-1 lists the ports used by the Dell OpenManage systems management software, other standard operating system services, and other agent applications. Correctly configured ports are necessary to allow Dell OpenManage systems management software to connect to a remote device through firewalls. If the attempt to communicate with a remote device fails, you may have specified an incorrect port number.

   NOTE: "Version" in Table 2-1 refers to the minimum product version that uses the port (or explicit version if specified).

Table 2-1. Dell OpenManage UDP/TCP Ports Default Locations

Port #	Protocol	Port Type	Version	Max. Encryption Level	Direction	Usage	Configurable
Dell OpenManage Baseboard Management Controller - PowerEdge™ x8xx systems							
623	RMCP	UDP	PowerEdge *x800* systems only	None	In/Out	IPMI access via LAN	No
Dell OpenManage Baseboard Management Utility							
623	Telnet	TCP	1.*x*	None	In/Out	Accepts incoming Telnet connections	Yes
623	RMCP	UDP	1.*x*	None	In/Out	Basic BMC commands: server status, power up/down, and so on.	No
623	RMCP	UDP	1.*x*	None	In/Out	Basic BMC commands and console redirection	No
Dell OpenManage Client Connector							
135	RPC	TCP/UDP	2.0	None	In/Out	Viewing of client management data	No
389	LDAP	TCP	2.0	128 bit	In/Out	Domain authentication	No
4995	HTTPS	TCP	2.0	128 bit SSL	In/Out	Web GUI	Yes
1024 - 65535 (Dynamically assigned)	DCOM	TCP/UDP	2.0	None	In/Out	Viewing of client management data	Port range can be restricted.
Dell OpenManage Client Instrumentation							
20	HTTP and FTP	TCP	6.*x*, 7.*x*	None	In/Out	Flash BIOS communication	No
21	HTTP and FTP	TCP	6.*x*, 7.*x*	None	In/Out	Flash BIOS communication	No
80	HTTP and FTP	TCP	6.*x*, 7.*x*	None	In/Out	Flash BIOS communication	No
135	DCOM	TCP/UDP	6.*x*, 7.*x*	None	In/Out	Monitoring and configuration via WMI	No

135	DCOM	TCP	7.x	None	Out	Event transmission via WMI	No
162	SNMP	UDP	6.x	None	Out	Event transmission via SNMP	No
1024-65535 (Dynamically assigned)	DCOM	TCP/UDP	6.x, 7.x	None	In/Out	Monitoring and configuration via WMI	
> 32780 (Dynamically assigned)	DMI	TCP/UDP	6.x	None	In/Out	Monitoring and configuration via DMI	Varies from one system to another.
Dell OpenManage IT Assistant							
20	FTP	TCP	6.x	None	In/Out	Flash BIOS	No
22	SSH	TCP	7.x	128 bit	In/Out	IT Assistant contextual application launch — SSH client Remote software updates to Server Administrator — For systems supporting Linux	Yes
23	Telnet	TCP	7.x	None	In/Out	IT Assistant contextual application launch — Telnet to Linux device	No
25	SMTP	TCP	7.x	None	In/Out	Optional e-mail alert action from IT Assistant	No
68	UDP	UDP	6.x, 7.x	None	Out	Wake-on-LAN	Yes
80	HTTP	TCP	6.x	None	In/Out	Flash BIOS	No
80	HTTP	TCP	7.x	None	In/Out	IT Assistant contextual application launch — PowerConnect™ console	No
135	RPC	TCP	6.x, 7.x	None	In/Out	Event reception via CIM from Server Administrator — For systems supporting Windows®	No
135	RPC	TCP/UDP	6.x	None	In/Out	DMI discovery of remote systems	No
135	RPC	TCP/UDP	7.x	None	In/Out	Remote software update transfer to Server Administrator — For systems supporting Windows Remote Command Line — For systems supporting Windows	No
161	SNMP	UDP	6.x, 7.x	None	In/Out	SNMP query management	No
162	SNMP	UDP	6.x, 7.x	None	In	Event reception via SNMP	No
162	SNMP	UDP	7.x	None	Out	SNMP trap forwarding action from IT Assistant	No
389	LDAP	TCP	7.x	128 bit	In/Out	Domain authentication for IT Assistant log on	No
1433	Proprietary	TCP	7.x	None	In/Out	Optional remote SQL server access	Yes
2606	Proprietary	TCP	6.x, 7.x	None	In/Out	Network monitoring service communication port	Yes
2607	HTTPS	TCP	7.x	128 bit SSL	In/Out	IT Assistant web GUI	Yes
3389	RDP	TCP	7.x	128 bit SSL	In/Out	IT Assistant contextual application launch — Remote desktop to Windows terminal services	Yes
11487/11489	Proprietary	TCP/UDP	6.x	None	Out	Flash BIOS	No
443	Proprietary	TCP	8.0	None	In/Out	EMC Storage discovery and inventory	No
623	RMCP	UDP	8.0	None	In/Out	IPMI access via LAN	No
6389	Proprietary	TCP	8.0	None	In/Out	Enables communication between a host system (through NaviCLI/NaviSecCLI or Navisphere Host Agent) and a Navisphere Array Agent on a Storage system.	No
Dell OpenManage Server Administrator							
22	SSH	TCP	2.0	128 bit	In/Out	Remote Server Administrator Command Line (for IT Assistant). Remote Software Update feature (for Linux).	Yes
25	SMTP	TCP	2.0	None	In/Out	Optional e-mail alert messages from Server Administrator	No
135	RPC	TCP/UDP	2.0	None	In/Out	CIM management queries	No
135	RPC	TCP/UDP	2.0	None	In/Out	Remote Server Administrator Command Line (for IT Assistant). Remote software update feature (for Windows).	No
139	NetBIOS	TCP	2.0	None	In/Out	Remote Server Administrator Command Line (for IT Assistant). Remote Software Update (for Windows).	No
161	SNMP	UDP	1.x, 2.0	None	In/Out	SNMP query management	No
162	SNMP	UDP	1.x, 2.0	None	Out	SNMP trap event	No
445	NetBIOS	TCP	2.0	None	In/Out	Remote software updates to Server Administrator (for Windows)	No
1311	HTTPS	TCP	1.x	128 bit SSL	In/Out	Web GUI	Yes
11487	Proprietary	UDP	1.x	None	In	Remote Flash BIOS update initiation from IT Assistant	Yes
11489	Proprietary	TCP	1.x	None	In	Remote Flash BIOS update file transfer from IT Assistant	Yes
1024 -65535	DCOM	TCP/UDP	2.0	None	In/Out	CIM/WMI query management	Yes

Dell Remote Access Controller (DRAC): DRAC III, DRAC III/XT, ERA, and ERA/O							
21	FTP	TCP	1.0	None	In/Out	Firmware update via FTP and certificate upload/download	No
23	Telnet	TCP	1.0	None	In/Out	Optional Telnet-based CLI management	No
25	SMTP	TCP	1.0	None	In/Out	Optional e-mail alert messages	No
68	DHCP	UDP	1.2	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update via Trivial FTP. Remote floppy boot via TFTP	No
80	HTTP	TCP	1.0	None	In/Out	Web GUI redirected to HTTPS	No
162	SNMP	UDP	1.0	None	Out	SNMP trap event	No
443	HTTPS	TCP	1.0	128 bit SSL	In/Out	Web management GUI	No
443	HTTPS	TCP	3.2	128 bit SSL	In/Out	Remote racadm CLI utility	No
5869	Proprietary	TCP	1.0	None	In/Out	Remote racadm CLI utility	No
5900	VNC	TCP	1.0	56 bit DES	In/Out	Video redirection	Yes
5900	VNC	TCP	3.2	128 bit RC	In/Out	Video redirection	Yes
5981	VNC	TCP	1.0	None	In/Out	Video redirection	Yes
random and > 32768	Proprietary	TCP	1.0	None	In/Out	Firmware update from the Web GUI	No
DRAC 4							
22	SSHv2	TCP	1.30	128 bit	In/Out	Optional Secure Shell (SSH) CLI management	Yes
23	Telnet	TCP	1.0	None	In/Out	Optional Telnet CLI management	Yes
25	SMTP	TCP	1.0	None	In/Out	Optional e-mail alert messages	No
53	DNS	UDP	1.20	None	In/Out	Dynamic Domain name server (DNS) registration of the host name assigned within DRAC	No
68	DHCP	UDP	1.0	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update via Trivial FTP	No
80	HTTP	TCP	1.0	None	In/Out	Web GUI redirected to HTTPS	Yes
161	SNMP	UDP	1.0	None	In/Out	SNMP query management	No
162	SNMP	UDP	1.0	None	Out	SNMP trap event	No
443	HTTPS	TCP	1.0	128 bit SSL	In/Out	Web management GUI and remote racadm CLI utility	Yes
636	LDAPS	TCP	1.0	128 bit SSL	In/Out	Optional Active Directory Services (ADS) authentication	No
3269	LDAPS	TCP	1.0	128 bit SSL	In/Out	Optional Active Directory Services (ADS) authentication	No
3668	Proprietary	TCP	1.0	None	In/Out	CD/diskette virtual media service	Yes
5869	Proprietary	TCP	1.0	None	In/Out	Remote racadm	No
5900	Proprietary	TCP	1.0	128bit RC4, Keyboard/mouse traffic only	In/Out	Video redirection	Yes
DRAC/MC							
23	Telnet	TCP	1.0	None	In/Out	Optional Telnet CLI management	Yes
25	SMTP	TCP	1.0	None	In/Out	Optional e-mail alert messages	No
53	DNS	UDP	1.0	None	In/Out	Dynamic DNS registration of host name assigned within DRAC	No
68	DHCP	UDP	1.0	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update via Trivial FTP	No
80	HTTP	TCP	1.0	None	In/Out	Web GUI redirected to HTTPS	Yes
161	SNMP	UDP	1.0	None	In/Out	SNMP query management	No
162	SNMP	UDP	1.0	None	Out	SNMP trap event	No
389	LDAP	TCP	1.0	None	In/Out	Optional Active Directory Services (ADS) authentication	No
443	HTTPS	TCP	1.0	128 bit SSL	In/Out	Web management GUI and remote racadm CLI utility	No
636	LDAPS	TCP	1.0	128 bit SSL	In/Out	Optional Active Directory Services (ADS) authentication	No
3269	LDAPS	TCP	1.0	128 bit SSL	In/Out	Optional Active Directory Services (ADS) authentication	No
Digital KVM							
2068	Proprietary	TCP	1.0	128 bit SSL	In/Out	Video Redirection — Keyboard/Mouse	No
3668	Proprietary	TCP	1.0	None	In/Out	Virtual Media	No
8192	Proprietary	TCP	1.0	None	In/Out	Video redirection to client viewer	No

NOTE: CIM ports are dynamic. See the Microsoft knowledge base at **support.microsoft.com** for information on CIM port usage.

NOTE: If you are using a firewall, you must open all of the ports listed in to ensure that IT Assistant and other Dell OpenManage applications function properly.

Security Management

Dell provides security and access administration through role-based access control (RBAC), authentication, and encryption, or through Active Directory for both the Web-based and command line interfaces.

Role-Based Access Control (RBAC)

RBAC manages security by determining the operations that can be executed by users in specific 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 can correspond closely to an organization's structure. For information about setting up Dell OpenManage users, see "Assigning User Privileges."

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 administrator access to users logged in with Administrator privileges. See .

Table 2-**2. User Privileges**

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

Admin access allows you to shut down the managed system.

Write access allows you to modify or set the values on the managed system.

Read access allows you to view the data reported by Server Administrator. Read access does not allow you to change or set the values on the managed system.

Privilege Levels to Access Server Administrator Services

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

Table 2-**3. Server Administrator User Privilege Levels**

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

defines the user privilege level abbreviations used in .

Table 2-**4. Legend for Server Administrator User Privilege Levels**

U	User

P	Power User
A	Administrator

Authentication

The Server Administrator authentication scheme ensures that the correct access types are assigned to the correct user privileges. Additionally, when you invoke the CLI, 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 Windows operating systems, Server Administrator authentication uses Integrated Windows Authentication (formerly called NTLM) to authenticate. This authentication system allows Server Administrator security to be incorporated in an overall security scheme for your network.

Red Hat® Enterprise Linux and SUSE® Linux Enterprise Server Authentication

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

Encryption

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

Microsoft Active Directory

The Active Directory service software acts as the central authority for network security, letting the operating system readily verify a user's identity and control that user's access to network resources for Dell OpenManage applications running on supported Windows platforms. Dell provides schema extensions for customers to modify their Active Directory database to support remote management authentication and authorization. IT Assistant, Server Administrator, and Dell remote access controllers can now interface with Active Directory to add and control users and privileges from one central database. For information about using Active Directory, see "Using Microsoft® Active Directory®."

Setup and Administration

Dell OpenManage™ Version 5.1 Installation and Security User's Guide

- ● Before You Begin
- ● Installation Requirements
- ● Dependencies and Prerequisites
- ● Configuring a Supported Web Browser
- ● Assigning User Privileges
- ● Configuring the SNMP Agent
- ● Secure Port Server and Security Setup

Before You Begin

- l   Read the applicable instructions in this chapter.

- l   Read the installation requirements to ensure that your system meets or exceeds the minimum requirements.

- l   Read the *Dell OpenManage™ Server Administrator Compatibility Guide*. This document contains compatibility information about Dell OpenManage software installation and operation on various hardware platforms (systems) running supported Microsoft® Windows®, Red Hat® Enterprise Linux, and SUSE® Linux Enterprise Server operating systems.

- l   Read the applicable Dell OpenManage readme files on the Dell OpenManage CDs or on the Dell™ Support website at **support.dell.com**. These files contain the latest information about software, firmware, and driver versions, in addition to information about known issues. The installation **readme_ins.txt** file also contains a list of supported servers.

- l   Read the installation instructions for your operating system.

Installation Requirements

The following sections describe the Dell OpenManage systems management software general requirements. Operating system-specific installation prerequisites are listed as part of the installation procedures.

- l   Supported Operating Systems
- l   System Requirements

Supported Operating Systems

Dell OpenManage systems management software runs, at a minimum, on each of the following operating systems:

- l   Windows 2000 Server family (with SP4) — Includes Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Professional

- l   **Windows Server™ 2003 family (with R2)** — Includes Standard and Enterprise editions

- l   Windows Server 2003 x64 R2 — Includes Standard and Enterprise editions (except IT Assistant)

     ![NOTE] **NOTE:** IT Assistant is not supported on systems running Microsoft Windows Server 2003 x64.

- l   Windows Server 2003 SP1 (Web Edition)

- l   Windows SBS 2003 SP1 (except IT Assistant)

- l   Windows XP SP2

- l   Windows Storage Server 2003 R2 — Includes Express, Standard, Workgroup, and Enterprise editions

- l   Red Hat Enterprise Linux AS, ES, and WS (version 3) x86, Update 6

     ![NOTE] **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 "Dynamic Kernel Support (DKS)" for a description of this feature).

- l   Red Hat Enterprise Linux AS, ES, and WS (version 3) for Intel® Extended Memory 64 Technology (Intel EM64T) Update 6

- l   Red Hat Enterprise Linux AS, ES, and WS (version 4) for Intel x86

- l   Red Hat Enterprise Linux AS, ES, and WS (version 4) for Intel EM64T

- l   SUSE Linux Enterprise Server (version 9), SP3 for Intel EM64T

- l   SUSE Linux Enterprise Server (version 10) Gold for Intel EM64T

     ![NOTE] **NOTE:** Support for updated kernels released by Novell® and for later versions of SUSE Linux Enterprise Server may require the use of Dynamic Kernel Support (see "Dynamic Kernel Support (DKS)" for a description of this feature).

System Requirements

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

Managed System Requirements

- One of the Supported Operating Systems

- A minimum of 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 (see "Minimum Supported Web Browser Requirements")

- One of the Supported Systems Management Protocol Standards (see "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) be installed on the system to be managed. See the *Dell Remote Access Controller 4 User's Guide,* the *Dell Remote Access Controller 5 User's Guide,* 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** or **Typical Setup** and **Custom Setup** installation options when installing managed system software from the *Dell PowerEdge™ 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.

Remote Management System Requirements

- One of the supported Web browsers to manage a system remotely from a graphical user interface (GUI)

- 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

Minimum Supported Web Browser Requirements

- Internet Explorer 6.0 SP1 and SP2 (Windows only)

- Mozilla Firefox 1.07 (SUSE Linux Enterprise Server and Red Hat Enterprise Linux)

- Mozilla 1.7.8, 1.7.10, and 1.7.11 (SUSE Linux Enterprise Server and Red Hat Enterprise Linux)

Supported Systems Management Protocol Standards

A supported systems management protocol standard must be installed on the managed system before installing your management station or managed system software. On supported Windows operating systems, Dell OpenManage software 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 SUSE Linux Enterprise Server operating systems, Dell OpenManage software supports the SNMP systems management standard.

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

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

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

Operating System	SNMP	CIM/WMI
Supported 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 SUSE Linux Enterprise Server operating systems.	You must install the SNMP package provided with the operating system.	Unavailable.

Dependencies and Prerequisites

Upgrading from Dell OpenManage Software Versions 1.*x*, 2.*x*, and 3.*x*–4.2

Upgrades from Dell OpenManage software versions 1.*x*, 2.*x*, and 3.*x* through 4.2 **are not supported. You must manually uninstall Dell OpenManage software versions 1.*x*, 2.*x*, and 3.*x* through 4.2 before launching the Dell OpenManage software installation. The installer will notify you if it detects Dell OpenManage software versions 1.*x* through 4.2 on the system.** Another way of upgrading from these versions is to upgrade to version 4.3 first, then upgrade to the current version. For Microsoft Windows, you can upgrade from version 4.3 to a later version through a full Microsoft Software Installer (MSI) installation only.

Configuring a Supported Web Browser

The following sections provide instructions for configuring the supported Web browsers. For a list of supported Web browsers, see "Minimum Supported Web Browser Requirements."

Configuring Internet Explorer to Connect to the Web-Based Interface

If you are connecting to a Web-based interface from a management station that connects to the Internet through a proxy server, you need to configure the Web browser to connect properly. If you are using Microsoft's Internet Explorer browser, follow these steps:

1. From the Internet Explorer main window, click **Tools**, and then click **Internet Options**.

2. From the **Internet Options** window, click the **Connections** tab.

3. Under **Local Area Network (LAN) settings**, click **LAN Settings**.

4. If the **Use a proxy server** box is selected, select the **Bypass proxy server for local addresses** box.

5. Click **OK** twice.

Configure other browsers for the same functionality.

Viewing Localized Versions of the Web-Based Interface

When using Internet Explorer or Netscape Navigator on systems running Windows, to view localized versions of the Web-based interface, do the following:

1. Open the Windows **Control Panel** and double-click the **Regional Options** icon.

2. Select the desired locale from the **Your locale (location)** drop-down menu.

Assigning User Privileges

To ensure critical system component security, you must properly assign user privileges to all Dell OpenManage software users before installing Dell OpenManage software.

The following sections provide step-by-step instructions for creating users and assigning user privileges for each supported operating system.

- Creating Users for Supported Windows Operating Systems
- Creating Users for Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems
- Microsoft Active Directory

NOTICE: To protect access to your critical system components, you must assign a password to every user account that can access Dell OpenManage software.

NOTICE: You should disable guest accounts for supported 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 Users for Supported Windows Operating Systems

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

The following procedures create user accounts, assign user privileges, and add users to domains.

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**.

You must assign a password to every user account that can access Dell OpenManage software to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Dell OpenManage software 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 Dell OpenManage software 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**.

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 Dell OpenManage software 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 Microsoft Active Directory® installed on your system to perform the following procedures. See "Microsoft Active Directory" for more information about using Active Directory.

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**.

You must assign a password to every user account that can access Dell OpenManage software to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Dell OpenManage software 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 that you just created.

6. Click the **Member of** tab.

7. Click **Add**.

8. Select the appropriate group and click **Add**.

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

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

Disabling Guest and Anonymous Accounts in Supported Windows Operating Systems

NOTE: You must be logged in with Administrator 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.

NOTE: Consider renaming the accounts so that remote scripts cannot enable the accounts using the name.

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

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

NOTE: You must be logged in as root 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.

You must assign a password to every user account that can access Dell OpenManage software to protect access to your critical system components.

The new user can now log in to Dell OpenManage software 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.

You must assign a password to every user account that can access Dell OpenManage software to protect access to your critical system components.

The new user can now log in to Dell OpenManage software with Power User group privileges.

Microsoft Active Directory

If you use Active Directory service software, you can configure it to control access to your network. Dell has modified the Active Directory database to support remote management authentication and authorization. IT Assistant and Server Administrator, as well as Dell remote access controllers, can now interface with Active Directory. With this tool, you can add and control users and privileges from one central database. If you use Active Directory to control user access to your network, see "Using Microsoft® Active Directory®."

Configuring the SNMP Agent

Dell OpenManage software supports the SNMP systems management standard on all supported operating systems. The SNMP support may or may not be installed depending on your operating system and how the operating system was installed. An installed supported systems management protocol standard, such as SNMP, is required before installing Dell OpenManage software. 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 IT Assistant, perform the procedures described in the following sections.

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

The following sections 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 SUSE Linux Enterprise Server Operating Systems

Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems

Dell OpenManage software uses the SNMP services provided by the Windows SNMP agent. (SNMP is one of the two supported ways of connecting to a System Administrator session; the other is CIM/WMI.) You can configure the SNMP agent to change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as IT Assistant, perform the procedures described in the following sections.

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

Enabling SNMP Access By Remote Hosts on Windows Server 2003

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 remote shutdown of a system from IT Assistant, SNMP Set operations must be enabled.

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

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 IT Assistant 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 Dell OpenManage software system so that the management applications can retrieve management information from Dell OpenManage software.

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 Dell OpenManage software system to change Dell OpenManage software attributes using IT Assistant. To enable remote shutdown of a system from IT Assistant, SNMP Set operations must be enabled.

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

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 opens.

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 opens.

7. Set the **Community Rights** to **READ WRITE** or **READ CREATE**, and click **OK**.

   The **SNMP Service Properties** window opens.

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

Configuring Your System to Send SNMP Traps to a Management Station

Dell OpenManage software 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 Dell OpenManage software 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 opens.

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 opens.

5. Click the **Traps** tab to add a community for traps or to add a trap destination for a trap community**.**

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

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

      The **SNMP Service Configuration** window opens.

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

      The **SNMP Service Properties** window opens.

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

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

SNMP Agent Access Control Configuration

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

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 1.3.6.1.2.1.1 OID) of the MIB tree. This configuration does not allow management applications to retrieve or change Server

Administrator or other systems management information outside of the MIB-II "system" branch.

Server Administrator SNMP Agent Install Actions

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

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

    view all included .1

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

    access notConfigGroup "" any noauth exact systemview none none

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

    access notConfigGroup "" any noauth exact all none none

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

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

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

    smuxpeer .1.3.6.1.4.1.674.10892.1

Changing the SNMP Community Name

Configuring the SNMP community names determines which systems are able to manage your system through SNMP. The SNMP community name used by management applications must match an SNMP community name configured on the Server Administrator software system, so 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 software attributes using IT Assistant. To enable remote shutdown of a system from IT Assistant, SNMP Set operations must be enabled.

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

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

1. Add the following line to the file:

```
trapsink IP_address community_name
```

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

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

```
service snmpd restart
```

Firewall Configuration on Systems Running 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. See "Ports" for additional information.

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 opens.

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

   The **Firewall Configuration** screen opens.

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 Windows GUI, pressing <F1> might not provide information about firewall security levels on newer versions of the Red Hat Enterprise Linux operating system.

   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.

   d. Tab to **Customize** and press <Enter>.

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

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 opens.

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

   The **Choose a Tool** menu opens.

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

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

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

NOTE: On SUSE Linux Enterprise Server (version 9), the SNMP agent configuration file is located at **/etc/snmpd.conf**. On SUSE Linux Enterprise Server (version 10), the SNMP agent configuration file is located at **/etc/snmp/snmpd.conf**.

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

Sever Administrator SNMP Install Actions

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

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Enabling SNMP Access From Remote Hosts

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

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

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

1. Find the line that reads:

```
rocommunity public 127.0.0.1
```

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

```
rocommunity public IP_address
```

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

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

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

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

1. Find the line that reads:

```
rocommunity public 127.0.0.1
```

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

```
rocommunity public
```

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

   `/etc/init.d/snmpd restart`

Changing the SNMP Community Name

Configuring the SNMP community name determines which 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 the management applications can retrieve management information from Server Administrator.

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

1. Find the line that reads:

   `rocommunity public 127.0.0.1`

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

   `rocommunity community_name 127.0.0.1`

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

   `/etc/init.d/snmpd restart`

Enabling SNMP Set Operations

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

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

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

1. Find the line that reads:

   `rocommunity public 127.0.0.1`

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

   `rwcommunity public 127.0.0.1`

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

   `/etc/init.d/snmpd restart`

Configuring Your System to Send Traps to a Management Station

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

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

1. Add the following line to the file:

   `trapsink IP_address community_name`

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

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

   `/etc/init.d/snmpd restart`

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 can set user and secure port server preferences for Server Administrator and IT Assistant from the respective **Preferences** Web page. Click **General Settings** and click either the **User** tab or **Web Server** tab.

📝 **NOTE:** You must be logged in with Administrator 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 session can remain active. Select the **Enable** radio button to allow a time-out if there is no user interaction for a specified number of minutes. Users whose sessions time-out must log in again to continue. Select the **Disable** radio button to disable the Server Administrator session time-out 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:** A user with Administrator privileges cannot use Server Administrator when logged into the system remotely.

   📝 **NOTE:** Changing the **IP Address to Bind to** value to a value other than **All** may prevent other applications or browsers from remotely 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 Web address 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 **,**.

- 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 Administrator privileges to perform certificate management.

You can manage X.509 certificates for Server Administrator and IT Assistant from the respective **Preferences** Web 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.

Dell OpenManage™ Version 5.1 Installation and Security 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.

_____